National Nuclear Security Administration

Instrumentation and Control
Qualification Standard

DOE-STD-1162-2013

June 2013 | Reference Guide

The Functional Area Qualification Standard References Guides are developed to assist operators, maintenance personnel, and the technical staff in the acquisition of technical competence and qualification within the Technical Qualification Program (TQP).

Please direct your questions or comments related to this document to the Office of Leadership and Career Management, TQP Manager, NNSA Albuquerque Complex.

This page is intentionally blank.

Table of Contents

FIGURES

TABLES

VIDEOS

ACRONYMS

24/7	twenty four hours a day, seven days a week
AC	alternating current
ALARA	as low as reasonably achievable
ANS	American Nuclear Society
ANSI	American National Standards Institute
API	American Petroleum Institute
ASIC	application specific integrated circuit
ASME	American Society of Mechanical Engineers
ASRS	alarm system requirements specification
ASTM	American Society for Testing and Materials
BIBO	bounded input—bounded output
BPCS	basic process control system
BTP	branch technical position
CCF	common cause failure
COTS	commercial off-the-shelf
cm	cubic meter
CM	configuration management
CMOS	complementary metal–oxide–semiconductor
CPLD	complex programmable logic device
CPU	central processing unit
DC	direct current
DCS	distributed control system
DD	description document
DO	dissolved oxygen
DOE	U.S. Department Energy
DSA	documented safety analysis
DSP	digital signal processor
DTL	diode-transistor logic
EDA	electronic design automation
EFCOG	Energy Facilities Contractor Group
EMF	electromotive force
EPA	U.S. Environmental Protection Agency
ESA	electrical signal analysis
ES&H	environment, safety, and health
FAQS	functional area qualification standard
FDD	facility design descriptions
FIB	focused ion beam
FMEA	failure modes and effects analysis
FMEDA	failure modes, effects, and diagnostic analysis
FPGA	field-programmable gate arrays
FTA	fault tree analysis
GOCO	government-owned contractor operated

GOGO	government-owned government-operated
HEPA	high-efficiency particulate air
HFE	human factors engineering
HMA	highly management alarm
HMI	human-machine interface
HPE	human performance evaluation
HSI	human-system interface
HVAC	heating, ventilation, air-conditioning
IAEA	International Atomic Energy Agency
Hz	hertz
I&C	instrumentation and control
IEC	International Electrotechnical Commission
IEEE	Institute for Electrical and Electronic Engineers
I/O	input/output
IPL	independent protection layer
ISA	International Society of Automation
ISO	International Organization for Standardization
ITS	International Temperature Scale
kPa	kilopascal
KSA	Knowledge, skills, and abilities
kV	kilovolts
LAN	local area network
LCO	limiting condition for operation
LCS	limiting control setting
LED	light emitting diode
LSSS	limiting safety system setting
MAWP	maximum allowable working pressure
MCSA	motor current signature analysis
MIP	maintenance implementation plan
MORT	management oversight and risk tree
MOS	metal-oxide-semiconductor
MOV	motor operated valve
mrad	millirad
mrem	millirem
MTBF	mean time between failure
NCTC	normally-closed, timed-closed
NCTO	normally-closed, timed-open
NIST	National Institute of Standards and Technology
NMMP	nuclear maintenance management program
NNSA	National Nuclear Security Administration
NOTC	normally-open, timed-closed contact
NOTO	normally-open, timed-open
NPH	natural phenomena hazard
NRC	U.S. Nuclear Regulatory Commission
OBE	operating basis earthquake

ORNL	Oak Ridge National Laboratory
OSHA	Occupational Safety and Health Administration
Pa	pascal
P&F	Pepperl+Fuchs
PFDavg	average probability of failure on demand
P&ID	process and instrument drawing
PID	proportional integral derivative
PLC	programmable logic controller
PLD	programmable logic device
psi	pounds per square inch
psig	pounds per square inch gauge
PST	partial stroke testing
PV	process variable
QA	quality assurance
RAGAGEP	recognized and generally accepted good engineering practices
RC	reconfigurable computing
RCA	root cause analysis
R&D	research and development
RETS	radiological effluent technical specifications
RGA	residual gas analyzer
RPN	risk priority numbers
RRF	risk reduction factors
RTD	resistance temperature detector
S	siemen
SAC	specific administrative control
SCADA	supervisory control and data acquisition
SDD	system design description
SDIT	safety design integration team
SDS	safety design strategy
SI	international system of units
SIF	safety instrumented function
SIL	safety integrity level
SIS	safety instrumented system
SL	safety limit
SO	Secretarial Officer
SoC	system-on-chip
SP	set point
SPRT	standard platinum resistance thermometer
SQA	software quality assurance
SS	safety significant
SSA	single-stuck at
SSC	structure, system, and component
SSE	safe shutdown earthquake
STD	standard
TGW	things gone wrong

TQP	Technical Qualification Program
TSR	technical safety requirement
TTL	Transistor-transistor logic
μm	micrometer
UPS	uninterruptible power supply
USQ	unreviewed safety question
U.S.	United States
VAC	volts alternating current

PURPOSE

The purpose of this reference guide is to provide a document that contains the information required for a Department of Energy (DOE)/National Nuclear Security Administration (NNSA) technical employee to successfully complete Instrumentation and Control Functional Area Qualification Standard (FAQS). Information essential to meeting the qualification requirements is provided; however, some competency statements require extensive knowledge or skill development. Reproducing all the required information for those statements in this document is not practical. In those instances, references are included to guide the candidate to additional resources.

SCOPE

This reference guide has been developed to address the competency statements in the June 2013 edition of DOE-Standard (STD)-1162-2013, *Instrumentation and Control Functional Area Qualification Standard*. The qualification standard for Instrumentation and Control Functional Area Qualification Standard contains 16 competency statements.

PREFACE

Competency statements and supporting knowledge and/or skill statements from the qualification standard are shown in contrasting bold type, while the corresponding information associated with each statement is provided below it.

A comprehensive list of acronyms, abbreviations, and symbols is provided at the beginning of this document. It is recommended that the candidate review the list prior to proceeding with the competencies, as the acronyms, abbreviations, and symbols may not be further defined within the text unless special emphasis is required.

The competencies and supporting knowledge, skill, and ability (KSA) statements are taken directly from the FAQS. Most corrections to spelling, punctuation, and grammar have been made without remark. Only significant corrections to errors in the technical content of the discussion text source material are identified. Editorial changes that do not affect the technical content (e.g., grammatical or spelling corrections, and changes to style) appear without remark. When they are needed for clarification, explanations are enclosed in brackets.

Every effort has been made to provide the most current information and references available as of June 2013. However, the candidate is advised to verify the applicability of the information provided. It is recognized that some personnel may oversee facilities that utilize predecessor documents to those identified. In those cases, such documents should be included in local qualification standards via the TQP.

In the cases where information about an FAQS topic in a competency or KSA statement is not available in the newest edition of a standard (consensus or industry), an older version is referenced. These references are noted in the text and in the bibliography.

This reference guide includes streaming videos to help bring the learning experience alive. To activate the video, click on any hyperlink under the video title. Note: Hyperlinks to video are shown in entirety, due to current limitations of eReaders.

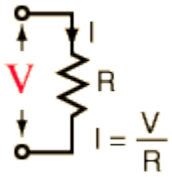
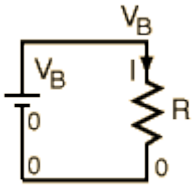
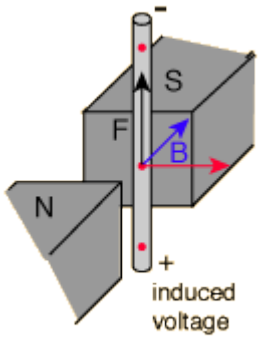
1. **Instrumentation and Control (I&C) personnel must demonstrate a familiarity level knowledge of basic electrical engineering fundamentals.**

   a. **.Meet needs of students2.Meet needs of employees3.Focus on curriculum and best practices in contemporary education4.Commit to accountability, workforce development and the principles of continuous improvement Explain the relationships between voltage, current, resistance, reactance, and impedance. This includes understanding of electrical circuits and their application in I&C systems design and operation.**

Voltage

The following is taken from Georgia State University, *Hyperphysics*, "Voltage."

Voltage is electric potential energy per unit charge, measured in joules per coulomb (volts). It is often referred to as "electric potential," which then must be distinguished from electric potential energy by noting that the "potential" is a "per-unit-charge" quantity. Like mechanical potential energy, the zero of potential can be chosen at any point, so the difference in voltage is the quantity which is physically meaningful. The difference in voltage measured when moving from point A to point B is equal to the work which would have to be done, per unit charge, against the electric field to move the charge from A to B.

			
Used to calculate current in Ohm's law	Used to express conservation of energy around a circuit in the voltage law	Used to calculate the potential from a distribution of charges	Generated by moving a wire in a magnetic field

Source: Georgia State University, Hyperphysics, Voltage

Figure 1. Measurement with voltmeter

Current

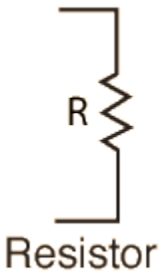
The following is taken from Georgia State University, *Hyperphysics*, "Electric Current."

Electric current is the rate of charge flow past a given point in an electric circuit, measured in Coulombs/second (amperes). In most direct current (DC) electric circuits, it can be assumed that the resistance to current flow is a constant; the current in the circuit is related to voltage and resistance by Ohm's law. The standard abbreviations for the units are 1 A = 1C/s

Resistance

The electrical resistance of a circuit component or device is defined as the ratio of the voltage applied to the electric current that flows through it:

$$R = \frac{V}{I}$$



If the resistance is constant over a considerable range of voltage, then Ohm's law, I = V/R, can be used to predict the behavior of the material. Although the definition above involves DC current and voltage, the same definition holds for the alternating current (AC) application of resistors.

Whether or not a material obeys Ohm's law, its resistance can be described in terms of its bulk resistivity. The resistivity, and thus the resistance, is temperature dependent. Over sizable ranges of temperature, this temperature dependence can be predicted from a temperature coefficient of resistance.

Video 1. Voltage, current, and resistance
http://wn.com/voltage#/videos

Reactance

The following is taken from Wikipedia, *Electrical Reactance*.

In electrical and electronic systems, reactance is the opposition of a circuit element to a change of electric current or voltage, due to that element's inductance or capacitance. A built-up electric field resists the change of voltage on the element, while a magnetic field resists the change of current. The notion of reactance is similar to electrical resistance, but they differ in several respects.

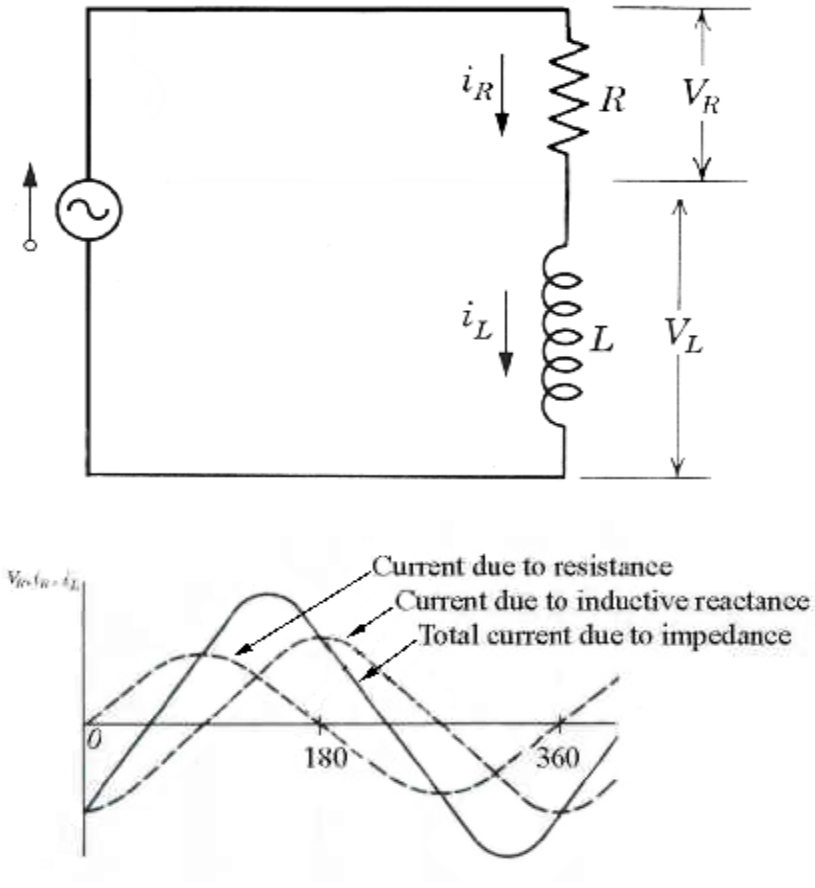
Like resistance, capacitance and inductance are inherent properties of an element. Reactive effects are not exhibited under constant direct current, but only when the conditions in the circuit change. Thus, the reactance differs with the rate of change, and is a constant only for circuits under alternating current of constant frequency. In vector analysis of electric circuits, resistance is the real part of complex impedance, while reactance is the imaginary part. Both share the same unit of measurement, the ohm.

Video 2. Reactance
http://www.youtube.com/watch?feature=player_embedded&v=uPO95pLzOQo

Impedance

The following is taken from the NDT Resource Center, *Impedance.*

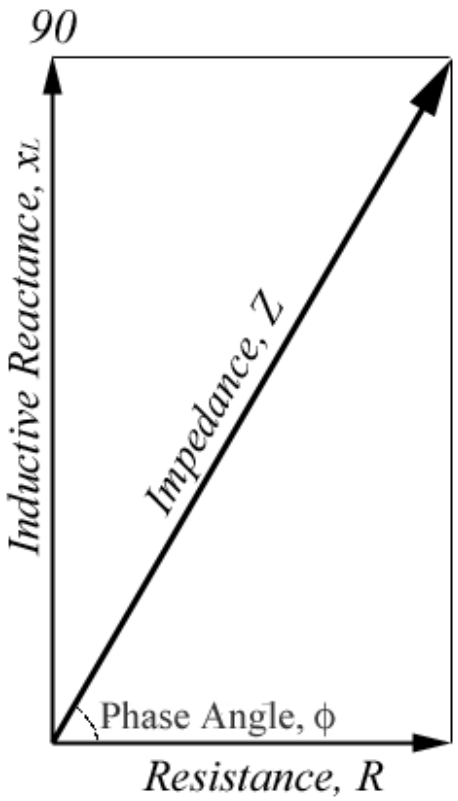
Electrical impedance is the total opposition that a circuit presents to alternating current. Impedance is measured in ohms, and may include resistance, inductive reactance, and capacitive reactance. However, the total impedance is not simply the algebraic sum of the resistance, inductive reactance, and capacitive reactance. Since the inductive reactance and capacitive reactance are 90º out of phase with the resistance and, therefore, their maximum values occur at different times, vector addition must be used to calculate impedance.



Source: NDT Resource Center, Impedance

Figure 2. Circuit diagram

In figure 2, a circuit diagram is shown that represents an eddy current inspection system. The eddy current probe is a coil of wire that contains resistance and inductive reactance when driven by alternating current. The capacitive reactance can be eliminated as most eddy current probes have little capacitive reactance. The solid line in the graph shows the circuit's total current, which is affected by the total impedance of the circuit. The two dashed lines represent the portion of the current that is affected by the resistance and the inductive reactance components individually. It can be seen that the resistance and the inductive reactance lines are 90º out of phase, so when combined to produce the impedance line, the phase shift is somewhere between zero and 90º. The phase shift is always relative to the resistance line since the resistance line is always in-phase with the voltage. If more resistance than inductive reactance is present in the circuit, the impedance line will move toward the resistance line and the phase shift will decrease. If more inductive reactance is present in the circuit, the impedance line will shift toward the inductive reactance line and the phase shift will increase.



The relationship between impedance and its individual components can be represented using a vector as shown in figure 3. The amplitude of the resistance component is shown by a vector along the x-axis and the amplitude of the inductive reactance is shown by a vector along the y-axis. The amplitude of the impedance is shown by a vector that stretches from zero to a point that represents both the resistance value in the x-direction and the inductive reactance in the y-direction. Eddy current instruments with impedance plane displays present information in this format.

The impedance in a circuit with resistance and inductive reactance can be calculated using the following equation. If capacitive reactance was present in the circuit, its value would be added to the inductance term before squaring.

$$Z = \sqrt{\left(X_L^2 + R^2\right)}$$

Figure 3. Impedance vector

Video 3. Impedance

http://www.bing.com/videos/search?q=impedance&view=detail&mid=29A78EDF419654&first=0

b. Explain alternating current (AC), direct current (DC), batteries, Uninterruptible Power Supplies (UPS), diesel generators, and other backup power supplies and their application in I&C systems.

Alternating Current

The following is taken from the NDT Resource Center, *Alternating Current*.

AC is short for alternating current. This means that the direction of current flowing in a circuit is constantly being reversed back and forth. This is done with any type of AC current/voltage source.

The electrical current in houses is alternating current. It comes from power plants that are operated by the electric company. The big wires stretching across the countryside carry AC current from the power plants to the loads, which are in homes and businesses. The direction of current switches back and forth 60 times each second.

Direct Current

The following is taken from Wikipedia, *Direct Current*.

Direct current is the unidirectional flow of electric charge. Direct current is produced by sources such as batteries, thermocouples, solar cells, and commutator-type electric machines of the dynamo type. Direct current may flow in a conductor such as a wire, but can also flow through semiconductors, insulators, or even through a vacuum as in electron or ion beams. The electric charge flows in a constant direction, distinguishing it from AC.

Video 4. Alternating and direct current

http://www.bing.com/videos/search?q=Alternating+And+Direct+Current&view=detail&mid=EC618CBADA99FE60F72EEC618CBADA99FE60F72E&first=0

Batteries

The following is taken from Wikipedia, *Battery*.

In electricity, a battery is a device consisting of one or more electrochemical cells that convert stored chemical energy into electrical energy.

There are two types of batteries: primary batteries (disposable batteries), which are designed to be used once and discarded, and secondary batteries (rechargeable batteries), which are designed to be recharged and used multiple times. Batteries come in many sizes; from miniature cells used to power hearing aids and wristwatches to battery banks the size of rooms that provide standby power for telephone exchanges and computer data centers.

A battery is a device that converts chemical energy directly to electrical energy. It consists of a number of voltaic cells; each voltaic cell consists of two half-cells connected in series by a conductive electrolyte containing anions and cations. One half-cell includes an electrolyte and the electrode to which anions migrate, i.e., the anode or negative electrode; the other half-cell includes an electrolyte and the electrode to which cations migrate, i.e., the cathode or positive electrode. In the redox reaction that powers the battery, cations are reduced at the cathode, while anions are oxidized at the anode. The electrodes do not touch each other but are electrically connected by the electrolyte. Some cells use two half-cells with different electrolytes. A separator between half-cells allows ions to flow, but prevents mixing of the electrolytes.

Each half-cell has an electromotive force (EMF) determined by its ability to drive electric current from the interior to the exterior of the cell. The net EMF of the cell is the difference between the EMFs of its half-cells, as first recognized by Volta. Therefore, if the electrodes have EMFs $\mathcal{E}_1$ and $\mathcal{E}_2$, then the net EMF is $\mathcal{E}_2$-$\mathcal{E}_1$ in other words, the net EMF is the difference between the reduction potentials of the half-reactions.

The electrical driving force or ΔV_{bat} across the terminals of a cell is known as the terminal voltage (difference) and is measured in volts.

Uninterruptible Power Supplies

The following is taken from Wikipedia, *Uninterruptible Power Supply*.

An uninterruptible power supply (UPS) is an electrical apparatus that provides emergency power to a load when the input power source, typically mains power, fails. A UPS differs from an auxiliary or emergency power system or standby generator in that it will provide near-instantaneous protection from input power interruptions, by supplying energy stored in batteries or a flywheel. The on-battery runtime of most uninterruptible power sources is relatively short but sufficient to start a standby power source or properly shut down the protected equipment.

A UPS is typically used to protect computers, data centers, telecommunication equipment or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious business disruption, or data loss. UPS units range in size from units designed to protect a single computer without a video monitor to large units powering entire data centers or buildings.

Diesel Generator

The following is taken from Wikipedia, *Diesel Generator*.

A diesel generator combines a diesel engine with an electrical generator to generate electrical energy. Diesel generating sets are used in places without connection to the power grid, as emergency power-supply if the grid fails, as well as for more complex applications such as peak-lopping, grid support, and export to the power grid. Sizing of diesel generators is critical to avoid low-load or a shortage of power and is complicated by modern electronics, specifically non-linear loads.

c. Explain the use of various types of electrical equipment and components, such as, motors, generators, transformers (e.g., current vs. potential transformers), capacitors, inductors, resistors, circuit breakers, electrical switchgear, motor control centers, motor operated valves, electrical relays, time delay relays, fuses, etc) and their application in I&C systems design.

Motors

The following is taken from Wikipedia, *Electric Motor*.

An electric motor is an electromechanical device that converts electrical energy into mechanical energy.

Most electric motors operate through the interaction of magnetic fields and current-carrying conductors to generate force. The reverse process, producing electrical energy from mechanical energy, is done by generators such as an alternator or a dynamo; some electric motors can also be used as generators, for example, a traction motor on a vehicle may perform both tasks. Electric motors and generators are commonly referred to as electric machines.

Electric motors are found in applications as diverse as industrial fans, blowers and pumps, machine tools, household appliances, power tools, and disk drives. They may be powered by

direct current, e.g., a battery powered portable device or motor vehicle, or by alternating current from a central electrical distribution grid or inverter. Small motors may be found in electric wristwatches. Medium-size motors of highly standardized dimensions and characteristics provide convenient mechanical power for industrial uses. The very largest electric motors, with ratings in the millions of watts, are used for propulsion of ships, pipeline compressors, and water pumps. Electric motors may be classified by the source of electric power, by their internal construction, by their application, or by the type of motion they supply.

Generators

The following is taken from Wikipedia, *Electric Generator*.

In electricity generation, an electric generator is a device that converts mechanical energy to electrical energy. A generator forces electric charge to flow through an external electrical circuit. The source of mechanical energy may be a reciprocating or turbine steam engine, water falling through a turbine or waterwheel, an internal combustion engine, a wind turbine, a hand crank, compressed air, or any other source of mechanical energy.

The reverse conversion of electrical energy into mechanical energy is done by an electric motor, and motors and generators have many similarities. Many motors can be mechanically driven to generate electricity and frequently make acceptable generators.

Transformers

The following is taken from Wikipedia, *Transformer*.

A transformer is a power converter that transfers electrical energy from one circuit to another through inductively coupled conductors—the transformer's coils. A varying current in the first or primary winding creates a varying magnetic flux in the transformer's core, and thus a varying magnetic field through the secondary winding. This varying magnetic field induces a varying EMF, or "voltage", in the secondary winding. This effect is called inductive coupling.

If a load is connected to the secondary winding, current will flow in this winding, and electrical energy will be transferred from the primary circuit through the transformer to the load. In an ideal transformer, the induced voltage in the secondary winding (V_s) is in proportion to the primary voltage (V_p) and is given by the ratio of the number of turns in the secondary (N_s) to the number of turns in the primary (N_p) as follows:

$$\frac{V_\mathrm{s}}{V_\mathrm{p}} = \frac{N_\mathrm{s}}{N_\mathrm{p}}$$

By appropriate selection of the ratio of turns, a transformer thus enables an AC voltage to be "stepped up" by making N_s greater than N_p, or "stepped down" by making N_s less than N_p. The windings are coils wound around a ferromagnetic core. Air-core transformers are a notable exception to this.

Transformers range in size from a thumbnail-sized coupling transformer hidden inside a stage microphone to huge units weighing hundreds of tons used in power stations, or to interconnect portions of power grids. All operate on the same basic principles, although the range of designs is wide. While new technologies have eliminated the need for transformers in some electronic circuits, transformers are still found in nearly all electronic devices designed for household voltage. Transformers are essential for high-voltage electric power transmission, which makes long-distance transmission economically practical.

The following is taken from eHow, *Difference Between Potential Transformer & Current Transformer*.

POTENTIAL TRANSFORMERS
Potential power or voltage transformers change commercial power from generators to high voltage and low current for nationwide distribution. Substations use similar transformers in reverse to reduce the voltage and increase the current to usable levels.

In the home and in industry, potential transformers have thousands of other uses. TVs and cell phone chargers have potential transformers to raise or lower the voltage for internal distribution and use.

CURRENT TRANSFORMERS
Transformers designated as current transformers have far more limited uses. Current or current sense transformers only lower current for use in meters and measuring devices, with little regard for power or voltage changes.

Capacitors

The following is taken from *Electrical and Electronic Principles and Technology* by John Bird.

A capacitor is a passive two-terminal electrical component used to store energy in an electric field. The forms of practical capacitors vary widely, but all contain at least two electrical conductors separated by a dielectric; for example, one common construction consists of metal foils separated by a thin layer of insulating film. Capacitors are widely used as parts of electrical circuits in many common electrical devices.

When there is a potential difference across the conductors, a static electric field develops across the dielectric, causing positive charge to collect on one plate and negative charge on the other plate. Energy is stored in the electrostatic field. An ideal capacitor is characterized by a single constant value, capacitance, measured in farads. This is the ratio of the electric charge on each conductor to the potential difference between them.

The capacitance is greatest when there is a narrow separation between large areas of conductor; hence capacitor conductors are often called plates, referring to an early means of construction. In practice, the dielectric between the plates passes a small amount of leakage current and also has an electric field strength limit, resulting in a breakdown voltage, while the conductors and leads introduce an undesired inductance and resistance.

Capacitors are widely used in electronic circuits for blocking direct current while allowing alternating current to pass; in filter networks, for smoothing the output of power supplies; in the resonant circuits that tune radios to particular frequencies; in electric power transmission systems for stabilizing voltage and power flow; and for many other purposes.

Video 5. Capacitors

http://www.bing.com/videos/search?q=capacitor&view=detail&mid=BC8D27754F065659FB35BC8D27754F065659FB35&first=0

Inductors

The following is taken from Wikipedia, *Inductors*.

An inductor, sometimes called a coil or reactor, is a passive two-terminal electrical component that resists changes in electric current passing through it. It consists of a conductor such as wire, usually wound into a coil. When a current flows through it, energy is stored temporarily in a magnetic field in the coil. When the current flowing through an inductor changes, the time-varying magnetic field induces a voltage in the conductor, according to Faraday's law of electromagnetic induction that opposes the change in current that created it.

An inductor is characterized by its inductance, the ratio of the voltage to the rate of change of current that has units of henries. Many inductors have a magnetic core made of iron or ferrite inside the coil that serves to increase the magnetic field and thus the inductance. Along with capacitors and resisters, inductors are one of the three passive linear circuit elements that make up electric circuits. Inductors are widely used in AC electronic equipment, particularly in radio equipment. They are used to block the flow of AC current while allowing DC to pass; inductors designed for this purpose are called chokes. They are used in electronic filters to separate signals of different frequencies, and in combination with capacitors to make tuned circuits, used to tune radio and television receivers.

Video 6. Inductors

http://www.youtube.com/watch?v=NgwXkUt3XxQ

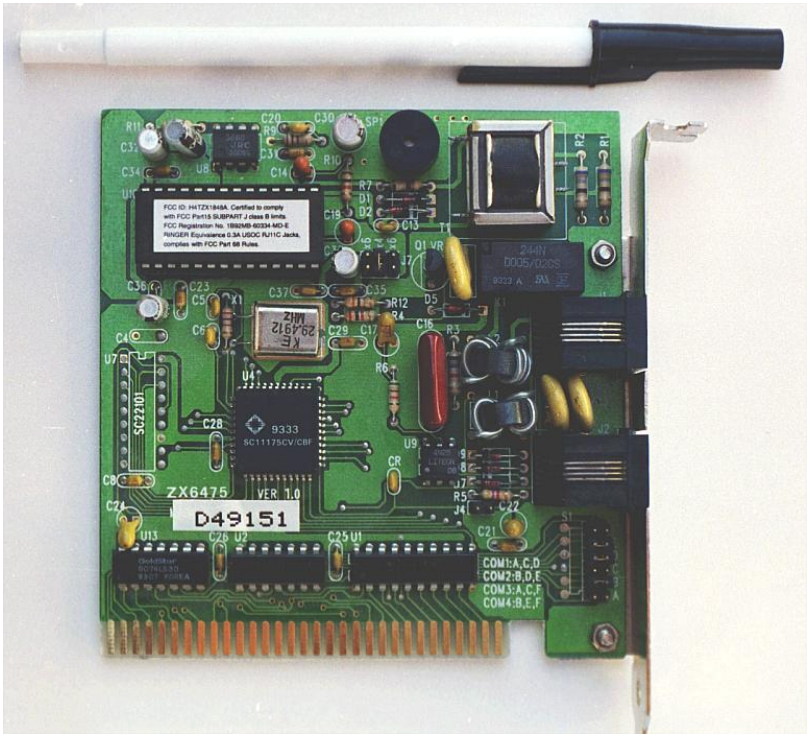
Resistors

The following is taken from All About Circuits, *Resistors*.

Because the relationship between voltage, current, and resistance in any circuit is so regular, any variable in a circuit can be controlled reliably simply by controlling the other two. The easiest variable in any circuit to control is its resistance. This can be done by changing the material, size, and shape of its conductive components.

Resistors are special components made for the express purpose of creating a precise quantity of resistance for insertion into a circuit. They are typically constructed of metal wire or carbon, and engineered to maintain a stable resistance value over a wide range of environmental conditions. Unlike lamps, they do not produce light, but they do produce heat as they dissipate electric power in a working circuit. Typically, the purpose of a resistor is not to produce usable heat, but to provide a specific quantity of electrical resistance.

A practical illustration of resistors' usefulness is shown in figure 4. It is a picture of a printed circuit board: an assembly made of sandwiched layers of insulating phenolic fiber-board and conductive copper strips, into which components may be inserted and secured by solder. The various components on this circuit board are identified by printed labels. Resistors are denoted by any label beginning with the letter "R".



Source: All About Circuits, Resistors

Figure 4. Printed circuit board and resistors

Circuit Breakers

The following is taken from Wikipedia, *Circuit Breaker*.

A circuit breaker is an automatically operated electrical switch designed to protect an electrical circuit from damage caused by overload or short circuit. Its basic function is to detect a fault condition and, by interrupting continuity, to immediately discontinue electrical flow. Unlike a fuse, which operates once and then must be replaced, a circuit breaker can be reset to resume normal operation. Circuit breakers are made in varying sizes, from small devices that protect an individual household appliance to large switchgear designed to protect high voltage circuits feeding an entire city.

Video 7. Circuit breakers

http://www.ehow.com/video_4908466_different-types-circuit-breakers.html

Electrical Switchgear

The following is taken from Wikipedia, *Switchgear*.

In an electric power system, switchgear is the combination of electrical disconnect switches, fuses, or circuit breakers used to control, protect, and isolate electrical equipment. Switchgear is used to de-energize equipment to allow work to be done and to clear faults downstream. This type of equipment is important because it is directly linked to the reliability of the electricity supply.

Source: Wikipedia, Switchgear

Figure 5. High voltage switchgear

High voltage switchgear, as shown in figure 5, was invented at the end of the 19th century for operating motors and other electric machines. The technology has been improved over time and can be used with voltages up to 1,100 kV.

Typically, the switchgear in substations is located on the high voltage and the low voltage sides of large power transformers. The switchgear on the low voltage side of the transformer may be located in a building, with medium-voltage circuit breakers for distribution circuits, along with metering, control, and protection equipment. For industrial applications, a transformer and switchgear line-up may be combined in one housing, called a unitized substation.

Motor Control Centers

The following is taken from eHow, *What is a Motor Control Center*?

Motor controllers, which manage electric motors, can be housed in a motor control center. Electric motors typically require a controller of some kind to operate. This device, called a motor controller, manages the speed and torque of the connected motor. A single device that enables one or more motors to be controlled from a central location is a motor control center.

Motor control centers are combination starters grouped into one assembly. A combination starter is an enclosure that houses the motor starter, or device that regulates an electric motor's performance and the fuses or devices used in electrical systems that prevent excessive current.

Motor control centers contain vertical metal cabinets used to house the individual motor controller units, and typically draw their power from an AC generator. Power enters the motor controllers via separate connectors. Motor controllers govern electric motors through a closed loop system, or a control system that modifies output based on differences between the input and feedback systems.

Motor control centers are used to centralize motor control and simplify the addition of components such as transformers and service entrance switches. They also enable simplified installation and wiring, and require less total space than single motor controller units.

Motor Operated Valves

The following is taken from Instrumentation and Process Control, *Motor Operated Valve (MOV)*.

A motor operated valve (MOV) is an ordinary ball valve or any other valve that is operated by an electric actuator. In general, the MOV is used as an isolation valve for equipment that requires regular access. The MOV is also used on any valve that requires substantial energy to manually open or close.

The typical MOV construction consists of an electric motor actuator, a gear box, and the valve itself. First, the motor is rotated by AC voltage. Next, the motor rotation is transferred through a gear mechanism to the output thrust part. Finally, the output thrust is transferred to the gear mechanism in the gear box to rotate the valve stem.

Electrical Relays

The following is taken from Wikipedia, *Relays*.

A relay is an electrically operated switch. Many relays use an electromagnet to operate a switching mechanism mechanically, but other operating principles are also used. Relays are used where it is necessary to control a circuit by a low-power signal, or where several circuits must be controlled by one signal. The first relays were used in long distance telegraph circuits, repeating the signal coming in from one circuit and retransmitting it to another. Relays were used extensively in telephone exchanges and early computers to perform logical operations.

A type of relay that can handle the high power required to directly control an electric motor or other loads is called a contactor. Solid-state relays control power circuits with no moving parts; using a semiconductor device to perform switching. Relays with calibrated operating characteristics, and sometimes multiple operating coils, are used to protect electrical circuits from overload or faults; in modern electric power systems these functions are performed by digital instruments still called “protective relays.”

Time Delay Relays

The following is taken from All About Circuits, *Time Delay Relays*.

Some relays are constructed with a kind of “shock absorber” mechanism attached to the armature that prevents immediate, full motion when the coil is either energized or de-energized. This addition gives the relay the property of time-delay actuation. Time-delay relays can be constructed to delay armature motion on coil energization, de-energization, or both.

Time-delay relay contacts must be specified not only as either normally-open or normally-closed, but also must specify whether the delay operates in the direction of closing or in the direction of opening. The following is a description of the four basic types of time-delay relay contacts:

1. The NOTC (normally-open, timed-closed) contact is normally open when the coil is unpowered (de-energized). It is closed by the application of power to the relay coil,

but only after the coil has been continuously powered for the specified amount of time. The direction of the contact's motion (either to close or to open) is identical to a regular normally-open contact, but there is a delay in closing direction. Because the delay occurs in the direction of coil energization, this type of contact is alternatively known as a normally-open, on-delay.

2. The NOTO (normally-open, timed-open) contact is like the NOTC contact, in that it is normally open when the coil is unpowered (de-energized), and closed by the application of power to the relay coil. Unlike the NOTC contact, the timing action occurs upon de-energization of the coil rather than upon energization. Because the delay occurs in the direction of coil de-energization, this type of contact is alternatively known as a normally-open, off-delay.
3. The NCTO (normally-closed, timed-open) contact is normally closed when the coil is unpowered (de-energized). The contact is opened with the application of power to the relay coil, but only after the coil has been continuously powered for the specified amount of time. The direction of the contact's motion (either to close or to open) is identical to a regular normally-closed contact, but there is a delay in the opening direction. Because the delay occurs in the direction of coil energization, this type of contact is alternatively known as a normally-closed, on-delay.
4. The NCTC (normally-closed, timed-closed) contact is like the NCTO contact, in that it is normally closed when the coil is unpowered (de-energized), and opened by the application of power to the relay coil. Unlike the NCTO contact, the timing action occurs upon de-energization of the coil rather than upon energization. Because the delay occurs in the direction of coil de-energization, this type of contact is alternatively known as a normally-closed, off-delay.

Time-delay relays are very important for use in industrial control logic circuits. Some examples of their uses include the following:

- *Flashing light control (time on, time off*). Two time-delay relays are used in conjunction with one another to provide a constant-frequency on/off pulsing of contacts for sending intermittent power to a lamp.
- *Engine autostart control*. Engines that are used to power emergency generators are often equipped with "autostart" controls that allow for automatic start-up if the main electric power fails. To properly start a large engine, certain auxiliary devices must be started first and allowed some brief time to stabilize (fuel pumps, pre-lubrication oil pumps) before the engine's starter motor is energized. Time-delay relays help sequence these events for proper start-up of the engine.
- *Furnace safety purge control*. Before a combustion-type furnace can be safely lit, the air fan must be run for a specified amount of time to "purge" the furnace chamber of any potentially flammable or explosive vapors. A time-delay relay provides the furnace control logic with this necessary time element.
- *Motor soft-start delay control*. Instead of starting large electric motors by switching full power from a dead stop condition, reduced voltage can be switched for a "softer" start and less inrush current. After a prescribed time delay (provided by a time-delay relay), full power is applied.
- *Conveyor belt sequence delay*. When multiple conveyor belts are arranged to transport material, the conveyor belts must be started in reverse sequence (the last one first and the first one last) so that material doesn't get piled on to a stopped or slow-

moving conveyor. In order to get large belts up to full speed, some time may be needed (especially if soft-start motor controls are used). For this reason, there is usually a time-delay circuit arranged on each conveyor to give it adequate time to attain full belt speed before the next conveyor belt feeding it is started.

Fuses

The following is taken from Wikipedia, *Fuse*.

In electronics and electrical engineering, a fuse is a type of low resistance resistor that acts as a sacrificial device to provide overcurrent protection, of either the load or source circuit. Its essential component is a metal wire or strip that melts when too much current flows, which interrupts the circuit in which it is connected. Short circuit, overloading, mismatched loads, or device failure are the prime reasons for excessive current.

A fuse interrupts excessive current so that further damage by overheating or fire is prevented. Wiring regulations often define a maximum fuse current rating for particular circuits. Overcurrent protection devices are essential in electrical systems to limit property damage and threats to human life. Fuses are selected to allow passage of normal current plus a marginal percentage and to allow excessive current only for short periods. Slow blow fuses are designed to allow harmless short-term higher currents but still clear on a sustained overload. Fuses are manufactured in a wide range of current and voltage ratings and are widely used to protect wiring systems and electrical equipment. Self-resetting fuses automatically restore the circuit after the overload has cleared; these are useful, for example, in aerospace or nuclear applications where fuse replacement is impossible.

d. Explain the use of electrical test instruments and measuring devices (e.g., voltmeter, ammeter, and ohmmeter). Also explain the importance of and relationship between calibration, precision, and accuracy etc., to the design and maintenance of I&C systems.

Voltmeter

The following is taken from Wikipedia, *Voltmeter*.

A voltmeter is an instrument used for measuring electrical potential difference between two points in an electric circuit. Analog voltmeters move a pointer across a scale in proportion to the voltage of the circuit; digital voltmeters give a numerical display of voltage by use of an analog to digital converter.

Voltmeters are made in a wide range of styles. Instruments permanently mounted in a panel are used to monitor generators or other fixed apparatus. Portable instruments, usually equipped to also measure current and resistance in the form of a multimeter, are standard test instruments used in electrical and electronics work. Any measurement that can be converted to a voltage can be displayed on a meter that is suitably calibrated; for example, pressure, temperature, flow, or level in a chemical process plant.

General purpose analog voltmeters may have an accuracy of a few percent of full scale, and are used with voltages from a fraction of a volt to several thousand volts. Digital meters can be made with high accuracy, typically better than one percent. Specially calibrated test instruments have higher accuracies, with laboratory instruments capable of measuring to

accuracies of a few parts per million. Meters using amplifiers can measure tiny voltages of microvolts or less.

Part of the problem of making an accurate voltmeter is that of calibration to check its accuracy. In laboratories, the Weston Cell is used as a standard voltage for precision work. Precision voltage references are available based on electronic circuits.

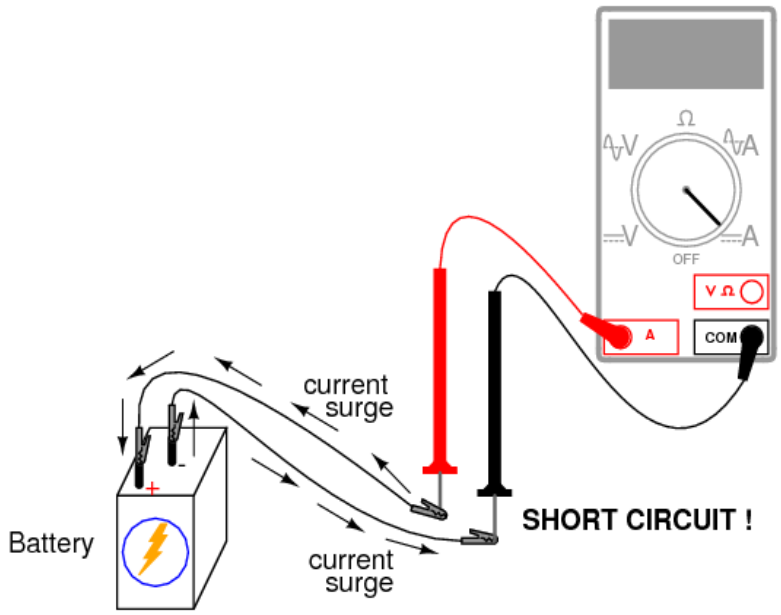
Video 8. How to use a voltmeter
http://www.bing.com/videos/search?q=voltmeter&view=detail&mid=E91291ACB0148DC9D71DE91291ACB0148DC9D71D&first=0

Ammeter

The following is taken from All About Circuits, *Ammeter*.

The most common way to measure current in a circuit is to break the circuit open and insert an ammeter in series with the circuit so that all electrons flowing through the circuit also have to go through the meter. Because measuring current in this manner requires the meter be made part of the circuit, it is more difficult to measure than voltage or resistance.

Some digital meters, like the unit shown in figure 6, have a separate jack to insert the red test lead plug when measuring current. Other meters, like most inexpensive analog meters, use the same jacks for measuring voltage, resistance, and current.



Source: All About Circuits, Ammeter

Figure 6. Digital ammeter

When an ammeter is placed in series with a circuit, it ideally drops no voltage as current goes through it. It acts very much like a piece of wire, with very little resistance from one test

probe to the other. Consequently, an ammeter will act as a short circuit if placed in parallel (across the terminals) of a substantial source of voltage. If this is done, a surge in current will result, potentially damaging the meter.

Ammeters are generally protected from excessive current by means of a small fuse located inside the meter housing. If the ammeter is accidently connected across a substantial voltage source, the resultant surge in current will blow the fuse and render the meter incapable of measuring current until the fuse is replaced.

Ohmmeter

The following is taken from eHow, *What is an Ohmmeter*?

An ohmmeter is an electronic device used to measure a material's resistance to electrical current. An ohmmeter is useful in troubleshooting electrical or electronic circuits and devices to help pinpoint the cause of component failures.

A simple ohmmeter has a readout display, two probes, and a source of electrical current—usually a small, internal battery.

When the meter's probes are applied to a material, the electrical source introduces a small current in the material between the tips of the probes. The meter detects the difference in voltage between the two probe tips and displays a measurement of the material's resistance. This difference in voltage results from the material's resistance to current flow and is called resistance. The readout on the ohmmeter's display is given in units of measurement called ohms.

If the material is a good conductor of electrical current, such as a piece of copper wire, then the resistance is low. When resistance is low, the ohm readout on the meter will be a very low number and might even be zero. If the resistance is very high such as in insulating material, the readout on the meter will be high; maybe tens of thousands of ohms or higher.

If the probes of the meter are applied to two points that have no physical connection, there will be no current flow. This condition is known as an open. In the case of an open, the meter's display will show infinite resistance.

An ohmmeter can be used to find broken or shorted wires by taking resistance measurements at different points along the path of a circuit. The meter can also be used to help diagnose failures in closed components such as electrical motors or in solid state devices by comparing readings measured.

Video 9. How to use an ohmmeter

http://www.bing.com/videos/search?q=ohmmeter&view=detail&mid=5460D019125DF38A0EE95460D019125DF38A0EE9&first=0

Calibration and Accuracy

The following is taken from Fluke, *Electrical Calibration*, "Why Calibrate Test Equipment?"

Calibration typically requires a standard that has at least 10 times the accuracy of the instrument under test. Otherwise, calibration is occurring within overlapping tolerances and the tolerances of the standard render an "in cal" instrument "out of cal" or vice-versa. For example, two instruments, A and B, measure 100 V within one percent. At 480 V, both are

within tolerance. At 100 V input, A reads 99.1 V and B reads 100.9 V. But if B is used as the standard, A will appear to be out of tolerance. However, if B is accurate to 0.1 percent, then the most B will read at 100 V is 100.1 V. Comparing A to B, A is in tolerance, and A is at the low end of the tolerance range. Modifying A to bring that reading up will presumably keep A from giving a false reading as it experiences normal drift between calibrations.

Calibration, in its purest sense, is the comparison of an instrument to a known standard. Proper calibration involves use of a National Institute of Standards and Technology (NIST)-traceable standard: one that has paperwork showing it compares correctly to a chain of standards going back to a master standard maintained by the NIST.

In practice, calibration includes correction. Usually when an instrument is calibrated, repairs are authorized to bring the instrument back into calibration if it was "out of cal."

A report will show how far out of calibration the instrument was before, and how far out it is after.

e. Explain the requirements of electrical safety class and safety significant systems (e.g., application of DOE O 420.1C, *Facility Safety*, DOE G 420.1-1A, IEEE Std 379, *Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*, IEEE Std-384, *Criteria for Independence of Class 1E Equipment and Circuits, etc)* and their application in I&C systems design.

DOE G 420.1-1

The following is taken from DOE G 420.1-1A.

The safety functions of instrumentation, control, and alarm systems are to provide information on out-of-tolerance conditions/abnormal conditions; ensure the capability for manual or automatic actuation of safety systems and components; ensure safety systems have the means to achieve and maintain a fail-safe shutdown condition on demand under normal or abnormal conditions; and/or actuate alarms to reduce public or site-personnel risk.

The design of safety-class and safety-significant instrumentation and control systems must incorporate sufficient independence, redundancy, diversity, and separation to ensure that all safety-related functions associated with such equipment can be performed under postulated accident conditions as identified in the safety analysis. Safety-significant components should be evaluated as to the need for redundancy on a case-by-case basis. Under all circumstances, safety-class instrumentation, controls, and alarms must be designed so that failure of non-safety equipment will not prevent the former from performing their safety functions.

Safety-significant and safety-class instrumentation, control, and alarm-system designs must ensure accessibility for inspection, maintenance, calibration, repair, or replacement. Safety-class instrumentation, control, and alarm systems must provide the operators sufficient time, information, and control capabilities to perform the following safety functions:

- Determine the status of critical facility parameters to ensure compliance with the limits specified in the technical safety requirements
- Initiate automatic or manual safety functions

- Determine the status of safety systems required to ensure proper mitigation of the consequences of postulated accident conditions and/or to safely shut down the facility

ANSI/IEEE standards contain design, installation, and testing requirements that should be considered for instrumentation, control, and alarm components without invoking all of the safety class 1E requirements. See table 1 for the relevant codes.

Table 1. Codes for safety-significant and safety-class instrumentation, control, and alarm components

Instruments, Controls, and Alarms	Safety Significant	Safety Class
Hardware	NFPA-70, -110; ANSI C2; ANSI/ANS-8.3, -N42.18, -N13.1; ANSI/ISA-Series; ANSI/IEEE-141, -142, -242, -493, -1050	NFPA-70, -110; ANSI C2; ANSI/ANS-8.3, -N42.18, -N13.1; ANSI-N320, -N323; ANSI/ISA-Series; ANSI/IEEE-141, -142, -242, -323, -336, -338, -344, -379, -384, -493, -1050

Source: DOE G 420.1-1: Titles and dates of listed codes are available in the bibliography.

IEEE-379

The following is taken from the Institute for Electrical and Electronic Engineers, IEEE-379-2000.

In applying the single-failure criterion to the design of safety systems, the following conditions are implicit:

- *Independence and redundancy.* The principle of independence is basic to the effective use of the single-failure criterion. The design of a safety system shall be such that no single failure of a component will interfere with the proper operation of an independent redundant component or system.
- *Non-detectable failure.* The detectability of failures is implicit in the application of the single-failure criterion. Detectability is a function of the system design and the specified tests. A failure that cannot be detected through periodic testing, or revealed by alarm or anomalous indication, is non-detectable. An objective in an analysis of safety systems is to identify non-detectable failures. When non-detectable failures are identified, one of the following courses of action shall be taken:
  - Preferred course—the system or the test scheme shall be redesigned to make the failure detectable.
  - Alternative course—when analyzing the effect of each single failure, all identified non-detectable failures shall be assumed to have occurred.
- *Cascaded failures.* Whenever the design is such that additional failures could be expected from the occurrence of a single failure from any source, these cascaded failures, collectively, shall be considered to be a single failure.

- *Design basis events*. A design basis event that results in the need for safety functions may cause failure of system components, modules, or channels. To provide protection from these failures, the equipment should be designed, qualified, and installed to be immune to such anticipated challenges. When analysis indicates that failures in a safety system result from design basis events, these failures shall be considered a consequence of the event.
- *Common-cause failures*. Certain common-cause failures shall be treated as single failures when conducting the single-failure analysis. Such failures can be in dissimilar components and can have dissimilar failure modes. Common-cause failures not subject to single-failure analysis include those that can result from external environmental effects, design deficiencies, manufacturing errors, maintenance errors, and operator errors. Design qualification and quality assurance programs are intended to afford protection from external environmental effects, design deficiencies, and manufacturing errors. Personnel training; proper control room design; and operating, maintenance, and surveillance procedures are intended to afford protection from maintenance and operator errors. Additionally, provisions should be made to address common-cause failures. Examples of techniques are detailed defense-in-depth studies, failure mode and effects analysis, and analyses of abnormal conditions or events. Design techniques, such as diversity and defense-in-depth, can be used to address common-cause failures.

IEEE Std-384

The following is taken from the Institute for Electrical and Electronic Engineers, IEEE-384-1999.

GENERAL INDEPENDENCE CRITERIA

Required independence. Physical separation and electrical isolation shall be provided to maintain the independence of Class 1E circuits and equipment so that the safety functions required during and following any design basis event can be accomplished.

Methods of achieving independence. The physical separation of circuits and equipment shall be achieved by the use of safety class structures, separation distance, or barriers or any combination thereof. Electrical isolation shall be achieved by the use of separation distance, isolation devices, shielding and wiring techniques, or combinations thereof.

Equipment and circuits requiring independence. Equipment and circuits requiring independence shall be determined and delineated during the plant design and shall be identified on documents and drawings in a distinctive manner.

Compatibility with auxiliary supporting features. The independence of Class 1E circuits and equipment shall not be compromised by the functional failure of auxiliary supporting features. For example, an auxiliary supporting feature shall be assigned to the same division as the Class 1E system it is supporting to prevent the loss of mechanical function in one division from causing loss of electrical function in another division.

ASSOCIATED CIRCUITS

Non-Class 1E power, control, and instrumentation circuits become associated in one or more of the following ways:

- Electrical connection to a Class 1E power supply without the use of an isolation device
- Electrical connection to an associated power supply without the use of an isolation device
- Proximity to Class 1E circuits and equipment without the required physical separation or barriers
- Proximity to associated circuits and equipment without the required physical separation or barriers
- Sharing a Class 1E or associated signal source without the use of an isolation device

Associated circuits shall comply with one of the following requirements:

- They shall be uniquely identified as such or as Class 1E and shall remain with (traceable to the associated Class 1E division), or be physically separated the same as those Class 1E circuits with which they are associated. They shall be subject to the requirements placed on Class 1E circuits, unless it can be demonstrated by analysis or testing that the absence of such requirements cannot degrade the Class 1E circuits below an acceptable level.
- They shall be in accordance with the above from the Class 1E equipment to and including an isolation device. Beyond the isolation device, such a circuit is non-Class 1E, provided that it does not again become associated with a Class 1E system.
- They shall be analyzed or tested to demonstrate that Class 1E circuits are not degraded below an acceptable level.

Associated circuits, including their isolation devices or the connected loads without the isolation devices, shall be subject to the qualification requirements placed on Class 1E circuits to assure that the Class 1E circuits are not degraded below an acceptable level. Associated circuits need not be qualified for performance of function, since the function is non-Class 1E.

The independence of non-Class 1E circuits from Class 1E circuits or associated circuits shall be achieved by complying with the following requirements:

- Non-Class 1E circuits shall be physically separated from Class 1E circuits and associated circuits by the minimum separation requirements specified in IEEE-384.
- Non-Class 1E circuits shall be electrically isolated from Class 1E circuits and associated circuits by the use of isolation devices, shielding, and wiring techniques, or separation distance or the non-Class 1E circuits shall be associated circuits.
- The effects of less than minimum separation or the absence of electrical isolation between the non-Class 1E circuits and the Class 1E circuits or associated circuits shall be analyzed to demonstrate that Class 1E circuits are not degraded below an acceptable level, or the non-Class 1E circuits shall be associated circuits.
- Non-Class 1E instrumentation signal and control circuits are not required to be physically separated or electrically isolated from associated circuits provided that a) the non-Class 1E circuits are not routed with associated cables of a redundant division and b) the non-Class 1E circuits are analyzed to demonstrate that Class 1E circuits are

not degraded below an acceptable level. As part of the analysis, consideration shall be given to potential energy and identification of the circuits involved.

f. Explain the use of electrical components (e.g., using analog relays, relay logic, motors, and motor operated valves, etc) as they relate to I&C systems design, and explain how they are reviewed and analyzed to ensure that they demonstrate that the design meets the requirements of the Documented Safety Analysis (DSA), DOE O 420.1C, and other industry standards.

Analog Relays

The following is taken from Wikipedia, *Analog Switch*.

The analog switch, also called the bilateral switch, is an electronic component that acts like a relay, but has no moving parts. The switching element is normally a pair of metal-oxide-semiconductor (MOS) field-effect transistor transistors; one is an N-channel device, the other a P-channel device. The device can conduct analog or digital signals in either direction when on, and isolates the switched terminals when off. Analog switches are usually manufactured as integrated circuits in packages containing multiple switches.

The control input to the device may be a signal that switches between the positive and negative supply voltages, with the positive voltage switching the device on and the negative switching the device off. Other circuits are designed to communicate through a serial port with a host controller to set switches on or off.

The signal being switched must remain within the bounds of the positive and negative supply rails that are connected to the P-MOS and N-MOS body terminals. The switch generally provides good isolation between the control signal and the input/output signals.

Important parameters of an analog switch are

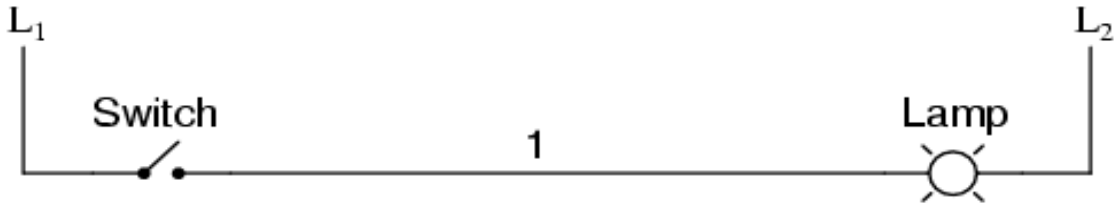
- on-resistance—the resistance when switched on. This commonly ranges from 5 ohms to a few hundred ohms;
- off-resistance—the resistance when switched off. This is typically a number of megohms or gigaohms;
- signal range—the minimum and maximum voltages allowed for the signal to be passed through. If these are exceeded, the switch may be destroyed by excessive currents. Older types of switches can even latch up, which means that they continue to conduct excessive currents even after the faulty signal is removed; and
- charge injection—the effect that causes the switch to inject a small electric charge into the signal when it switches on, causing a small spike or glitch. The charge injection is specified in coulombs.

Relay Logic

The following is taken from OpAmp-Electronics, *Digital Theory*, chapter 6, "Ladder Logic, Ladder Diagrams."

Ladder diagrams are specialized schematics commonly used to document industrial control logic systems. They are called "ladder" diagrams because they resemble a ladder, with two vertical rails (supply power) and as many "rungs" (horizontal lines) as there are control

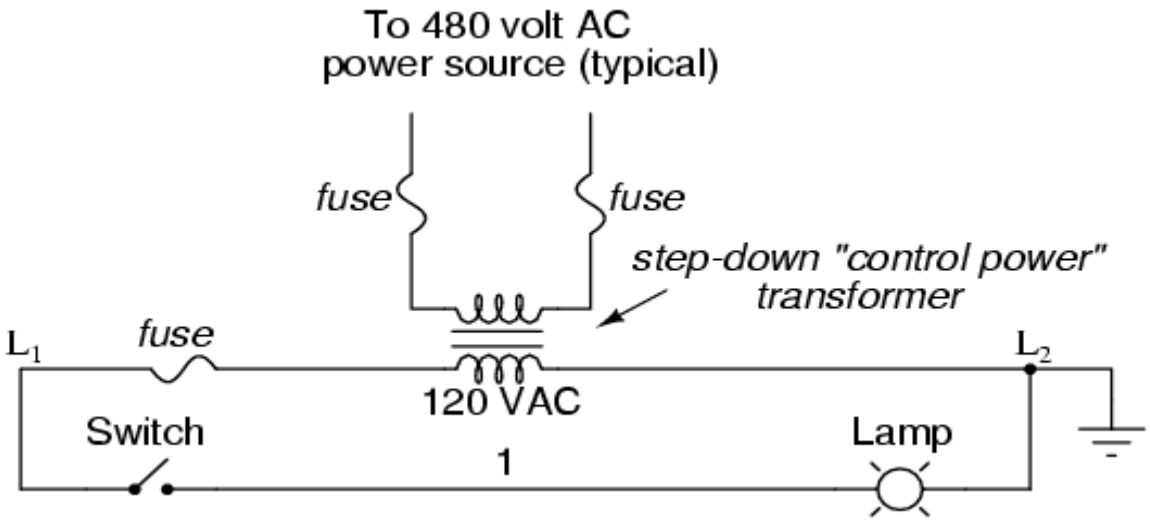
circuits to represent. A simple ladder diagram showing a lamp that is controlled by a hand switch would look like figure 7.



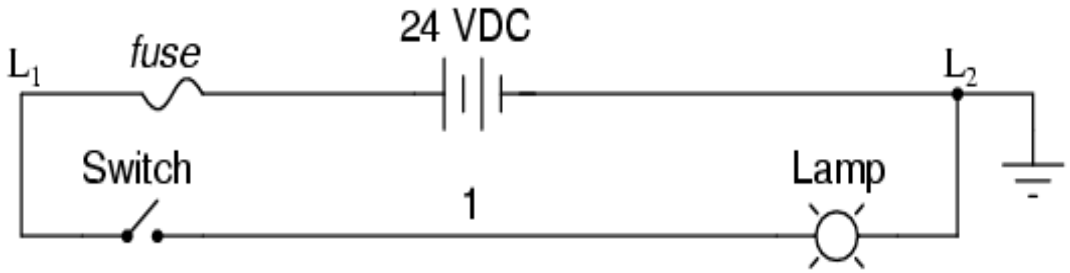
Source: OpAmp, Ladder Diagrams

Figure 7. Simple ladder diagram

The "L_1" and "L_2" designations refer to the two poles of a 120 volts alternating current (VAC) supply, unless otherwise noted. L_1 is the "hot" conductor, and L_2 is the grounded (neutral) conductor. It can be confusing that these designations have nothing to do with inductors. The actual transformer or generator supplying power to this circuit is omitted for simplicity. In reality, the circuit looks something like the sample circuit in figure 8.



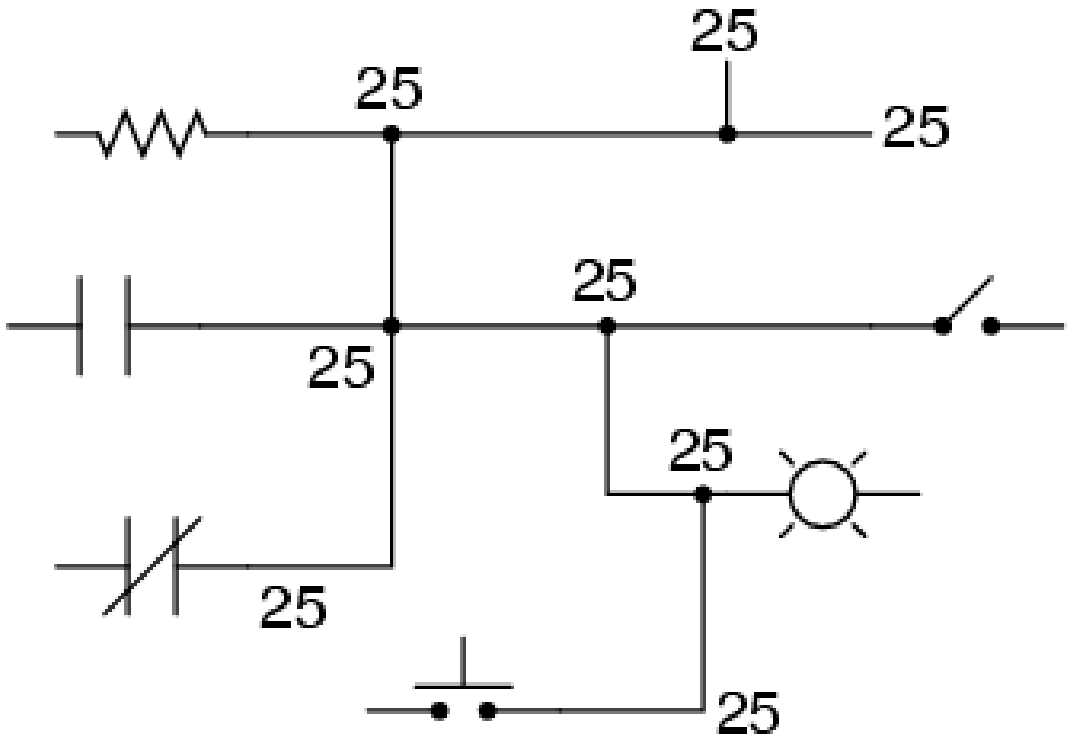
Source: OpAmp, Ladder Diagrams
Figure 8. Sample circuit



Source: OpAmp, Ladder Diagrams
Figure 9. Relay logic circuit

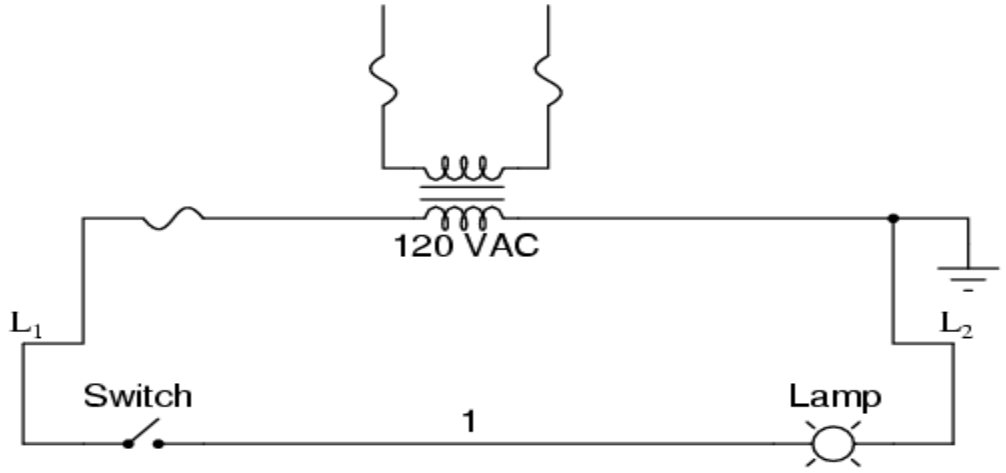
Typically in industrial relay logic circuits, the operating voltage for the switch contacts and relay coils will be 120 VAC. Lower voltage AC and even DC systems are sometimes built and documented according to ladder diagrams such as the one shown in figure 9.

So long as the switch contacts and relay coils are all adequately rated, it really does not matter what level of voltage is chosen for the system to operate.
Note the number "1" on the wire between the switch and the lamp in figure 9. In the real world, that wire would be labeled with that number, using heat-shrink or adhesive tags, wherever it was convenient to identify. Wires leading to the switch would be labeled "L_1" and "1," respectively. Wires leading to the lamp would be labeled "1" and "L_2," respectively. These wire numbers make assembly and maintenance very easy. Each conductor has its own unique wire number for the control system for which it is used. Wire numbers do not change at any junction or node, even if wire size, color, or length change going into or out of a connection point. It is preferable to maintain consistent wire colors, but this is not always practical. What matters is that any one, electrically continuous point in a control circuit possesses the same wire number. Figure 10, for example, shows wire #25 as a single, electrically continuous point threading to many different devices.



Source: OpAmp, Ladder Diagrams
Figure 10. Continuous circuit

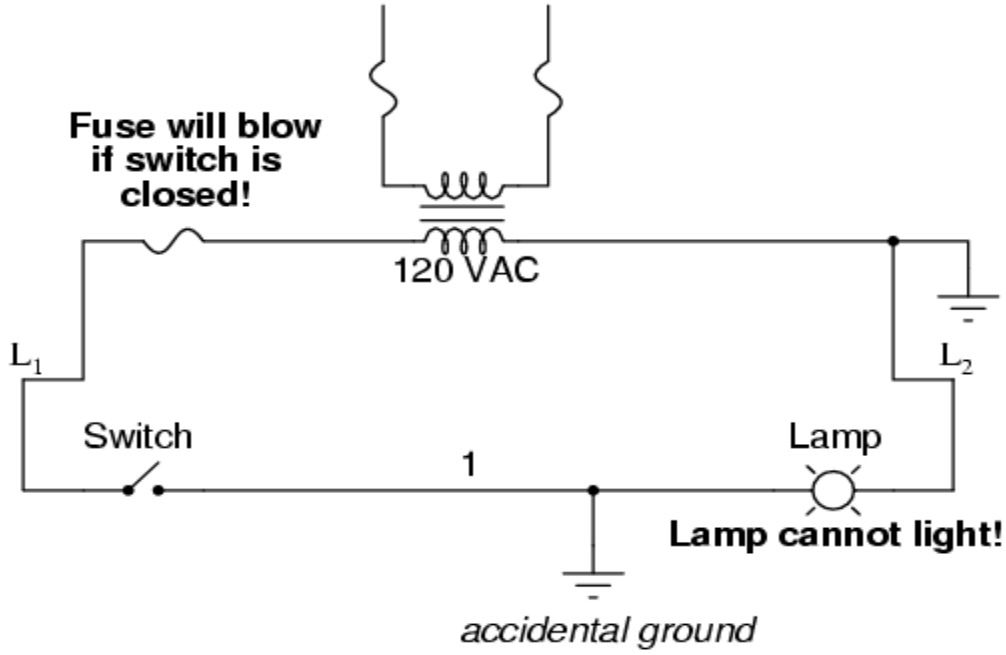
In ladder diagrams, the load device (lamp, relay coil, solenoid coil, etc.) is almost always drawn at the right-hand side of the rung. While it does not matter electrically where the relay coil is located within the rung, for reliable operation it does matter which end of the ladder's power supply is grounded; for example, the circuit in figure 11.



Source: OpAmp, Ladder Diagrams

Figure 11. Ladder diagram for a load device

Here, the lamp (load) is located on the right-hand side of the rung, and so is the ground connection for the power source. This is no accident or coincidence; rather, it is a purposeful element of good design practice. If wire #1 were to accidently come in contact with ground, (the insulation of that wire having been rubbed off so that the bare conductor came in contact with grounded metal conduit), the circuit would now function as shown in figure 12.

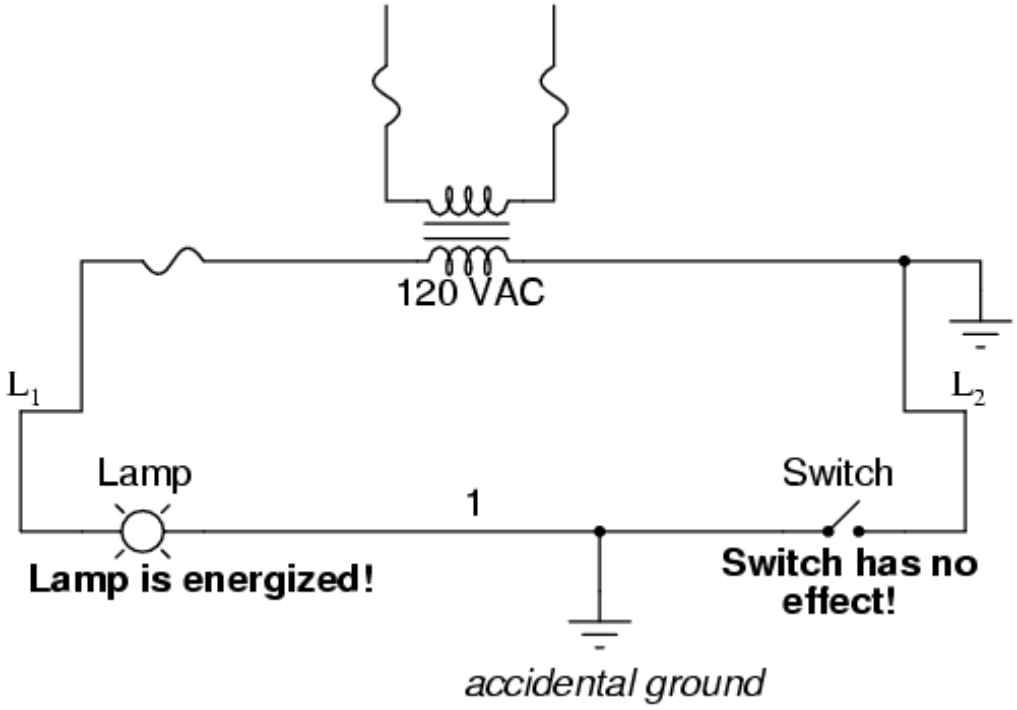


Source: OpAmp, Ladder Diagrams

Figure 12. Short circuit

With both sides of the lamp connected to ground, the lamp will be "shorted out" and unable to receive power to light up. If the switch closed, there would be a short-circuit, immediately blowing the fuse.

However, consider what would happen to the circuit with the same fault (wire #1 coming in contact with ground), except this time swap the positions of switch and fuse (L_2 still grounded).



Source: OpAmp, Ladder Diagrams

Figure 13. Corrected ground fault

Figure 13 shows that the accidental grounding of wire #1 will force power to the lamp while the switch will have no effect. It is much safer to have a system that blows a fuse in the event of a ground fault than to have a system that uncontrollably energizes lamps, relays, or solenoids in the event of the same fault. For this reason, the load(s) must always be located nearest the grounded power conductor in the ladder diagram.

Review and Analysis

The following is taken from Oak Ridge National Laboratory, *Electrical Signal Analysis (ESA)*.

Electrical signature analysis (ESA), a versatile and powerful, yet truly non-intrusive technology pioneered at Oak Ridge National Laboratory (ORNL), can be readily integrated into most electro-mechanical equipment to greatly enhance condition diagnostics and prognostics capabilities. ESA provides diagnostic and prognostic information comparable to conventional vibration analysis, but requires only access to electrical lines carrying input or output power rather than to the equipment itself. Thus, either onboard or remote analysis is possible—even continuous monitoring if desired. ESA has already been tested on and

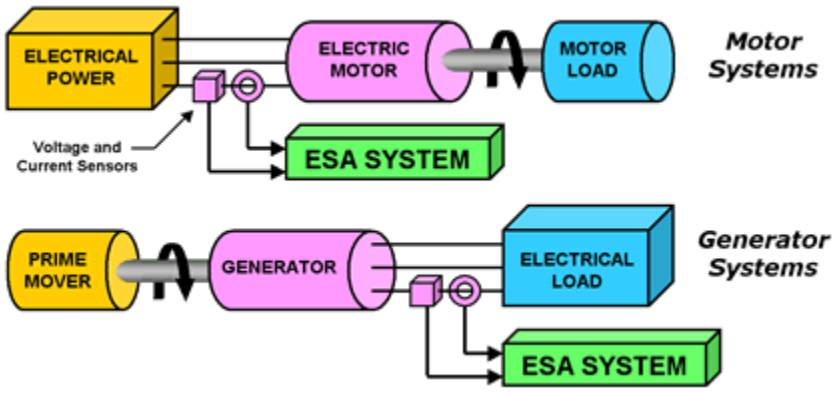
successfully applied to a wide variety of systems, including those in military, industrial, and consumer equipment.

Load and speed variations in electro-mechanical systems generally produce correlated variations in current and voltage. ESA analyzes these small perturbations and matches them to their source. The resulting time and frequency signatures reflect loads, stresses, and wear throughout the system, and allow an extensive range of mechanical diagnostic information to be obtained from a single sensor attached to an electrical line.

Few available technologies can be so seamlessly integrated into existing maintenance programs. With the addition of a few sensors, ESA diagnostics can pinpoint electrical and mechanical problems and target maintenance on an as-needed basis, thereby increasing equipment reliability and maintenance efficiency while minimizing unexpected downtime.

TECHNICAL BASIS

ESA provides a breakthrough in the ability to detect and quantify mechanical defects and degradations in electro-mechanical equipment and unwanted changes in process conditions. ESA is truly non-intrusive and does not interfere with the operation of the equipment being monitored.



Source, Oak Ridge National Laboratory, Electrical Signal Analysis

Figure 14. Electrical signal analysis

As a result of continued research and development (R&D) by ORNL, ESA has matured as a diagnostic/prognostic technology. ORNL has developed several signal processing and signature analysis methods to capitalize on the intrinsic abilities of conventional electric motors and generators to act as transducers.

Time-dependent load and speed variations occurring throughout an electro-mechanical system will generally induce small variations in the motor's and/or generator's electrical response. These variations are observed as a change in current (for a motor) or a change in voltage (for a generator). ORNL researchers have pioneered the development and application of signal conditioning techniques for extracting these small electrical perturbations and relating them to their source, and have thus opened a new field for diagnostic innovations.

MOTOR-OPERATED VALVES

Motor-operated valves are used in large numbers throughout many industries. In the mid-1980s, ORNL, with funding from the United States (U.S.) Nuclear Regulatory Commission,

evaluated methods for monitoring aging and service wear of nuclear power plant MOVs. In addition to evaluating standard condition monitoring methods employing equipment-mounted sensors, ORNL researchers focused their efforts on developing diagnostic techniques that used the motor's running current, since it could be acquired remotely and non-intrusively. These new techniques provided a breakthrough in detecting load and speed variations generated anywhere within the MOV and converting them into revealing "signatures" that could be used to detect component degradation and precursors to MOV failures.

ORNL named this new monitoring technology motor current signature analysis (MCSA), a term that is widely shown by ORNL to provide the sensitivity necessary to detect a large variety of MOV problems including gear wear and binding, degraded lubrication, over-tightened stem packing, valve seating problems, bent valve stem, improperly set switches, etc. The successful application of MSCA as a monitoring technology for MOVs provided a foundation on which additional tools were developed by ORNL for monitoring and analyzing electrical current, voltage, and power signals. These developments are applicable to both motor and generator systems and now comprise the powerful technology suite called ESA.

g. Explain the importance of considering normal and anticipated abnormal environmental conditions (e.g., temperature, humidity, radiation, etc.) when selecting electrical components for use in I&C systems design (e.g., guidance of IEEE Std 323, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,* and DOE O 420.1C, etc.).

The following is taken from U.S. Nuclear Regulatory Commission, NUREG 1.209.

The ANSI/IEEE-323 definition of qualification is "generation and maintenance of evidence to ensure that the equipment will operate on demand to meet system performance requirements."

In effect, environmental qualification is verification and validation that a design adequately accommodates the effects of, and is compatible with, the environmental conditions associated with the normal, abnormal, and accident conditions that the equipment or system might encounter. 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants" defines a mild environment as one "that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences."

However, as a mild environment in a nuclear power plant can encompass environmental conditions that can affect the performance of sensitive equipment, qualification to demonstrate compatibility with those environmental conditions is necessary in those cases.

The practices in IEEE Std. 323-2003 are sufficiently comprehensive to address qualification for the less severe environmental conditions of typical plant locations where safety-related computer-based I&C systems are generally located. These plant areas are unaffected by design-basis accidents and the most severe conditions to which the equipment is subjected, which arise from the environmental extremes resulting from normal and abnormal operational occurrences.

Addressing qualification requirements for safety-related computer-based I&C systems is one method of ensuring that the probability of common-cause failure attributable to environmental stressors is reduced to an acceptable level.

Computer-based I&C systems present unique characteristics that must be considered in the qualification process. These characteristics include functional and hardware considerations.

One significant difference between analog and digital equipment is the higher functional density that is possible with computer-based I&C systems. Due to the expanding single-chip capabilities, many safety-related installations involve replacement of multiple functional modules with a multifunction microprocessor-based module. Another difference involves the sequential function execution that typifies computer-based I&C systems compared to the essentially parallel execution of analog modules.

The effect of these differences can be compounded for multiple systems that rely on either successful completion of digital data communication or error detection before continuation of discrete functional steps. The capability of digital system design accommodates the potentially cumulative effects of environmental stress and is an important consideration for qualification of computer-based I&C systems.

One stressor not previously considered for analog safety system qualification is smoke exposure from an electrical fire. Based on the investigation of smoke susceptibility and the resulting understanding of key failure mechanisms, smoke clearly has the potential to be a significant environmental stressor that can result in adverse consequences.

The most reasonable approach to minimizing smoke susceptibility is to employ design, construction, installation, and procedural practices that can reduce the possibility of smoke exposure and enhance smoke tolerance. In particular, current fire protection methods focus on a preventive approach, employing isolation and detection practices. In addition, post-event recovery procedures can mitigate the extent of smoke damage. Moreover, certain design choices and construction practices, such as chip packaging and conformal coatings, can reduce equipment susceptibility to smoke exposure. The most effective approach for addressing smoke susceptibility is to minimize the likelihood of smoke exposure by rigorously adhering to the fire protection requirements in 10 CFR 50.48, “Fire Protection,” or other individual plant license commitments.

The safety goal of qualification is to avoid a common-cause failure of the safety-related system when it is needed to perform its safety function. The unique functional and hardware characteristics of computer-based I&C systems suggest that qualification guidance should explicitly state special considerations. These special considerations constitute good engineering practices that the industry generally follows.

2. I&C personnel must demonstrate a familiarity level knowledge of basic mechanical engineering fundamentals, including thermodynamics and hydraulics.

a. Explain basic theory of thermodynamics and hydraulics as related to process systems control and operations (e.g., relationship between fluid system pressure, temperature, density, flow, etc.).

Thermodynamics

The following is taken from Wikipedia, *Laws of Thermodynamics*.

The four laws of thermodynamics define fundamental physical quantities (temperature, energy, and entropy) that characterize thermodynamic systems. The laws describe how these quantities behave under various circumstances, and forbid certain phenomena (such as perpetual motion).

The four laws of thermodynamics are as follows:

- *Zeroth law of thermodynamics*. If two systems are in thermal equilibrium with a third system, they must be in thermal equilibrium with each other. This law helps define the notion of temperature.
- *First law of thermodynamics*. Heat and work are forms of energy transfer. Energy is invariably conserved but the internal energy of a closed system changes as heat and work are transferred in or out of it. Equivalently, perpetual motion machines of the first kind are impossible.
- *Second law of thermodynamics.* The entropy of any isolated system not in thermal equilibrium almost always increases. Isolated systems spontaneously evolve towards thermal equilibrium—the state of maximum entropy of the system—in a process known as "thermalization." Equivalently, perpetual motion machines of the second kind are impossible.
- *Third law of thermodynamics.* The entropy of a system approaches a constant value as the temperature approaches zero. The entropy of a system at absolute zero is typically zero, and in all cases is determined only by the number of different ground states it has. Specifically, the entropy of a pure crystalline substance at absolute zero temperature is zero.

Hydraulics

The following is taken from Wikipedia, *Hydraulics*.

Hydraulics is a topic in applied science and engineering dealing with the mechanical properties of liquids. At a very basic level, hydraulics is the liquid version of pneumatics. Fluid mechanics provides the theoretical foundation for hydraulics, which focuses on the engineering uses of fluid properties. In fluid power, hydraulics is used for the generation, control, and transmission of power by the use of pressurized liquids. Hydraulic topics range through some part of science and most of engineering modules, and cover concepts such as pipe flow, dam design, fluidics and fluid control circuitry, pumps, turbines, hydropower, computational fluid dynamics, flow measurement, river channel behavior, and erosion.

The following is taken from DesignAerospace LLC, *Hydraulic Fluid—Properties*.

The effects of temperature and pressure on hydraulic system fluid properties and flow characteristics are listed below.

DENSITY
Affects orifice and valve volume flow rates—as density increases, orifice and valve flow rates will decrease (see orifice flow equations).

- Increasing pressure increases density
- Increasing temperature decreases density

KINEMATIC VISCOSITY
Affects pipe (tube) volumetric flow rate—as viscosity increases, pipe flow rate will decrease). Kinematic viscosity increases with increased pressure and decreasing temperature.

- Increasing pressure increases kinematic viscosity
- Increasing temperature decreases kinematic viscosity

BULK MODULUS
Affects compressibility of fluid and system response time—as bulk modulus decreases, the pressure derivative will decrease, leading to slower response times. Compressibility will affect the performance of actuators, motors, and pumps because the stiffness of the fluid is less as bulk modulus is reduced.

- Increasing pressure increases bulk modulus
- Increasing temperature decreases bulk modulus
- Entrained air and compliance of hoses/tubes/parts decreases bulk modulus

b. Explain how the following components may be applied to I&C systems design, and the importance of their characteristics to I&C systems design and operations:

- **Gate valve**
- **Globe valve**
- **Butterfly valve**
- **Diaphragm valve**
- **Check valve**
- **Relief valve**
- **Pressure regulating valve**
- **Solenoid valve actuator**
- **Pneumatic valve actuator**
- **Orifice plate**
- **Centrifugal pump**
- **Positive displacement pump**
- **Compressor**
- **Instrument air system**
- **Dampers**
- **HEPA filters**

Gate Valve

The following is taken from Wikipedia, *Gate Valve*.

Source: Wikipedia, Gate Valve

Figure 15. Gate valve

The gate valve, as shown in figure 15, is a valve that opens by lifting a round or rectangular gate/wedge out of the path of the fluid. The distinct feature of a gate valve is that the sealing surfaces between the gate and seats are planar, so gate valves are often used when a straight-line flow of fluid and minimum restriction is desired. The gate faces can form a wedge shape or they can be parallel. Gate valves are primarily used to permit or prevent the flow of liquids, but typical gate valves shouldn't be used for regulating flow, unless they are specifically designed for that purpose. Due to their ability to cut through liquids, gate valves are often used in the petroleum industry. For extremely thick fluids, a specialty valve often known as a knife valve is used to cut through the liquid. When open, the gate valve's flow path is enlarged in a highly nonlinear manner with respect to percent of opening. This means that flow rate does not change evenly with stem travel. Also, a partially open gate disk tends to vibrate from the fluid flow. Most of the flow change occurs near shutoff with a relatively high fluid velocity causing disk and seat wear and eventual leakage if used to regulate flow. Typical gate valves are designed to be fully opened or closed. When fully open, the typical gate valve has no obstruction in the flow path, resulting in very low friction loss.

Gate valves are characterized as having either a rising or a non-rising stem. Rising stems provide a visual indication of valve position because the stem is attached to the gate such that the gate and stem raise and lower together as the valve is operated. Non-rising stem valves may have a pointer threaded onto the upper end of the stem to indicate valve position, since the gate travels up or down the stem on the threads without raising or lowering the stem. Non-rising stems are used underground or where vertical space is limited.

Bonnets provide leak proof closure for the valve body. Gate valves may have a screw-in, union, or bolted bonnet. Screw-in bonnets are the simplest, offering a durable, pressure-tight seal. Union bonnets are suitable for applications requiring frequent inspection and cleaning. They also give the body added strength. Bolted bonnets are used for larger valves and higher pressure applications.

Globe Valve

The following is taken from Wikipedia, *Globe Valve*.

A globe valve is a type of valve used for regulating flow in a pipeline. It consists of a movable disk-type element and a stationary ring seat in a generally spherical body.

Globe valves are named for their spherical body shape. The two halves of the body are separated by an internal baffle that has an opening that forms a seat onto which a movable plug can be screwed in to close (or shut) the valve. The plug is also called a disc or disk. In globe valves, the plug is connected to a stem which is operated by screw action using a hand

wheel in manual valves. Typically, automated globe valves use smooth stems rather than threaded stems, and are opened and closed by an actuator assembly.

Globe valves are used for applications requiring throttling and frequent operation. For example, globe valves or valves with a similar mechanism may be used as sampling valves, which are normally shut except when liquid samples are being taken. Since the baffle restricts flow, they are not recommended where full, unobstructed flow is required.

Butterfly Valve

The following is taken from Wikipedia, *Butterfly Valve*.

A butterfly valve is a valve that can be used for isolating or regulating flow. The closing mechanism takes the form of a disk. Operation is similar to that of a ball valve, which allows for quick shut off. Butterfly valves are generally favored because they are lower in cost than other valve designs as well as being lighter in weight, meaning less support is required. The disc is positioned in the center of the pipe; passing through the disc is a rod connected to an actuator on the outside of the valve. Rotating the actuator turns the disc either parallel or perpendicular to the flow. Unlike a ball valve, the disc is always present within the flow; therefore a pressure drop is always induced in the flow, regardless of valve position.

A butterfly valve is from a family of valves called quarter-turn valves. The butterfly is a metal disc mounted on a rod. When the valve is closed, the disc is turned so that it completely blocks off the passageway. When the valve is fully open, the disc is rotated a quarter turn so that it allows an almost unrestricted passage of the fluid. The valve may also be opened incrementally to throttle flow.

There are different kinds of butterfly valves, each adapted for different pressures and different usages. The resilient butterfly valve, which uses the flexibility of rubber, has the lowest pressure rating. The high performance butterfly valve, used in slightly higher-pressure systems, features a slight offset in the way the disc is positioned, which increases the valve's sealing ability and decreases its tendency to wear. The valve best suited for high-pressure systems is the triple offset butterfly valve, which uses a metal seat, and is therefore able to withstand a greater amount of pressure.

Diaphragm Valve

The following is taken from Wikipedia, *Diaphragm Valve*.

Diaphragm valves (or membrane valves) consist of a valve body with two or more ports, a diaphragm, and a saddle or seat upon which the diaphragm closes the valve. The valve is constructed from either plastic or steel.

Originally, the diaphragm valve was developed for use in non-hygienic applications. Later, the design was adapted for use in the bio-pharmaceutical industry by using compliant materials that can withstand sanitizing and sterilizing methods.

There are two main categories of diaphragm valves: one type seals over a "weir" (saddle) and the other (sometimes called a "straight-way" valve) seals over a seat. The saddle type is the most common in process applications and the seat-type is more commonly used as a tank bottom valve but exists also as a process valve. While diaphragm valves usually come in two-port forms (2/2-way diaphragm valve), they can also come with three ports (3/2-way diaphragm valves, also called t-valves) and more (block-valves). When more than three ports are included, they generally require more than one diaphragm seat; however, special dual actuators can handle more ports with one membrane.

Diaphragm valves can be manual or automated. They are generally used as shut-off valves in process systems in the food and beverage, pharmaceutical, and biotech industries. The older generation of these valves are not suited for regulating and controlling process flows; however, newer models can successfully regulate and control process flows.

Source: Wikipedia, Relief valve

Figure 16. Relief valve

Check Valve

The following is taken from Wikipedia, *Check Valve*.

A check valve, clack valve, non-return valve, or one-way valve is a valve that normally allows fluid (liquid or gas) to flow through it in only one direction.

Check valves are two-port valves, meaning they have two openings in the body, one for fluid to enter and the other for fluid to exit. There are various types of check valves used in a wide variety of applications. Check valves are often part of common household items. Although they are available in an extensive range of sizes and costs, check valves are generally very small, simple, and/or inexpensive. Most check valves work automatically and are not regulated by a person or any external control; accordingly, most do not have any valve handle or stem. The bodies (external shells) of most check valves are made of plastic or metal.

An important concept in check valves is the cracking pressure, which is the minimum upstream pressure at which the valve will operate. Typically the check valve is designed for, and can therefore be specified for, a specific cracking pressure.

Relief Valve

The following is taken from Wikipedia, *Relief Valve*.

The relief valve, as shown in figure 16, is a type of valve used to control or limit the pressure in a system or vessel, which can build up by a process upset, instrument or equipment failure, or fire.

The pressure is relieved by allowing the pressurized fluid to flow from an auxiliary passage out of the system. The relief valve is designed or set to open at a predetermined set pressure to protect pressure vessels and other equipment from being subjected to pressures that exceed their design limits. When the set pressure is exceeded, the relief valve becomes the "path of least resistance" as the valve is forced open and a portion of the fluid is diverted through the auxiliary route. The diverted fluid is usually routed through a piping system known as a flare header or relief header to a central, elevated gas flare where it is usually burned and the resulting combustion gases are released to the atmosphere. As the fluid is diverted, the pressure inside the vessel will drop. Once it reaches the valve's reseating pressure, the valve will close. The blow down is usually stated as a percentage of set pressure and refers to how much the pressure needs to drop before the valve reseats. The blow down can vary from roughly 2–20 percent; some valves have adjustable blow downs.

In high-pressure gas systems, it is recommended that the outlet of the relief valve is in the open air. In systems where the outlet is connected to piping, the opening of a relief valve will cause a pressure build up in the piping system downstream of the relief valve. This often means that the relief valve will not re-seat once the set pressure is reached. For these systems, differential relief valves are regularly used. This means that the pressure is only working on an area that is much smaller than the opening of the valve. If the valve is opened, the pressure has to decrease enormously before the valve closes, and the outlet pressure of the valve can easily keep the valve open. Another consideration is that if other relief valves are connected to the outlet pipe system, they may open as the pressure in exhaust pipe system increases. This may cause undesired operation.

In some cases, a bypass valve acts as a relief valve to return all or part of the fluid discharged by a pump or gas compressor back to either a storage reservoir or the inlet of the pump or gas compressor. This is done to protect the pump or gas compressor and any associated equipment from excessive pressure. The bypass valve and bypass path can be internal or external. Many fire engines have such relief valves to prevent the overpressurization of fire hoses.

In other cases, equipment must be protected against being subjected to an internal vacuum that is lower than the equipment can withstand. In such cases, vacuum relief valves are used to open at a predetermined low pressure limit and to admit air or an inert gas into the equipment control the amount of vacuum.

Video 10. Relief valve

http://www.bing.com/videos/search?q=relief+valve&view=detail&mid=0F17B8B723338C815DA10F17B8B723338C815DA1&first=0

Pressure Regulating Valve

The following is taken from Wikipedia, *Pressure Regulator*.

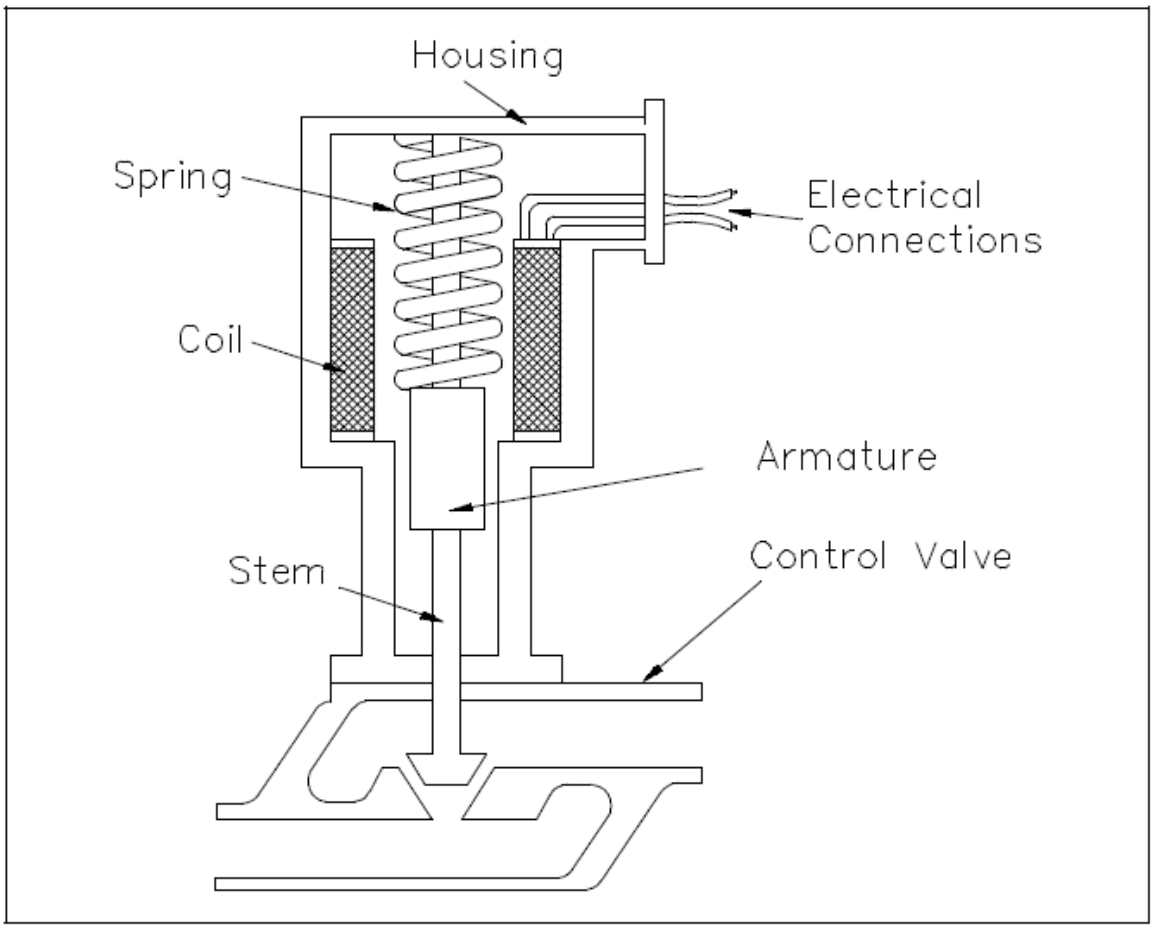
A pressure regulator is a valve that automatically cuts off the flow of a liquid or gas at a certain pressure. Regulators are used to allow high-pressure fluid supply lines or tanks to be reduced to safe and/or usable pressures for various applications.

Gas pressure regulators are used to regulate the gas pressure and are not appropriate for measuring flow rates. Flowmeters, rotometers or mass flow controllers should be used to accurately regulate gas flow rates.

Electronic Solenoid Actuators

The following is taken from DOE-HDBK-1013/2-92.

A typical electric solenoid actuator is shown in figure 17. It consists of a coil, armature, spring, and stem.



Source: DOE-HDBK-1013/2-92

Figure 17. Electric Solenoid Actuator

The coil is connected to an external current supply. The spring rests on the armature to force it downward. The armature moves vertically inside the coil and transmits its motion through the stem to the valve.

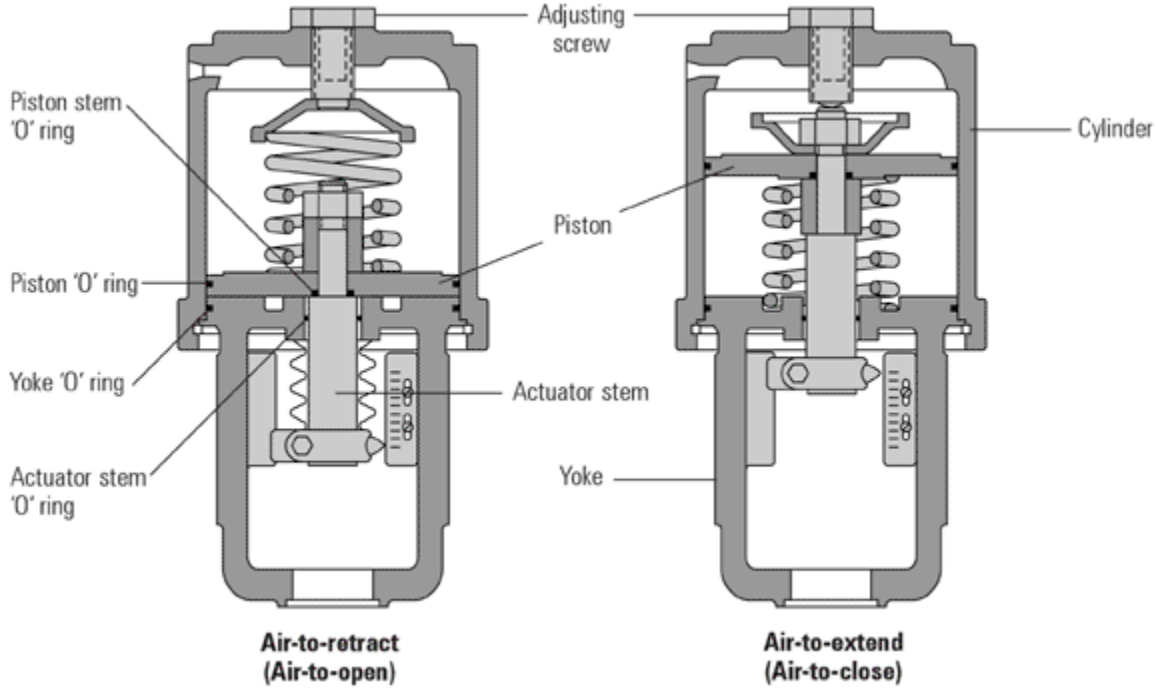
When current flows through the coil, a magnetic field forms around the coil. The magnetic field attracts the armature toward the center of the coil. As the armature moves upward, the spring collapses and the valve opens. When the circuit is opened and the current stops flowing to the coil, the magnetic field collapses. This allows the spring to expand and shut the valve.

A major advantage of solenoid actuators is their quick operation. Also, they are much easier to install than pneumatic or hydraulic actuators. However, solenoid actuators have two disadvantages. First, they have only two positions: fully opened and fully closed. Second, they don't produce much force, so they usually only operate relatively small valves.

Pneumatic Valve Actuator

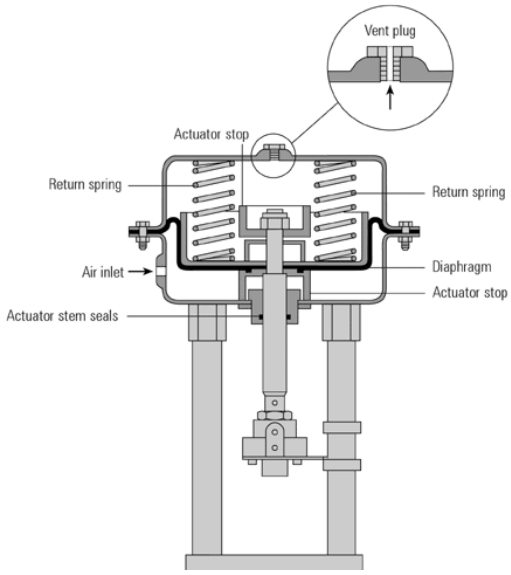
The following is taken from Spiraxsarco, *Control Value Actuators and Positioners*.

Pneumatic actuators are commonly used to actuate control valves and are available in two main forms; piston actuators (Figure 18) and diaphragm actuators (Figure 19).



Source: Spiraxsarco, Control Actuators and Positioners

Figure 18. Typical piston actuators



Source: Spiraxsarco, Control Actuators and Positioners

Figure 19. Diaphragm actuator

Piston actuators are generally used where the stroke of a diaphragm actuator would be too short or the thrust too small. Compressed air is applied to a solid piston contained within a solid cylinder. Piston actuators can be single acting or double acting, can withstand higher input pressures, and can offer smaller cylinder volumes, which can act at high speed.

DIAPHRAGM ACTUATORS

Diaphragm actuators apply compressed air to a flexible membrane called the diaphragm. Figure 19 shows a rolling diaphragm where the effective diaphragm area is virtually constant throughout the actuator stroke. These types of actuators are single acting, in that air is only supplied to one side of the diaphragm, and they can be either direct acting (spring-to-retract) or reverse acting (spring-to-extend).

REVERSE ACTING (SPRING-TO-EXTEND)

The operating force is derived from compressed air pressure, which is applied to a flexible diaphragm. The actuator is designed so that the force resulting from the air pressure, multiplied by the area of the diaphragm, overcomes the force exerted (in the opposite direction) by the spring(s).

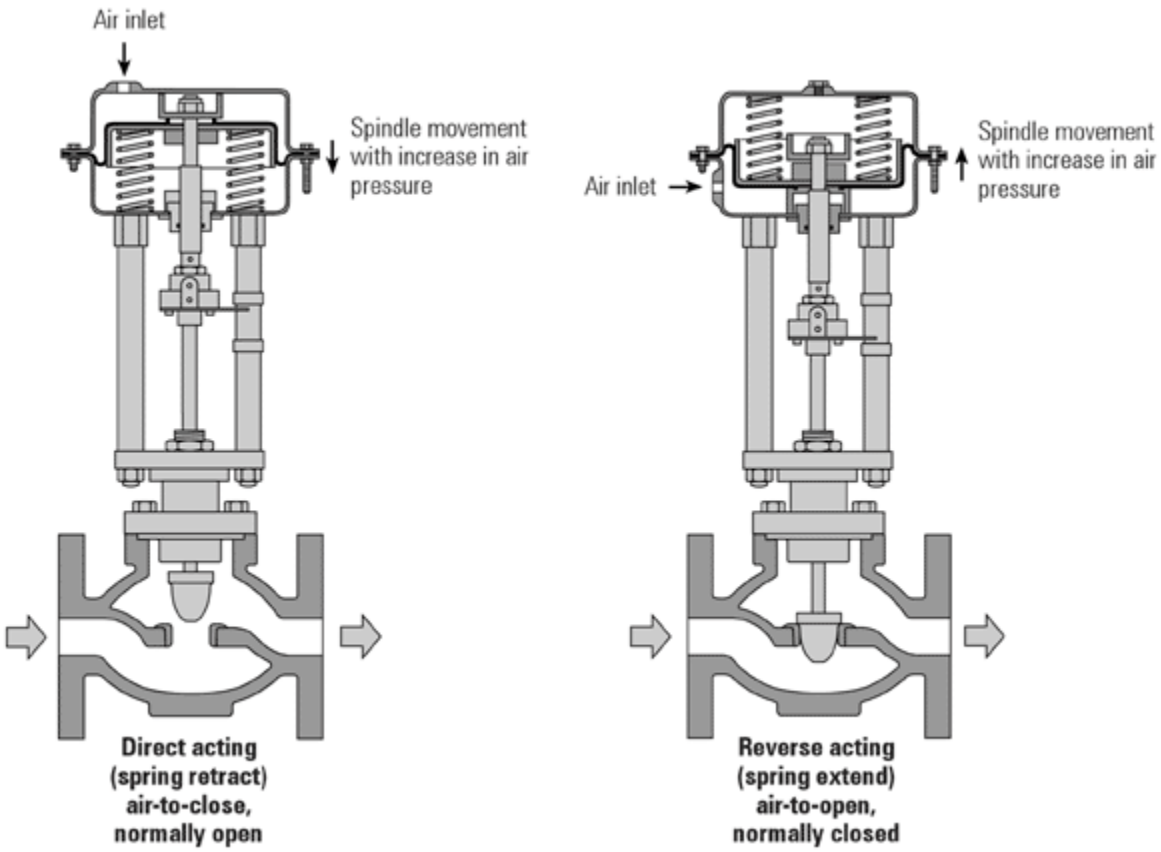
The diaphragm in figure 19 is pushed upwards, pulling the spindle up, and if the spindle is connected to a direct acting valve, the plug is opened. The actuator is designed so that with a specific change of air pressure, the spindle will move sufficiently to move the valve through its complete stroke from fully-closed to fully-open.

As the air pressure decreases, the spring(s) moves the spindle in the opposite direction. The range of air pressure is equal to the stated actuator spring rating, for example 0.2 - 1 bar.

With a larger valve and/or a higher differential pressure to work against, more force is needed to obtain full valve movement.

To create more force, a larger diaphragm area or higher spring range is needed. This is why control manufacturers offer a range of pneumatic actuators to match a range of valves comprising increasing diaphragm areas, and a choice of spring ranges to create different forces.

The diagrams in figure 20 show the components of a basic pneumatic actuator and the direction of spindle movement with increasing air pressure.



Source: Spiraxsarco, Control Actuators and Positioners

Figure 20. Valve and actuator configurations

DIRECT ACTING ACTUATOR (SPRING-TO-RETRACT)

The direct acting actuator is designed with the spring below the diaphragm, and air supplied to the space above the diaphragm. The result, with increasing air pressure, is spindle movement in the opposite direction to the reverse acting actuator.

The effect of this movement on the valve opening depends on the design and type of valve used, and is illustrated in figure 20. The alternative, which is shown in figure 21, is a direct acting pneumatic actuator coupled to a control valve with a reverse acting plug.

The choice between direct acting and reverse acting pneumatic controls depends on what position the valve should revert to in the event of failure of the compressed air supply. Should the valve close or be wide-open? This choice depends upon the nature of the application and safety requirements. It makes sense for steam valves to close on air failure, and cooling valves to open on air failure. The combination of actuator and valve type must be considered.

Orifice Plate

The following is taken from Wikipedia, *Orifice Plate*.

An orifice plate is a device used for measuring the volumetric flow rate. It uses the same principle as a Venturi nozzle, namely Bernoulli's principle, which states that there is a relationship between the pressure of the fluid and the velocity of the fluid. When the velocity increases, the pressure decreases and vice versa.

Orifice plates are most commonly used for continuous measurement of fluid flow in pipes. They are also used in some small river systems to measure flow rates at locations where the river passes through a culvert or drain. Only a small number of rivers are appropriate for the use of the technology since the plate must remain completely immersed; i.e., the approach pipe must be full, and the river must be substantially free of debris.

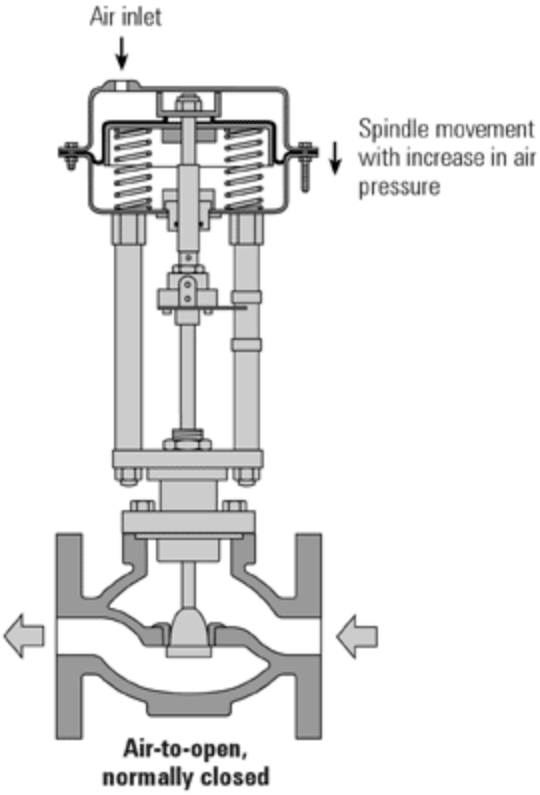


Figure 21. Direct acting actuator and reverse acting control valve

A restrictive flow orifice, a type of orifice plate, is a safety device to control maximum flow from a compressed gas cylinder.

In the natural environment, large orifice plates are used to control onward flow in flood relief dams. In these structures, a low dam is placed across a river. In normal operation, the water flows through the orifice plate unimpeded as the orifice is substantially larger than the normal flow cross section. However, during floods, the flow rate rises and floods out the orifice plate, which can only pass a flow determined by the physical dimensions of the orifice. Flow is then held back behind the low dam in a temporary reservoir, which is slowly discharged through the orifice when the flood subsides.

Video 11. Orifice plate

http://wn.com/orifice_plate_theory#/videos

Centrifugal Pump

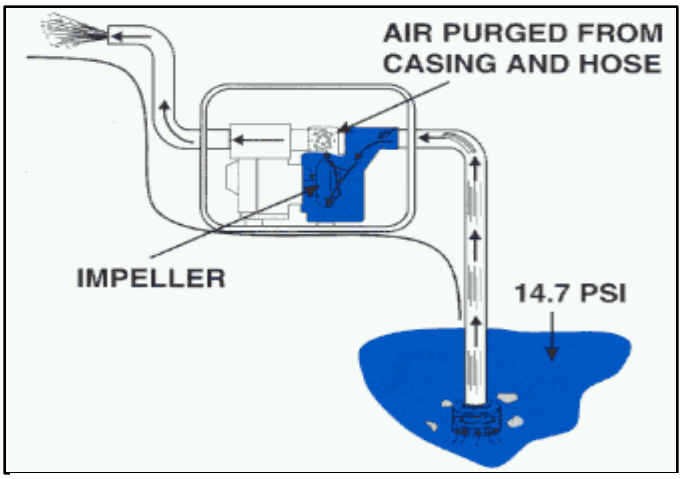
The following is taken from Pumps-in-Stock, *Centrifugal Pump Design*.

The overwhelming majority of contractor pumps use centrifugal force to move water. Centrifugal force is defined as the action that causes something, in this case water, to move away from its center of rotation.

All centrifugal pumps use an impeller and volute to create the partial vacuum and discharge pressure necessary to move water through the casing. The impeller and volute form the heart of the pump and help determine its flow, pressure, and solid handling capability.

An impeller is a rotating disk with a set of vanes coupled to the engine/motor shaft that produces centrifugal force within the pump casing. A volute is the stationary housing (in which the impeller rotates) that collects, discharges, and recirculates water entering the pump. A diffuser is used on high pressure pumps and is similar to a volute but more compact in design. Many types of material can be used in a centrifugal pump's manufacture, but cast iron is most commonly used for construction applications.

For a centrifugal, or self priming, pump to attain its initial prime, the casing must first be manually primed or filled with water. Afterwards, unless it is run dry or drained, a sufficient amount of water should remain in the pump to ensure quick priming the next time it is needed.



Source: Pumps-in-Stock Centrifugal Pump Design

Figure 22. Centrifugal pump

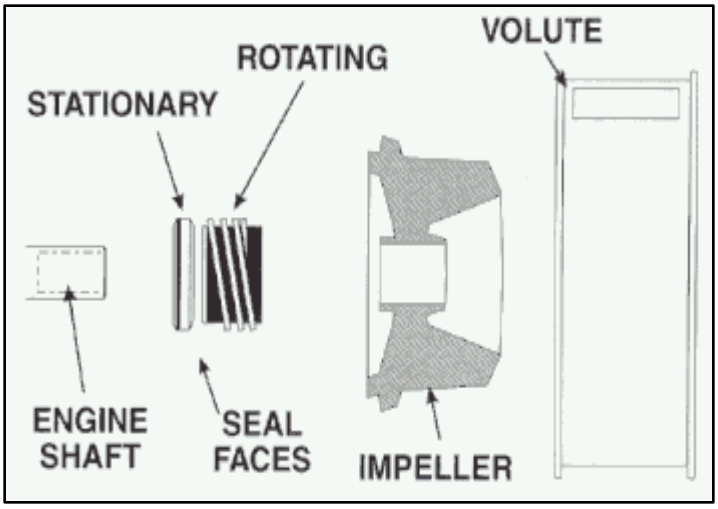
As the impeller churns the water (see figure 22), it purges air from the casing, creating an area of low pressure, or partial vacuum, at the eye (center) of the impeller. The weight of the atmosphere on the external body of water pushes water rapidly through the hose and pump casing toward the eye of the impeller.

Centrifugal force created by the rotating impeller pushes water away from the eye, where pressure is lowest, to the vane tips, where the pressure is highest. The velocity of the rotating vanes pressurizes the water forced through the volute and discharges it from the pump.

Water passing through the pump brings with it solids and other abrasive material that will gradually wear down the impeller or volute. This wear can increase the distance between the impeller and the volute, resulting in decreased flows, decreased heads, and longer priming times. Periodic inspection and maintenance is necessary to keep pumps running like new.

Another key component of the pump is its mechanical seal. This spring loaded component consists of two faces, one stationary and another rotating, and is located on the engine shaft between the impeller and the rear casing (see figure 23). It is designed to prevent water from seeping into and damaging the engine. Pumps designed for work in harsh environments require a seal that is more abrasion resistant than pumps designed for regular household use.

Typically, seals are cooled by water as it passes through the pump. If the pump is dry, or has insufficient water for priming, it could damage the mechanical seal. Oil-lubricated, and occasionally grease-lubricated, seals are available on some pumps that provide positive lubrication in the event that the pump is run without water. The seal is a common wear part that should be periodically inspected. Regardless of whether the application calls for a standard, high pressure, or trash, every centrifugal pump lifts and discharges water in the same way. The following section will point out design differences between these pumps.



Source: Pumps-in-Stock

Figure 23. Mechanical seal

Positive Displacement Pump

The following is taken from the Rensselaer Polytechnic Institute, *Positive-Displacement Pumps.*

Positive-displacement pumps operate by forcing a fixed volume of fluid from the inlet pressure section of the pump into the discharge zone of the pump. There are three types of positive-displacement pumps: reciprocating, metering, and rotary pumps. These pumps generally tend to be larger than equal-capacity dynamic pumps. Positive-displacement pumps are frequently used in hydraulic systems at pressures ranging up to 5000 pounds per square inch (psi). A principal advantage of hydraulic power is the high power density (power per unit weight) that can be achieved. They also provide a fixed displacement per revolution and, within mechanical limitations, infinite pressure to move fluids.

RECIPROCATING PUMPS

In a reciprocating pump, a volume of liquid is drawn into the cylinder through the suction valve on the intake stroke, and is discharged under positive pressure through the outlet valves on the discharge stroke. The discharge from a reciprocating pump is pulsating and changes only when the speed of the pump is changed. This is because the intake is always a constant volume. Often an air chamber is connected on the discharge side of the pump to provide a more even flow by equalizing the pressure surges. Reciprocating pumps are often used for sludge and slurry.

One construction style of a reciprocating pump is the direct-acting steam pump. This consists of a steam cylinder end in line with a liquid cylinder end, with a straight rod connection between the steam piston and the pump piston or plunger. The pistons are double acting, which means that each side pumps on every stroke.

Another construction style is the power pump, which converts rotary motion to low speed reciprocating motion using a speed reducing gear. The power pump can be either single or double-acting. A single-acting design discharges liquid only on one side of the piston or plunger; only one suction stroke and one discharge stroke per revolution of the crankshaft can occur. The double-acting design applies suction and discharges on both sides of the piston, resulting in two suctions and discharges per crankshaft revolution. Power pumps are generally very efficient and can develop high pressures. These pumps do, however, tend to be expensive.

METERING PUMPS

Metering pumps, also called proportioning or controlled-volume pumps, provide precision control of very low flow rates. They are usually used to control additives to the main flow stream, and flow rates are generally less than 1/2 gallon per minute. Metering pumps are available in either a diaphragm or packed plunger style, and are designed for clean service. Dirty liquid can easily clog the valves and nozzle connections.

ROTARY PUMPS

Rotary pumps trap fluid in a closed casing and discharge a smooth flow. They can handle almost any liquid that does not contain hard and abrasive solids, including viscous liquids. They are also simple in design and efficient in handling flow conditions that are usually considered too low for economic application of centrifuges. Types of rotary pumps include cam-and-piston, internal-gear, lobular, screw, and vane pumps. Gear pumps are found in oil-fired home heating systems. Rotary pumps find wide use for viscous liquids. When pumping highly viscous fluids, rotary pumps must be operated at reduced speeds, because at higher speeds the liquid cannot flow into the casing fast enough to fill it. Unlike a centrifugal pump, the rotary pump will deliver a capacity that is not greatly affected by pressure variations on either the suction or discharge ends. In services where large changes in pressure are anticipated, the rotary design should be considered.

Video 12. Positive displacement pump operation
http://vimeo.com/10377075

Compressor

The following is taken from SA Instrumentation and Control, *Compressor Optimization and Surge Elimination*.

Exceptional demands are placed on control systems applied to centrifugal compressors. Not only must these systems regulate the delivery of process gas or air at specified pressures or flow rates, but they must also effectively prevent surge and its attendant problems. The surge phenomenon adversely affects the quality of control, machine life, and plant operating costs.

SURGE

Surge is a phenomenon associated with axial and centrifugal compressors. It occurs when, at any given speed, guide vane angle, or inlet valve position, flow in the system decreases sufficiently to cause momentary flow reversal in the compressor. Flow reversal occurs at an instant when the pressure developed by the compressor no longer exceeds the pressure in the downstream system. This is an unstable condition, which triggers self-oscillation between

flow and pressure, resulting in erratic compressor capacity. Surge appears as rapid pulsations in the flow and discharge pressure, which invariably causes damage to the compressor and associated piping, and upsets to the process.

Broadly stated, an improperly protected compressor plant can incur increased running costs, expensive equipment repairs, more frequent compressor overhauls, and expensive plant downtimes, as well as representing a danger to plant personnel.

Anti-surge and capacity controls are the main elements of compressor control. Anti-surge prevents surge by maintaining a safe minimum flow through the compressor. This is accomplished by manipulating a blow-off or recycle valve. The capacity control is generally based on a pressure or flow by manipulating a suction or discharge valve, guide vanes, or rotational speed.

During steady-state operation, the capacity control of the compressor can conflict with the anti-surge control, since each attempts to vary the flow through the compressor in opposite directions. Therefore, the control system must also decouple the capacity control with the anti-surge control to avoid possible instability.

A sound anti-surge system will prevent surge with a surge control line. To maximize compressor efficiency, the control margin between the surge and the surge control lines must be minimized. To accommodate the minimized control margin, the surge and the surge control lines must be calculated dynamically from the operating point of the compressor. The safety line and adaptive gain further enhance this control algorithm. An optional surge detector serves as a back-up for the anti-surge control system.

CAPACITY CONTROL

To meet process requirements, the capacity of the compressor must be controlled. This is accomplished by manipulating a discharge valve, suction valve, inlet guide vanes, or rotational speed. The choice of which process variable will be controlled and the manipulated variable are often dictated by the process dynamics.

DECOUPLING OF ANTI-SURGE AND CAPACITY CONTROL

Both of the above systems control the mass balance around the compressor. Therefore strong interaction between these two functions can be expected. Of the two control systems, anti-surge must take precedence over capacity control, because of the possible damages caused by surge. Repairs on possible damages and downtimes caused by surge can be expensive.

To minimize the effect of the interaction between the two systems, they must be effectively decoupled. Decoupling will reduce the response of one system with respect to the other system, which will minimize unwanted side effects caused by the interaction.

AUTOMATIC START-UP AND SHUTDOWN

Experience had shown that most surges happen during start-up or shut down. One of the most common factors is inconsistency of the operator. The possibility of surges during an automated start-up or shutdown is dramatically reduced, because the compressor is controlled exactly the same way during every start-up or shut down.

PARALLEL OPERATION

Compressors will interact when they are operated in parallel to a common discharge header. This interaction must be optimized to minimize the interaction, particularly when the flow is reduced towards the surge line.

SERIES OPERATION

Compressors are often operated in series because of the required pressure ratio. The compressors can be driven by the same shaft or separately. Each one of the compressors should be seen as separate and be controlled accordingly. The compressors and the anti-surge control will interact, which could lead to instability. This interaction must also be optimized to minimize the interaction, particularly when the flow is reduced towards the surge line.

Instrument Air System

The following is taken from Piping-Designer, *Instrument Air*.

Instrument air is used in a facility to operate valves and certain types of pumps. Pneumatic actuators rely on instrument air for operation. Some types of modulating valves require instrument air for throttling. Instrument air is provided by a compressor and requires minimal treatment to ensure that the air is free of oil, water, or particulate matter. This is usually accomplished with some type of filter regulator on the compressor outlet, and a dryer.

CONSUMPTION

Different pieces of equipment consume different amounts of air. For example, a shutdown valve will consume air when it is being actuated. A throttling valve will have a constant bleed rate with additional consumption when the valve is modulating. A diaphragm pump consumes air when it is being actuated.

SIZING

Sizing an instrument air system is different than sizing a piping system where there are constant flow rates. Instrument air systems should be designed to ensure the safe and consistent operation of the end devices.

When sizing an instrument air system, there are several different approaches. One approach would be to tabulate all the instruments and devices that consume air. However, because so many systems in a plant are dependent on instrument air, it is far better to have too much air available than too little.

Another approach would be to size the system for all instruments consuming air at the same time. As a rule of thumb, a great starting point is to assume that each end device requires 2 standard cubic feet per minute. Add all the end devices up, account for future expansion, and add 10 percent for leaks and contingency.

Dampers

The following is taken from Wikipedia, *Dampers*.

A damper is a valve or plate that stops or regulates the flow of air inside a duct, chimney, variable air volume box, air handler, or other air handling equipment. A damper may be used to cut off central air conditioning to an unused room, or to regulate it for room-by-room

temperature and climate control. Its operation can be manual or automatic. Manual dampers are turned by a handle on the outside of a duct. Automatic dampers are used to regulate airflow constantly and are operated by electric or pneumatic motors, which are in turn controlled by a thermostat or building automation system. Automatic or motorized dampers may also be controlled by a solenoid, and the degree of air-flow calibrated (perhaps according to signals from the thermostat going to the actuator of the damper) in order to modulate the flow of air-conditioned air in order to effect climate control.

ZONE DAMPER

A zone damper is a specific type of damper used to control the flow of air in a heating, ventilation, air conditioning (HVAC) system. In order to improve efficiency and occupant comfort, HVAC systems are commonly divided up into multiple zones. For example, in a house, the main floor may be served by one heating zone while the upstairs bedrooms are served by another. In this way, the heat can be directed principally to the main floor during the day and principally to the bedrooms at night, allowing the unoccupied areas to cool down.

Zone dampers as used in home HVAC systems are usually electrically powered. In large commercial installations, vacuum or compressed air may be used instead. In either case, the motor is usually connected to the damper via a mechanical coupling.

For electrical zone dampers, there are two principal designs. In one design, the motor is often a small, shaded-pole synchronous motor combined with a rotary switch that can disconnect the motor at either of the two stopping points. In this way, applying power to the open damper terminal causes the motor to run until the damper is open, while applying power at the close damper terminal causes the motor to run until the damper is closed. The motor is commonly powered from the same 24 volt AC power source that is used for the rest of the control system. This allows the zone dampers to be directly controlled by low-voltage thermostats and wired with low-voltage wiring. Because simultaneous closure of all dampers might harm the furnace or air handler, this style of damper is often designed to only obstruct a portion of the air duct, for example, 75 percent.

Another style of electrically powered damper uses a spring-return mechanism and a shaded-pole synchronous motor. In this case, the damper is normally opened by the force of the spring but can be closed by the force of the motor. Removal of electrical power re-opens the damper. This style of damper is advantageous because it is fail safe; if the control to the damper fails, the damper opens and allows air to flow. However, in most applications, fail safe indicates the damper will close upon loss of power, thus preventing the spread of smoke and fire to other areas. These dampers may also allow adjustment of the closed position so that they only obstruct, for example, 75 percent of the air flow when closed.

For vacuum- or pneumatically-operated zone dampers, the thermostat usually switches the pressure or vacuum on or off, causing a spring-loaded rubber diaphragm to move and actuate the damper. As with the second style of electrical zone dampers, these dampers automatically return to the default position without the application of any power, and the default position is usually open, allowing air to flow. Like the second style of electrical zone damper, these dampers may allow adjustment of the closed position.

Highly sophisticated systems may use some form of building automation to control the zone dampers. The dampers may also support positions other than fully open or fully closed, are usually capable of reporting their current position, and, often, the temperature and volume of the air flowing past the smart damper.

Regardless of the style of damper employed, the systems are often designed so that when no thermostat is calling for air, all dampers in the system are opened. This allows air to continue to flow while the heat exchanger in a furnace cools down after a heating period completes.

HEPA Filters

The following is taken from Wikipedia, *HEPA*.

High-efficiency particulate air (HEPA) is a type of air filter. Filters meeting the HEPA standard have many applications, including use in medical facilities, automobiles, aircraft, and homes. The filter must satisfy certain standards of efficiency such as those set by DOE. To qualify as HEPA by U.S. government standards, an air filter must remove 99.97 percent of all particles greater than 0.3 micrometer (μm) from the air that passes through. A filter that is qualified as HEPA is also subject to interior classifications.

HEPA filters are composed of a mat of randomly arranged fibers. The fibers are typically composed of fiberglass and possess diameters between 0.5 and 2.0 micrometers. Key factors affecting function are fiber diameter, filter thickness, and face velocity. The air space between HEPA filter fibers is much greater than 0.3 μm. The common assumption that a HEPA filter acts like a sieve where particles smaller than the largest opening can pass through is incorrect. Unlike membrane filters at this pore size, where particles as wide as the largest opening or distance between fibers cannot pass in between them at all, HEPA filters are designed to target much smaller pollutants and particles. These particles are trapped through a combination of the following three mechanisms:

1. Interception, where particles following a line of flow in the air stream come within one radius of a fiber and adhere to it
2. Impaction, where larger particles are unable to avoid fibers by following the curving contours of the air stream and are forced to embed in one of them directly; this effect increases with diminishing fiber separation and higher air flow velocity
3. Diffusion, an enhancing mechanism that is a result of the collision with gas molecules by the smallest particles, especially those below 0.1 μm in diameter, which are thereby impeded and delayed in their path through the filter; this behavior is similar to Brownian motion and raises the probability that a particle will be stopped by either of the two mechanisms above; it becomes dominant at lower air flow velocities

Diffusion predominates below the 0.1 μm diameter particle size. Impaction and interception predominate above 0.4 μm. In between, near the most penetrating particle size, 0.3 μm, diffusion and interception are comparatively inefficient. Because this is the weakest point in the filter's performance, the HEPA specifications use the retention of these particles to classify the filter.

Lastly, it is important to note that HEPA filters are designed to effectively arrest very fine particles, but they do not filter out gasses and odor molecules. Circumstances requiring

filtration of volatile organic compounds, chemical vapors, cigarette, pet, and/or flatulence odors call for the use of an activated carbon (charcoal) filter instead of, or in addition to, a HEPA filter.

c. Explain the thermodynamic concepts and operational considerations for fluid systems (e.g., HVAC system, liquid process systems, etc) related to I&C systems design.

The following is taken from eHow, *How Does A Fluid System Work?*

A fluid is a substance that flows freely and takes the shape of its container. Fluids include both liquids and gases. A system that uses gas or liquid is a fluid power system. Fluid power is used to harness energy rather than actually generating it.

In 1650, Blaise Pascal, a French scientist, discovered the principles of the fluid system. The primary force that drives a fluid system is pressure. Changes in the pressure of the fluid cause it to move, which drives the system. The fluid must be enclosed and pressure applied to force the fluid to move in the desired direction. The two types of fluid systems are hydraulic and pneumatic. There are open and closed systems within each of these types.

Hydraulics

A hydraulic system harnesses the power of a pressurized liquid. Some liquids that can be used are oil, gasoline, or water. Each hydraulic system must have a reservoir for the liquid, a pump, valves to control the pressure and flow of the fluid, and a motor or hydraulic cylinder to move the required load. Hydraulic systems are considered the stronger of the two types of fluid systems.

Pneumatics

A pneumatic system gathers power from pressurized gas or air. When compressed air expands, the result is kinetic energy. When a valve in the tank is opened, the pressure inside the tank will expand to match the atmospheric pressure outside the tank. The air pressure must be controlled at each point in the system for the pneumatic system to work properly. Hydraulic systems tend to use much higher pressures than do pneumatic systems. Pneumatic systems are considered to be faster than hydraulic systems. In a pneumatic system, the amount of force is equal to the pressure times the area. The pressure in a pneumatic system is given in pounds per square inch. The area may be in square inches or meters. The force is then reported in pounds.

Closed Fluid Systems

A closed fluid system is one that retains and reuses the fluid involved in the function of the system. Some examples of closed systems include the human body, a hydraulic motor, a garden water feature, and a car's brake fluid system.

Open Fluid Systems

An open fluid system is one in which the fluid passes through the system only once. Examples of open systems include a garden hose, a fuel pump, and a municipal water system.

3. I&C personnel must demonstrate a familiarity level knowledge of basic civil/structural engineering fundamentals.

a. Explain seismic design constraints imposed on I&C systems.

The following is taken from the Nuclear Regulatory Guide, 1.12.

Solid-state digital instrumentation that will enable the processing of data at the plant site within 4 hours of the seismic event should be used.

A triaxial time-history accelerograph should be provided at the following locations:

- Free-field
- Containment foundation
- Two elevations on a structure inside the containment
- An independent seismic category I structure foundation where the response is different from that of the containment structure
- An elevation on the independent seismic category I structure selected in 4 above.
- If seismic isolators are used, instrumentation should be placed on the rigid and isolated portions of the same or an adjacent structure, as appropriate, at approximately the same elevations.

The specific locations for instrumentation should be determined by the nuclear plant designer to obtain the most pertinent information consistent with maintaining occupational radiation exposures as low as reasonably achievable (ALARA) for the location, installation, and maintenance of seismic instrumentation. In general

- the free-field sensors should be located and installed so that they record the motion of the ground surface and so that the effects associated with surface features, buildings, and components on the recorded ground motion will be insignificant;
- the in-structure instrumentation should be placed at locations that have been modeled as mass points in the building dynamic analysis so that the measured motion can be directly compared with the design spectra. The instrumentation should not be located on a secondary structural frame member that is not modeled as a mass point in the building dynamic model;
- a design review of the location, installation, and maintenance of proposed instrumentation for maintaining exposures ALARA should be performed by the facility in the planning stage in accordance with Nuclear Regulatory Guide 8.8, *Information Relevant to Ensuring that Occupational Radiation Exposures at Nuclear Power Stations Will Be As Low As Reasonably Achievable*;
- instrumentation should be placed in a location with as low a dose rate as is practical, consistent with other requirements; and
- instruments should be selected to require minimal maintenance and in-service inspection, as well as minimal time and numbers of personnel to conduct installation and maintenance.

Seismic Instrumentation Operability

The seismic instrumentation should operate during all modes of plant operation, including periods of plant shutdown. The maintenance and repair procedures should provide for

keeping the maximum number of instruments in service during plant operation and shutdown.

Instrumentation Characteristics

The design should include provisions for in-service testing. The instruments should be capable of periodic channel checks during normal plant operation.

The instruments should have the capability for in-place functional testing.

Instrumentation that has sensors located in inaccessible areas should contain provisions for data recording in an accessible location, and the instrumentation should provide an external remote alarm to indicate actuation.

The instrumentation should record, at a minimum, 3 seconds of low-amplitude motion prior to seismic trigger actuation, continue to record the motion during the period in which the earthquake motion exceeds the seismic trigger threshold, and continue to record low-amplitude motion for a minimum of 5 seconds beyond the last exceedance of the seismic trigger threshold.

The instrumentation should be capable of recording 25 minutes of sensed motion.

The battery should be of sufficient capacity to power the instrumentation to sense and record 25 minutes of motion over a period of not less than the channel check test interval. This can be accomplished by providing enough battery capacity for a minimum of 25 minutes of system operation at any time over a 24-hour period, without recharging, in combination with a battery charger whose line power is connected to a UPS or a line source with an alarm that is checked at least every 24 hours. Other combinations of larger battery capacity and alarm intervals may be used.

ACCELERATION SENSORS

- The dynamic range should be 1000:1 zero to peak, or greater; for example, 0.001g to 1.0g.
- The frequency range should be 0.20 hertz (Hz) to 50 Hz or an equivalent demonstrated to be adequate by computational techniques applied to the resultant accelerogram.

RECORDER

- The sample rate should be at least 200 samples per second in each of the three directions.
- The bandwidth should be at least from 0.20 Hz to 50 Hz.
- The dynamic range should be 1000:1 or greater, and the instrumentation should be able to record at least 1.0g zero to peak.

INSTRUMENTATION INSTALLATION

- The instrumentation should be designed and installed so that the mounting is rigid.
- The instrumentation should be oriented so that the horizontal components are parallel to the orthogonal horizontal axes assumed in the seismic analysis.
- Protection against accidental impacts should be provided.

b. Explain the effect of vibration on I&C systems and methods to mitigate that effect.

The following is taken from California Department of Transportation, *Transportation- and Construction-Induced Vibration Guidance Manual*.

The operation of equipment for research, microelectronics manufacturing, medical diagnostics, and similar activities can be adversely affected by vibration. For the purposes of designing facilities to house this equipment, vibration criteria that are generic (i.e., applicable to classes of equipment or activity) rather than specific have been developed. These criteria are expressed in terms of one-third octave band velocity spectra and are summarized in table 2.

Table 2. Vibration Criteria for Sensitive Equipment

Criterion Curve	Max Level[1] (microinches/sec) (dB)	Detail Size[2] (microns)	Description of Use
Workshop	32,000 (90)	NA	Distinctly feelable vibration. Appropriate to workshops and nonsensitive areas.
Office	16,000 (84)	NA	Feelable vibration. Appropriate to offices and nonsensitive areas.
Residential Day	8,000 (78)	75	Barely feelable vibration. Probably adequate for computer equipment, probe test equipment, and low-power microscopes.
Op. Theatre	4,000 (72)	25	Vibration not feelable. Suitable in most instances for microscopes to 100% and for other equipment of low sensitivity
VC-A	2,000 (66)	8	Adequate in most instances for optical microscopes to 400X, microbalances, optical balances, proximity and projection aligners.
VC-B	1,000 (60)	3	An appropriate standard for optical microscopes to 1,000S, inspection and lithography equipment to 3μ line widths.
VC-C	500 (54)	1	A good standard for most lithography and inspection equipment.
VC-D	250 (48)	0.3	Suitable in most instances for the most demanding equipment, including electron microscopes, and systems operating to the limits of their capability.
VC-E	125 (42)	0.1	Assumed to be adequate for the most demanding of sensitive systems that require extraordinary dynamic stability.

[1] As measured in one-third octave bands of frequency over the frequency range 8 to 100 Hz. The dB scale is referred to 1 micro-inch/second.

[2] The detail size refers to the line width in the case of microelectronics fabrication. The values given take into account the observation that the vibration requirements of many items of the equipment depend on the detail size of the process.

Source: California Department of Transportation, Transportation and Construction-Induced Vibration Guidance Manual

c. Explain the requirements of seismic qualification of I&C structures, systems and components (e.g., IEEE Std 344 requirements).

The following is taken from ANSI/IEEE-Std-344.

The seismic qualification of equipment should demonstrate the equipment's ability to perform its safety function during and after the time it is subject to the forces resulting from one safe shutdown earthquake (SSE). In addition, the equipment must withstand the effects of a number of operating basis earthquakes (OBEs) prior to the application of an SSE. The methods are grouped into four general categories that

1. predict the equipment's performance by analysis
2. test the equipment under simulated seismic conditions
3. qualify the equipment by a combination of test and analysis
4. qualify the equipment through the use of experience data

Each of these methods, or other justifiable methods, may be adequate to verify the ability of the equipment to meet the seismic qualification requirements. The choice should be based on the practicality of the method for the type, size, shape, and complexity of the equipment configuration; whether the safety function can be assessed in terms of operability or structural integrity alone; and the reliability of the conclusions.

Equipment being qualified must demonstrate that it can perform its safety function during and after an earthquake. The required safety function depends not only on the equipment itself but also on the system and plant in which it is to function. The safety function during the earthquake may be the same, but is often different from the safety function required after the earthquake. For example, an electrical device may be required to not have spurious operations during the earthquake or to perform an active function during and after the earthquake, or it may be required to survive during the earthquake and perform an active function after the earthquake, or any combinations of these. Another device may only be required to maintain structural integrity during and after the earthquake.

When the safety function of equipment requires a demonstration of operability during the earthquake, it shall be demonstrated during the strong motion portion of the qualification simulation.

Seismic testing, when part of an overall qualification program, should be performed in its proper sequence as indicated in ANSI/IEEE Std 323-1983, and care should be taken to identify and account for significant aging mechanisms as discussed therein. Within these guidelines, it must be demonstrated that the equipment is capable of performing its safety function throughout its qualified life, including its function operability during and after an SSE and the end of that qualified life.

Video 13. Equipment qualification process

http://www.bing.com/videos/search?q=seismic+qualification+certification&view=detail&mid=A0184947809E460ED940A0184947809E460ED940&first=0

Source: Power Engineering, Seismic Instrumentation and Nuclear Power Plants
Figure 24. Seismic instrumentation systems

d. Explain the function and operation of seismic instrumentation systems.

The following is taken from Power Engineering, *Seismic Instrumentation and Nuclear Power Plants*.

To assess most effectively whether an earthquake has exceeded the OBE for a nuclear power plant, it is important for a modern, online, digital seismic instrumentation system to be in place. Electric Power Research Institute guidance is presented in the context of three fundamental options for a seismic instrumentation system:

- A minimum system
- A basic automatic system
- A complete system

The basic characteristics of and differences among these systems are depicted in figure 24. Each category of system is described further in the sections that follow.

The Minimum System

The minimum system would include one or two accelerographs, depending on how the OBE was defined for the plant. If the OBE had been defined in the free-field, one instrument in the free-field would be sufficient. On the other hand, if the OBE had been defined at a building location (for example, at the top of the basemat of the reactor containment), an instrument at that location and one in the free-field would be required. In addition to being placed in the

locations at which the OBE is defined, these instruments would need to meet minimum qualifications.

In general, the following are minimum characteristics for these instruments:

- The accelerographs need to have battery backup, with pre-event memory sufficient to record the entire earthquake motion and a storage device that could accommodate rapid data retrieval.
- The instruments must be digital, with a sampling rate of at least 200 samples per second.
- The instruments need to cover a frequency bandwidth of 0.2–50 Hz.
- A stand-alone desktop or laptop computer equipped with software to perform the necessary calculations on the collected data is required. The software would need to generate the cumulative absolute velocity and the response spectra. The nature of the data retrieval and transfer to the computer would need to be such that the calculations could be completed within 4 hours after the earthquake.

The Basic Automatic System

Improved functionality can be achieved by automating certain steps that must be performed manually using the minimum seismic instrumentation system. The basic automatic system would add a dedicated online computer to automatically retrieve data from the accelerographs and perform the calculations related to possible exceedance of the OBE. Such a capability would expedite the process of assembling the information needed to make a decision with regard to whether a plant shutdown is required.

To upgrade from the minimum system to the basic automatic system, a dedicated cable would be needed from each instrument to the recording location to capture the acceleration time history. The analysis results should be displayed to the control room operators in a form that is easy to understand. A UPS for the computer that records and analyzes the data would also be needed to ensure that the results could be available within the 4-hour timeframe.

The Complete System

The complete system is the most advanced of the three. Such a system would incorporate an online computer for data acquisition and analysis along with more extensive instrumentation. The system could be configured so that it complies with Regulatory Guide 1.12. Although the minimum and basic automatic systems could facilitate short-term response, the complete system would facilitate the collection of more extensive response data from within plant structures, enabling more comprehensive long-term evaluations of the earthquake's damage potential.

A complete system would incorporate additional accelerograph locations, rather than only accounting for the free-field and the location at which the OBE is defined. Data collected from other response locations within the containment and auxiliary buildings would provide more definitive information regarding the impact of the earthquake. The system would be fully battery-backed. This system is strongly recommended as the best option for ensuring timely and effective response to earthquakes and to more quickly and confidently determine whether plant shutdown is necessary.

4. I &C personnel must demonstrate a familiarity level knowledge of basic chemical engineering fundamentals.

a. Explain the additional design requirements that must be considered when applying I&C systems for use in chemical processes.

The following is taken from the National Center for Biotechnology Information, *Vision 2020: Computational Needs of the Chemical Industry*.

A molecular-level understanding of chemical manufacturing processes would greatly enhance the ability of chemical engineers to optimize process design and operations as well as ensure adequate protection of the environment and safe operating conditions. Currently there is considerable uncertainty in thermodynamic and reaction models, so plants are normally overdesigned to allow for this uncertainty. Also plants are operated conservatively due to an inadequate understanding of dynamic process behavior and the dire consequences if an unsafe condition arises. Chemical reactors are at the heart of this issue, with uncertainties in kinetic mechanisms and rate constants and the effects of reactor geometry (such as catalyst beds) on heat and mass transfer. Clearly the availability of better microscopic mathematical models for macroscopic plant simulation will help the chemical industry operate more profitably and more reliably in the future.

Besides providing fundamental data for process simulations, computational chemistry plays an important role in the molecular design process beginning at the basic research level. By predicting accurate thermochemistry, one can quickly determine from the feasibility of reaction pathways whether a reaction is allowed or not. Computational chemistry can also reliably predict a wide range of spectroscopic properties to aid in the identification of chemical species: especially important reaction intermediates. Electronic structure calculations can also provide quantitative insights into bonding, orbital energies, and form, facilitating the design of new molecules with the appropriate reactivity.

The computational chemistry subgroup of Vision 2020 under the sponsorship of the Council for Chemical Research has outlined a set of computational grand challenges or technology bundles that will have a dramatic impact on the practice of chemistry throughout the chemical enterprise, especially the chemical industry. The computational grand challenges are given in table 3.

Table 3. Computational grand challenges for materials and process design in the chemical enterprise

A. Reliable prediction of biological activity from chemical structure
B. Reliable prediction of environmental fate from chemical structure
C. Design of efficient catalysts for chemical processes
D. Design of efficient processes in chemical plants from an understanding of microscopic molecular behavior
E. Design of a material with a given set of target properties

Source: National Center for Biotechnology Information, Vision 2020: Computational Needs of the Chemical Industry

Grand challenge A or bundle A in table 3 has received recent emphasis because this area includes drug design. However, biological activity due to a specific chemical is needed for other areas such as agricultural pesticide design and predictive toxicology. The potential for toxic impact of any chemical must be addressed before a chemical is manufactured, sold to the public, or released to the environment. Furthermore, the toxic behavior must be evaluated not only for human health issues but also for its potential ecological impact on plants and animals. Examining chemical toxicity is currently an extremely expensive process that can take years of detailed testing. Such evaluations usually occur late in development, and the inability to anticipate the evaluation of toxicological testing can place large R&D investments at risk. Also, the possibility exists that unanticipated toxicological problems with intermediates and by-products may create liabilities. The cost of toxicology testing is generally too high to complete testing early in the development process. Thus, reliable, cost-effective means for predicting toxicological behavior would be of great benefit to the industry.

Grand challenge B in table 3 is focused on the need to predict the fate of any compound that is released into the environment. For example, even if a compound is not toxic, a degradation product may show toxic behavior. Besides being toxic to various organisms, chemicals released into the environment can affect it in other ways. A difficulty in dealing with the environmental impact of a chemical is that the temporal and spatial scales cover many orders of magnitude from picoseconds to 100,000 years in time, and from angstroms to thousands of kilometers in distance. Furthermore, the chemistry can be extremely complex and the chemistry that occurs on different scales may be coupled. For example, chemical reactions that occur on a surface may be influenced not only by the local site but also by distant sites that affect the local electronic structure or the surrounding medium.

Grand challenges C and D in table 3 are tightly coupled but are separated here because different computational aspects may be needed to address these areas. Catalysis and catalytic processes are involved in manufacturing most petroleum and chemical products, and account for nearly 20 percent of the U.S. gross domestic product. Improved catalysts would increase efficiency, leading to reduced energy requirements, while increasing product selectivity and concomitantly decreasing wastes and emissions. Considerable effort has been devoted to the ab initio design of catalysts, but such work is difficult due to the types of atoms involved (often transition metals) and due to the fact that extended surfaces are often involved. Besides the complexity of the materials themselves, an additional requirement is the need for accurate results. Although computational results can often provide insight into how a catalyst works, the true design of a catalyst will require the ability to predict accurate thermodynamic and kinetic results. For example, a factor of two to four in catalyst efficiency can determine the economic feasibility of a process. Such accuracies mean that thermodynamic quantities should be predicted to within 0.1 to 0.2 kilocalories/molecule kcal/mol and rate constants to within approximately 15 percent—certainly difficult, if not impossible, by today's standards. Even for the nominally simple area of acid/base catalysis, many additional features may have to be included in the model; for example, the effects of solvation.

Grand challenge E in table 3 is extremely difficult to treat at the present time. Given a structure, we can often predict at some level what the properties of the material are likely to be. The accuracy of the results and the methods used to treat them depend critically on the

complexity of the structure as well as the availability of information on similar structures. For example, various quantitative structure property relationship models are available for the prediction of polymer properties. However, the inverse engineering design problem, designing structures given a set of desired properties, is far more difficult. The market may demand or need a new material with a specific set of properties, yet given the properties it is extremely difficult to know which monomers to put together to make a polymer, and what molecular weight the polymer should have. Today the inverse design problem is attacked empirically by the synthetic chemist with his/her wealth of knowledge based on intuition and on experience. A significant amount of work is already under way to develop the "holy grail" of materials design, namely, effective and powerful reverse-engineering software to solve the problem of going backwards from a set of desired properties to realistic chemical structures and material morphologies that may have these properties. These efforts are usually based on artificial intelligence techniques and have, so far, had only limited success. Much work needs to be done before this approach reaches the point of being used routinely and with confidence by the chemical industry.

b. Explain special design requirements for the use of instrumentation in chemically harsh environments (e.g., corrosive, toxic, etc.).

The following is taken from the National Institute of Standards and Technology, *Microsystems for Harsh Environment Testing*.

The goal at NIST is to develop and demonstrate a micro-electromechanical systems-based methodology for evaluating time-dependent mechanical properties of materials that undergo exposure to extreme and harsh environments (e.g., temperature extremes, high radiation, corrosive chemistries, etc.). Such test methods hold promise for providing a high throughput route to thoroughly measuring the remaining lifetime of highly irradiated materials present in today's nuclear power plants, as well as the suitability of new alloys for next generation nuclear plants.

Classically, measurement of the mechanical properties and reliability of bulk-scale materials is performed with macroscopic specimens and methods. Specimen preparation limitations, miniaturized load-frame tooling problems, and inadequate understanding of the roles of specimen size and constraint on properties have hindered the use of micrometer-scale specimens and techniques. NIST is developing a new approach that combines specimen preparation techniques such as focused ion beam (FIB) milling with microtechnology-based test tools. This will enable evaluation of large populations of specimens, on-chip, and in parallel, to provide statistically significant results. Properties of small-scale structures are linked to those of bulk-scale structures through application of three-dimensional, image-based finite element modeling. Currently, FIB is used to obtain micrometer-scale specimens from structural materials irradiated in test reactors, accelerators, or working power reactors for insertion into prefabricated on-chip test structures. Ultimately, NIST will fabricate arrays of test structures with on-chip control, actuation, and sensing. This will provide long-term, in situ testing of time-dependent mechanical properties of materials to be used in next generation nuclear plants and fusion reactors.

5. I&C personnel must demonstrate a working level knowledge of basic I&C systems fundamentals and their applications in process systems operations.

a. Explain the construction, operation, characteristics, limitations, and application of commonly used sensing instruments in process systems, monitoring parameters such as

- **pressure**
- **temperature**
- **flow**
- **level**
- **vibration**

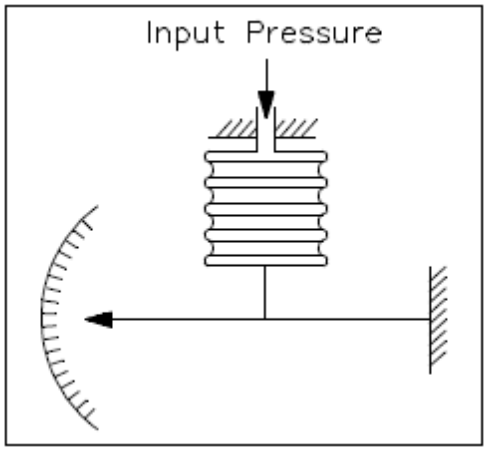
Pressure

The following is taken from DOE-HDBK-1013/1-92.

Many processes are controlled by measuring pressure. This section describes the detectors associated with measuring pressure.

BELLOWS-TYPE DETECTORS

The need for a pressure sensing element that was extremely sensitive to low pressures and that would provide power for activating recording and indicating mechanisms resulted in the development of the metallic bellows pressure sensing element. The metallic bellows is most accurate when measuring pressures from 0.5 to 75 pounds per square inch gauge (psig). However, when used in conjunction with a heavy range spring, some bellows can be used to measure pressures of over 1000 psig. Figure 25 shows a basic metallic bellows pressure sensing element.



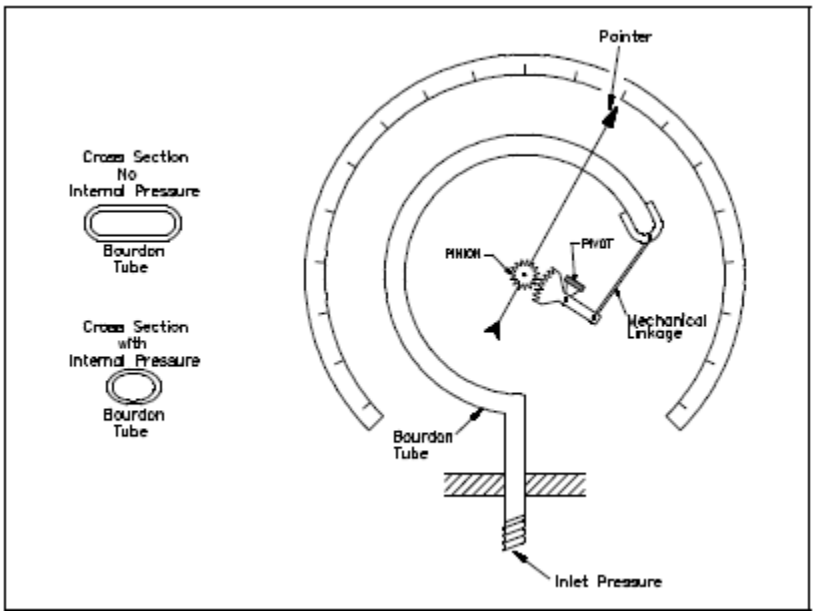
Source: DOE-HDBK-1013/1-92

Figure 25. Bellows type detector

The bellows is a one-piece, collapsible, seamless metallic unit that has deep folds formed from very thin-walled tubing. The diameter of the bellows ranges from 0.5 to 12 in. and may have as many as 24 folds. System pressure is applied to the internal volume of the bellows. As the inlet pressure to the instrument varies, the bellows will expand or contract. The moving end of the bellows is connected to a mechanical linkage assembly. As the bellows and linkage assembly moves, either an electrical signal is generated or a direct pressure indication is provided. The flexibility of a metallic bellows is similar in character to that of a helical, coiled compression spring. Up to the elastic limit of the bellows, the relation between increments of load and deflection is linear. However, this relationship exists only when the bellows is under compression. It is necessary to construct the bellows such that all of the travel occurs on the compression side of the point of equilibrium. Therefore, in practice, the bellows must always be opposed by a spring, and the deflection characteristics will be the resulting force of the spring and bellows.

BOURDON TUBE-TYPE DETECTORS

The bourdon tube pressure instrument is one of the oldest pressure sensing instruments in use today. The bourdon tube (refer to figure 26) consists of a thin-walled tube that is flattened diametrically on opposite sides to produce a cross-sectional area elliptical in shape, having two long flat sides and two short round sides. The tube is bent lengthwise into an arc of a circle of 270 to 300 degrees.



Source: DOE-HDBK-1013-92

Figure 26. Bourdon tube

Pressure applied to the inside of the tube causes distention of the flat sections and tends to restore its original round cross-section.

This change in cross-section causes the tube to straighten slightly. Since the tube is permanently fastened at one end, the tip of the tube traces a curve that is the result of the change in angular position with respect to the center. Within limits, the movement of the tip of the tube can then be used to position a pointer or to develop an equivalent electrical signal to indicate the value of the applied internal pressure.

Video 14. Bourdon tube

http://www.bing.com/videos/search?q=bourdon+tube&view=detail&mid=CD3B741A5EBE375BB2F8CD3B741A5EBE375BB2F8&first=0

PRESSURE DETECTOR FUNCTIONS

Although the pressures that are monitored vary slightly depending on the details of facility design, all pressure detectors are used to provide up to three basic functions: indication, alarm, and control. Since the fluid system may operate at saturation and subcooled conditions, accurate pressure indication must be available to maintain proper cooling. Some pressure detectors have audible and visual alarms that occur when specified preset limits are exceeded. Some pressure detector applications are used as inputs to protective features and control functions.

DETECTOR FAILURE

If a pressure instrument fails, spare detector elements may be used if installed. If spare detectors are not installed, the pressure may be read at an independent local mechanical gauge, if available, or a precision pressure gauge may be installed in the system at a convenient point.

If the detector is functional, it may be possible to obtain pressure readings by measuring voltage or current values across the detector leads and comparing this reading with calibration curves.

ENVIRONMENTAL CONCERNS

Pressure instruments are sensitive to variations in the atmospheric pressure surrounding the detector. This is especially apparent when the detector is located within an enclosed space. Variations in the pressure surrounding the detector will cause the pressure indicated by the detector to change. This will greatly reduce the accuracy of the pressure instrument and should be considered when installing and maintaining these instruments.

Ambient temperature variations will affect the accuracy and reliability of pressure detection instrumentation. Variations in ambient temperature can directly affect the resistance of components in the instrumentation circuitry, and, therefore, affect the calibration of electric/electronic equipment. The effects of temperature variations are reduced by the design of the circuitry and by maintaining the pressure detection instrumentation in the proper environment.

The presence of humidity will also affect most electrical equipment, especially electronic equipment. High humidity causes moisture to collect on the equipment. This moisture can cause short circuits, grounds, and corrosion, which, in turn, may damage components. The effects due to humidity are controlled by maintaining the equipment in the proper environment.

Temperature

The following is taken from DOE-HDBK-1013/1-92.

The hotness or coldness of a piece of plastic, wood, metal, or other material depends on the molecular activity of the material. Kinetic energy is a measure of the activity of the atoms that make up the molecules of any material. Therefore, temperature is a measure of the kinetic energy of the material in question.

Most temperature measuring devices use the energy of the material or system they are monitoring to raise (or lower) the kinetic energy of the device. A normal household thermometer is one example. The mercury, or other liquid, in the bulb of the thermometer expands as its kinetic energy is raised.

Because temperature is one of the most important parameters of a material, many instruments have been developed to measure it. One type of detector used is the resistance temperature detector (RTD). The RTD is used at many DOE nuclear facilities to measure temperatures of the process or materials being monitored.

RESISTANCE TEMPERATURE DETECTOR

The following is taken from Wikipedia, *Resistance Thermometer*.

RTDs are sensors used to measure temperature by correlating the resistance of the RTD element with temperature. Most RTD elements consist of a length of fine, coiled wire wrapped around a ceramic or glass core. The element is usually quite fragile, so it is often placed inside a sheathed probe to protect it. The RTD element is made from a pure material: platinum, nickel or copper. The material has a predictable change in resistance as the temperature changes; it is this predictable change that is used to determine temperature.

There are three main categories of RTD sensors; thin film, wire-wound, and coiled elements. While these types are the ones most widely used in industry, there are some places where other more exotic shapes are used, for example, carbon resistors are used at ultra low temperatures.

Carbon resistor elements are widely available and are quite inexpensive. They have very reproducible results at low temperatures. They are the most reliable element at extremely low temperatures. They do not generally suffer from significant hysteresis or strain gauge effects.

Strain free elements use a wire coil that is minimally supported within a sealed housing filled with an inert gas. These sensors are used up to 961.78°C and are used in the standard platinum resistance thermometer (SPRT)'s that define International Temperature Scale (ITS)-90. They consist of platinum wire loosely coiled over a support structure so the element is free to expand and contract with temperature, but they are very susceptible to shock and vibration as the loops of platinum can sway back and forth causing deformation.

Thin film elements have a sensing component that is formed by depositing a very thin layer of resistive material, normally platinum, on a ceramic substrate. This layer is usually just 10 to 100 angstroms thick. It is then coated with an epoxy or glass that helps protect the deposited film and also acts as a strain relief for the external lead-wires. Disadvantages of thin film elements are that they are not as stable as their wire wound or coiled counterparts; and they can only be used over a limited temperature range due to the different expansion rates of the substrate and resistive deposited giving a strain gauge effect that can be seen in the resistive temperature coefficient. These elements work with temperatures to 300°C.

Wire-wound elements can have greater accuracy, especially for wide temperature ranges. The coil diameter provides a compromise between mechanical stability and allowing expansion of the wire to minimize strain and consequential drift. The sensing wire is wrapped around an insulating mandrel or core. The winding core can be round or flat, but must be an electrical insulator. The coefficient of thermal expansion of the winding core material is matched to the sensing wire to minimize any mechanical strain. Strain on the element wire will result in a thermal measurement error. The sensing wire is connected to a larger wire, usually referred to as the element lead or wire. This wire is selected to be compatible with the sensing wire so that the combination does not generate an EMF that would distort the thermal measurement. These elements work with temperatures to 660 °C.

Coiled elements have largely replaced wire-wound elements in industry. This design has a wire coil which can expand freely over temperature, held in place by some mechanical support which lets the coil keep its shape. This strain free design allows the sensing wire to expand and contract free of influence from other materials; in this respect it is similar to the SPRT, the primary standard upon which ITS-90 is based, while providing the durability necessary for industrial use. The basis of the sensing element is a small coil of platinum sensing wire. This coil resembles a filament in an incandescent light bulb. The housing, or mandrel, is a hard fired ceramic oxide tube with equally spaced bores that run transverse to the axes. The coil is inserted in the bores of the mandrel and then packed with a very finely ground ceramic powder. This permits the sensing wire to move while still remaining in good thermal contact with the process. These elements work with temperatures to 850°C.

Function

Resistance thermometers are constructed in a number of forms and, in some cases, offer greater stability, accuracy, and repeatability than thermocouples. While thermocouples use the Seebeck effect to generate a voltage, resistance thermometers use electrical resistance and require a power source to operate. The resistance ideally varies linearly with temperature.

The platinum detecting wire needs to be kept free of contamination to remain stable. A platinum wire or film is supported on a former so that it gets minimal differential expansion or other strains from its former, yet is reasonably resistant to vibration. RTD assemblies made from iron or copper are also used in some applications. The sensor is usually made to have a resistance of 100 Ω at 0°C.

Measurement of resistance requires a small current to be passed through the device under test. This can generate resistive heating, causing significant loss of accuracy if manufacturers' limits are not respected, or the design does not properly consider the heat path. Mechanical strain on the resistance thermometer can also cause inaccuracy. Lead wire resistance can also be a factor; adopting three- and four-wire, instead of two-wire, connections can eliminate connection lead resistance effects from measurements; three-wire connection is sufficient for most purposes and almost universal industrial practice. Four-wire connections are used for the most precise applications.

Advantages and Limitations

The advantages of platinum resistance thermometers include

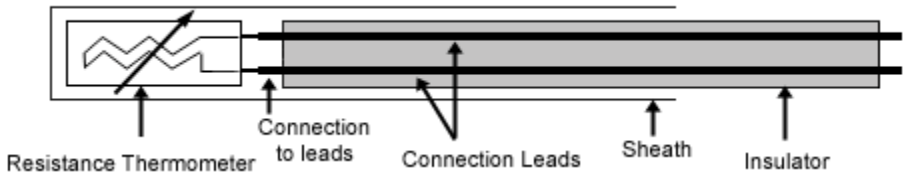
- high accuracy
- low drift
- wide operating range
- suitability for precision applications

Limitations—RTDs in industrial applications are rarely used above 660°C. At temperatures above 660°C it becomes increasingly difficult to prevent the platinum from becoming contaminated by impurities from the metal sheath of the thermometer. This is why laboratory standard thermometers replace the metal sheath with a glass construction. At very low temperatures (for example, below -270°C), because there are very few phonons, the resistance of an RTD is mainly determined by impurities and boundary scattering and thus

basically independent of temperature. As a result, the sensitivity of the RTD is essentially zero and therefore not useful.

Compared to thermistors, platinum RTDs are less sensitive to small temperature changes and have a slower response time. However, thermistors have a smaller temperature range and stability.

Construction



Source: Wikipedia, Resistance Thermometer

Figure 27. Typical resistance thermometer

Resistance thermometer elements nearly always require insulated leads to be attached. At temperatures below about 250 °C polyvinyl chloride, silicon rubber or polytetrafluoroethylene insulators are used. At higher temperatures, glass fiber or ceramic are used. The measuring points, and usually most of the leads, require a housing or protective sleeve, often made of a metal alloy, which is chemically inert to the process being monitored. Selecting and designing protection sheaths can require more care than selecting and designing the actual sensor, as the sheath must withstand chemical or physical attack and provide convenient attachment points.

THERMOCOUPLES

The following is taken from The Engineering ToolBox, *Thermocouples*.

One of the most common industrial thermometers is the thermocouple. It was discovered by Thomas Seebeck in 1822. He noted that a voltage difference appeared when a wire was heated at one end. Regardless of temperature, if both ends of the wire were at the same temperature, there was no voltage difference. If the circuit was made with wire of the same material, there was no current flow.

A thermocouple consists of two dissimilar metals, joined together at one end, that produce a small unique voltage at a given temperature. This voltage is measured and interpreted by a thermocouple thermometer.

The thermoelectric voltage resulting from the temperature difference from one end of the wire to the other is actually the sum of all the voltage differences along the wire from end to end. Thermocouples can be made from a variety of metals and cover a temperature range of 200ºC to 2,600ºC.

Types of Thermocouples

Thermocouples are available in different combinations of metals or calibrations. The four most common calibrations are J, K, T, and E. Each calibration has a different temperature

range and environment, although the maximum temperature varies with the diameter of the wire used in the thermocouple.

Some of the thermocouple types have been standardized with calibration tables, color codes, and assigned letter-designations. The ASTM E230, *Standard Specification and Temperature-Electromotive Force (EMF) Tables for Standardized Thermocouples*, provides all the specifications for most of the common industrial grades, including letter designation, color codes (USA only), suggested use limits, and the complete voltage versus temperature tables for cold junctions maintained at 32ºF and 0ºC.

There are four classes of thermocouples:

1. The home body class (called base metal)
2. The upper crust class (called rare metal or precious metal)
3. The rarified class (refractory metals)
4. The exotic class (standards and developmental devices).

The home bodies are the types E, J, K, N, and T. The upper crusts are types B, S, and R, all platinum to varying percentages. The exotic class includes several tungsten alloy thermocouples usually designated as type W.

The advantages of thermocouples are

- they are capable of being used to directly measure temperatures up to 2600ºC; and
- the thermocouple junction may be grounded and brought into direct contact with the material being measured.

The disadvantages of thermocouples are

- temperature measurement with a thermocouple requires that two temperatures be measured, the junction at the work end (the hot junction) and the junction where wires meet the instrumentation copper wires (cold junction). To avoid error, the cold junction temperature is in general compensated in the electronic instruments by measuring the temperature at the terminal block using a semiconductor, thermistor, or RTD;
- thermocouples operations are relatively complex with potential sources of error. The materials of which thermocouple wires are made are not inert and the thermoelectric voltage developed along the length of the thermocouple wire may be influenced by corrosion, etc.;
- the relationship between the process temperature and the thermocouple signal is not linear; and
- the calibration of the thermocouple must be carried out while it is in use by comparing it to a nearby comparison thermocouple. If the thermocouple is removed and placed in a calibration bath, the output integrated over the length is not reproduced exactly.

Flow

This section provides a description of the basic construction of the following types of head flow detectors:

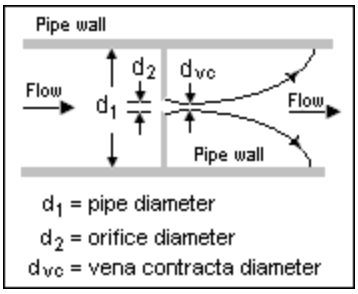
- Orifice plates
- Venturi tube
- Dall flow tube
- Pitot tube

ORIFICE PLATES

The following is taken from Wikipedia, *Orifice Plate*.

An orifice plate is a device used for measuring the volumetric flow rate. It uses the same principle as a Venturi nozzle, namely Bernoulli's principle, which states that there is a relationship between the pressure of the fluid and the velocity of the fluid. When the velocity increases, the pressure decreases, and vice versa.

An orifice plate is a thin plate with a hole in the middle. It is usually placed in a pipe in which fluid flows. When the fluid reaches the orifice plate, the fluid is forced to converge to go through the small hole; the point of maximum convergence actually occurs shortly downstream of the physical orifice, at the so-called vena contracta point (see figure 28). As it does so, the velocity and the pressure change. Beyond the vena contracta, the fluid expands and the velocity and pressure change once again. By measuring the difference in fluid pressure between the normal pipe section and at the vena contracta, the volumetric and mass flow rates can be obtained from Bernoulli's equation.



Source: Wikipedia, Orifice Plate

Figure 28. Orifice plate internal view

Orifice plates are most commonly used for continuous measurement of fluid flow in pipes. They are also used in some small river systems to measure flow rates at locations where the river passes through a culvert or drain. Only a small number of rivers are appropriate for the use of this technology since the plate must remain completely immersed; i.e., the approach pipe must be full, and the river must be substantially free of debris.

A restrictive flow orifice, a type of orifice plate, is a safety device to control maximum flow from a compressed gas cylinder.

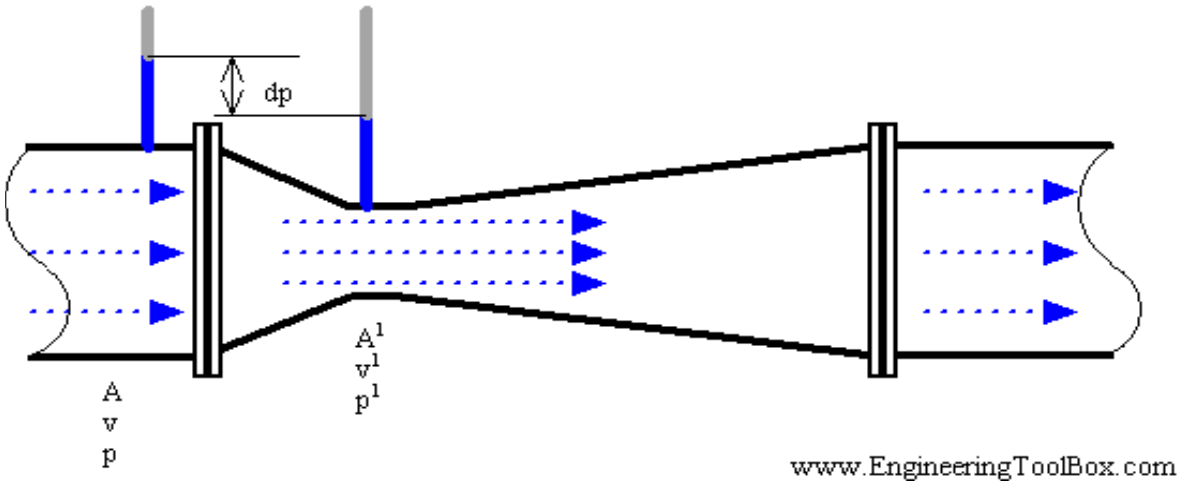
In the natural environment, large orifice plates are used to control onward flow in flood relief dams. In these structures, a low dam is placed across a river. In normal operation, the water flows through the orifice plate unimpeded as the orifice is substantially larger than the normal flow cross section. However, during floods, the flow rate rises and floods out the orifice plate, which can only pass a flow determined by the physical dimensions of the orifice. Flow is then held back behind the low dam in a temporary reservoir, which is slowly discharged through the orifice when the flood subsides.

VENTURI TUBE

The following is taken from The Engineering ToolBox, *Types of Fluid Flow Meters.*

Due to its simplicity and dependability, the Venturi tube flow meter is often used in applications with higher turn down rates or lower pressure drops than the orifice plate can provide.

In the Venturi tube as shown in figure 29, the fluid flow rate is measured by reducing the cross sectional flow area in the flow path, generating a pressure difference. After the constricted area, the fluid is passed through a pressure recovery exit section where up to 80 percent of the differential pressure generated at the constricted area is recovered.



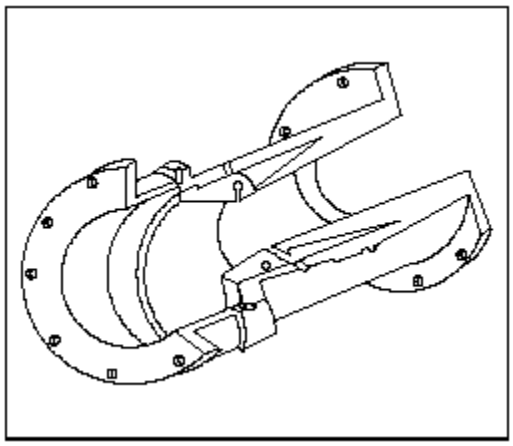
Source: The Engineering ToolBox, Types of Flow Meters

Figure 29. Venturi tube

With proper instrumentation and flow calibration, the Venturi tube flow rate can be reduced to about 10 percent of its full scale range with proper accuracy. This provides a turn down rate of 10:1.

DALL FLOW TUBE

The following is taken from Online Article-Openticle.com, *Head Flow Meters*, "Dall Flow Tube."



Source: Online Article, Openticle.com, Head Flow Meter: Dall Flow Tube

Figure 30. Dall flow tube

The dall flow tube, illustrated in figure 30, has a higher ratio of pressure developed to pressure lost than the venturi flow tube. It is more compact and is commonly used in large flow applications. The tube consists of a short, straight inlet section followed by an abrupt decrease in the inside diameter of the tube. This section, called the inlet shoulder, is followed by the converging inlet cone and a diverging exit cone. The two cones are separated by a slot or gap between the two cones.

The low pressure is measured at the slotted throat (area between the two cones). The high pressure is measured at the upstream edge of the inlet shoulder. The Dall flow tube is available in medium to very large sizes. In the large sizes, the cost is normally less than that of a Venturi flow tube. This type of flow tube has a pressure loss of about 5 percent.

PITOT TUBE

The following is taken from Wikipedia, *Pitot Tube*.

A pitot tube is a pressure measurement instrument used to measure fluid flow velocity. The pitot tube was invented by the French engineer Henri Pitot in the early 18th century, and was modified to its modern form in the mid-19th century by French scientist Henry Darcy. It is widely used to determine the airspeed of an aircraft and to measure air and gas velocities in industrial applications. The pitot tube is used to measure the local velocity at a given point in the flow stream; not the average velocity in the pipe or conduit.

The basic pitot tube consists of a tube pointing directly into the fluid flow. As this tube contains fluid, a pressure can be measured; the moving fluid is brought to rest (stagnates) as there is no outlet to allow flow to continue. This pressure is the stagnation pressure of the fluid, also known as the total pressure or (particularly in aviation) the pitot pressure.

In industry, the velocities being measured are often those flowing in ducts and tubing where measurements by an anemometer would be difficult to obtain. In these kinds of measurements, the most practical instrument to use is the pitot tube. The pitot tube can be inserted through a small hole in the duct with the pitot connected to a U-tube water gauge or some other differential pressure gauge (alnor) for determining the velocity inside the ducted wind tunnel. One use of this technique is to determine the amount of cooling that is being delivered to a room.

Video 15. Pitot static tube introduction

http://www.bing.com/videos/search?q=pitot+tube&view=detail&mid=02B7F495BB15AEA178AD02B7F495BB15AEA178AD&first=0

Level

The following is taken from DOE-HDBK-1013/1-92.

Liquid level measuring devices are classified into two groups: direct method, and inferred method. An example of the direct method is the dipstick in a car that measures the height of the oil in the oil pan. An example of the inferred method is a pressure gauge at the bottom of a tank that measures the hydrostatic head pressure from the height of the liquid.

This section provides a description of the following types of level detectors:

- Gauge glass
- Ball float
- Chain float
- Magnetic bond
- Conductivity probe
- Differential pressure (ΔP)

GAUGE GLASS

The following is taken from Wikipedia, *Sight Glass*.

Sight Glass

A sight glass or water gauge is a transparent tube through which the operator of a tank or boiler can observe the level of liquid contained within.

Simple sight glasses may be just a plastic or glass tube connected to the bottom of the tank at one end and the top of the tank at the other. The level of liquid in the sight glass will be the same as the level of liquid in the tank. Today, however, sophisticated float switches have replaced sight glasses in many such applications.

Reflex Gauges

A reflex gauge is more complex in construction than a sight glass, but can give a clearer distinction between gas (steam) and liquid (water). Instead of containing the media in a glass tube, the gauge consists of a vertically-oriented slotted metal body with a strong glass plate mounted on the open side of the slot facing the operator. The rear of the glass, in contact with the media, has vertical grooves molded into its surface. The grooves form a zig-zag pattern with 90° angles. Incident light entering the glass is refracted at the rear surface in contact with the media. In the region that is contact with the gas, most of the light is reflected from the surface of one groove to the next and back towards the operator, appearing silvery white. In the region that is in contact with the liquid, most of the light is refracted into the liquid causing this region to appear almost black to the operator.

Well-known makes of reflex gauge are Penberthy, Jerguson, Klinger, and Cesare-Bonetti.

Due to the caustic nature of boiler anti-scaling treatments (water softeners), reflex gauges tend to become relatively rapidly etched by the water and lose their effectiveness at

displaying the liquid level. Therefore, bi-color gauges are recommended for certain types of boiler, particularly those operating at pressure above 60 bar.

Bi-Color Gauges

A bi-color gauge is generally preferred for caustic media to afford protection to the glass. The gauge consists of a vertically-oriented, slotted metal body with a strong plain glass to the front and the rear. The front and rear body surfaces are in non-parallel vertical planes. Behind the gauge body are light sources with two quite different wavelengths, typically red and green. Due to the different refraction of the red and green light, the liquid region appears green to the operator, while the gas region appears red. Unlike the reflex gauge, the glass has a plane surface, which does not need to be in direct contact with the media, and can be protected with a layer of a caustic-resistant transparent material such as silica.

Magnetic Gauges

In a magnetic gauge, a float on the surface of the liquid contains a permanent magnet. The liquid is contained in a chamber of strong, non-magnetic material, avoiding the use of glass. The level indicator consists of a number of pivoting magnetic vanes arranged one above the other and placed close to the chamber containing the float. The two faces of the vanes are different colors. As the magnet passes up and down behind the vanes, it causes them to rotate, displaying one color for the region containing the liquid, and another for the region containing gas. Magnetic gauges are stated in various manufacturers' literature to be most suitable for very high pressure and/or temperature and for aggressive liquids.

Modern Industrial Sight Glass

Industrial observational instruments have changed with industry itself. More structurally sophisticated than the water gauge, the contemporary sight glass—also called the sight window or sight port—can be found on the media vessel at chemical plants and in other industrial settings, including pharmaceutical, food, beverage, and bio gas plants. Sight glasses enable operators to visually observe processes inside tanks, pipes, reactors and vessels. The modern industrial sight glass is a glass disk held between two metal frames, which are secured by bolts and gaskets, or the glass disc is fused to the metal frame during manufacture. The glass used for this purpose is either soda lime glass or borosilicate glass, and the metal, usually a type of stainless steel, is chosen for desired properties of strength. Borosilicate glass is superior to other formulations in terms of chemical corrosion resistance and temperature tolerance, as well as transparency. Fused sight glass is also called mechanically prestressed glass, because the glass is strengthened by compression of the metal ring. Heat is applied to a glass disc and its surrounding steel ring, causing a fusion of the materials. As the steel cools, it contracts, compressing the glass and making it resistant to tension. This is safer; glass typically breaks under tension, and mechanically prestressed glass is unlikely to break and endanger workers. The strongest sight glasses are made with borosilicate glass, due to the greater difference in its coefficient of expansion.

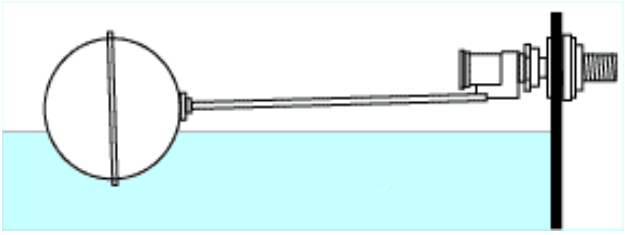
Video 16. Replacing a gauge glass

http://www.youtube.com/watch?feature=player_embedded&v=wjrjBT6hSNE

BALL FLOAT

The following is taken from diydata.com, *Ball (or float) Valves.*

One method of controlling the flow of water into water tanks and cisterns is the use of ball valves. Simply, a ball floating on the water inside the tank/cistern as shown in figure 31, moves an arm attached to the valve that controls the input of water. As the ball/arm falls, the valve is opened to allow water into the tank, and then as the water level rises, so does the ball/arm, closing off the valve.



Source: diydata.com, Ball Valves

Figure 31. Ball float

Note that although referred to here as a ball, the float can be any shape. Non-spherical floats will be found in narrow cisterns where space is limited.

The point at which the valve is closed (thus setting the level of the water) can be adjusted by the arm attached to the float; the method of adjustment depends on the type. The three basic set-ups are as follows:

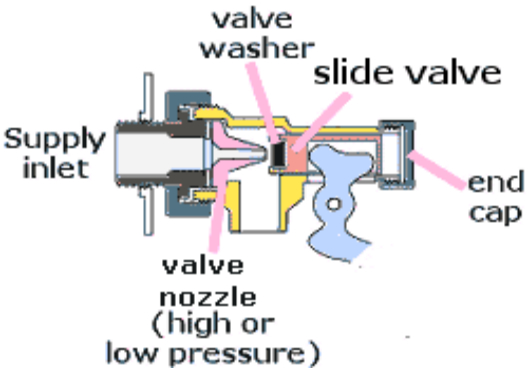
- A solid brass rod connects the valve and ball; in this case, the rod needs to be physically bent. To do this, firmly grip the rod in both hands, hold the hand next to the valve still (so as not to put any pressure onto the valve) and use the other hand to bend the rod a small amount, up to increase the water level or down to lower it. This is the most common arrangement.
- A hinge in the arm between the valve and the ball connects with a lock nut and adjustment screw. To adjust, loosen the lock nut and adjust the hinge to bend.
- An adjustable screw is at the valve end of the arm (normally with a lock nut). Release the lock nut and adjust the screw as necessary.

The two common types of valve mechanism are the slide (or piston) valve and the diaphragm valve. Both types use a valve nozzle to reduce the flow into the valve; there are two styles of valve, high and low pressure. The high pressure valve nozzle needs to be fitted where the tank is fed direct from the water main; the low pressure valve nozzle is fitted where the tank is fed from a water tank. If a high pressure nozzle is incorrectly fitted in a tank fed system, the tank will take a long time to fill up. If a low pressure nozzle is fitted in a main fed system, the valve may not close property causing leaks into the cistern/tank. At the time of installation, the correct supply valve nozzle must be fitted.

The Slide Valve

A typical slide valve is shown in figure 32.

As the float arm moves up and down with the water level in the cistern/tank, the cam on the end of the arm inside the slide valve body slides the piston towards or away from the feed hole through the middle of the valve nozzle. When the water is at the correct level, the valve washer is forced against the nozzle hole and the water supply is shut off.



Source: diydata.com, Ball Valves

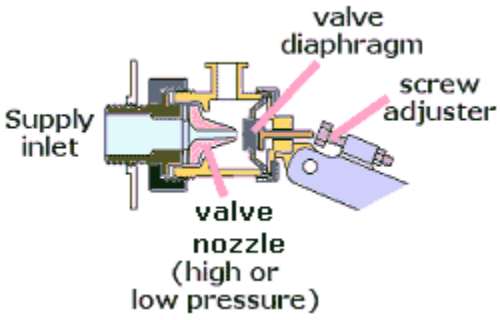
Figure 32. Slide valve

As the water in the cistern/tank drops, the slide valve is moved back to allow water to enter the tank and fill it up.

In the past, the outlets from slide valves were often fitted with a silent feed pipe. As the water was fed from the valve into the cistern/tank below the water level, there was reduced noise of water filling the tank. These pipes are now banned, due to the risk of water being drawn back from the tank in the event of mains pressure failure. If fitted, these pipes should be removed and discarded.

Slide valves are very robust and reliable. Modern slide valves may be made from plastic and these do not suffer so much as the brass ones from deposit build up or corrosion.

Wear in these valves is not normally a problem, but the valve washer may need replacement, especially if the supply water contains muck, etc.



Source: diydata.com, Ball Valves

Figure 33. Diaphragm valve

The Diaphragm Valve

The diaphragm valve, as shown in figure 33, operates with an arm from the float like the slide valve, but in this case, a screw adjuster on the top of the arm pushes against a plunger, which pushes the diaphragm against the supply valve nozzle.

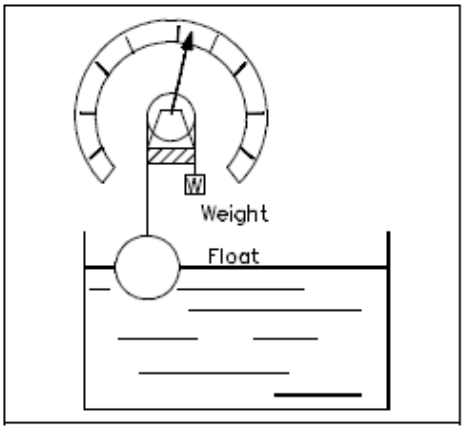
One advantage of the diaphragm valve is that the only moving part that is in contact with the water is the diaphragm itself. This reduces problems in hard water areas where deposit build-up and corrosion can occur.

Like the slide valve, in the past, the outlets from diaphragm valves were often fitted with a silent feed pipe so that the water was fed from the valve into the storage tank below the water level; these pipes are now banned due to the risk of water being drawn back from the tank in the event of mains pressure failure and, if fitted, should be removed and discarded.

CHAIN FLOAT

The following is taken from DOE-HDBK-1013/1-92.

This type of float gauge has a float size of up to 12 inches in diameter and is used where small level limitations imposed by ball floats must be exceeded.



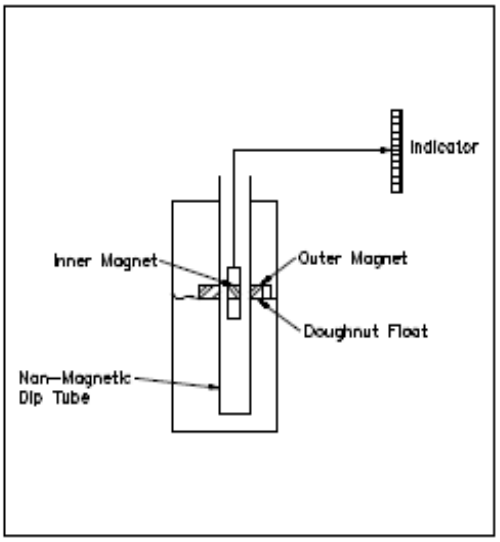
Source: DOE-HDBK-1013/1-92

Figure 34. Chain float

The range of level measured will be limited only by the size of the vessel. The operation of the chain float is similar to the ball float, except in the method of positioning the pointer and in its connection to the position indication. The float is connected to a rotating element by a chain with a weight attached to the other end to provide a means of keeping the chain taut during changes in level. (See figure 34).

MAGNETIC BOND METHOD

The following is taken from DOE-HDBK-1013/1-92.



Source: DOE-HDBK-1013/1-92

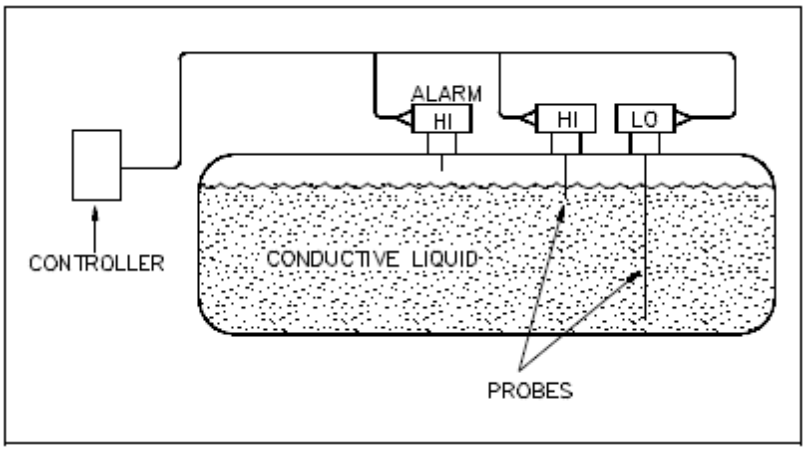
Figure 35. Magnetic bond method

The magnetic bond method was developed to overcome the problems of cages and stuffing boxes. The magnetic bond mechanism consists of a magnetic float which rises and falls with changes in liquid level. The float travels outside of a non-magnetic tube which houses an inner magnet connected to a level indicator. When the float rises and falls, the outer magnet will attract the inner magnet, causing the inner magnet to follow the liquid level within the vessel (See figure 35).

CONDUCTIVITY PROBE METHOD

Figure 36 illustrates a conductivity probe level detection system. It consists of one or more level detectors, an operating relay, and a controller.

When the liquid makes contact with any of the electrodes, an electric current will flow between the electrode and ground. The current energizes a relay which causes the relay contacts to open or close depending on the state of the process involved. The relay will, in turn, actuate an alarm, a pump, a control valve, or all three. A typical system has three probes: a low level probe, a high level probe, and a high level alarm probe.



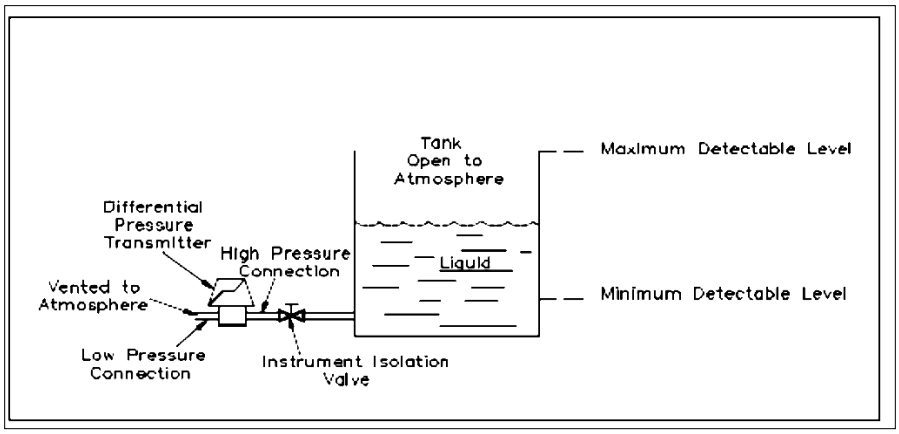
Source: DOE-HDBK-1013/1-92

Figure 36. Conductivity probe method

DIFFERENTIAL PRESSURE

The following is taken from DOE-HDBK-1013/1-92.

The differential pressure (ΔP) detector method of liquid level measurement uses a ΔP detector connected to the bottom of the tank being monitored. The higher pressure, caused by the fluid in the tank, is compared to a lower reference pressure (usually atmospheric). This comparison takes place in the ΔP detector. Figure 37 illustrates a typical differential pressure detector attached to an open tank.



Source: DOE-HDBK-1013/1-92

Figure 37. Differential pressure detector

Vibration

The following is taken from eHow, *Types of Vibration Sensors*.

Vibration sensors are used in a number of different projects, machines and applications, such as gauging the speed of a vehicle, or the power of an impending earthquake. Some of them operate on their own, and others require a separate power source, but all of them serve the same purpose in slightly different capacities.

ACCELEROMETER

One of the most common types of vibration sensor is an accelerometer. Accelerometers come in a variety of designs, and they can detect a wide range of different vibrations. One of the most popular versions of the accelerometer is a pizoelectric sensor. This sort of sensor contains a material (such as crystal quartz) that gives off an electric charge when it detects changes in pressure. By measuring the amounts of electric charge that pizoelectric accelerometers give off, it becomes possible to determine the amount of vibration going on in the connection.

VELOCITY SENSORS

A velocity sensor is mainly used to measure motion and balancing operations on rotating machinery. These sensors are ideal for sensing low and mid-frequency vibrations, but not high-frequency ones. Additionally, a velocity sensor requires no electrical input in order to measure the force of velocity. These sensors do require regular maintenance to be sure that they're operating properly, however. This is especially true for sensors that are placed on machinery that moves at a very high velocity, since the sensors need to be firmly anchored to get accurate measurements.

PROXIMITY SENSORS

Not all vibration sensors are installed directly onto the things they are supposed to measure. A proximity sensor is a type of vibration sensor that's meant to measure distance between an object and the probe. If the object is vibrating that means it will be moving towards and away from the probe, and by picking up that motion, the sensors can detect the range of vibration taking place. These probes may be used for small applications such as detecting vibrations within machinery, or for larger applications such as detecting vibrations in the earth as a sign of earthquakes.

b. Explain the function and use of final control elements (e.g., motor operated valves, solenoid actuated valves, dampers, and pumps, etc). Explain the importance of final control elements and considerations used during the selection process (e.g., reliability, response time, and other essential features).

The following is taken from DOE-HDBK-1013/2-92.

Final control elements are devices that complete the control loop. They link the output of the controlling elements with their processes. Some final control elements are designed for specific applications. For example, neutron-absorbing control rods of a reactor are specifically designed to regulate neutron-power level; however, the majority of final control elements are general application devices such as valves, dampers, pumps, and electric heaters. Valves and dampers have similar functions. Valves regulate flow rate of a liquid while dampers regulate flow of air and gases. Pumps, like valves, can be used to control flow of a fluid. Heaters are used to control temperature.

These devices can be arranged to provide a type of on-off control to maintain a variable between maximum and minimum values. This is accomplished by opening and shutting valves or dampers or energizing and de-energizing pumps or heaters. These devices can also be modulated over a given operating band to provide a proportional control. This is accomplished by positioning valves or dampers, varying the speed of a pump, or regulating

the current through an electric heater. There are many options to a process control. Of the final control elements discussed, the most widely used in power plants are valves. Valves can be easily adapted to control liquid level in a tank, temperature of a heat exchanger, or flow rate.

The following is taken from PAControl.com, *Final Control Elements–Control Valves*.

Process control engineers tend to treat final control elements in the same way they treat measurement devices–with absolute indifference. To most of them, a valve is a valve is a valve. Its job is to open and close according to what the controller tells it and it does just that. The problem is, in a shocking number of cases, it does not.

Control valves and dampers, being mechanical devices, are subjected to a lot of mechanical issues like wear and tear – deterioration with time. Present measurement devices are very robust and most do not deteriorate drastically with time. The controller running inside the modern distributed control system (DCS) is even more reliable with a hot standby ready to take over in case of failure. The same cannot be said about final control elements. Therefore the weakest link in the process control loop is frequently the final control element.

The problems of control valves usually manifest as deadband, stiction, and hysteresis.

Deadband

Deadband is a general phenomenon where a range or band of controller output values fails to produce a change in the measured process variable. This is bad for process control. Present process control systems execute at a rate of about 3 times per second. Each time they execute, the output changes in the magnitude of (usually) less than 1 percent. But most relevant in the case of deadband, the changes can occur in either direction.

If a control valve is suffering from a deadband problem, when the controller output reverses direction, the control valve does not respond; therefore, the process variable also does not respond to the command of the controller. The controller does not receive the command and so issues another (sometimes more drastic) command. When the control valve finally comes out of its deadband, the controller command has caused it to overshoot.

The controller then tries to go back the other direction only to be faced with the same situation; the process will be driven to overshoot in either direction and cycles continuously, forming what is called a limit cycle.

Stiction

This is somewhat similar to deadband except that it does not only happen when the controller changes direction. Again stiction (also known as sticky valve) can be due to a variety of reasons; a common one is packing friction.

In terms of process control, the effect of stiction is also like deadband whereby the valve fails to respond when required and when it does respond, it overshoots the set point. The controller then tries to bring it back the other way.

Hysteresis

Hysteresis occurs when the same change in the controller output in both directions results in a different change in the process value. For example, when the controller output is 20 percent, the process variable is 30°C. When the controller output increases to 25 percent, the temperature increases to 35°C. However, when the controller goes back down to 20 percent, the temperature only goes down to 33°C. This results in different process gains in both directions and will confuse the controller, which has been tuned for only one process gain.

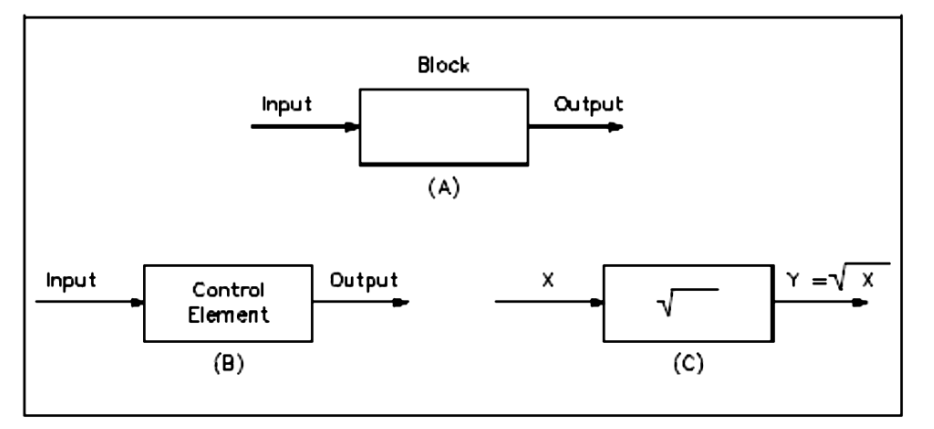
c. Explain the application of process and instrumentation diagrams (P&IDs) and their importance in I&C systems design and operation.

The following is taken from DOE-HDBK-1013/2-92

Block Diagram

A block diagram is a pictorial representation of the cause and effect relationship between the input and output of a physical system. A block diagram provides a means to easily identify the functional relationships among the various components of a control system.

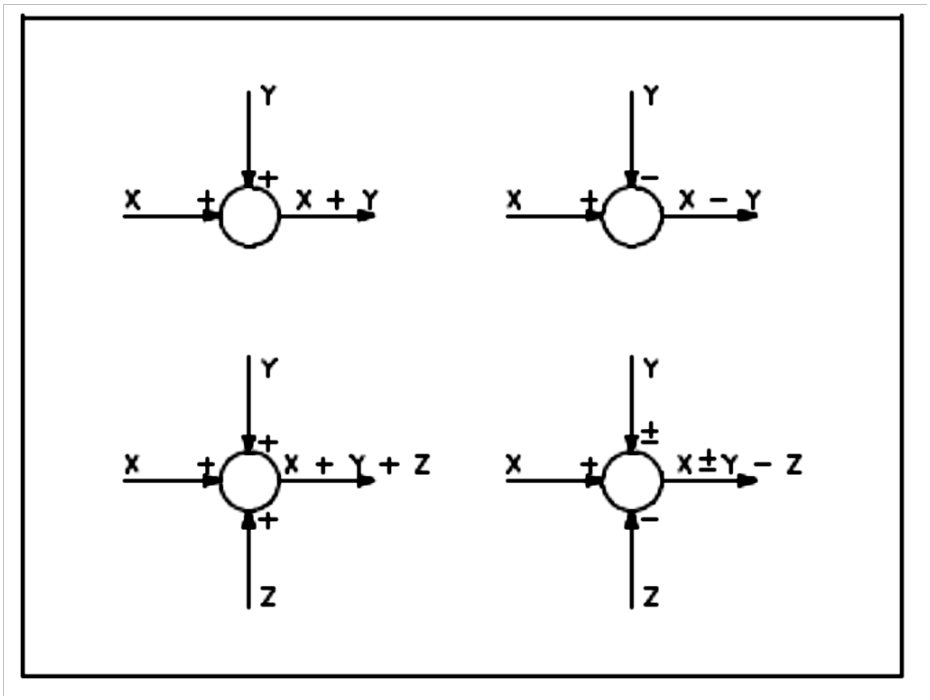
The simplest form of a block diagram is the block and arrows diagram. It consists of a single block with one input and one output (figure 38A). The block normally contains the name of the element (figure 38B) or the symbol of a mathematical operation (figure 38C) to be performed on the input to obtain the desired output. Arrows identify the direction of information or signal flow.



Source: DOE-HDBK-1013/2-92

Figure 38. Block and arrows

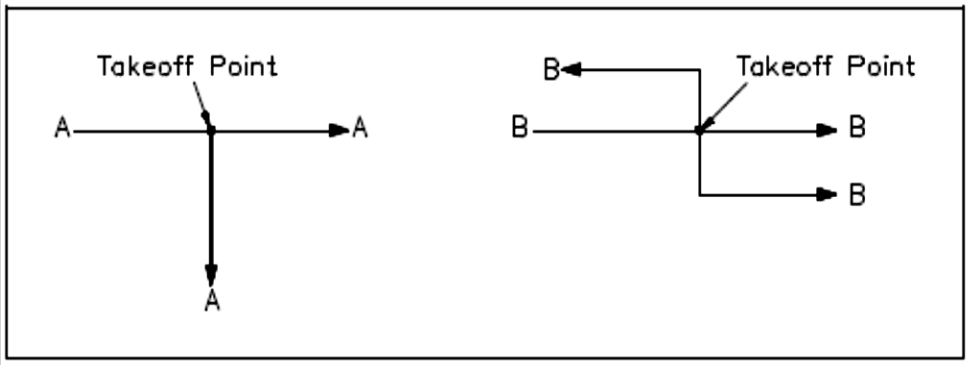
Although blocks are used to identify many types of mathematical operations, operations of addition and subtraction are represented by a circle, called a summing point. As shown in figure 39, a summing point may have one or several inputs. Each input has its own appropriate plus or minus sign. A summing point has only one output and is equal to the algebraic sum of the inputs.



Source: DOE-HDBK-1013/2-92

Figure 39. Summing points

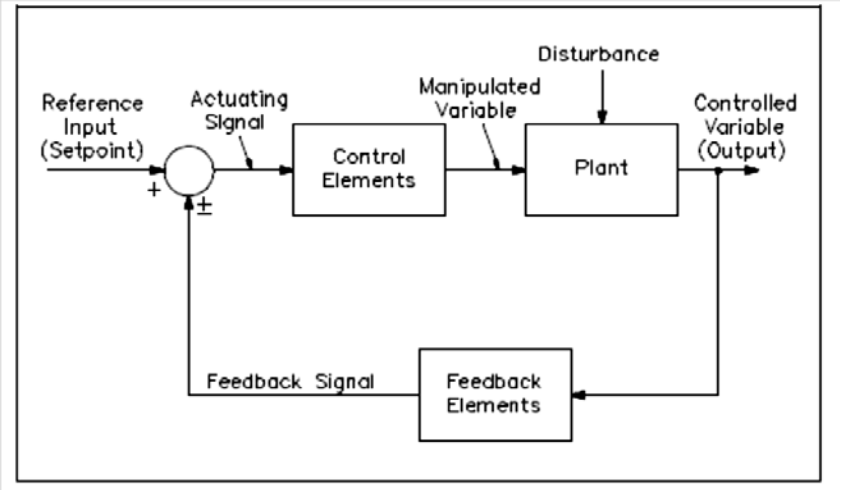
A takeoff point is used to allow a signal to be used by more than one block or summing point (figure 40).



Source: DOE-HDBK-1013/2-92

Figure 40. Takeoff point

Feedback Control System Block Diagram



Source: DOE-HDBK-1013/2-92

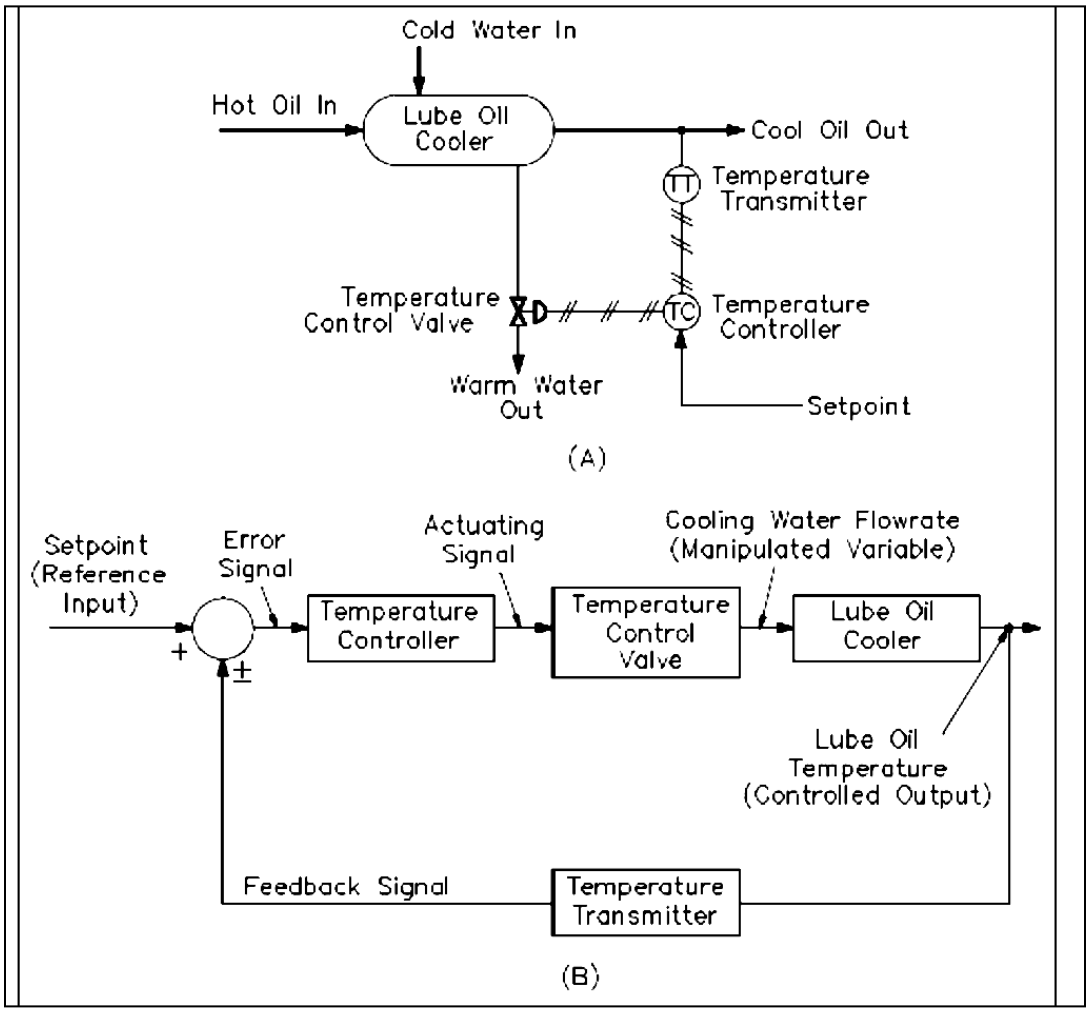
Figure 41. Feedback control system block diagram

Figure 41 shows basic elements of a feedback control system as represented by a block diagram. The functional relationships between these elements are easily seen. An important factor to remember is that the block diagram represents flow paths of control signals, but does not represent flow of energy through the system or process.

The following are several terms associated with the closed-loop block diagram:

- The plant is the system or process through which a particular quantity or condition is controlled. This is also called the *controlled system*.
- The *control elements* are components needed to generate the appropriate control signal applied to the plant. These elements are also called the "controller."
- The *feedback elements* are components needed to identify the functional relationship between the feedback signal and the controlled output.
- The *reference point* is an external signal applied to the summing point of the control system to cause the plant to produce a specified action. This signal represents the desired value of a controlled variable and is also called the "set point."
- The *controlled output* is the quantity or condition of the plant which is controlled. This signal represents the controlled variable.
- The *feedback signal* is a function of the output signal. It is sent to the summing point and algebraically added to the reference input signal to obtain the actuating signal.
- The *actuating signal* represents the control action of the control loop and is equal to the algebraic sum of the reference input signal and feedback signal. This is also called the "error signal."
- The *manipulated variable* is the variable of the process acted upon to maintain the plant output (controlled variable) at the desired value.
- The *disturbance* is an undesirable input signal that upsets the value of the controlled output of the plant.

Figure 42 shows a typical application of a block diagram to identify the operation of a temperature control system for lubricating oil. (A) in figure 42 shows a schematic diagram of the lube oil cooler and its associated temperature control system.



Source: DOE-HDBK-1013/2-92

Figure 42. Lube oil cooler temperature control system and equivalent block diagram

d. Explain the use of logic and loop diagrams, and explain how I&C systems design can be expressed using logic diagrams (e.g., application of Boolean logic).

The following is taken from DOE-HDBK-1013/2-92.

Lubricating oil reduces friction between moving mechanical parts and also removes heat from the components. As a result, the oil becomes hot. This heat is removed from the lube oil by a cooler to prevent breakdown of the oil and damage to the mechanical components it serves.

The lube oil cooler consists of a hollow shell with several tubes running through it. Cooling water flows inside the shell of the cooler and around the outside of the tubes. Lube oil flows inside the tubes. The water and lube oil never make physical contact.

As the water flows through the shell side of the cooler, it picks up heat from the lube oil through the tubes. This cools the lube oil and warms the cooling water as it leaves the cooler.

The lube oil must be maintained within a specific operating band to ensure optimum equipment performance. This is accomplished by controlling the flow rate of the cooling water with a temperature control loop.

The temperature control loop consists of a temperature transmitter, a temperature controller, and a temperature control valve. The diagonally crossed lines indicate that the control signals are air (pneumatic).

The lube oil temperature is the controlled variable because it is maintained at a desired value (the set point). Cooling water flow rate is the manipulated variable because it is adjusted by the temperature control valve to maintain the lube oil temperature. The temperature transmitter senses the temperature of the lube oil as it leaves the cooler and sends an air signal that is proportional to the temperature controller. Next, the temperature controller compares the actual temperature of the lube oil to the set point (the desired value). If a difference exists between the actual and desired temperatures, the controller will vary the control air signal to the temperature control valve. This causes it to move in the direction and by the amount needed to correct the difference. For example, if the actual temperature is greater than the set point value, the controller will vary the control air signal and cause the valve to move in the open direction, which results in more cooling water flowing through the cooler, and lowering the temperature of the lube oil leaving the cooler.

(B) in figure 42 represents the lube oil temperature control loop in block diagram form. The lube oil cooler is the plant in this example, and its controlled output is the lube oil temperature. The temperature transmitter is the feedback element. It senses the controlled output and lube oil temperature and produces the feedback signal.

The feedback signal is sent to the summing point to be algebraically added to the reference input (the set point). Notice the set point signal is positive, and the feedback signal is negative. This means the resulting actuating signal is the difference between the set point and feedback signals.

The actuating signal passes through the two control elements: the temperature controller and the temperature control valve. The temperature control valve responds by adjusting the manipulated variable (the cooling water flow rate). The lube oil temperature changes in response to the different water flow rate, and the control loop is complete.

Process Time Lags

In the last example, the control of the lube oil temperature may initially seem easy. Apparently, the operator need only measure the lube oil temperature, compare the actual temperature to the desired (set point), compute the amount of error (if any), and adjust the temperature control valve to correct the error accordingly. However, processes have the characteristic of delaying and retarding changes in the values of the process variables. This characteristic greatly increases the difficulty of control.

These process delays and retardations are called process time lags. They are caused by three properties of the process; capacitance, resistance, and transportation time:

1. Capacitance is the ability of a process to store energy. In figure 42, for example, the walls of the tubes in the lube oil cooler, the cooling water, and the lube oil can store heat energy. This energy-storing property gives the ability to retard change. If the cooling water flow rate is increased, it will take a period of time for more energy to be removed from the lube oil to reduce its temperature.
2. Resistance is that part of the process that opposes the transfer of energy between capacities. In figure 42, the walls of the lube oil cooler oppose the transfer of heat from the lube oil inside the tubes to the cooling water outside the tubes.
3. Transportation time is time required to carry a change in a process variable from one point to another in the process. If the temperature of the lube oil (figure 42) is lowered by increasing the cooling water flow rate, some time will elapse before the lube oil travels from the lube oil cooler to the temperature transmitter. If the transmitter is moved farther from the lube oil cooler, the transportation time will increase. This time lag is not just a slowing down or retardation of a change; it is an actual time delay during which no change occurs.

Stability of Automatic Control Systems

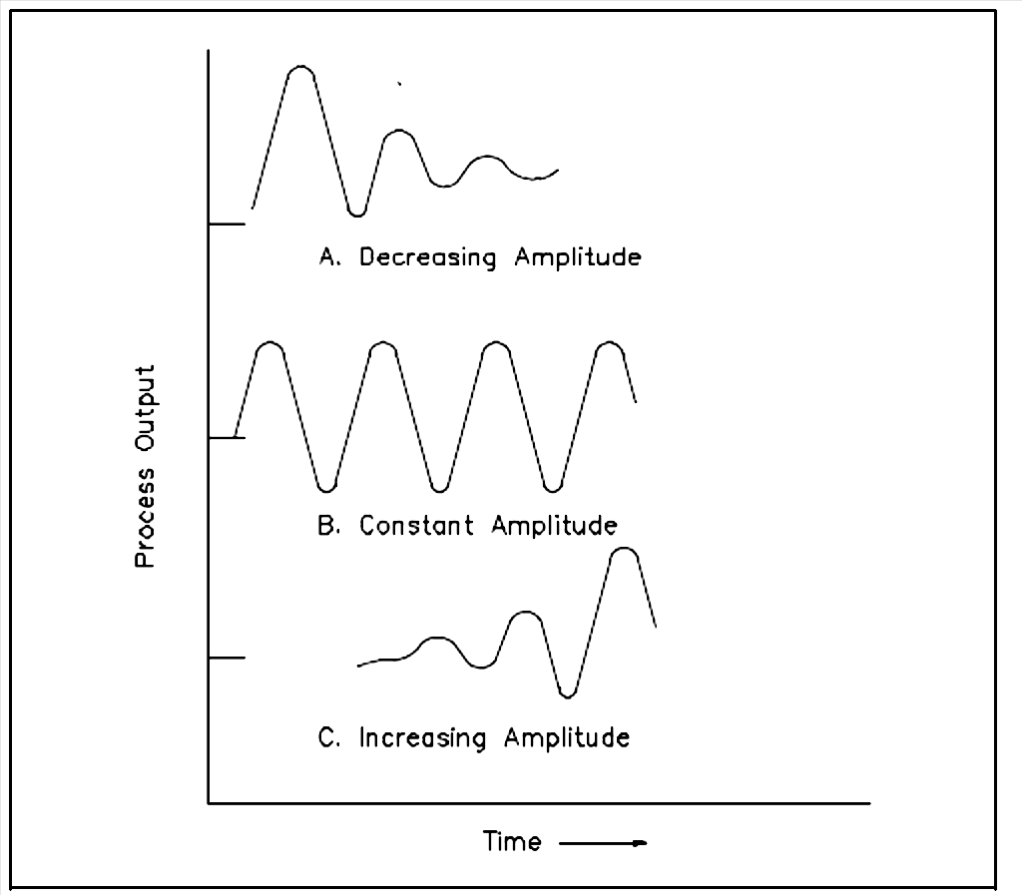
All control modes previously described can return a process variable to a steady value following a disturbance. This characteristic is called "stability."

Stability is the ability of a control loop to return a controlled variable to a steady, non-cyclic value, following a disturbance.

Control loops can be either stable or unstable. Instability is caused by a combination of process time lags discussed earlier (i.e., capacitance, resistance, and transport time) and inherent time lags within a control system. This results in slow response to changes in the controlled variable. Consequently, the controlled variable will continuously cycle around the set point value.

Oscillations describe this cyclic characteristic. There are three types of oscillations that can occur in a control loop; decreasing amplitude, constant amplitude, and increasing amplitude. (each is shown in figure 43):

1. *Decreasing amplitude (figure 43A).* These oscillations decrease in amplitude and eventually stop with a control system that opposes the change in the controlled variable. This is the condition desired in an automatic control system.
2. *Constant amplitude (figure 43B).* Action of the controller sustains oscillations of the controlled variable. The controlled variable will never reach a stable condition; therefore, this condition is not desired.
3. *Increasing amplitude (figure 43C).* The control system not only sustains oscillations but also increases them. The control element has reached its full travel limits and causes the process to go out of control.



Source: DOE-HDBK-1013/2-92

Figure 43. Types of oscillations

Logic Diagrams

The following is taken from DOE-HDBK-1016/2-93.

Logic diagrams have many uses. In the solid state industry, they are used as the principal diagram for the design of solid state components such as computer chips. They are used by mathematicians to help solve logical problems (called boolean algebra). However, their principle application at DOE facilities is their ability to present component and system operational information. The use of logic symbology results in a diagram that allows the user to determine the operation of a given component or system as the various input signals change.

To read and interpret logic diagrams, the reader must understand what each of the specialized symbols represents. This section discusses the common symbols used on logic diagrams. When mastered, this knowledge should enable the reader to understand most logic diagrams.

Facility operators and technical staff personnel commonly see logic symbols on equipment diagrams. The logic symbols, called gates, depict the operation/start/stop circuits of components and systems.

SYMBOLOGY

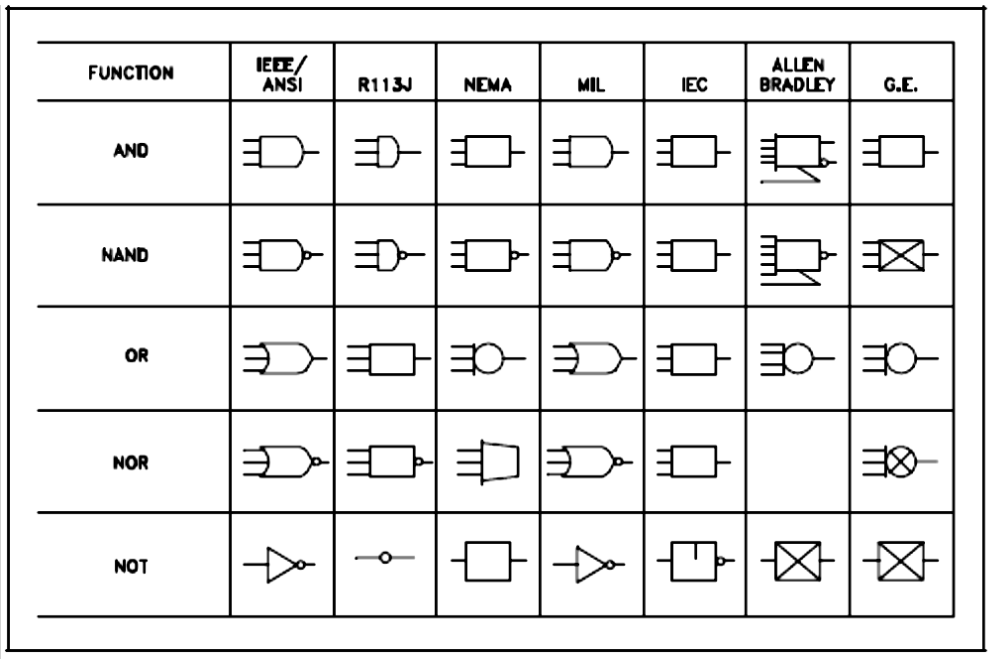
There are three basic types of logic gates. They are AND, OR, and NOT gates. Each gate is a very simple device that only has two states: on and off. The states of a gate are also commonly referred to as high or low, 1 or 0, or True or False, where on = high = 1 = True, and off = low = 0 = False. The state of the gate, also referred to as its output, is determined by the status of the inputs to the gate, with each type of gate responding differently to the various possible combinations of inputs. Specifically, these combinations are as follows:

- AND gate—provides an output (on) when all its inputs are on. When any one of the inputs is off, the gate's output is off.
- OR gate—provides an output (on) when any one or more of its inputs is on. The gate is off only when all of its inputs are off.
- NOT gate—provides a reversal of the input. If the input is on, the output will be off. If the input is off, the output will be on.

Because the NOT gate is frequently used in conjunction with AND and OR gates, special symbols have been developed to represent these combinations. The combination of an AND gate and a NOT gate is called a NAND gate. The combination of an OR gate with a NOT gate is called a NOR gate. The combinations are as follows:

- NAND gate—is the opposite (NOT) of an AND gate's output. It provides an output (on) except when all the inputs are on.
- NOR gate—is the opposite (NOT) of an OR gate's output. It provides an output only when all inputs are off.

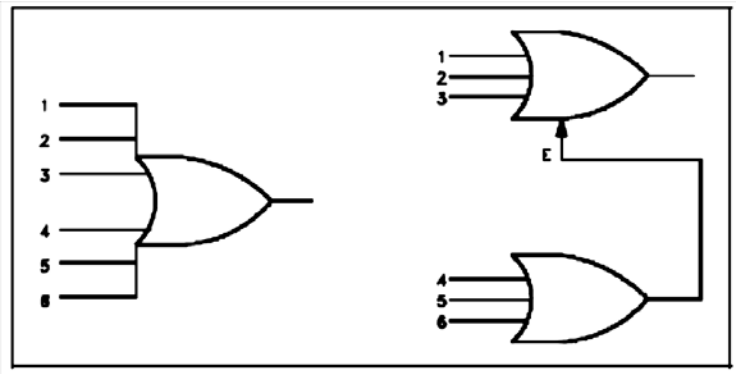
Figure 44 illustrates the symbols covering the three basic logic gates plus NAND and NOR gates. The IEEE/ANSI symbols are used most often; however, other symbol conventions are provided on figure 44 for information.



Source: DOE-HDBK-1016-93

Figure 44. Basic logic symbols

The AND gate has a common variation called a COINCIDENCE gate. Logic gates are not limited to two inputs. Theoretically, there is no limit to the number of inputs a gate can have. But, as the number of inputs increases, the symbol must be altered to accommodate the increased inputs. There are two basic ways to show multiple inputs. Figure 45 demonstrates both methods, using an OR gate as an example. The symbols used in figure 45 are used extensively in computer logic diagrams. The COINCIDENCE gate behaves like an AND gate except that only a specific number of the total number of inputs needs to be on for the gate's output to be on.

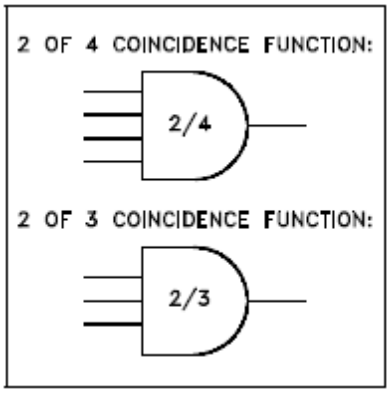


Source: DOE-HDBK-1016/2-93

Figure 45. Conventions for multiple inputs

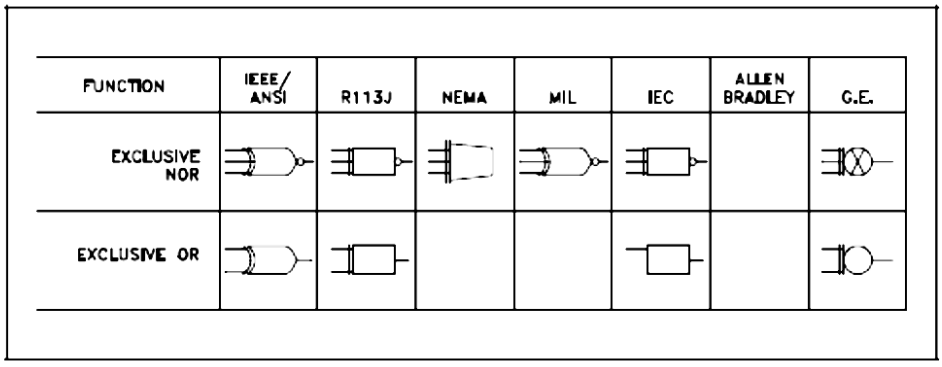
The symbol for a COINCIDENCE gate is shown in figure 46. The fraction in the logic symbol indicates that the AND gate is a COINCIDENCE gate. The numerator of the fraction indicates the number of inputs that must be on for the gate to be on. The denominator states the total number of inputs to the gate.

Two variations of the OR gate are the EXCLUSIVE OR and its opposite, the EXCLUSIVE NOR. The EXCLUSIVE OR and the EXCLUSIVE NOR are symbolized by adding a line on the back of the standard OR or NOR gate's symbol, as illustrated in figure 47.



Source: DOE-HDBK-1016/2-93

Figure 46. Coincidence gate



Source: DOE-HDBK-1016/2-93

Figure 47. EXCLUSIVE OR and EXCLUSIVE NOR gates

Or and NOR gates are described as follows:

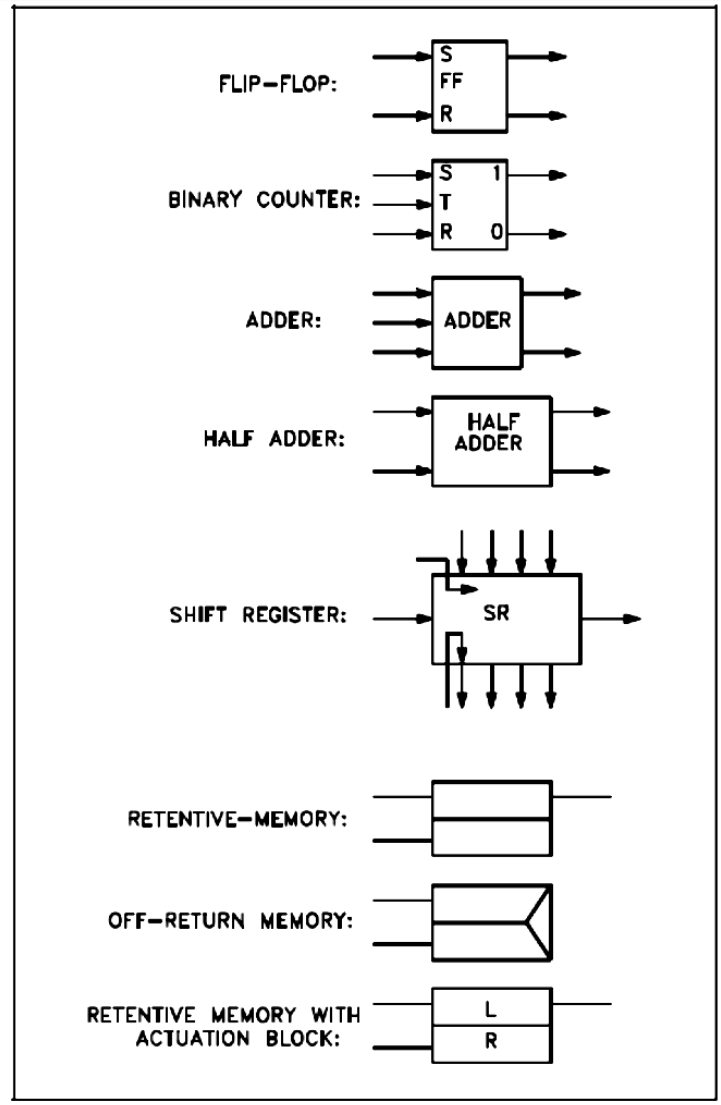
- EXCLUSIVE OR—provides an output (on) when only one of the inputs is on. Any other combination results in no output (off).
- EXCLUSIVE NOR—is the opposite (NOT) of an EXCLUSIVE OR gate's output. It provides an output only when all inputs are on or when all inputs are off.

COMPLEX LOGIC DEVICES

In addition to the seven basic logic gates, there are several complex logic devices that may be encountered in the use of logic prints.

Memory devices. In many circuits, a device that can "remember" the last command or the last position is required for a circuit to function. Like the AND and OR gates, memory devices have been designed to work with on/off signals. The two input signals to a memory device are called set and reset. Figure 48 shows the common symbols used for memory devices.

Flip-flop. As the name implies, a flip-flop is a device in which, as one or more of its inputs changes, the output changes. A flip-flop is a complex circuit constructed from OR and NOT gates, but is used so frequently in complex circuits that it has its own symbol. Figure 48 shows the common symbol used for a flip-flop. This device, although occasionally used on component and system type logic diagrams, is principally used in solid state logic diagrams (computers).



Source: DOE-HDBK-1016/2-93

Figure 48. Symbols for complex devices

Binary counter. Several types of binary counters exist, all of which are constructed of flip-flops. The purpose of a counter is to allow a computer to count higher than 1, which is the highest number a single flip-flop can represent. By ganging flip-flops, higher binary numbers can be constructed. Figure 48 illustrates a common symbol used for a binary counter.

Shift register. A storage device constructed of flip-flops that is used in computers to provide temporary storage of a binary word. Figure 48 shows the common symbol used for a shift register.

Half adder. A logic circuit that is used in computer circuits to allow the computer to "carry" numbers when it is performing mathematical operations (for example to perform the addition of 9 + 2, a single 10s unit must be "carried" from the ones column to the tens column). Figure 48 illustrates the symbol used for a half adder.

e. Explain the application, advantages, and disadvantages of pneumatic control systems applications (e.g., pneumatic control of solenoid valves, air compressors, air start of diesel generator, etc).

The following is taken from eHow, *How do Pneumatic Controls Work*?

Controlling a mechanism using pneumatics begins with pressurized gas. The gases most commonly used for this control are carbon dioxide, nitrogen, and high-pressured air. This gas is housed in a tank, which is usually compressed to thousands of pounds per square inch.

Pneumatic controls also depend on regulators, which are attached to the gas tank. A regulator reduces the high pressure from the tank and lowers it to a more manageable pressure. Regulators work on demand, meaning that instead of a constant stream, they release gas from the tank only when there is a drop in pressure in another part of the system.

Hoses and Valves

Pneumatic controls cannot function without hoses and valves delivering pressurized gas from the regulator to the rest of the system. These parts must be able to function under high pressure without rupturing. Hoses are often reinforced with steel to keep them strong as pressure moves through the lines.

Valves connect to the hoses and act as switches, stopping and starting the flow of pressurized gas as needed. When the user activates a valve, it opens very quickly and allows gas to move through. Closing the valve interrupts the flow and holds back the pressure. Valves can be activated manually or remotely using motors and electronics.

Actuators

All other pieces, from the tank to the valves, are useless without an actuator. The actuator is the part that directly pushes or pulls objects when the pneumatic controls are activated.

Actuators consist of a cylinder with a disk and a rod housed inside. When a valve opens and high-pressure gas is allowed to enter the actuator, it forces the disk to move. This pushes the rod, which can be connected to any object that needs to be moved. For example, the rod may connect to a door needing to be opened, or a box to be lifted. The actuator is the final piece of the control system.

Different types of actuators can be used, depending on the necessary task. Single-acting actuators move in only one direction when pressurized, and rely on gravity to return them to the start position. Double-acting actuators have pressure connections on both ends, allowing them to be forced in both directions.

The following is taken from Bright Hub Engineering, *Pneumatic vs. Electronic Control Mechanisms*.

Pneumatic Control System

ADVANTAGES

- Simplicity of the components and no complex structure
- Easy maintainability

- Useful in flame-proof applications
- Low cost of installation
- Good reliability and reproducibility
- Speed of response is relatively slow but steady
- Limited power capacity for large mass transfer

LIMITATIONS

- Great distance lag can be a crucial setback with pneumatic controls.
- Slow response
- Difficult to operate in sub-normal temperatures
- Copper piping is vulnerable to damage
- Pipe-couplings can give rise to leaks in certain ambient conditions

f. Explain the application, advantages, and disadvantages of hydraulic control systems applications (e.g., hydraulic lift, turbine controls).

Advantages and Disadvantages of Hydraulic Control System Applications.

The following is taken from eHow, *Advantages & Disadvantages of Hydraulic Systems.*

Hydraulic systems work because of Pascal's law, which states that an increase of pressure in any part of a confined fluid causes an equal increase of pressure throughout the container. If force is applied to one part of a hydraulic system, it travels through the hydraulic fluid to the rest of the system.

ADVANTAGES

Hydraulic systems allow users to accurately wield large amounts of power with little input force. They also provide constant force, according to the National Fluid Power Association. In addition, hydraulic systems are safe in chemical plants and mines because they do not cause sparks.

DISADVANTAGES

Hydraulic systems contain highly pressurized fluid. This can cause burns, bruises or the accidental injection of fluid into the body, according to Colorado State University. Hydraulic systems must be periodically checked for leaks and lubricated, and filters must be changed regularly.

Hydraulic Lifts

The following is taken from Hydraulicmania.com, *The Workings of a Hydraulic Lift,* "Various Uses for Hydraulic Lifts."

Table lifts and positioners are used for positioning the work material at an ergonomically comfortable access point. Truck or vehicle lifts are used to lift materials to the height of the truck bed for loading. Vehicle lifts come with attachments for mounting at the rear of a vehicle.

Transport companies use such lifts to move goods and materials. A dock lift is similar to a vehicle lift; however, this is mounted at the dock and is used to position material and/or personnel for loading purposes.

Personnel lifts, as the name implies, are used to move workers to materials or the work area. This is done when it is more feasible to move personnel to the work area than to move the work area to the personnel. Such situations can arise when the work has to be done at great heights, or the work area is very large and impossible to move.

Forklifts and pallet lifts are used to lift the load from the base or pallets. Forklift trucks are a common sight at docks, warehouses, and storage places. These trucks are used to lift and transport goods at short distances. Forklifts and pallet lifts are used for loading and unloading, as well as for storage and working purposes. Tilt tables are hollow bins with four sides, (usually) open at the top. These cannot only raise or lower the work piece, but can also tilt at an angle to place it in an ergonomically optimal position to be worked on.

The main reason for the widespread use of the hydraulic lift is the benefit it provides by creating ergonomically safe working conditions. This helps to greatly reduce, or even eliminate, the large number of injuries caused to workers by repetitive stress.

Such injuries frequently occur when the job puts physical demands on workers that exceed their physical limitations. Hydraulic lifts help to place the work material easily and safely in positions that are not awkward for the workers. The worker may not only benefit from the better posture, but the lifts can also space the objects so that the job requires the minimum force and labor to do. Creation of such a work friendly environment not only results in reduced injuries, but also more productive workers.

Hydraulic lifts can be helpful in a variety of conditions that are otherwise very demanding or dangerous. They can be used to move materials horizontally as well as vertically. Many hydraulic lifts come with wheels, and are mobile in nature, so they can be used in various situations (the best example being the forklift truck). For sustained use in a repetitive work environment, hydraulic lifts can be permanently fixed and be made a part of the process line. In a manufacturing workshop, smaller hydraulic lifts are commonly used for holding and moving various products.

For employees that are engaged in repetitive motion activities, the tilting, as well as the height adjustment capacities of hydraulic lifts, are very important capabilities for maintaining an ergonomically safe environment. A hydraulic lift can either be controlled by a remote control, or can be controlled manually, depending on the purpose and the size of the lift. Hydraulic lifts are commonly used in production facilities, auto repair shops, docks, warehouses, construction sites, etc. Strength and sturdiness, along with the dimension requirements of the purpose, are important criteria to consider when selecting a hydraulic lift.

Hydraulic lifts require special care and regular maintenance to make sure they work in the desired manner. Improperly maintained lifts can cause serious injury. As with any hydraulic system, care should always be taken when operating hydraulic lifts. Even when the whole system is shut down, the oil can still be under pressure, which can be very dangerous if not handled properly. Leaks of hydraulic fluid are especially dangerous, as they are at very high pressure, and have the capability of puncturing human skin.

Care should be taken to allow only those people that are properly trained in the use of hydraulic lifts and positioning vehicles to operate the equipment. The required hydraulic pressure should always be maintained, and should never be allowed to surpass the recommended levels. The lift area should be kept clean of dirt, oil, tools, grit, etc., and a hydraulic lift should never be overloaded.

Turbine Controls

The following is taken from Wikipedia, *Turbine*.

A turbine is a rotary mechanical device that extracts energy from a fluid flow and converts it into useful work. A turbine is a turbomachine with at least one moving part (the rotor assembly), which is a shaft or drum with blades attached. Moving fluid acts on the blades so that they move and impart rotational energy to the rotor. Early turbine examples are windmills and water wheels.

THEORY OF TURBINE OPERATIONS

Working fluid contains potential energy (pressure head) and kinetic energy (velocity head). The fluid may be compressible or incompressible. Several physical principles are employed by turbines to collect this energy.

Impulse turbines change the direction of flow of a high velocity fluid or gas jet. The resulting impulse spins the turbine and leaves the fluid flow with diminished kinetic energy. There is no pressure change of the fluid or gas in the turbine blades, as in the case of a steam or gas turbine; all the pressure drop takes place in the stationary blades. Before reaching the turbine, the fluid's pressure head is changed to velocity head by accelerating the fluid with a nozzle. Pelton wheels and de Laval turbines use this process exclusively. Impulse turbines do not require a pressure casement around the rotor since the fluid jet is created by the nozzle prior to reaching the blading on the rotor. Newton's second law describes the transfer of energy for impulse turbines.

Reaction turbines develop torque by reacting to the gas or fluid's pressure or mass. The pressure of the gas or fluid changes as it passes through the turbine rotor blades. A pressure casement is needed to contain the working fluid as it acts on the turbine stage(s) or the turbine must be fully immersed in the fluid flow. The casing contains and directs the working fluid and, for water turbines, maintains the suction imparted by the draft tube. Francis turbines and most steam turbines use this concept. For compressible working fluids, multiple turbine stages are usually used to efficiently harness the expanding gas. Newton's third law describes the transfer of energy for reaction turbines.

In the case of steam turbines, such as would be used for marine applications or for land-based electricity generation, a Parsons type reaction turbine would require approximately double the number of blade rows as a de Laval type impulse turbine for the same degree of thermal energy conversion. While this makes the Parsons turbine much longer and heavier, the overall efficiency of a reaction turbine is slightly higher than the equivalent impulse turbine for the same thermal energy conversion.

In practice, modern turbine designs use reaction and impulse concepts to varying degrees whenever possible. Wind turbines use an airfoil to generate a reaction lift from the moving fluid, imparting it to the rotor. Wind turbines also gain some energy from the impulse of the wind, by deflecting it at an angle. Crossflow turbines are designed as impulse machines, with nozzles, but in low head applications they maintain some efficiency through reaction, like traditional water wheels. Turbines with multiple stages may use either reaction or impulse blading at high pressure. Steam turbines were traditionally more impulse based but continue to move toward reaction designs similar to those used in gas turbines. At low pressure, the operating fluid medium expands in volume for small reductions in pressure. Under these conditions, blading becomes strictly a reaction type design with the base of the blade solely impulse. This is due to the effect of the rotation speed for each blade. As the volume increases, the blade height increases, and the base of the blade spins at a slower speed relative to the tip. This change in speed forces a designer to change from impulse at the base, to a high reaction style tip.

Classic turbine design methods were developed in the mid 19th century. Vector analysis related the fluid flow to turbine shape and rotation. Graphical calculation methods were used at first. Formulas for the basic dimensions of turbine parts are well documented, and a highly efficient machine can be reliably designed for any fluid flow condition. Some of the calculations are empirical or rule of thumb formula, and others are based on classic mechanics. As with most engineering calculations, simplifying assumptions were made.

Velocity triangles can be used to calculate the basic performance of a turbine stage. Gas exits the stationary turbine nozzle guide vanes at absolute velocity Va1. The rotor rotates at velocity U. Relative to the rotor; the velocity of the gas as it impinges on the rotor entrance is Vr1. The gas is turned by the rotor and exits, relative to the rotor, at velocity Vr2. However, in absolute terms, the rotor exit velocity is Va2. The velocity triangles are constructed using these various velocity vectors. Velocity triangles can be constructed at any section through the blading, but are usually shown at the mean stage radius.

g. Explain the consideration of process systems parameters (e.g., pressure, temperature, flow, etc.), instrument compatibility (e.g., range, accuracy, response time, sensitivity, reliability), role of safety functions stated in the documented safety analysis (DSA), (e.g., set points, process safety limits, control room displays, etc.), while selecting instruments for I&C systems design.

Pressure

The following is taken from Wikipedia, *Pressure*.

Pressure is the ratio of force to the area over which that force is distributed. In other words, pressure is force per unit area, applied in a direction perpendicular to the surface of an object. Gauge pressure is the pressure relative to the local atmospheric or ambient pressure. While pressure may be measured in any unit of force divided by any unit of area, the International System of Units (SI) unit of pressure is called the pascal (Pa) after the seventeenth-century philosopher and scientist Blaise Pascal. A pressure of 1 Pa is small; it equals approximately the pressure exerted by a dollar bill resting flat on a table. Everyday pressures are often stated in kilopascals (1 kPa = 1000 Pa).

Temperature

The following is taken from Wikipedia, *Temperature Measurem*ents.

Many methods have been developed for measuring temperature. Most of these rely on measuring some physical property of a working material that varies with temperature. One of the most common devices for measuring temperature is the glass thermometer. This consists of a glass tube filled with mercury or some other liquid, which acts as the working fluid. Temperature increase causes the fluid to expand, so the temperature can be determined by measuring the volume of the fluid. Such thermometers are usually calibrated so that one can read the temperature simply by observing the level of the fluid in the thermometer. Another type of thermometer that is not really used much in practice, but is important from a theoretical standpoint, is the gas thermometer.

Other important devices for measuring temperature include

- thermocouples
- thermistors
- RTDs
- pyrometers
- langmuir probes (for electron temperature of a plasma)
- infrared thermometers
- other thermometers

Flow

The following is taken from Wikipedia, *Volumetric Flow Rate*.

In physics and engineering, particularly fluid dynamics and hydrometry, the volumetric flow rate is the volume of fluid that passes through a given surface per unit time. The SI unit is $m^3 s^{-1}$ (cubic meters per second). In US Customary Units and British Imperial Units, volumetric flow rate is often expressed as ft^3/s (cubic feet per second). It is usually represented by the symbol Q.

Density

The following is taken from Wikipedia, *Density*.

The mass density or density of a material is its mass per unit volume. The symbol most often used for density is ρ (the lower case Greek letter rho). Mathematically, density is defined as mass divided by volume:

$$\rho = \frac{m}{V},$$

where ρ is the density, m is the mass, and V is the volume. In some cases (for instance, in the United States oil and gas industry), density is also defined as its weight per unit volume, although this quantity is more properly called specific weight.

Different materials usually have different densities, so density is an important concept regarding buoyancy, purity, and packaging. Osmium and iridium are the densest known elements at standard conditions for temperature and pressure but not the densest materials.

Less dense fluids float on more dense fluids if they do not mix. This concept can be extended, with some care, to less dense solids floating on more dense fluids. If the average density (including any air below the waterline) of an object is less than water's, it will float in water, and if it is more than water's, it will sink in water.

In some cases, density is expressed as the dimensionless quantities specific gravity or relative density, in which case it is expressed in multiples of the density of some other standard material, usually water or air/gas. (For example, a specific gravity less than one means that the substance floats in water.)

The mass density of a material varies with temperature and pressure. Increasing the pressure on an object decreases the volume of the object and therefore increases its density. Increasing the temperature of a substance decreases its density by increasing the volume of that substance. In most materials, heating the bottom of a fluid results in convection of the heat from bottom to top of the fluid due to the decrease of the density of the heated fluid. This causes it to rise relative to more dense unheated material.

The reciprocal of the density of a substance is called its specific volume, a representation commonly used in thermodynamics. Density is an intensive property in that increasing the amount of a substance does not increase its density; rather it increases its mass.

Viscosity

The following is taken from Wikipedia, *Viscosity*.

Viscosity is a measure of the resistance of a fluid that is being deformed by either shear stress or tensile stress. In everyday terms, viscosity is thickness or internal friction. Thus, water is thin, having a lower viscosity, while honey is thick, having a higher viscosity. The less viscous the fluid is, the greater its ease of movement (fluidity).

Viscosity describes a fluid's internal resistance to flow and may be thought of as a measure of fluid friction. For example, high-viscosity felsic magma will create a tall, steep stratovolcano, because it cannot flow far before it cools, while low-viscosity mafic lava will create a wide, shallow-sloped shield volcano.

With the exception of superfluids, all real fluids have some resistance to stress and therefore are viscous. A fluid that has no resistance to shear stress is known as an ideal fluid or inviscid fluid. In common usage, a liquid with the viscosity less than water is known as a mobile liquid, while a substance with a viscosity substantially greater than water is simply called a viscous liquid.

Role of Safety Function in the Documented Safety Analysis (DSA)

The following is taken from DOE-STD-3009-94.

The following sections are included in the DSA:

- The criticality instrumentation section summarizes the criticality alarm system and detection systems used to mitigate exposures from a criticality event. A summary of the methods and procedures used to determine the placement of the monitoring equipment and the selection of the equipment functions and sensitivity is included.

- The radiological protection instrumentation section summarizes plans and procedures governing radiation protection instrumentation. Such instrumentation, whether fixed, portable, or laboratory use, includes instruments for radiation and contamination surveys; sampling; area radiation monitoring; and personnel monitoring during normal operations and accidents. Selection and placement criteria for technical equipment and instrumentation, and types of detectors and monitors, as well as their quantity, sensitivity, and range are included. This section also summarizes plans and procedures for control of calibration processes and for quality assurance (QA) for calibration and maintenance.
- The hazardous material protection section summarizes plans and procedures governing hazardous protection instrumentation. Such instrumentation, whether fixed, portable, or laboratory use, includes instruments for hazardous material and contamination surveys; sampling; area hazardous material monitoring; and personnel monitoring during normal operations and accidents. The summary selection and placement criteria for technical equipment and instrumentation, and types of detectors and monitors, as well as their quantity, sensitivity, and range are included. This section also summarizes plans and procedures for control of calibration processes and for QA for calibration and maintenance.

The DSA also provides the basis and identifies information sufficient to derive safety limits (SLs), limiting control settings (LCSs), and limiting conditions for operation (LCOs) to support the facility technical safety requirement (TSR) documentation required by 10 CFR 830.205, "Technical Safety Requirements." SLs, if used, are reserved for a small set of extremely significant features that prevent potentially major offsite impact. LCSs are developed for any SL that is protected by an automatic device with setpoints.

LCSs/LCOs act to keep normal operating conditions below the SLs and are developed for each SL identified, thereby providing a margin of safety. Most LCOs are assigned without an accompanying SL.

Generally SLs are applicable only for protection of passive barriers as close to the accident source as possible whose failure, due to the occurrence of a specific event, will result in exceeding the evaluation guideline. Mitigation of releases is generally not amenable to useful definition of SLs. For example, a ventilation system directing airflow through HEPA filters to keep offsite radiological dose below the evaluation guideline during an accident is mitigative and is more appropriately covered by a LCO. Temporary loss of its function during normal operations does not initiate a significant hazardous material release. An LCO on the system would identify the specific responses necessary to compensate for the loss of safety function. Control of the ventilation system via an SL would be academic for preventing accidents that the ventilation system only mitigates. In contrast, consider a tank that acts as a barrier, preventing an uncontrolled release of hazardous material that could exceed the evaluation guideline without ventilation mitigation. If that tank could experience a hydrogen explosion and rupture, then the tank hydrogen concentration may warrant coverage by an SL.

h. Explain basic I&C systems installation requirements, such as design consideration for the installation of sensing lines, use of valve manifolds, accessibility for maintenance and calibration, etc.

Installation of Sensing Lines

The following is taken from Los Alamos National Laboratory, *LANL Engineering Standards Manual ISD 341-2.*

Instrument sensing lines should be installed in accordance with the guidance presented in *LANL Engineering Standards Manual ISD 341.2*. The safety classification of piping for instrument tubing systems should be, at a minimum, consistent with the requirements of the process system to which the instrument is connected.

Sensing lines should not be installed in a manner that would interfere with or prevent maintenance and/or operational activities. Minimum headroom clearance of known and identified passageways should be 7 feet.

Whenever practical, sensing lines should be routed along walls, columns, or ceilings, avoiding open or exposed areas. Structural channels or a track should be installed to protect sensing lines in exposed locations subject to accidental crushing or damage. This type of protection, however, should not render the tubing and fittings inaccessible.

Instrument sensing lines should be routed separately from process lines and equipment where vibration, abnormal heat, or stress could affect the lines. Tubing and piping that must be connected to vibrating equipment should be fabricated with adequate flexibility.

Instrument sensing lines should not come in contact with structural steel and concrete surfaces of building members. In no case should tubing be installed in direct contact with painted or unpainted concrete surfaces, except for penetrations requiring closure. Grout should only be used for tubing with temperatures below 200°F.

Instrument sensing lines routed through penetrations, shield walls, or other barriers where visual contact is impaired or lost, should be labeled with a permanent tag attached securely on each side of that barrier displaying the corresponding instrument identifier.

The spacing around sensing lines should always be wide enough to allow each tube to expand independently at all turns without striking adjacent tubes or other equipment.

Heat tracing should be used for sensing lines containing liquid that may freeze or become viscous, or wet gas from which moisture may condense. The heat tracing should provide enough heat to prevent freezing or condensation, but not great enough to boil the liquid in the sensing line.

Sensing lines should have continuous slope to promote their being kept either full or free of fluid. The preferred slope is 1 inch per foot, however, 1/4 inch per foot is acceptable. For instruments sensing steam at pressures up to 20 pounds per square inch, absolute (psia), the instrument lines should slope a minimum of 2 inches per foot. Minimum slope will begin after the root valve and terminate at the instrument valve inlet. The sensing lines may be

level through and on each side of a valve manifold or instrument connection shut off valve for a distance of up to 4 inches. Instrument sensing lines may be level through and on each horizontal leg of a vertically oriented tee or cross connection for a distance of up to 4 inches, and through a penetration for a total cumulative length of 12 inches outside the ends of each penetration.

Bends, rather than tube or pipe fittings, should be used to change the direction of sensing lines. The cold bending method is advised for all bends. A minimum bend radius of at least two and one quarter (2 1/4) times the tubing outside diameter should be employed for bends in stainless steel tubing and copper tubing. The minimum bend radius for capillary tubing, aluminum, and plastic tubing should be per manufacturer recommendations.

Where fittings must be used, and an installation detail document specifies the size and type of fitting, a combination of fittings of other sizes may be substituted if the specified part is unavailable or it is more convenient to use the combination. The fittings must, however, be of the same equivalent type and produce the same or better overall effect. A weld fitting may replace a threaded or flareless joint; however, a threaded or flareless connection should not be used if welded fittings are required. Flareless fittings should be installed using the manufacturer's assembly instructions.

For threaded connections of stainless steel to stainless steel, lubrication should be applied to prevent seizing and galling. Low or no chloride content lubricants should be used with stainless steel. Although Teflon tape is allowed in many applications, it should not be used as a sealant or lubricant on threaded instrument connections. The use of compound or lubricant on threads should consider the potential reaction with either the service fluid or the piping material.

Sensing lines should be blown clear of any foreign material with clean, oil free, dry air or nitrogen before the system is placed in operation. Demineralized water may be used to flush tubing, provided the process system to which the tubing is connected will also be flushed or hydro-tested with water in accordance with applicable construction procedures. Open lines, fittings, or valves should be sealed after being blown clear. Instrument tubing between the manifold valve and the instrument is not required to be blown down or flushed if visual inspection is performed prior to final connection and tightening of fittings.

Capillary tubes sealed to the instrument by the manufacturer should not be opened or cut during or after installation unless specifically required by the installation drawing or manufacturer's instruction. Slope requirements do not apply to capillary tubing. Manufacturer's installation requirements, including those relating to minimum bend radius, should be followed. Excess lengths of capillary tubing should be neatly coiled in protected enclosures. The maximum amount of unprotected capillary should be no more than 6 inches at any one location, except at capillary enclosures, process connections, instrument connections, and penetrations. At the entrance and exit of capillary enclosures, process connections and instrument connections, the maximum unprotected capillary should be 18 inches. Capillaries in trays should be tied down or clamped every three feet. At the entrance and exit of penetrations, the maximum unprotected capillary should be 12 inches.

Primary sensing lines at local panels and racks should be neatly arranged with easy access to test, drain, and vent connections, instruments valves, and manifold. Primary tubing between the instrument valve or manifold and the instrument should be arranged in accordance with the vendor's instruction and with adequate flexibility to avoid undue strain to the instruments.

Use of Valve Manifolds

The following is taken from Instrumentation and Process Control, *Valve Manifold for Pressure Instrument.*

A valve manifold is a standard accessory for pressure transmitters and differential pressure transmitters. Providing a valve manifold in the instrument allows a calibration or change to the instrument without the necessity of plant shutdown. There are three types of valve manifolds: 2-way valve manifold, 3-way valve manifold, and 5-way valve manifold.

A 2-way valve manifold is used for pressure transmitters only. The typical 2-way valve manifold consists of 1 block valve and 1 drain or test valve. To calibrate the pressure transmitter, close the block valve and open the drain valve. Then connect the drain valve to the pressure generator to test the pressure.

A 3-way valve manifold is used for a differential pressure transmitter. The typical 3-way valve manifold consists of 2 block valves and 1 equalizer valve. To check the zero of the differential pressure transmitter, close the block valve and open the equalizing valve. The 3-valve manifold is rarely used in the oil and gas industries—especially on offshore platforms—due to the absence of a test connection. Some manufacturers have modified the 3-valve manifold by providing a plugged test connection, but in general there is no test connection available.

Like the 3-way valve manifold, the 5-way valve manifold is also used for a differential pressure transmitter. The typical 5-way valve manifold consists of 2 block valves, 1 equalizer valve, and 2 vent or test valves. To check the zero of the transmitter, close the block valve and open the equalizing valve. To calibrate the transmitter for 3 or 5 point calibration, after the pressure is equalized, connect the test valve to a pressure generator. This 5-way valve manifold is the most common valve manifold for a differential pressure transmitter.

i. Explain how process chemistry parameters can apply to I&C system design (e.g., pH, conductivity, turbidity, moisture, humidity, hydrogen, oxygen, chlorine, etc.).

pH

The following is taken from Omega Engineering, *pH Control: A Magical Mystery Tour*.

Systems for pH control are characterized by extreme rangeability and sensitivity, and are also subject to difficulties arising from contact between measuring electrodes and hostile fluids. Case histories of representative installations show that success in implementing these control systems depends not only on assessing the complexity of the loop and selecting a control strategy, but also on recognizing and avoiding pitfalls while specifying and installing instrumentation, equipment, and piping.

One basic source of difficulty is that the pH scale corresponds to hydrogen ion concentrations from 100 to 10^{-14} moles per liter. No other common measurement covers such a tremendous range. Another intrinsic constraint is that measuring electrodes can respond to changes as small as 0.001 pH, so instruments can track hydrogen ion concentration changes as small as $5x10^{-10}$ moles per liter at 7 pH. No other common measurement has such tremendous sensitivity.

The implications of such great rangeability and sensitivity can be illustrated by considering a continuous feedback neutralization system for a strong acid and a strong base. The reagent flow should essentially be proportional to the difference between the hydrogen ion concentration of the process fluid and the set point. A reagent control valve must therefore have a rangeability greater than 10,000,000:1 for a set point of 7 pH when the incoming stream fluctuates between 0 and 7 pH. Moreover, uncertainties in the control valve stroke translate directly into pH errors, such that hysteresis of only 0.00005 percent can cause an offset of 1 pH for a 7 pH set point.

Conductivity

The following is taken from Radiometer Analytical, *Conductivity Theory and Practice*.

Conductivity measurement is an extremely widespread and useful method, especially for quality control purposes.

Surveillance of feedwater purity, control of drinking water and process water quality, estimation of the total number of ions in a solution, or direct measurement of components in process solutions can all be performed using conductivity measurements.

The high reliability and sensitivity, and relatively low cost, of conductivity instrumentation make it a potential primary parameter of any good monitoring program. Some applications are measured in units of resistivity, the inverse of conductivity. Other applications require the measurement of total dissolved solids, which is related to conductivity by a factor dependent upon the level and type of ions present.

Conductivity measurements cover a wide range of solution conductivity from pure water at less than $1x10^{-7}$ Siemens (S)/cubic meter (cm) to values of greater than 1 S/cm for concentrated solutions.

In general, the measurement of conductivity is a rapid and inexpensive way to determine the ionic strength of a solution. However, it is a nonspecific technique, unable to distinguish between different types of ions, giving instead a reading that is proportional to the combined effect of all the ions present.

Conductivity is the ability of a solution, a metal, or a gas to pass an electric current. In solutions, the current is carried by cations and anions; in metals, it is carried by electrons.

How well a solution conducts electricity depends on a number of factors:

- Concentration
- Mobility of ions
- Valence of ions
- Temperature

All substances possess some degree of conductivity. In aqueous solutions the level of ionic strength varies from the low conductivity of ultra pure water to the high conductivity of concentrated chemical samples.

Conductivity may be measured by applying an alternating electrical current (I) to two electrodes immersed in a solution and measuring the resulting voltage (V). During this process, the cations migrate to the negative electrode, the anions to the positive electrode and the solution acts as an electrical conductor.

Conductivity is typically measured in aqueous solutions of electrolytes. Electrolytes are substances containing ions, i.e., solutions of ionic salts or of compounds that ionize in solution. The ions formed in solution are responsible for carrying the electric current. Electrolytes include acids, bases, and salts and can be either strong or weak. Most conductive solutions measured are aqueous solutions, as water has the capability of stabilizing the ions formed by a process called solvation.

STRONG ELECTROLYTES

Strong electrolytes are substances that are fully ionized in solution. As a result, the concentration of ions in solution is proportional to the concentration of the electrolyte added. They include ionic solids and strong acids, for example hydrochloric acid (HCl).

Solutions of strong electrolytes conduct electricity because the positive and negative ions can migrate largely independently under the influence of an electric field.

WEAK ELECTROLYTES

Weak electrolytes are substances that are not fully ionized in solution. For example, acetic acid partially dissociates into acetate ions and hydrogen ions, so that an acetic acid solution contains both molecules and ions. A solution of a weak electrolyte can conduct electricity, but usually not as well as a strong electrolyte solution because there are fewer ions to carry the charge from one electrode to the other.

Turbidity

The following is taken from *Turbidity Instrumentation - An Overview of Today's Available Technology*, by Mike Sadar

In its simplest terms, turbidity is the optical measurement of scattered light resulting from the interaction of incident light with particulate material in a liquid sample. Typically, the liquid is a water sample and the suspended material causing the light to be scattered can be composed of a broad variety of components. Examples of particles include suspended solids such as silt, clay, algae, organic matter, various microorganisms, colloidal material, and even large molecules that are dissolved in the sample such as tannins and lignins.

Particulate matter in a water sample will cause the incident light beam to be scattered in directions other than a straight line through the sample. The scattered light that returns to the detector causes a response correlating to the level of turbidity in the sample. A higher level of scattered light reaching the detector results in a higher turbidity value.

The measurement of turbidity is not directly related to a specific number of particles or to particle shape. As a result, turbidity has historically been seen as a qualitative measurement. In an attempt to make turbidity methods more quantitative, standards and standardization methods can be used.

Although interferences have a dramatic and ever-present impact on turbidity measurements, the type and magnitude of the interference often depends on the turbidity level being measured. When performing low-level turbidity measurements, primary interferences are stray light, bubbles, ambient light, and contamination. For high turbidity testing, a greater impact from color, particle absorption, and particle density is seen.

In an attempt to minimize interferences, several new turbidity measurement methods have been developed. Many of these methods have been designed to maximize sensitivity and minimize the effects of interferences. It is important to understand and identify the prominent interferences in the sample stream. Doing so can help identify the instrument design that will provide the most accurate and "interference-free" measurement. Instrument designs can be categorized as shown in table 4.

Table 4. Summary of Instrument Design

Design	Prominent Feature and Application
Nephelometric non-ratio	White light turbidimeters—Comply with U.S. Environmental Protection Agency EPA 180.1, *Determination of Turbidity by Nephelometry*, for low level monitoring.
Ratio White Light turbidimeters	Comply with the Long Term 1 Enhanced Surface Water Treatment Rule and standard method. Use a nephelometric detector as the primary detector, but contain other detectors to minimize interference. Can be used for low and high level measurement.
Nephelometric near IR turbidimeters	Comply with International Organization for Standardization (ISO) 7027, *Water Quality: Determination of Turbidity*—The wavelength (860-890-nm) is less susceptible to color interferences. Good for samples with color and good for low level monitoring.
Nephelometric Near IR turbidimeters	GLI method 2, ISO 7027 and EPA approved. Compliant and contain a ratio algorithm to monitor and compensate for interferences.
Surface Scatter Turbidimeters	Turbidity is determined through light scatter from or near the surface of a sample. The detection angle is still nephelometric, but interferences are not as substantial as nephelometric non-ratio measurements. Primarily used in high-level turbidity applications.
Back Scatter/Ratio Technology	Backscatter detection for high levels and nephelometric detection for low levels. Backscatter is common.
Light attenuation in formazin attenuation units	Use a transmitted detector (180 degrees to the incident light beam). Most susceptible to interferences, best applied at medium turbidity levels (5-1000).

Source: Turbidity Instrumentation - An Overview of Today's Available Technology

The units for reporting turbidity are commonly the same, no matter which turbidimeter design is being used. Depending on the interferences present (especially in high level reporting), the instrument design can have a dramatic effect on the reported result. For example, if a high level sample is measured with a white light non-ratio instrument, the results will be dramatically different from a reading obtained using a 4-beam, IR ratio method. One solution is to apply the correct measurement units to the measured value to help rationalize the results.

Moisture

The following is taken from MyChemE, *Design Guides*, "Designing Compressed Air Systems".

It is vital to remove moisture from compressed air systems; otherwise, water will condense out causing blockages in pipelines and in equipment. This is particularly important for instrument air. Compressed air used to operate process instruments should be dried to a dew point of between -20ºC and - 40ºC.

Process air can be supplied at higher moisture contents. Typically it should be dried to a dew point of about 0ºC. This should be sufficient to prevent condensate collecting in the distribution pipe work, except in very cold climates, where lower moisture levels may be needed.

Humidity

The following is taken from GlobalSpec, *Humidity Measurement Instruments Information*.

Humidity measurement instruments and transducers test for absolute humidity, relative humidity, or dew point in air. Humidity measurement instruments typically operate in a range, from 0 to 100 percent humidity. They are sometimes combined with other sensing devices such as temperature sensors.

Humidity measurement instruments and sensors can assess a number of different factors. Absolute humidity, expressed as grams of water vapor per cubic meter volume of air, is a measure of the actual amount of water vapor or moisture in the air, regardless of the air's temperature. Relative humidity, expressed as a percent, also measures water vapor, but relative to the temperature of the air. The dew point temperature, which provides a measure of the actual amount of water vapor in the air, is the temperature to which the air must be cooled in order for the air to be saturated and dew to form. Due to the intertwining of atmospheric measurements, humidity measurement instruments are sometimes equipped with pressure and temperature sensors as well. Three main applications for humidity measurement instruments are judging moisture in gases or air, bulk solids or powders, or in fuels or other liquids.

There are many technologies for humidity measurement instruments. Capacitive or dielectric instruments include a material that absorbs moisture, which changes its dielectric properties and enhances its capacitance. Chilled mirror technology uses a mirror that is chilled to the point that moisture starts to condense on it. This temperature is the dew point. In electrolytic technology, moisture is proportional to the current needed to electrolyze it from a desiccant.

In resistivity or impedance style sensors, a material absorbs moisture, which changes its resistivity or impedance. In strain gage instruments, a material absorbs water, expands, and is measured with a strain gage. Psychrometers, often called wet/dry bulbs, measure relative humidity by gauging the temperature difference between two thermometers, one wet and one dry.

One critical specification for these devices is the humidity or moisture range to be measured or the dew point range. Humidity and moisture accuracy is expressed in terms of percentage of measurement. The dew point accuracy (a temperature reading) is expressed as a variance in temperature output.

Outputs from humidity measurement instruments can be analog current, voltage, or frequency; digital, including computer signals; or a switch or an alarm. They can have analog, digital, or video type displays and can have a number of different form factors. They can be standard sensors or transducers, or simple gauges or indicators. They can also be various types of instruments; handheld, bench top, or mounted.

In addition to pressure and temperature compensation, humidity measurement instruments can have a number of features to make them more useful or easier to use. These can include data logging, event triggering, self-testing, self-calibration, and battery power.

Hydrogen

The following is taken from Wikipedia, *Hydrogen*.

Hydrogen can be prepared in several different ways, but economically the most important processes involve removal of hydrogen from hydrocarbons. Commercial bulk hydrogen is usually produced by the steam reforming of natural gas. At high temperatures steam reacts with methane to yield carbon monoxide and H_2:

$CH_4 + H_2O \rightarrow CO + 3\ H_2$

This reaction is favored at low pressures but is nonetheless conducted at high pressures. This is because high-pressure H_2 is the most marketable product and pressure swing adsorption purification systems work better at higher pressures. The product mixture is known as synthesis gas because it is often used directly for the production of methanol and related compounds. Hydrocarbons other than methane can be used to produce synthesis gas with varying product ratios. One of the many complications to this highly optimized technology is the formation of coke or carbon:

$CH_4 \rightarrow C + 2\ H_2$

Consequently, steam reforming typically employs an excess of H_2O. Additional hydrogen can be recovered from the steam by use of carbon monoxide through the water gas shift reaction, especially with an iron oxide catalyst. This reaction is also a common industrial source of carbon dioxide:

$CO + H_2O \rightarrow CO_2 + H_2$

Other important methods for H_2 production include partial oxidation of hydrocarbons:

$2\ CH_4 + O_2 \rightarrow 2\ CO + 4\ H_2$

and the coal reaction, which can serve as a prelude to the shift reaction above:

$C + H_2O \rightarrow CO + H_2$

Hydrogen is sometimes produced and consumed in the same industrial process, without being separated. In the Haber process for the production of ammonia, hydrogen is generated from natural gas. Electrolysis of brine to yield chlorine also produces hydrogen as a co-product.

Oxygen

The following is taken from *Improved Technology for Dissolved Oxygen Measurement* by David M. Gray.

Dissolved oxygen (DO) is undesirable in pure waters for microelectronics manufacturing for several reasons. In the purification itself, there is concern that DO can oxidize ion exchange resins in mixed bed polishers, producing contamination downstream—the justification for an efficient degasifier. There has also been concern that high DO levels support microbiological growth in water systems. In some processes, DO levels influence the oxidation of the active silicon surface during rinse steps and can have a significant impact on chip yields. This can affect the quality of thin gate oxide, quality of polysilicon and dielectric thin film, and selective chemical vapor deposition and atomic layer epitaxy. Industry guidelines have set DO limits for ultrapure water used for various microelectronics line widths.

Deionized water monitoring and control for these critical processes requires accurate and reliable DO measurement at low concentrations. Since there is a variety of instrumentation available for this purpose, such equipment must be selected, operated, and maintained carefully to obtain optimum results.

DO sensors are electrochemical devices that take advantage of the gas permeability of polymer membranes to separate the heart of the sensor from the sample. This separation provides a controlled environment for the electrodes and electrolytes while allowing oxygen to enter from the sample and react. It keeps the electrochemistry contained and clean.

The diffusion rate of oxygen through a membrane is proportional to the partial pressure of oxygen in the sample. Of course the membrane material and thickness also affect the diffusion rate, but they are fixed, and those properties are accommodated in calibration.

The oxygen that permeates the membrane reacts at the cathode, producing a current in direct proportion to the quantity of oxygen. That current is the measurement signal that matches the oxygen partial pressure and the concentration of DO, at least at constant temperature.

To derive a concentration measurement from partial pressure with varying temperature, the signal must be compensated; that is, the DO concentration in water that a partial pressure represents depends on temperature. The sensor’s temperature signal is used by the instrument microprocessor to temperature compensate the measurement.

Chlorine

The following is taken from Wikipedia, *Chlorine*.

Source: Wikipedia, Chlorine

Figure 49. Chlorine induced cracking

Chlorine, due to its powerful oxidizing properties, is widely used for purifying water; especially potable water supplies and water used in swimming pools. But, several catastrophic collapses of swimming pool ceilings have occurred due to chlorine induced stress corrosion cracking of stainless steel rods used to suspend them. Some polymers, including acetal resin and polybutene, are also sensitive to chlorine attack. Both materials were used in hot and cold water domestic supplies, and stress corrosion cracking caused widespread failures in the USA in the 1980s and 1990s. Figure 49 on the right shows an acetal joint in a water supply system, which, when it fractured, caused substantial physical damage to computers in the labs below the supply. The cracks started at injection molding defects in the joint and grew slowly until finally triggered. The fracture surface shows iron and calcium salts that were deposited in the leaking joint from the water supply before failure.

Some organochlorine compounds are serious pollutants. These are produced either as by-products of industrial processes or as end products which are persistent in the environment, such as certain chlorinated pesticides and chlorofluorocarbons. Chlorine is added both to pesticides and pharmaceuticals to make the molecules more resistant to enzymatic degradation by bacteria, insects, and mammals, but this property also has the effect of prolonging the residence time of these compounds when they enter the environment. In this respect chlorinated organics have some resemblance to fluorinated organics.

6. I&C personnel must demonstrate a familiarity level knowledge of specialty instrumentation and its applications.

a. Explain the functional and safety requirements (e.g., as stated in DSA, "System Design Specification," etc.,) and applicability of the following specialty instruments:

- **Radiation monitors (e.g., CAMs, portal monitors, etc.)**
- **Gas analyzers**
- **Effluent monitors**
- **Refractometer**

Functional Requirements

The following is taken from Wikipedia, *Functional Requirements*.

In software engineering, a functional requirement defines a function of a software system or its component. A function is described as a set of inputs, the behavior, and outputs. Functional requirements may be calculations, technical details, data manipulation and

processing, and other specific functionality that define what a system is supposed to accomplish. Behavioral requirements describing all the cases where the system uses the functional requirements are captured in use cases. Functional requirements are supported by non-functional requirements, which impose constraints on the design or implementation, such as performance requirements, security, or reliability. Generally, functional requirements are expressed in the form "system must do" requirement, while non-functional requirements are "system shall be" requirement. The plan for implementing functional requirements is detailed in the system design. The plan for implementing non-functional requirements is detailed in the system architecture.

As defined in requirements engineering, functional requirements specify particular results of a system. This should be contrasted with non-functional requirements**,** which specify overall characteristics such as cost and reliability. Functional requirements drive the application architecture of a system, while non-functional requirements drive the technical architecture of a system.

Video 17. Functional requirements

http://www.bing.com/videos/search?q=functional+requirements&view=detail&mid=6A4FF01DF01A84563FAF6A4FF01DF01A84563FAF&first=0

Safety Requirements

The following is taken from Wikipedia, *Safety Instrumented System*.

A safety instrumented system (SIS) consists of an engineered set of hardware and software controls which are especially used on critical process systems. A critical process system can be identified as one which, if an operational problem occurs once running, may need to be put into a safe state to avoid adverse environment, safety, and health (ES&H) consequences. Examples of critical processes have been common since the beginning of the industrial age. One of the more well known critical processes is the operation of a steam boiler. Critical parts of the process would include the lighting of the burners, controlling the level of water in the drum, and controlling the steam pressure.

An SIS is engineered to perform specific control functions to failsafe or maintain safe operation of a process when unacceptable or dangerous conditions occur. Safety instrumented systems must be independent from all other control systems that govern the same equipment to ensure SIS functionality is not compromised. SIS is composed of the same types of control elements as a basic process control system (BPCS). However, all of the control elements in an SIS are dedicated solely to the proper functioning of the SIS.

The specific control functions performed by an SIS are called safety instrumented functions. They are implemented as part of an overall risk reduction strategy that is intended to eliminate the likelihood of a previously identified ES&H event that could range from minor equipment damage up to an event involving an uncontrolled catastrophic release of energy and/or materials.

A safe state is a process condition, whether the process is operating or shutdown, which keeps a hazardous ES&H event from occurring. The safe state must be achieved in a timely manner or within the process safety time.

A formal process of hazard identification is performed by the project team engineers and other experts at the completion of the engineering design phase of each section of the process, known as a unit of operation. This team performs a systematic, rigorous, procedural review of each point of possible hazard, or node, in the completed engineering design. This review and its resulting documentation is called a HAZOP study. Safety integrity levels are defined for the SISs. Based on HAZOP study recommendations and the SIL rating of the SISs, the engineering, the BPCS, and the SISs designs for each unit operation can be finalized.

The correct operation of an SIS requires a series of equipment to function properly. It must have sensors capable of detecting abnormal operating conditions, such as high flow, low level, or incorrect valve positioning. A logic solver is required to receive the sensor input signal(s), make appropriate decisions based on the nature of the signal(s), and change its outputs according to user-defined logic. The logic solver may use electrical, electronic, or programmable electronic equipment, such as relays, trip amplifiers, or programmable logic controllers. Next, the change of the logic solver output(s) results in the final element(s) taking action on the process (e.g., closing a valve) to bring it to a safe state. Support systems, such as power, instrument air, and communications, are generally required for SIS operation. The support systems should be designed to provide the required integrity and reliability.

The International Electrotechnical Commission (IEC) 61511, *Functional Safety—Safety Instrumented Systems for the Process Industry Sector—Part 1: Framework, Definitions, System, Hardware and Software Requirements*, was published in 2003 to provide guidance to end-users on the application of SISs in the process industries.

Radiation Monitors

The following is taken from DOE-STD-1098-99.

Area radiation monitors should be installed in frequently occupied locations with the potential for unexpected increases in dose rates and in remote locations where there is a need for local indication of dose rates prior to personnel entry.

Area radiation monitors should not be substituted for radiation exposure surveys in characterizing a workplace.

The need for and placement of area radiation monitors should be documented and assessed when changes to facilities, systems, or equipment occur.

Area radiation monitors should be tested at least quarterly to verify audible alarm system operability and audibility under ambient working conditions and operability of visual alarms when so equipped.

If installed instrumentation is removed from service for maintenance or calibration, a radiation monitoring program providing similar detection capability should be maintained, consistent with the potential for unexpected increases in radiation dose rates.

Where an area radiation monitor is incorporated into a safety interlock system, the circuitry should be such that a failure of the monitor either prevents entry into the area or prevents operation of the radiation producing device. If the circuitry is required to ensure compliance with the high radiation area access control requirements of 10 CFR 835.502, "High and Very High Radiation Areas," then the circuitry shall be fail-safe.

Video 18. Radiation monitors
http://wn.com/Radiation_Monitoring_ALARMS

Gas Analyzers

The following is taken from Wikipedia, *Residual Gas Analyzers*.

A residual gas analyzer (RGA) is a small, usually rugged, mass spectrometer, typically designed for process control and contamination monitoring in vacuum systems. Using quadrupole technology, two implementations exist; employing either an open ion source or a closed ion source. RGAs may be found in high vacuum applications such as research chambers, surface science setups, accelerators, scanning microscopes, etc. RGAs are used in most cases to monitor the quality of the vacuum and easily detect minute traces of impurities in the low-pressure gas environment. These impurities can be measured down to 10^{-14} Torr levels, possessing sub-ppm detectability in the absence of background interferences.

RGAs would also be used as sensitive in-situ, helium leak detectors. With vacuum systems pumped down to lower than 10^{-5} Torr—checking of the integrity of the vacuum seals and the quality of the vacuum—air leaks, virtual leaks, and other contaminants at low levels may be detected before a process is initiated.

Effluent Monitors

The following is taken from U.S. Nuclear Regulatory Commission, *Background Information on NRC Effluent and Environmental Monitoring Requirements*.

Radiological environmental monitoring and effluent monitoring at nuclear power plants is required by U.S. Nuclear Regulatory Commission (NRC) regulations. The monitoring of radioactive effluents and the environment around the nuclear power plant is important for normal operations, and in the event of an accident. During normal operations, environmental monitoring verifies the effectiveness of in-plant measures for controlling the release of radioactive materials, and makes sure that the levels of radioactive materials in the environment do not exceed those originally anticipated prior to licensing the plant. For accidents, it allows an additional means for estimating doses to members of the general public.

The principal regulatory basis for requiring environmental monitoring and effluent monitoring at nuclear power plants is contained in general design criteria 60, 61, and 64 of Appendix A of 10 CFR 50, "Domestic Licensing of Production and Utilization Facilities."

The criteria require that a licensee control, monitor, perform radiological evaluations of all releases, document, and report all radiological effluents discharged into the environment.

There is also specific criteria that requires power reactor licensees to keep the public dose from radioactive effluents as low as reasonably achievable (ALARA). The ALARA criteria is contained in Appendix I of 10 CFR 50. This criteria is very clear as to what the NRC expects of power reactors concerning their effluent discharges.

The licensee shall establish an appropriate surveillance and monitoring program to

- provide data on quantities of radioactive material released in liquid and gaseous effluents;
- provide data on measurable levels of radiation and radioactive materials in the environment to evaluate the relationship between quantities of radioactive material released in effluents and resultant radiation doses to individuals from principal pathways of exposure; and
- identify changes in the use of unrestricted areas to permit modifications in monitoring programs for evaluating doses to individuals from principal pathways of exposure.

Results from the environmental and effluent monitoring programs are reviewed by the NRC during routine inspections, and if the data indicate that the relationship between the quantities of effluents and the calculated doses to individuals is significantly different than that assumed in the licensing calculations, then the NRC may modify the allowable quantities in the technical specifications for the nuclear power plant.

Prior to licensing a nuclear power plant, the NRC staff reviews the applicant's proposed radiological environmental program. The applicant conducts a pre-operational program at least two years prior to initial criticality of the reactor. The pre-operational program documents the background levels of direct radiation and concentrations of radionuclides that exist in the environment. It also provides an opportunity for the licensee to train personnel, and to evaluate procedures, equipment, and techniques.

A licensee's pre-operational environmental monitoring program is reviewed by NRC staff in regard to the criteria contained in the NRC's Radiological Assessment Branch Technical Position, Revision 1, November 1979, *An Acceptable Radiological Environmental Monitoring Program*. The branch technical position (BTP) contains an example of an acceptable minimum radiological monitoring program. Highlights of the BTP include monitoring of air at the offsite locations where the highest concentrations of radionuclides are expected; placement of dosimeters in two concentric rings around the plant; water samples upstream and downstream; milk samples at locations where the highest doses are expected; and various food samples. Lower limits of detection for the various types of samples and nuclides are specified.

The operational radiological environmental monitoring program is essentially a continuation of the pre-operational program. The minimum requirements of the program are specified in the radiological effluent technical specifications (RETS) that are required pursuant to 10 CFR 50.36a "Technical Specifications on Effluents from Nuclear Power Reactors." In addition, more detailed information about the program is contained in the licensee's offsite dose

calculational manual, which is referenced in the plant's RETS. The RETS also require that the licensee submit 1) an annual radiological environmental monitoring report that is designed to assess the impact of radiological effluent releases into the environment; and 2) a special report within 30 days of discovery of the event if predetermined levels of radioactivity are exceeded. The NRC also requires that the licensee participate in an interlaboratory comparison program to ensure the accuracy and precision of the licensee's data. The results of licensee's radiological environmental monitoring and effluent release programs are required to be reported annually to the NRC, and are available to the public.

10 CFR 20.1501, "General," requires a licensee to perform a radiological survey to evaluate the radiological hazard from radioactive material in the air, soil, or water.

In appendix I of 10 CFR 50, the NRC imposes specific requirements for nuclear power reactors for airborne and waterborne effluent releases. These requirements are contained in 10 CFR 50.36a and detailed in appendix I to 10 CFR 50.

These requirements are structured to maintain the dose to members of the public from all radioactive effluent releases to levels that are ALARA.

The controls imposed on licensees are not based on the quantity or concentration of radioactive material released, but are based on the calculated dose to members of the public. The licensee's RETS contain the dose values to the maximally exposed member of the public living near a nuclear power plant. They are as follows:

- Gaseous effluents shall not produce doses to offsite air of more than 10 millirads (mrads) from gamma radiation and 20 mrads from beta radiation in a year. Radioiodine, tritium, and particulate radiation in gaseous effluents shall not produce doses to a member of the public of more than 15 millirems (mrems) to the thyroid (or other organ) in a year.
- Liquid effluents shall not produce doses to any member of the public of more than 3 mrems to the total body or 10 mrems to any organ in a year.
- The licensee shall take other measures to reduce offsite doses that cost less than $1000 per person-rem saved.

In addition to the annual doses listed above, the RETS impose controls on the dose to a member of the public in a calendar quarter. They are as follows:

- Gaseous effluents, during any calendar quarter, shall be less than or equal to 5 mrads for gamma radiation and less than or equal to 10 mrads for beta radiation.
- Radioiodine, tritium, and particulate radiation in gaseous effluents, during any calendar quarter, shall be less than or equal to 7.5 mrems to any organ.
- Liquid effluents, during any calendar quarter, shall be limited to less than or equal to 1.5 mrems to the total body and to less than or equal to 5 mrems to any organ.

In addition to the controls imposed by the RETS on the dose to members of the public from radioactive effluents, there are controls on the rate at which radioactive material can be released. These controls, imposed on liquid and gaseous effluents, represent a defense in depth approach to further ensure that radioactive effluents and the resulting doses are ALARA.

Refractometer

The following is taken from Wikipedia, *Traditional Handheld Refractometer*.

Source: Wikipedia, Traditional handheld refractometer

Figure 50. Handheld refractometer

A traditional handheld refractometer is an analog instrument that measures a liquid's refractive index. It works on the critical angle principle: lenses and prisms project a shadow line onto a small glass reticle inside the instrument, which is then viewed by the user through a magnifying eyepiece.

In use, a sample is placed between a measuring prism and a small cover plate. Light traveling through the sample is either passed through to the reticle or totally internally reflected. The net effect is that a shadow line forms between the illuminated area and the dark area. A reading is taken where this shadow line crosses the scale. Because the refractive index is very temperature dependent, it is important to use a refractometer with automatic temperature compensation. Compensation is accomplished through the use of a small bi-metallic strip that moves a lens or prism in response to temperature changes.

Video 19. How to use a refractometer

http://www.bing.com/videos/search?q=refractometer&view=detail&mid=C858EECCBD0CFB5F76F8C858EECCBD0CFB5F76F8&first=0

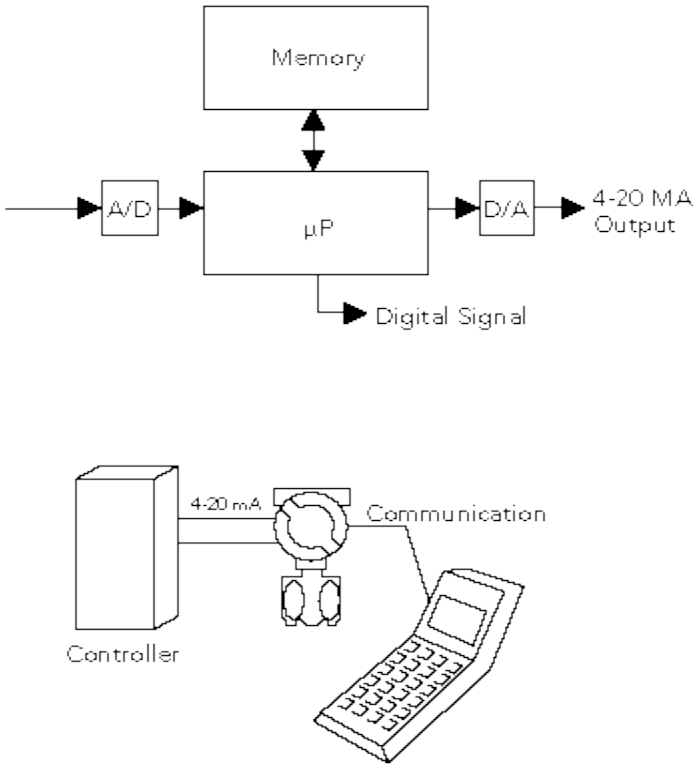
7. I&C personnel must demonstrate a working level knowledge of application of digital systems in I&C systems design.

a. Explain the application of electronics and programmable electronics in I&C systems (e.g., smart transmitters, programmable logic controllers, processors, communication modules, input/output modules, interface modules, power supplies, fieldbus, etc.).

Smart Transmitters

The following is taken from Newcastle University, *Overview of Measurement Systems and Devices*.

A smart transmitter is a microprocessor-based transmitter that can be programmed; has a memory; can perform calculations; can perform self-diagnostics; reports faults; and can be communicated with from a remote location.



Source: Newcastle University, Overview of Measurement Systems and Devices

Figure 51. Smart transmitter

Smart transmitters can convert analog signals to digital signals, making communication swift and easy, and can even send analog and digital signals at the same time.

A smart transmitter has a number of other capabilities as well. For instance, inputs can be varied, as denoted by A/D. If a temperature transmitter is a smart transmitter, it will accept millivolt signals from thermocouples, and resistance signals from RTDs and thermistors.

Components of the smart transmitter are illustrated in the lower figure. The transmitter is built into a housing, about the size of a softball, as seen in figure 51.

The controller takes the output signal from the transmitter and sends it back to the final control element. The communicator is shown on the right.

The communicator is a hand-held interface device that allows digital "instructions" to be delivered to the smart transmitter. Testing, configuring, and supplying or acquiring data are all accomplished through the communicator. The communicator has a display that lets the technician see the input or output information. The communicator can be connected directly to the smart transmitter, or in parallel anywhere on the loop.

CONFIGURATION

Smart transmitters can be configured to meet the demands of the process in which they are used. For example, the same transmitter can be set up to read almost any range or type of thermocouple, RTD, or thermistor; reducing the need for a large number of specific replacement devices.

RE-RANGING

The range that the smart transmitter functions under can be easily changed from a remote location, for example, by the technician in a control room. The technician or the operator has access to any smart device in the loop, and does not even have to be at the transmitter to perform the change. The operator does need to use a communicator, however. A communicator allows the operator to interface with the smart transmitter. The communicator

could be a PC, a programmable logic controller (PLC), or a hand-held device. The type of communicator depends on the manufacturer.

Re-ranging is simple with the smart transmitter; using a communicator, the operator can change from a 100 ohm RTD to a type-J thermocouple just by reprogramming the transmitter. The transmitter responds immediately and changes from measuring resistance to measuring millivoltage.

A smart transmitter will accept a wide range of inputs; for instance, with pressure units, the operator can determine ahead of time whether to use inches of water, inches of mercury, psi, bars, millibars, pascals, or kilopascals.

CHARACTERISTICS

Another characteristic of a smart transmitter is its ability to act as a stand-alone transmitter. In such a capacity, it sends the output signal to a distributed control system or a PLC.

SIGNAL CONDITIONING

Smart transmitters can also perform signal conditioning, scanning the average signal and eliminating any noise spikes. Signals can be delayed (dampened) so that the response does not fluctuate. This is especially useful with a rapidly changing process.

SELF-DIAGNOSIS

Finally, a smart transmitter can diagnose itself and report on any problems in the process. For example, it can report on a circuit board that is not working properly.

SUMMARY OF SMART TRANSMITTER BENEFITS

There are distinct advantages in using a smart transmitter. The most important include ease of installation and communication, self-diagnosis, improved and digital reliability. Smart transmitters are less subject to effects of temperature and humidity than analog devices, and although vibration can still affect them, the effects are far less than with analog devices. Smart transmitters also provide increased accuracy, and because they can replace several different types of devices, using them allows for inventory reduction.

Programmable Logic Controllers

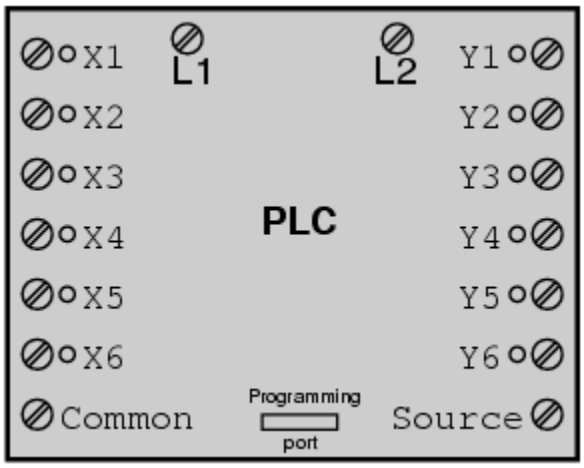
The following is taken from All About Circuits, *Programmable Logic Controllers*.

In the late 1960s, an American company, Bedford Associates, released a computing device they called the MODICON. The acronym meant modular digital controller, and later became the name of a company division devoted to the design, manufacture, and sale of these special-purpose control computers. Other engineering firms developed their own versions of this device, and it eventually came to be known in non-proprietary terms as a PLC, or programmable logic controller. The purpose of a PLC was to directly replace electromechanical relays as logic elements, substituting a solid-state digital computer with a stored program, able to emulate the interconnection of many relays to perform certain logical tasks.

A PLC has many input terminals, through which it interprets high and low logical states from sensors and switches. It also has many output terminals, through which it outputs high and low signals to power lights, solenoids, contactors, small motors, and other devices lending

themselves to on/off control. In an effort to make PLCs easy to program, their programming language was designed to resemble ladder logic diagrams. Thus, an industrial electrician or electrical engineer accustomed to reading ladder logic schematics would feel comfortable programming a PLC to perform the same control functions.

PLCs are industrial computers, and as such their input and output signals are typically 120 volts AC, just like the electromechanical control relays they were designed to replace. Although some PLCs have the ability to input and output low-level DC voltage signals of the magnitude used in logic gate circuits, this is the exception and not the rule.



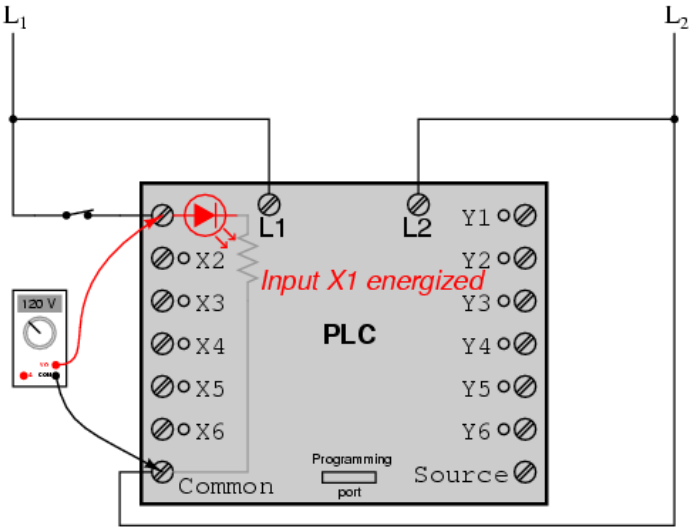
Source: All About Circuits, Programmable Logic Controllers

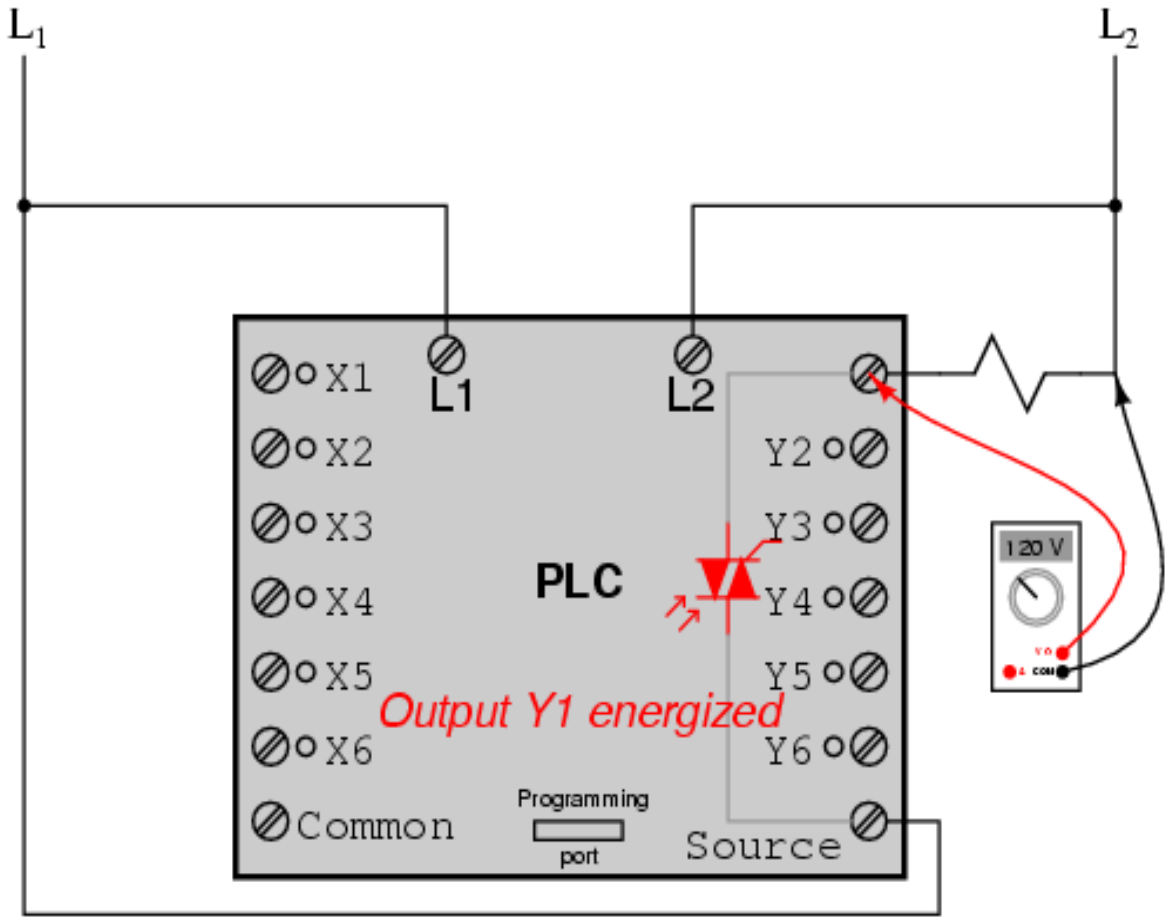
Figure 52. A simple PLC

Signal connection and programming standards vary somewhat between different models of PLC, but they are similar enough to allow a generic introduction to PLC programming here. Figure 52 shows a simple PLC, as it might appear from a front view. Two screw terminals provide connection to 120 volts AC for powering the PLC's internal circuitry, labeled L1 and L2. Six screw terminals on the left-hand side provide connection to input devices, each terminal representing a different input channel with its own X label. The lower-left screw terminal is a common connection, which is generally connected to L2 (neutral) of the 120 VAC power source.

Inside the PLC housing, connected between each input terminal and the common terminal, is an opto-isolator device that provides an electrically isolated high logic signal to the computer's circuitry when there is 120 VAC power applied between the respective input terminal and the common terminal. An indicating light emitting diode (LED) on the front panel of the PLC gives visual indication of an energized input.

Output signals are generated by the PLC's computer circuitry activating a switching device, connecting the source terminal to any of the Y-labeled output terminals. The source terminal, correspondingly, is usually connected to the L1 side of the 120 VAC power source. As with each input, an indicating LED on the front panel of the PLC gives visual indication of an energized output.

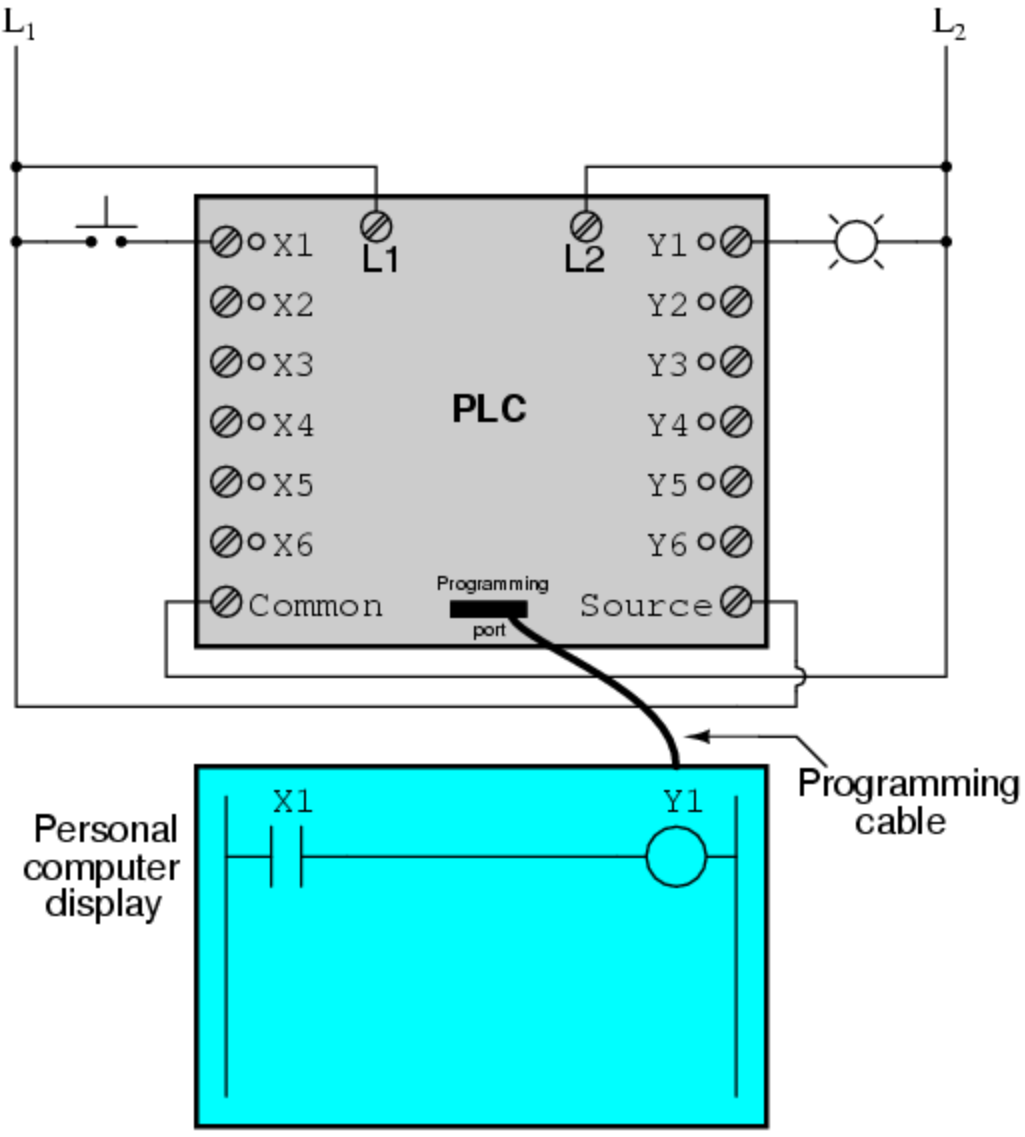




In this way, the PLC is able to interface with real-world devices such as switches and solenoids.

The actual logic of the control system is established inside the PLC by means of a computer program. This program dictates which output gets energized under which input conditions. Although the program itself appears to be a ladder logic diagram, with switch and relay symbols, there are no actual switch contacts or relay coils operating inside the PLC to create the logical relationships between input and output. These are “imaginary” contacts and coils. The program is entered and viewed via a personal computer connected to the PLC’s programming port.

Consider the circuit and PLC program illustrated in figures 53 and 54.

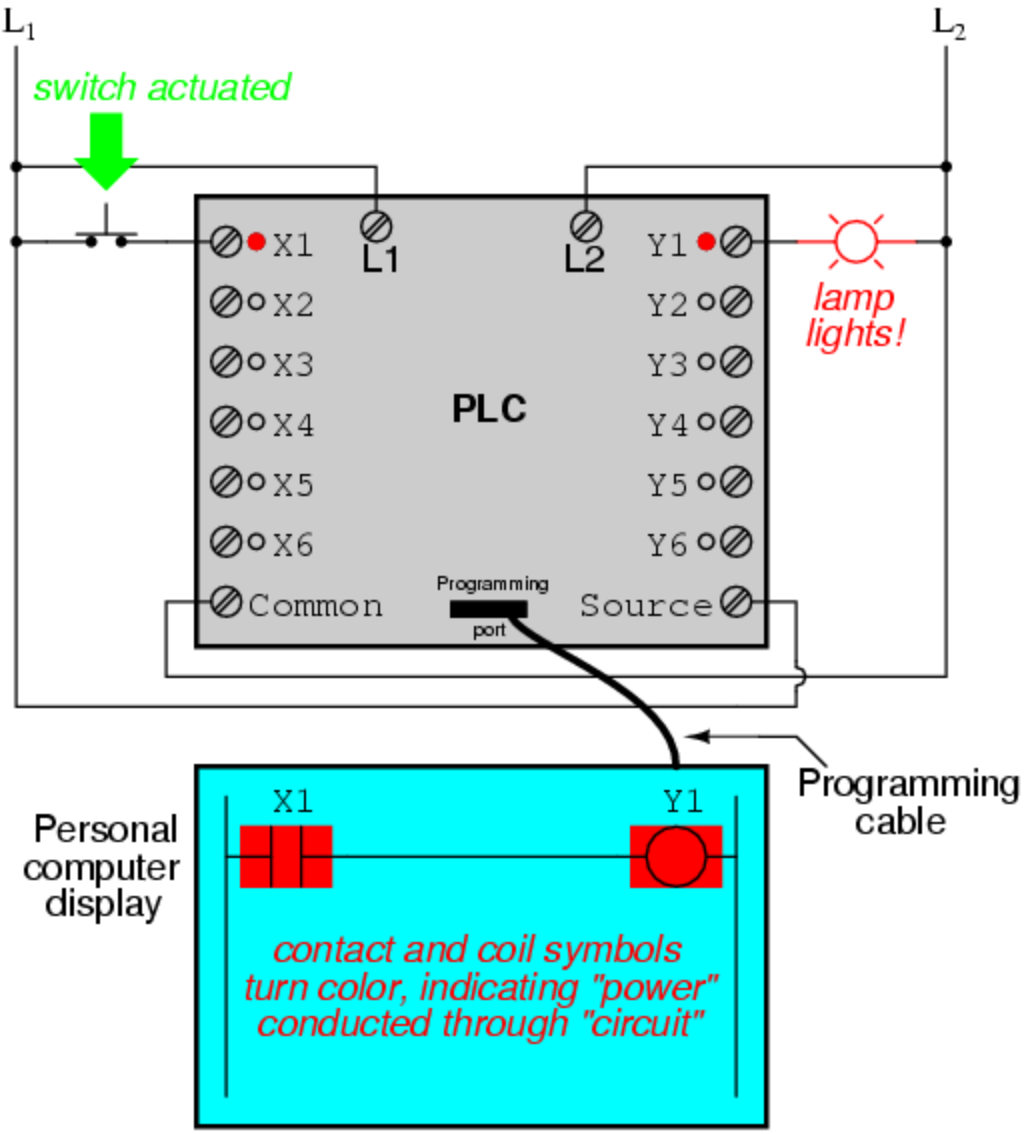


Source: All About Circuits, Programmable Logic Controllers

Figure 53. A circuit and PLC program

When the pushbutton switch is unactuated (unpressed), no power is sent to the X1 input of the PLC. Following the program, which shows a normally-open X1 contact in series with a Y1 coil, no power will be sent to the Y1 coil. Thus, the PLC's Y1 output remains de-energized, and the indicator lamp connected to it remains dark.

If the pushbutton switch is pressed, however, power will be sent to the PLC's X1 input. Any and all X1 contacts appearing in the program will assume the actuated state, as though they were relay contacts actuated by the energizing of a relay coil named X1. In this case, energizing the X1 input will cause the normally-open X1 contact to close, sending power to the Y1 coil. When the Y1 coil of the program energizes, the real Y1 output will become energized, lighting up the lamp connected to it.



Source: All About Circuits, Programmable Logic Controllers

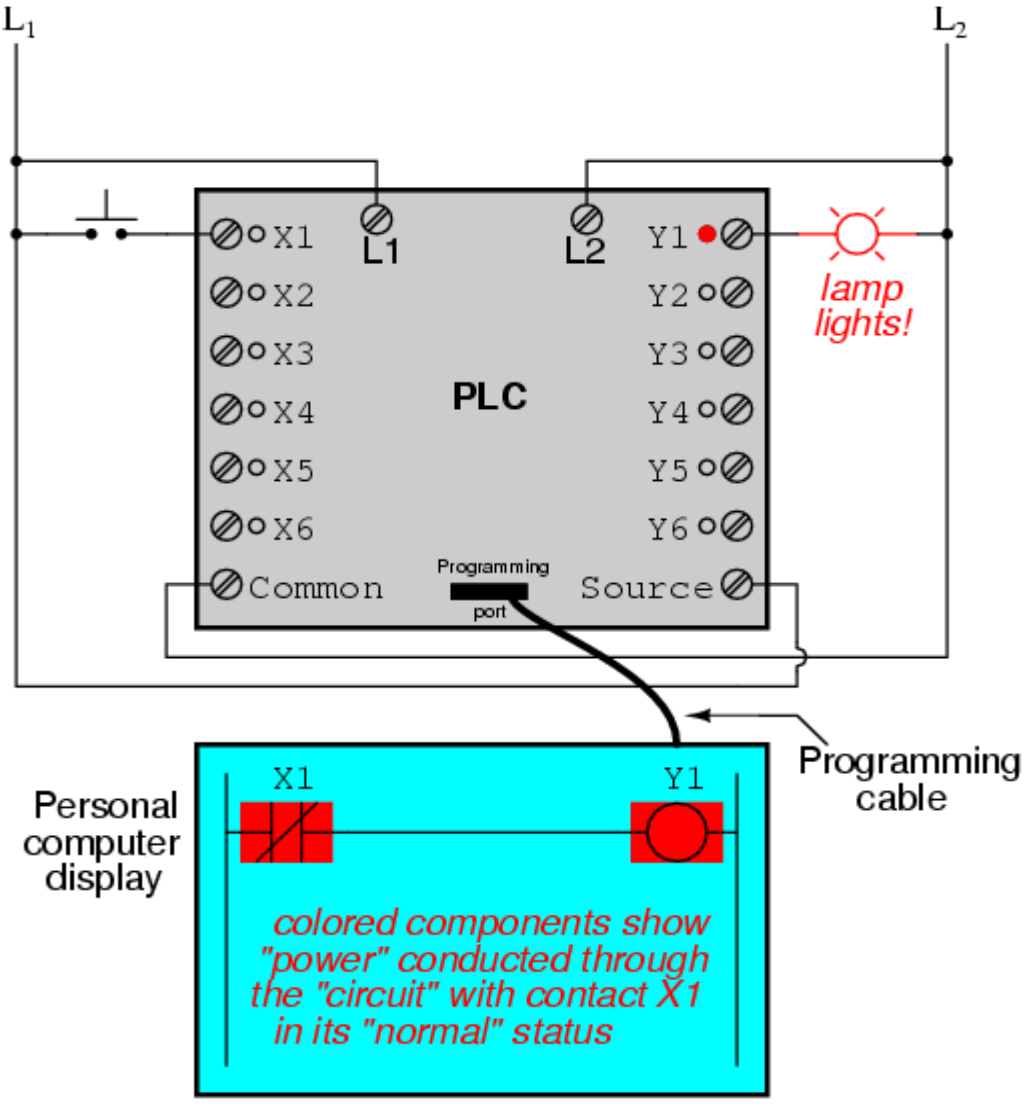
Figure 54. An energized circuit and PLC

The X1 contact, Y1 coil, connecting wires, and power appearing in the personal computer's display are all virtual. They do not exist as real electrical components. They exist as commands in a computer program—a piece of software only— that just happens to resemble a real relay schematic diagram.

The personal computer used to display and edit the PLC's program is not necessary for the PLC's continued operation. Once a program has been loaded to the PLC from the personal computer, the personal computer may be unplugged from the PLC, and the PLC will continue to follow the programmed commands.

The true power and versatility of a PLC is revealed when the engineer wants to alter the behavior of a control system. Since the PLC is a programmable device, the engineer can alter

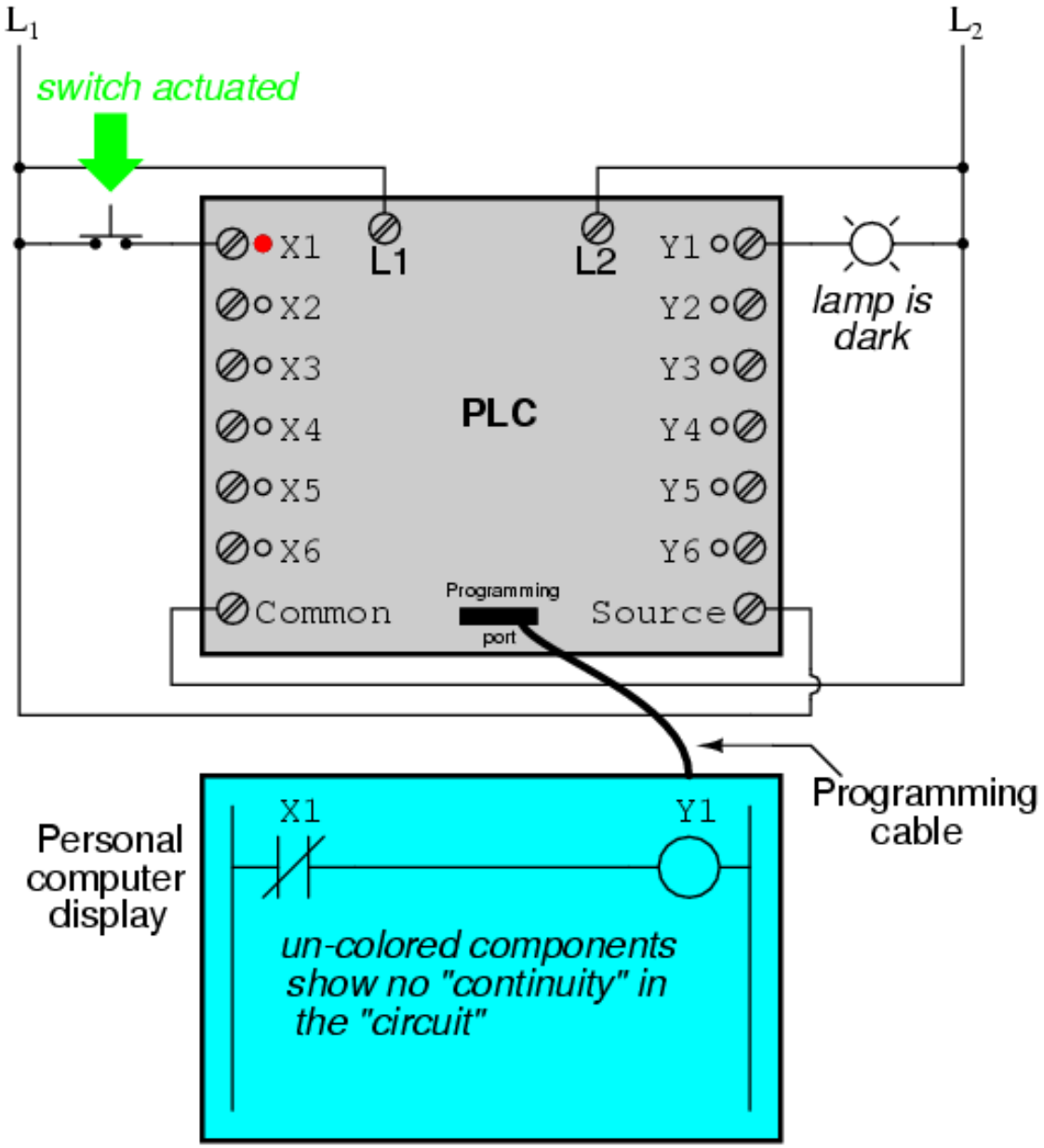
its behavior by changing the commands he/she gives it, without having to reconfigure the electrical components connected to it. For example, suppose the engineer wanted to make this switch-and-lamp circuit function in an inverted fashion: push the button to make the lamp turn off, and release it to make it turn on. The hardware solution would require that a normally-closed pushbutton switch be substituted for the normally-open switch currently in place. The software solution is much easier: just alter the program so that contact X1 is normally-closed rather than normally-open.
In figure 55, the altered system shown is in the state where the pushbutton is unactuated (not being pressed):



Source: All About Circuits, Programmable Logic Controllers

Figure 55. Unactuated system

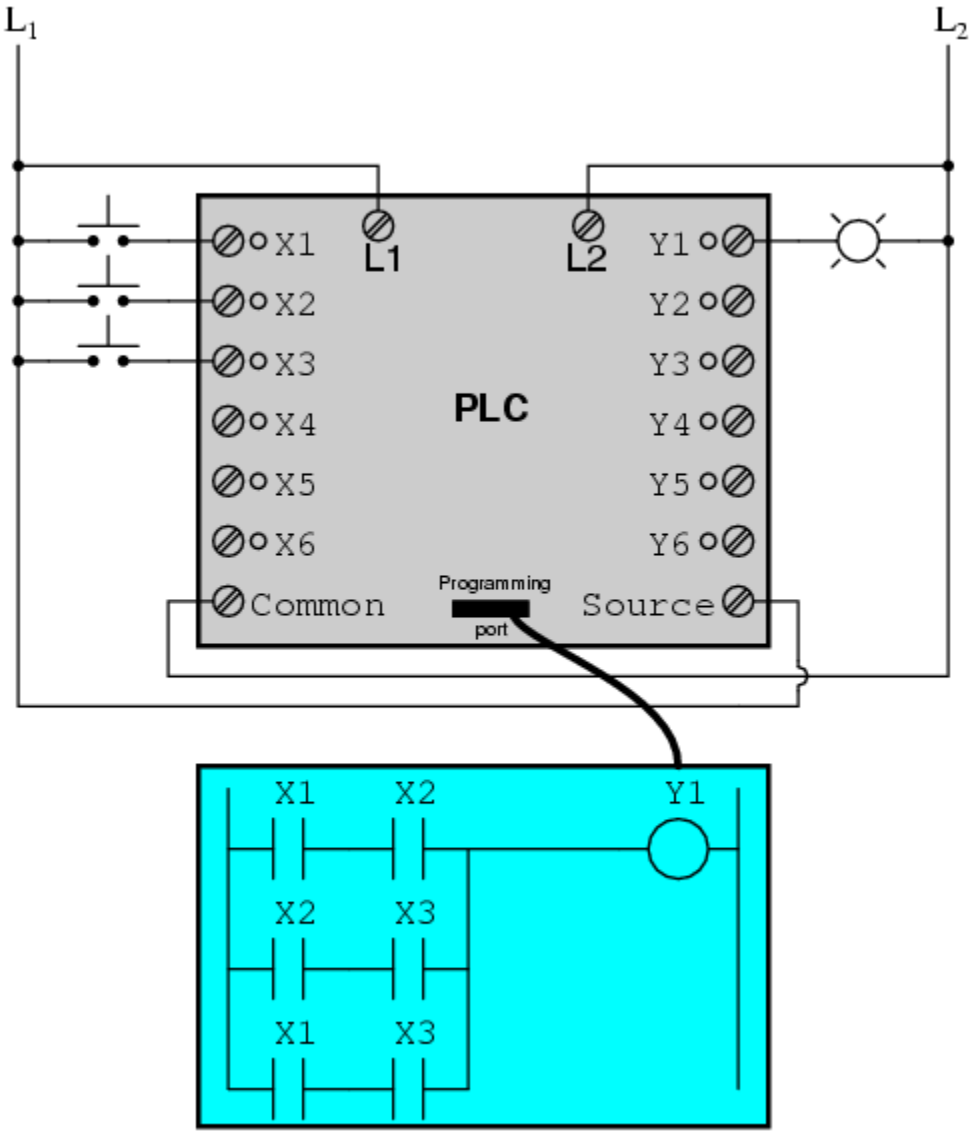
In figure 56, the switch is shown actuated (pressed):



Source: All About Circuits, Programmable Logic Controllers

Figure 56. Actuated system

One of the advantages of implementing logical control in software rather than in hardware is that input signals can be re-used as many times in the program as is necessary. For example, take the circuit and program shown in figure 57, designed to energize the lamp if at least two of the three pushbutton switches are simultaneously actuated.



Source: All About Circuits, Programmable Logic Controllers

Figure 57. Circuit with multiple relays

To build an equivalent circuit using electromechanical relays, three relays with two normally-open contacts each would have to be used, to provide two contacts per input switch. Using a PLC, however, we can program as many contacts as we wish for each X input without adding additional hardware, since each input and each output is nothing more than a single bit in the PLC's digital memory (either 0 or 1), and can be recalled as many times as necessary.

Furthermore, since each output in the PLC is nothing more than a bit in its memory as well, we can assign contacts in a PLC program actuated by an output (Y) status.

Video 20. What is a PLC

http://www.bing.com/videos/search?q=programmable+logic+controller&view=detail&mid=F0ED3CBA0DFCB20D5581F0ED3CBA0DFCB20D5581&first=0

Processors

The following is taken from Wikipedia, *Digital Signal Processors*.

A digital signal processor (DSP) is a specialized microprocessor with an architecture optimized for the operational needs of digital signal processing.

Digital signal processing algorithms typically require a large number of mathematical operations to be performed quickly and repeatedly on a series of data samples. Signals (perhaps from audio or video sensors) are constantly converted from analog to digital, manipulated digitally, and then converted back to analog form. Many DSP applications have constraints on latency; that is, for the system to work, the DSP operation must be completed within some fixed time, and deferred (or batch) processing is not viable.

Most general-purpose microprocessors and operating systems can execute DSP algorithms successfully, but are not suitable for use in portable devices such as mobile phones due to power supply and space constraints. A specialized DSP, however, will tend to provide a lower-cost solution, with better performance, lower latency, and no requirements for specialized cooling or large batteries.

The architecture of a DSP is optimized specifically for digital signal processing. Most DSPs also support some of the features as applications processors or microcontrollers, since signal processing is rarely the only task of a system.

Communication Modules

The following is taken from Wolf Automation, *Communication Modules*.

In industrial automation, applications communication modules are used as connectors for sending different electric signals, and making the series information of control devices compatible with one another.

Input/Output Modules

The following is taken from Wikipedia, *Input/Output*.

In computing, input/output, or I/O, is the communication between an information processing system, possibly a human or another information processing system, and the outside world. Inputs are the signals or data received by the system, and outputs are the signals or data sent from it. The term can also be used as part of an action; to perform I/O is to perform an input or output operation. I/O devices are used by a person to communicate with a computer. For instance, a keyboard or a mouse may be an input device for a computer, while monitors and printers are considered output devices for a computer. Devices for communication between computers, such as modems and network cards, typically serve for both input and output.

Note that the designation of a device as either input or output depends on the perspective. Mouse and keyboards take as input physical movement that the human user outputs and convert it into signals that a computer can understand. The output from these devices is input for the computer. Similarly, printers and monitors take as input signals that a computer outputs. They then convert these signals into representations that human users can see or read. For a human user, the process of reading or seeing these representations is receiving input. These interactions between computers and humans is studied in a field called human–computer interaction.

In computer architecture, the combination of the central processing unit (CPU) and main memory is considered the brain of a computer, and from that point of view any transfer of information from or to that combination, for example to or from a disk drive, is considered I/O. The CPU and its supporting circuitry provide memory-mapped I/O that is used in low-level computer programming, such as the implementation of device drivers. An I/O algorithm is one designed to exploit locality and perform efficiently when data reside on secondary storage, such as a disk drive.

Interface Modules

The following is taken from Whatis.com, *Interface Devices*.

An interface device is a hardware component or system of components that allows a human being to interact with a computer, a telephone system, or other electronic information system. The term is often encountered in the mobile communication industry where designers are challenged to build the proper combination of portability, capability, and ease of use into the interface device. The overall set of characteristics provided by an interface device is often referred to as the user interface. Today's desktop and notebook computers have what has come to be called a graphical user interface to distinguish it from earlier, more limited interfaces such as the command line interface.

An interface device generally must include some form or forms of output interface, such as a display screen or audio signals, and some form or forms of input interface, such as buttons to push, a keyboard, a voice receiver, or a handwriting tablet.

Fieldbus

The following is taken from Wikipedia, *Fieldbus.*

Fieldbus is the name of a family of industrial computer network protocols used for real-time distributed control, now standardized as IEC 61158, *Industrial Communication Networks—Fieldbus Specifications*.

A complex automated industrial system, such as a manufacturing assembly line, usually needs an organized hierarchy of controller systems to function. In this hierarchy there is usually a human-machine interface at the top, where an operator can monitor or operate the system. This is typically linked to a middle layer of PLCs via a non-time-critical communications system. At the bottom of the control chain is the fieldbus that links the PLCs to the components that actually do the work, such as sensors, actuators, electric motors, console lights, switches, valves and contactors.

Video 21. Fieldbus

http://www.bing.com/videos/search?q=Fieldbus+Training&view=detail&mid=42011C63E37C70AEAB1142011C63E37C70AEAB11&first=21

b. Explain the application of software development concepts, including software quality assurance activities and their importance to ensuring I&C systems perform their functions correctly (e.g., requirements of DOE O 414.1D and additional guidance of DOE G 414.1-4).

The following is taken from the National Research Council, *Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues*.

Software can be used to execute relatively simple combinational logic, such as that used for reactor trip functions, or more elaborate sequential logic, such as that used for actuating engineered safety features or for process control and monitoring. In either case, it must be ensured that required actions are taken and unnecessary trips are avoided.

One way of assuring software quality is by examining and approving the process used to produce it. The assumption behind assessing the process by which software is produced is that high-quality software development processes will produce software products with similar qualities. An alternate approach to QA is to directly evaluate properties of the software. Software properties include correctness, reliability, and safety.

Assurance of software correctness is sought either experimentally via program testing or analytically through formal verification techniques. Software may be correct but still not perform as intended; however, because of flaws in requirements or assurance techniques.

Software reliability is the probability that a given program will operate correctly in a specified environment for a specified duration. Several models have been proposed for estimating software reliability.

Software is safe if it does not exhibit behaviors that contribute to a system hazard. Safety analysis and assurance techniques have been developed for all stages of the software life cycle. Complexity is an important aspect of assessing correctness, reliability, and safety of software.

Analog and digital systems should be analyzed differently because the assumptions underlying their design and production are different. Reliability estimation for analog systems primarily measures failures caused by parts wearing out; whereas, for digital systems it seeks to address failures primarily caused by latent design flaws. Analog systems can be modeled using continuous and discrete functions; whereas, digital systems must be modeled using discrete mathematics only. Although analog systems could contain similar latent design flaws, they are believed to be accommodated by existing evaluation techniques. When an analog system functions correctly on two close test points and continuous mathematics is applicable, it can be assumed that it will function on all points between the two test points. This is not necessarily true for digital systems that may produce very different results for similar test points.

The following is taken from DOE O 414.1D.

Safety software must be acquired, developed, and implemented using American Society of Mechanical Engineers (ASME) National Quality Assurance (NQA)-1-2008 standard with the NQA-1a-2009 addenda, *Quality Assurance Requirements for Nuclear Facility Applications*, part I and subpart 2.7, or other national or international consensus standards that provide an equivalent level of QA requirements as NQA-1-2008. DOE-approved QAPs applicable to safety software based on requirements from DOE O 414.1D are acceptable. The standards used must be specified by the user and approved by the designated DOE approval authority. Management of safety software must include the following elements:

- Involve the facility design authority, as applicable, in the identification of; requirements specification; acquisition; design; development; verification and validation ; configuration; management; maintenance; and retirement.
- Identify, document, control, and maintain safety software inventory. The inventory entries must include at a minimum the following: software description, software name, version identifier, safety software designation, grade level designation, specific nuclear facility application used, and the responsible individual.
- Establish and document grading levels for safety software using the graded approach. Grading levels must be submitted to and approved by the responsible DOE approval authority.
- Using the consensus standard selected and the grading levels established and approved, select and implement applicable SSQA work activities from the list below:
  - Software project management and quality planning
  - Software risk management
  - Software configuration management
  - Procurement and supplier management
  - Software requirements identification and management
  - Software design and implementation
  - Software safety analysis and safety design methods
  - Software verification and validation
  - Problem reporting and corrective action

Training of personnel in the design, development, use, and evaluation of safety software

The following is taken from DOE G 414.1-4.

Software typically is either custom developed or acquired software. Further characterizing these two basic types aids in the selection of the applicable practices and approaches for the software QA work activities. For the purposes of DOE G 414.1-4, five types of software have been identified as commonly used in DOE applications: custom developed, configurable, acquired, utility calculation, and commercial design and analysis.

Developed and acquired software types as discussed in ASME NQA-1-2008 are compatible with these five software types. Developed software as described is directly associated with custom developed, configurable, and utility calculation software. Acquired software included in DOE G 414.1-4 is easily mapped to that of acquired software in ASME NQA-1-2008.

Custom Developed Software

Custom developed software is built specifically for a DOE application or to support the same function for a related government organization. It may be developed by DOE or one of its management and operating contractors or contracted with a qualified software company through the procurement process. Examples of custom developed software include material inventory and tracking database applications, accident consequence applications, control system applications, and embedded custom developed software that controls a hardware device.

Configurable Software

Configurable software is commercially available software or firmware that allows the user to modify the structure and functioning of the software in a limited way to suit user needs. An example is software associated with programmable logic controllers.

Acquired Software

Acquired software is generally supplied through basic procurements, two-party agreements, or other contractual arrangements. Acquired software includes commercial off-the-shelf (COTS) software, such as operating systems, database management systems, compliers, software development tools, and commercial calculational software and spreadsheet tools. Downloadable software that is available at no cost to the user is considered acquired software. Firmware is acquired software. Firmware is usually provided by a hardware supplier through the procurement process and cannot be modified after receipt.

Utility Calculation Software

Utility calculation software typically uses COTS spreadsheet applications as a foundation and user developed algorithms or data structures to create simple software products. The utility calculation software within the scope of DOE G 414.1-4 is used frequently to perform calculations associated with the design of a structure, systems, and component. Utility software that is used with high frequency may be labeled as custom software and may justify the same safety software QA work activities as custom developed software. With utility calculation software, it is important to recognize the difference between QA of the algorithms, macros, and logic that perform the calculations versus QA of the COTS software itself. Utility calculation software includes the associated data sets, configuration information, and test cases for validation and/or calibration.

Commercial Design and Analysis Software

Commercial design and analysis software is used in conjunction with design and analysis services provided to DOE from a commercial contractor. An example would be where DOE or a management and operating contractor contracts for a specified design services support. The design service provider uses its independently developed or acquired software without DOE involvement or support. DOE then receives a completed design. Procurement contracts can be enhanced to require that the software used in the design or analysis services meet the requirements in DOE O 414.1D.

c. Explain the advantages, disadvantages, and issues involved in the application of wireless technology for field instruments.

The following is taken from eHow, *Advantages and Disadvantages of Wireless Media*.

Enhanced Mobility

The greatest advantage of wireless media and wireless networks is the ability to easily gain access to them, both locally and from remote locations. The technology provides a network for communication using mobile phones. In business, this allows workers in information-based industries to move about their work area to collaborate with others (local) as well as access information stored on company databases while at home or on the road (remotely), increasing productivity.

Infrastructure Costs

To connect to servers, networks, and other computers using wireless media, the machine merely has to have wireless capabilities and provide security access codes. If all computers in a home or office are connected using wireless media, initial setup and changes to the network like access and security can all be performed by an administrator with access to the network. There is no need for wiring machines or servers together, which saves money and time in hardware and labor costs.

Security

According to the SANS institute, a cooperative research and education organization, all forms of networking and transmitting data come with some form of security vulnerability, but security is most compromised using wireless media. Since data and information is sent remotely through the air using radio or microwaves, it can be captured and deciphered by anyone in range with wireless connectivity capabilities. Encryption techniques are used as a security measure which leaves data undecipherable without having the security codes to unlock it. However, hackers have shown that even encryption is not foolproof, and there are ways to gain access to seemingly the most secure wireless network.

Health Effects

According to a June 2011 CNET report, the World Health Organization has declared radiation from wireless media as a "possible carcinogen." This means that although definitive causality between the two has not been established, further research is warranted. It is speculated that increased microwave and radio signals to the brain can cause brain tissue damage as well as cancerous tumor growth, particularly on the same side of the head that wireless handsets are used. Warnings have been issued in countries such as Russia, Germany, and France against children using mobile phones.

d. Explain the advantages, disadvantages, and limitations for the use of digital and/or wireless systems in I&C applications (e.g., signal interference, security, software quality, etc.).

The following is taken from Information Point Technologies, *Wireless Networking, Advantages and Disadvantages to Wireless Networking*.

Advantages of Wireless Networking

The popularity of wireless local area networks (LANs) is a testament primarily to their convenience, cost efficiency, and ease of integration with other networks and network components. The majority of computers sold to consumers today come pre-equipped with all necessary wireless LAN technology.

The following are advantages of wireless networking:

- *Convenience*. The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment. With the increasing saturation of laptop-style computers, this is particularly relevant.
- *Mobility*. With the emergence of public wireless networks, users can access the internet even outside their normal work environment. Most chain coffee shops, for example, offer their customers a wireless connection to the internet at little or no cost.
- *Productivity*. Users connected to a wireless network can maintain a nearly constant affiliation with their desired network as they move from place to place. For a business, this implies that an employee can potentially be more productive as his or her work can be accomplished from any convenient location.
- *Deployment*. Initial setup of an infrastructure-based wireless network requires little more than a single access point. Wired networks, on the other hand, have the additional cost and complexity of actual physical cables being run to numerous locations, which can even be impossible for hard-to-reach locations within a building.
- *Expandability*. Wireless networks can serve a suddenly-increased number of clients with the existing equipment. In a wired network, additional clients would require additional wiring.
- *Cost.* Wireless networking hardware is at worst a modest increase from wired counterparts. This potentially increased cost is almost always more than outweighed by the savings in cost and labor associated with running physical cables.

Disadvantages of Wireless Networking

For a given networking situation, wireless LANs may not be desirable for a number of reasons. Most of these have to do with the inherent limitations of the technology.

The following are disadvantages of wireless networking:

- *Security*. To combat this consideration, wireless networks may choose to utilize some of the various encryption technologies available. Some of the more commonly used encryption methods, however, are known to have weaknesses that a dedicated adversary can compromise.
- *Range*. The typical range of a common 802.11g network with standard equipment is on the order of tens of meters. While sufficient for a typical home, it will be insufficient for a larger structure. To obtain additional range, repeaters or additional access points will have to be purchased. Costs for these items can add up quickly.
- *Reliability*. Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference, as well as complex propagation effects that are beyond the control of the network administrator.
- *Speed*. The speed of most wireless networks (typically 1-54 Mbps) is far slower than even the slowest common wired networks (100Mbps up to several Gbps). However, in specialized environments, the throughput of a wired network might be necessary.

Video 22. Wireless Technology

http://video.about.com/compnetworking/What-is-Wireless-Networking-.htm

Digital Electronics

The following is taken from Wikipedia, *Digital Electronics*.

Digital electronics, or digital (electronic) circuits, represent signals by discrete bands of analog levels, rather than by a continuous range. All levels within a band represent the same signal state. Relatively small changes to the analog signal levels due to manufacturing tolerance, signal attenuation, or parasitic noise do not leave the discrete envelope, and as a result are ignored by signal state sensing circuitry.

In most cases the number of these states is two, and they are represented by two voltage bands: one near a reference value (typically termed as ground or zero volts) and a value near the supply voltage, corresponding to the false (0) and true (1) values of the Boolean domain respectively.

Digital techniques are useful because it is easier to get an electronic device to switch into one of a number of known states than to accurately reproduce a continuous range of values.

Digital electronic circuits are usually made from large assemblies of logic gates: simple electronic representations of Boolean logic functions.

Video 23. Digital Electronics

http://www.bing.com/videos/search?q=digital+electronics+tutorial&view=detail&mid=D5DAEEA1D17901C972AED5DAEEA1D17901C972AE&first=0

ADVANTAGES OF DIGITAL CIRCUITS

An advantage of digital circuits when compared to analog circuits is that signals represented digitally can be transmitted without degradation due to noise. For example, a continuous audio signal transmitted as a sequence of 1s and 0s can be reconstructed without error, provided the noise picked up in transmission is not enough to prevent identification of the 1s and 0s. An hour of music can be stored on a compact disc using about 6 billion binary digits.

In a digital system, a more precise representation of a signal can be obtained by using more binary digits to represent it. While this requires more digital circuits to process the signals, each digit is handled by the same kind of hardware. In an analog system, additional resolution requires fundamental improvements in the linearity and noise characteristics of each step of the signal chain.

Computer-controlled digital systems can be controlled by software, allowing new functions to be added without changing hardware. Often this can be done outside of the factory by updating the product's software. So, the product's design errors can be corrected after the product is in a customer's hands.

Information storage can be easier in digital systems than in analog ones. The noise-immunity of digital systems permits data to be stored and retrieved without degradation. In an analog

system, noise from aging and wear degrade the information stored. In a digital system, as long as the total noise is below a certain level, the information can be recovered perfectly.

DISADVANTAGES OF DIGITAL CIRCUITS

In some cases, digital circuits use more energy than analog circuits to accomplish the same tasks; producing more heat and increasing the complexity of the circuits with the inclusion of heat sinks. In portable or battery-powered systems this can limit the use of digital systems.

For example, battery-powered cellular telephones often use a low-power analog front-end to amplify and tune in to radio signals from the base station. However, a base station has grid power and can use power-hungry, but very flexible, software radios. Such base stations can be easily reprogrammed to process the signals used in new cellular standards.

Digital circuits are sometimes more expensive, especially in small quantities.

Most useful digital systems must translate from continuous analog signals to discrete digital signals. This causes quantization errors. Quantization error can be reduced if the system stores enough digital data to represent the signal to the desired degree of fidelity. The Nyquist-Shannon sampling theorem provides an important guideline as to how much digital data is needed to accurately portray a given analog signal.

In some systems, if a single piece of digital data is lost or misinterpreted, the meaning of large blocks of related data can completely change. Due to the cliff effect, it can be difficult for users to tell if a particular system is right on the edge of failure, or if it can tolerate much more noise before failing.

Digital fragility can be reduced by designing a digital system for robustness. For example, a parity bit or other error management method can be inserted into the signal path. These schemes help the system detect errors, and then either correct the errors, or at least ask for a new copy of the data. In a state-machine, the state transition logic can be designed to catch unused states and trigger a reset sequence or other error recovery routine.

Digital memory and transmission systems can use techniques such as error detection and correction to use additional data to correct any errors in transmission and storage.

On the other hand, some techniques used in digital systems make those systems more vulnerable to single-bit errors. These techniques are acceptable when the underlying bits are reliable enough that such errors are highly unlikely.

A single-bit error in audio data stored directly as linear pulse code modulation causes, at worst, a single click. Instead, many people use audio compression to save storage space and download time, even though a single-bit error may corrupt an entire song.

DESIGN ISSUES IN DIGITAL CIRCUITS

Digital circuits are made from analog components. The design must assure that the analog nature of the components doesn’t dominate the desired digital behavior. Digital systems must manage noise and timing margins, parasitic inductances and capacitances, and filter power connections.

Bad designs have intermittent problems such as glitches, vanishingly-fast pulses that may trigger some logics but not others, runt pulses that do not reach valid threshold voltages, or unexpected combinations of logic states.

Additionally, where clocked digital systems interface to analog systems or systems that are driven from a different clock, the digital system can be subject to metastability where a change to the input violates the set-up time for a digital input latch. This situation will self-resolve in a random amount of time, but while it persists, can result in invalid signals being propagated within the digital system for a short period.

Since digital circuits are made from analog components, digital circuits calculate more slowly than low-precision analog circuits that use a similar amount of space and power. However, the digital circuit will calculate more repeatably, because of its high noise immunity. On the other hand, in the high-precision domain, analog circuits require much more power and area than digital equivalents.

CONSTRUCTION

A digital circuit is often constructed from small electronic circuits (logic gates) that can be used to create combinational logic. Each logic gate represents a function of boolean logic. A logic gate is an arrangement of electrically controlled switches, better known as transistors.

Each logic symbol is represented by a different shape. The actual set of shapes was introduced in 1984 under IEEE\ANSI standard 91-1984, *Graphic Symbols for Logic Functions*. The logic symbols given under this standard are being increasingly used and have even started appearing in the literature published by manufacturers of digital integrated circuits.

The output of a logic gate is an electrical flow or voltage that can, in turn, control more logic gates.

Logic gates often use the fewest number of transistors possible to reduce their size, power consumption and cost, and increase their reliability.

Integrated circuits are the least expensive way to make logic gates in large volumes. Integrated circuits are usually designed by engineers using electronic design automation software.

Another form of digital circuit is constructed from lookup tables. Lookup tables can perform the same functions as machines based on logic gates, but can be easily reprogrammed without changing the wiring. This means that a designer can often repair design errors without changing the arrangement of wires. Therefore, in small volume products, programmable logic devices are often the preferred solution. They are usually designed by engineers using electronic design automation software.

When the volumes are medium to large, and the logic can be slow, or involves complex algorithms or sequences, often a small microcontroller is programmed to make an embedded system. These are usually programmed by software engineers.

When only one digital circuit is needed, and its design is totally customized (as in a factory production line controller), the conventional solution is a programmable logic controller, or PLC. These are usually programmed by electricians, using ladder logic.

STRUCTURE OF DIGITAL SYSTEMS

Engineers use many methods to minimize logic functions to reduce the circuit's complexity. When the circuit is less complex, it also has fewer errors and less electronics, and is therefore less expensive.

The most widely used simplification is a minimization algorithm, like the Espresso heuristic logic minimizer, within a computer-aided design system. Historically, binary decision diagrams, an automated Quine–McCluskey algorithm, truth tables, Karnaugh maps, and Boolean algebra have been used.

Representations are crucial to an engineer's design of digital circuits. Some analysis methods only work with particular representations.

The classic way to represent a digital circuit is with an equivalent set of logic gates. Another way, often with the least electronics, is to construct an equivalent system of electronic switches. One of the easiest ways is to simply have a memory containing a truth table. The inputs are fed into the address of the memory, and the data outputs of the memory become the outputs.

For automated analysis, these representations have digital file formats that can be processed by computer programs. Most digital engineers are very careful to select computer programs with compatible file formats.

To choose representations, engineers consider types of digital systems. Most digital systems divide into combinational systems and sequential systems. A combinational system always presents the same output when given the same inputs. It is basically a representation of a set of logic functions.

A sequential system is a combinational system with some of the outputs fed back as inputs. This makes the digital machine perform a sequence of operations. The simplest sequential system is probably a flip flop, a mechanism that represents a binary digit or bit.

Sequential systems are often designed as state machines. In this way, engineers can design a system's gross behavior, and even test it in a simulation, without considering all the details of the logic functions.

Sequential systems divide into two further subcategories. Synchronous sequential systems change state all at once, when a clock signal changes state. Asynchronous sequential systems propagate changes whenever inputs change. Synchronous sequential systems are made of well-characterized asynchronous circuits, such as flip-flops, that change only when the clock changes, and which have carefully designed timing margins.

The usual way to implement a synchronous sequential state machine is to divide it into a piece of combinational logic and a set of flip flops called a state register. Each time a clock

signal ticks, the state register captures the feedback generated from the previous state of the combinational logic, and feeds it back as an unchanging input to the combinational part of the state machine. The fastest rate of the clock is set by the most time-consuming logic calculation in the combinational logic.

The state register is just a representation of a binary number. If the states in the state machine are numbered, the logic function is some combinational logic that produces the number of the next state.

In comparison, asynchronous systems are very hard to design because all possible states, in all possible timings, must be considered. The usual method is to construct a table of the minimum and maximum time that each such state can exist, and then adjust the circuit to minimize the number of such states, and force the circuit to periodically wait for all of its parts to enter a compatible state. Without such careful design, it is easy to accidentally produce asynchronous logic that is unstable; that is, real electronics will have unpredictable results because of the cumulative delays caused by small variations in the values of the electronic components. Certain circuits are inherently asynchronous in their design and must be analyzed as such.

As of 2005, almost all digital machines are synchronous designs because it is much easier to create and verify a synchronous design—the software currently used to simulate digital machines does not yet handle asynchronous designs. However, asynchronous logic is thought to be superior, if it can be made to work, because its speed is not constrained by an arbitrary clock; instead, it runs at the maximum speed of its logic gates. Building an asynchronous circuit using faster parts makes the circuit faster.

Many digital systems are data flow machines. These are usually designed using synchronous register transfer logic, using hardware description languages such as VHSIC (very high speed integrated circuit) hardware description language or Verilog.

In register transfer logic, binary numbers are stored in groups of flip-flops called registers. The outputs of each register are a bundle of wires, called a bus, that carry that number to other calculations. A calculation is simply a piece of combinational logic. Each calculation also has an output bus, which may be connected to the inputs of several registers. Sometimes a register will have a multiplexer on its input, so that it can store a number from any one of several buses. Alternatively, the outputs of several items may be connected to a bus through buffers that can turn off the output of all of the devices except one. A sequential state machine controls when each register accepts new data from its input.

In the 1980s, some researchers discovered that almost all synchronous register-transfer machines could be converted to asynchronous designs by using first-in-first-out synchronization logic. In this scheme, the digital machine is characterized as a set of data flows. In each step of the flow, an asynchronous synchronization circuit determines when the outputs of that step are valid, and presents a signal that says, “grab the data” to the stages that use that stage’s inputs. Just a few relatively simple synchronization circuits are needed.

The most general-purpose register-transfer logic machine is a computer. This is basically an automatic binary abacus. The control unit of a computer is usually designed as a microprogram run by a microsequencer. A microprogram is much like a player-piano roll. Each table entry or word of the microprogram commands the state of every bit that controls the computer. The sequencer then counts, and the count addresses the memory or combinational logic machine that contains the microprogram. The bits from the microprogram control the arithmetic logic unit, memory, and other parts of the computer, including the microsequencer itself. In this way, the complex task of designing the controls of a computer is reduced to a simpler task of programming a collection of much simpler logic machines.

Computer architecture is a specialized engineering activity that tries to arrange the registers, calculation logic, buses and other parts of the computer in the best way for some purpose. Computer architects have applied large amounts of ingenuity to computer design to reduce the cost and increase the speed and immunity to programming errors. An increasingly common goal is to reduce the power used in a battery-powered computer system, such as a cell-phone. Many computer architects serve an extended apprenticeship as microprogrammers.

Specialized computers are usually conventional computers with special-purpose microprograms.

AUTOMATED DESIGN TOOLS

To save costly engineering effort, much of the design of large logic machines has been automated. The computer programs are called electronic design automation (EDA) tools.

Simple truth table-style descriptions of logic are often optimized with EDA, which automatically produces reduced systems of logic gates or smaller lookup tables that still achieve the desired outputs. The most common example of this kind of software is the Espresso heuristic logic minimizer.

Most practical algorithms for optimizing large logic systems use algebraic manipulations or binary decision diagrams, and there are promising experiments with genetic algorithms and annealing optimizations.

To automate costly engineering processes, some EDA can take state tables that describe state machines and automatically produce a truth table or a function table for the combinational logic of a state machine. The state table is a piece of text that lists each state, together with the conditions controlling the transitions between them and the associated output signals. It is common for the function tables of such computer-generated state-machines to be optimized with logic-minimization software such as Minilog.

Often, real logic systems are designed as a series of sub-projects, which are combined using a tool flow. The tool flow is usually a script, a simplified computer language that can invoke the software design tools in the right order.

Tool flows for large logic systems such as microprocessors can be thousands of commands long, and combine the work of hundreds of engineers.

Writing and debugging tool flows is an established engineering specialty in companies that produce digital designs. The tool flow usually terminates in a detailed computer file or set of files that describe how to physically construct the logic. Often it consists of instructions to draw the transistors and wires on an integrated circuit or a printed circuit board.

Parts of tool flows are debugged by verifying the outputs of simulated logic against expected inputs. The test tools take computer files with sets of inputs and outputs, and highlight discrepancies between the simulated behavior and the expected behavior.

Once the input data is believed correct, the design itself must still be verified for correctness. Some tool flows verify designs by first producing a design, and then scanning the design to produce compatible input data for the tool flow. If the scanned data matches the input data, then the tool flow has probably not introduced errors.

The functional verification data are usually called test vectors. The functional test vectors may be preserved and used in the factory to test that newly constructed logic works correctly. However, functional test patterns don't discover common fabrication faults. Production tests are often designed by software tools called test pattern generators. These generate test vectors by examining the structure of the logic and systematically generating tests for particular faults. This way the fault coverage can closely approach 100 percent provided the design is made properly testable.

Once a design exists, and is verified and testable, it often needs to be processed to be manufacturable as well. Modern integrated circuits have features smaller than the wavelength of the light used to expose the photoresist. Manufacturability software adds interference patterns to the exposure masks to eliminate open-circuits, and enhance the masks' contrast.

DESIGN FOR TESTABILITY

There are several reasons for testing a logic circuit. When the circuit is first developed, it is necessary to verify that the design circuit meets the required functional and timing specifications. When multiple copies of a correctly designed circuit are being manufactured, it is essential to test each copy to ensure that the manufacturing process has not introduced any flaws.

A large logic machine can have an astronomical number of possible states. Obviously, in the factory, testing every state is impractical if testing each state takes a microsecond, and there are more states than the number of microseconds since the universe began. Unfortunately, this ridiculous-sounding case is typical.

Fortunately, large logic machines are almost always designed as assemblies of smaller logic machines. To save time, the smaller sub-machines are isolated by permanently-installed design for test circuitry, and are tested independently.

One common test scheme, scan design, moves test bits serially from external test equipment through one or more serial shift registers (scan chains). Serial scans have only one or two wires to carry the data, and minimize the physical size and expense of the infrequently-used test logic.

After all the test data bits are in place, the design is reconfigured to be in normal mode and one or more clock pulses are applied to test for faults and capture the test result into flip-flops and/or latches in the scan shift register(s). Finally, the result of the test is shifted out to the block boundary and compared against the predicted good machine result.

In a board-test environment, serial to parallel testing has been formalized with a standard called JTAG (named after the "Joint Test Action Group" that proposed it).

Another common testing scheme provides a test mode that forces some part of the logic machine to enter a test cycle. The test cycle usually exercises large independent parts of the machine.

TRADE-OFFS

Several numbers determine the practicality of a system of digital logic: cost, reliability, fanout, and speed. Engineers explored numerous electronic devices to get an ideal combination of these traits.

COST

The cost of a logic gate is crucial. In the 1930s, the earliest digital logic systems were constructed from telephone relays because these were inexpensive and relatively reliable. After that, engineers always used the cheapest available electronic switches that could still fulfill the requirements.

The earliest integrated circuits were a happy accident. They were constructed not to save money, but to save weight, and permit the Apollo guidance computer to control an inertial guidance system for a spacecraft. The first integrated circuit logic gates cost nearly $50. To everyone's surprise, by the time the circuits were mass-produced, they had become the least-expensive method of constructing digital logic. Improvements in this technology have driven all subsequent improvements in cost.

With the rise of integrated circuits, reducing the absolute number of chips used represented another way to save costs. The goal of a designer is not just to make the simplest circuit, but to keep the component count down. Sometimes this results in slightly more complicated designs with respect to the underlying digital logic but nevertheless reduces the number of components, board size, and even power consumption.

For example, in some logic families, NAND gates are the simplest digital gate to build. All other logical operations can be implemented by NAND gates. If a circuit already required a single NAND gate, and a single chip normally carried four NAND gates, then the remaining gates could be used to implement other logical operations like logical and. This could eliminate the need for a separate chip containing those different types of gates.

RELIABILITY

The reliability of a logic gate describes its mean time between failure (MTBF). Digital machines often have millions of logic gates. Also, most digital machines are optimized to reduce their cost. The result is that often, the failure of a single logic gate will cause a digital machine to stop working.

Digital machines first became useful when the MTBF for a switch got above a few hundred hours. Even so, many of these machines had complex, well-rehearsed repair procedures, and would be nonfunctional for hours because a tube burned out or a moth got stuck in a relay. Modern transistorized integrated circuit logic gates have MTBFs greater than 82 billion hours, and need them because they have so many logic gates.

FANOUT

Fanout describes how many logic inputs can be controlled by a single logic output without exceeding the current ratings of the gate. The minimum practical fanout is about five. Modern electronic logic using complementary metal–oxide–semiconductor (CMOS) transistors for switches have fanouts near fifty, and can sometimes go much higher.

SPEED

The switching speed describes how many times per second an inverter can change from true to false and back. Faster logic can accomplish more operations in less time. Digital logic first became useful when switching speeds got above fifty hertz, because that was faster than a team of humans operating mechanical calculators. Modern electronic digital logic routinely switches at five gigahertz (5×109 hertz), and some laboratory systems switch at more than a terahertz (1×1012 hertz).

LOGIC FAMILIES

Design started with relays. Relay logic was relatively inexpensive and reliable, but slow. Occasionally a mechanical failure would occur. Fanouts were typically about ten, limited by the resistance of the coils and arcing on the contacts from high voltages.

Later, vacuum tubes were used. These were very fast, but generated heat, and were unreliable because the filaments would burn out. Fanouts were typically five to seven, limited by the heating from the tubes' current. In the 1950s, special computer tubes were developed with filaments that omitted volatile elements like silicon. These ran for hundreds of thousands of hours.

The first semiconductor logic family was resistor-transistor logic. This was a thousand times more reliable than tubes, ran cooler, and used less power, but had a very low fan-in of three. Diode-transistor logic (DTL) improved the fanout up to about seven, and reduced the power. Some DTL designs used two power-supplies with alternating layers of NPN and PNP transistors to increase the fanout.

Transistor-transistor logic (TTL) was a great improvement over these. In early devices, fanout improved to ten, and later variations reliably achieved twenty. TTL was also fast, with some variations achieving switching times as low as twenty nanoseconds. TTL is still used in some designs.

Emitter coupled logic (ECL) is very fast but uses a lot of power. It is extensively used for high-performance computers made up of many medium-scale components.

By far, the most common digital integrated circuits built today use CMOS logic, which is fast, offers high circuit density and low power per gate. This is used even in large, fast computers, such as the IBM System z.

RECENT DEVELOPMENTS

In 2009, researchers discovered that memristors can implement a boolean state storage, providing a complete logic family with very small amounts of space and power, using familiar CMOS semiconductor processes.

The discovery of superconductivity has enabled the development of rapid single flux quantum circuit technology, which uses Josephson junctions instead of transistors. Most recently, attempts are being made to construct purely optical computing systems capable of processing digital information using nonlinear optical elements.

e. Explain various failure modes and design considerations that are specific to digital I&C systems.

The following is taken from DOE G 414.1-4.

The development of software applications requires identification of hazards that have the potential for defeating a safety function and the implementation of design strategies to eliminate or mitigate those hazards. It is recommended that the software safety process address the mitigation strategy for the components that have potential safety consequences if a fault occurs; whereas, the software design and implementation process addresses the architecture of the safety software application.

Methods to mitigate the consequences of software failures should be an integral part of the software design. Specific software analysis and design methods for ensuring that safety functions are well thought out and addressed properly should be performed throughout the software development and operations life cycles. These methods include dynamic and static analyses. The techniques and methods described in DOE G 414.1-4 are only a selection of those available. Several resources are available to assist in the selection and use of these methods.

During the initial concept and requirement analysis phases for the software, potential failures need to be identified and evaluated for their consequences of failure and probability of occurrence. Some potential problems are 1) complex or faulty algorithms, 2) lack of proper handling of incorrect data or error conditions, 3) buffer overflow, and 4) incorrect sequence of operations due to either logic or timing faults.

There are several hazard analysis techniques that may be used for this purpose. Many of these techniques are performed as preliminary analyses and later updated as more information is known about the requirements and design structure. These techniques include failure modes and effects analysis, fault-tree modeling, event-tree modeling, cause-consequence diagrams, hazard and operability analysis, and interface analysis. Techniques such as these should be applied and appropriately documented to understand and assess the impact of software failures on the system.

When hazards related to software functions cannot be eliminated, the hazard should be reduced and/or monitored. Additionally, software can experience partial failures that can degrade the capabilities of the overall system that may not be immediately detectable by the system. In these instances, other design techniques, such as building fault detection and self-

diagnostics into the software, should be implemented. Using external monitors for the software safety functions, n-version programming, and Petri nets are examples of techniques that can ensure the software design adequately addresses safety issues and minimizes failure modes by adding fault tolerant concepts. Self-diagnostics detect and report software faults and failures in a timely manner and allow actions to be taken to avoid an impact on the system operating safety. Some of these techniques include memory functionality and integrity tests, such as checksums and watch dog timers for software processes, including operating system processes. Additionally, software control functions can be performed incrementally rather than in a single step, reducing the potential that a single failure of a software component would cause an unsafe state.

The software safety work activity for level A custom developed, configurable, and acquired safety software should fully meet this requirement. For this software type, the safety analysis for the software components should be performed. This analysis may be part of the overall safety system analysis if detailed software failures are included. For level A custom developed safety software, the design concepts that include simplicity of modules that perform safety functions and isolation of those modules should be part of the design considerations. Where the design of the software modules still presents an unacceptable risk to failure of the safety system, fault tolerant and self-diagnostics designs should be implemented.

Custom developed, configurable, and acquired level B or level C software applications may be graded. This grading may include fully performing the safety analysis activities for the software components to ensure the safety aspects are being addressed. The design concepts of simplicity and isolation and fault tolerance and self-diagnostics may not apply to level B or level C software applications and, thus, can optionally be applied.

This work activity does not apply to utility calculation or commercial design and analysis safety software types. Utility calculations are typically simple calculations where techniques and methods described in DOE G 414.1-4 could add undue burden to the development of these applications and not increase the assurance that any software failure would not impact safety. However, if the safety analysis determines that complexity of the utility calculation warrants the use of these techniques, they should be applied. For commercial design and analysis software, the software safety activities are performed by the service supplier. DOE controls the software QA activities of that software through procurement agreements and specifications.

Video 24. Failure modes and effects analysis
http://www.youtube.com/watch?v=59LYAsH3MB4

8. I&C personnel must demonstrate a working level knowledge of I&C Systems Design and Analysis.

a. Explain the role of DSAs, System Design Descriptions, and process P&IDs for I&C systems design.

DSAs

The following is taken from DOE-STD-3009-94.

Section 6.6 of the DSA summarizes the criticality alarm system and detection systems used to mitigate exposures from a criticality event. The methods and procedures used to determine the placement of the monitoring equipment and the selection of the equipment functions and sensitivity is included.

Section 7.8 of the DSA summarizes plans and procedures governing radiation protection instrumentation. Such instrumentation, whether fixed, portable, or laboratory use, includes instruments for radiation and contamination surveys; sampling; area radiation monitoring; and personnel monitoring during normal operations and accidents. Selection and placement criteria for technical equipment and instrumentation, types of detectors and monitors, and their quantity, sensitivity, and range are included in the summary This section also summarizes plans and procedures for control of calibration processes and for QA for calibration and maintenance.

Section 8.8 of the DSA summarizes plans and procedures governing hazardous protection instrumentation. Such instrumentation, whether fixed, portable, or laboratory use, includes instruments for hazardous material and contamination surveys; sampling; area hazardous material monitoring; and personnel monitoring during normal operations and accidents. Selection and placement criteria for technical equipment and instrumentation, types of detectors and monitors, and their quantity, sensitivity, and range are included in the summary. This section also summarizes plans and procedures for control of calibration processes and QA for calibration and maintenance.

System Design Descriptions

The following is taken from DOE-STD-3024-2011.

A system design description (SDD) identifies the requirements associated with structures, systems, and components (SSCs); explains why those requirements exist; and describes the features of the system design provided to meet those requirements. As part of a configuration management change control process, the SDD helps ensure consistency among the engineering requirements for systems, the actual installed physical configuration, and the associated documentation.

The SDD is a central coordinating link among the engineering design documents, the facility authorization basis, and implementing procedures. An SDD does not originate requirements or basis information, but rather collects that information into a convenient, usable form. The SDD consolidates information about a particular system into one document. This provides the advantage that a reader does not have to wade through many different documents and pull out the pertinent parts, or have to decipher the details in vendor technical manuals and engineering documents.

During the design and construction of a new facility or new system, the SDD might serve as the vehicle for collecting and conveying the system requirements and their bases. The SDD should contain requirements that are derived from programmatic needs as well as from the associated safety analyses. Accordingly, the development of the SDD must be coordinated with the engineering design process and with the safety analysis development. The SDD may be used for controlling changes as the design evolves from a concept through the preliminary

design to the final design. Sometimes this is accomplished in conjunction with facility design descriptions (FDDs). In an FDD, all the systems in a facility can be addressed with their top-level functions and requirements, and the FDD refers to SDDs for more detailed information. An FDD provides a mechanism for addressing simple, less important systems such as a potable water system, without having to develop separate SDDs. The SDD is updated periodically and hence becomes more complete and detailed as the design and safety analysis processes mature. Toward the end of the design phase, the SDD may be used as a source document for the development of the facility authorization basis. Safety information in the SDDs is extracted and placed into the DSA. In this case, the authorization basis mirrors the safety information in the SDD. Even though the SDD may precede the development of the DSA, and hence may become a source document for the authorization basis, an SDD is not a part of the authorization basis. DOE does not rely on information found uniquely in the SDD to make decisions regarding the safety of the facility.

For an existing facility or system, when the development and approval of the authorization basis have preceded the development of SDDs, the safety portions of the SDDs must mirror the authorization basis documents. Accordingly, the SDD is not an authorization basis document. Controlling equipment changes depends on recognizing changes, knowing what the existing requirements are, and understanding why those requirements exist. The modification might involve a change in how the requirement will be met, or might involve modifying a requirement or establishing a new requirement. Evaluating the acceptability of a change in requirements is difficult if the reasons behind the requirements are not understood. The SDD can help meet this change control need. When a change to the system is proposed, the SDD can be consulted to identify the pertinent requirements and the referenced engineering source documents. The results of the change would be reflected back into the SDD. Changes to the SDD itself are entirely within the purview of the DOE contractor within an appropriate change control process.

An SDD supports the authorization basis and helps ensure that operations of the system will be consistent with the authorization basis. While the authorization basis is focused on safety, the SDD is broader because it also addresses other important features provided to accomplish the programmatic mission, to maintain system reliability, and to promote effectiveness, efficiency, and flexibility in operations and maintenance. To treat the SDD as a part of the facility authorization basis would be counter-productive to these broader purposes.

The SDD promotes safe and efficient operation by providing the information necessary for a solid technical understanding of the system. The SDD collects and provides significantly more detail than is appropriate for authorization basis documents but less detail than the engineering design documents. This level of detail is particularly appropriate for the intended audience of facility operations personnel, maintenance personnel, and technical support personnel. The SDD identifies procedures for facility operations, testing, and maintenance related to the system being described, and points the reader to those specific documents in their proper context. This information leads to fewer operational errors and incidents. SDDs also identify which performance characteristics of the system are the most important. This information promotes a better understanding of where to exercise greatest care and attention to detail. In operations and maintenance, an understanding of why requirements exist

promotes better employee performance and adherence to safety management programs, implementing procedures, and administrative controls.

The SDD is a convenient reference for evaluating the performance of the system. System performance evaluations are important for several reasons. These include assessing overall facility operational effectiveness and efficiency, compliance with regulatory requirements, the possible need for improvements to increase system reliability, and the possible need for system design modifications to meet changing programmatic mission needs and demands.

The SDD should be a controlled document and maintained as an authoritative up-to-date source of technical information on the system. The SDD records technical information that might tend to get lost as personnel changes occur over the years. SDDs can also be used as technical source documents for the development of personnel training programs.

P&IDs

The following is taken from DOE-STD-3009-94.

When describing the SSC, a basic summation of the physical information known about the SSC, including P&IDs, or a simplified system drawing with reference to P&IDs is included in the DSA.

b. Explain the importance of instrument response time, accuracy, precision, set points, and process safety limits for I&C systems design.

Instrument Response Time

The following is taken from DOE-HDBK-1122-99.

The response time of the instrument is controlled by the microcomputer and is based on the input count rate and whether the mode switch is in FAST or SLOW. In the FAST position, the instrument response time varies between one and ten seconds. In the SLOW position, the instrument response time will vary up to a maximum of 29 seconds. No correction factors are required to correct the displayed value. The sealed detector is not affected by changes in atmospheric density, humidity, or radioactive gases. The instrument has a microcomputer controlled over range indication. When the radiation rate exceeds the useful range of the detector, the computer will cause an over range alarm. When the instrument alarms, the meter needle will sweep back and forth and an interrupted tone will sweep in the speaker.

Accuracy and Precision

The following is taken from Wikipedia, *Accuracy and Precision*.

In the fields of science, engineering, industry, and statistics, the accuracy of a measurement system means to what degree measurements of a quantity approximate that quantity's actual (true) value. The precision of a measurement system, also called reproducibility or repeatability, is the degree to which repeated measurements, under unchanged conditions, show the same results. Although the two words reproducibility and repeatability can be synonymous in colloquial use, they are deliberately contrasted in the context of the scientific method.

A measurement system can be accurate but not precise, precise but not accurate, neither, or both. For example, if an experiment contains a systematic error, then increasing the sample size generally increases precision but does not improve accuracy. The result would be a consistent yet inaccurate string of results from the flawed experiment. Eliminating the systematic error improves accuracy but does not change precision.

Ideally, a measurement device is both accurate and precise, with measurements all close to and tightly clustered around the known value. The accuracy and precision of a measurement process is usually established by repeatedly measuring some traceable reference standard. Such standards are defined in the International System of Units and maintained by national standards organizations such as the National Institute of Standards and Technology in the United States.

This also applies when measurements are repeated and averaged. In that case, the term standard error is properly applied: the precision of the average is equal to the known standard deviation of the process divided by the square root of the number of measurements averaged. Further, the central limit theorem shows that the probability distribution of the averaged measurements will be closer to a normal distribution than that of individual measurements.

With regard to accuracy, the following can be determined:

- The difference between the mean of the measurements and the reference value: the bias. Establishing and correcting for bias is necessary for calibration.
- The combined effect of the process described in the above and precision.

A common convention in science and engineering is to express accuracy and/or precision implicitly by means of significant figures. Here, when not explicitly stated, the margin of error is understood to be one-half the value of the last significant place. For instance, a recording of 843.6 m, or 843.0 m, or 800.0 m would imply a margin of 0.05 m (the last significant place is the tenths place), while a recording of 8,436 m would imply a margin of error of 0.5 m (the last significant digits are the units).

A reading of 8,000 m, with trailing zeroes and no decimal point is ambiguous; the trailing zeroes may or may not be intended as significant figures. To avoid this ambiguity, the number could be represented in scientific notation: 8.0×10^3 m indicates that the first zero is significant (hence a margin of 50 m) while 8.000×10^3 m indicates that all three zeroes are significant, giving a margin of 0.5 m. Similarly, it is possible to use a multiple of the basic

measurement unit: 8.0 km is equivalent to 8.0×10^3 m. In fact, it indicates a margin of 0.05 km (50 m). However, reliance on this convention can lead to false precision errors when accepting data from sources that do not obey it.

Precision is sometimes stratified into the following:

- Repeatability—the variation arising when all efforts are made to keep conditions constant by using the same instrument and operator, and repeating during a short time period; and
- Reproducibility—the variation arising using the same measurement process among different instruments and operators, and over longer time periods.

Set Point

Figure 1 of ISA-S67.04-2006, *Setpoints For Nuclear Safety-Related Instrumentation*, provides set point relationships for nuclear safety-related setpoints. The figure denotes relative position and not direction, but it should be noted that the uncertainty relationships depicted by figure 1 do not represent any one particular for the development of a trip set point or allowable value.

Section 4 of ISA-S67.04-2006 states that the safety significance of various types of setpoints for safety-related instrumentation may differ, and thus a less rigorous set point determination method may be applied for certain functional units and LCOs. A set point methodology can include such a graded approach. However, the grading technique chosen by the licensee should be consistent with the standard and should consider applicable uncertainties regardless of the set point application. Additionally, the application of the standard, using a graded approach, is also appropriate for non-safety system instrumentation for maintaining design limits described in the technical specification requirements. Examples may include instrumentation relied on in emergency operating procedures, and for meeting applicable LCOs.

ISA-S67.04-2006 states that the limiting safety system setting (LSSS) may be the trip set point, an allowable value, or both. For the standard technical specifications, the staff designated the allowable value as the LSSS. In association with the trip set point and LCOs, the LSSS establishes the threshold for protective system action to prevent acceptable limits being exceeded during design basis accidents. The LSSS therefore ensures that automatic protective action will correct the abnormal situation before a safety limit is exceeded. A licensee, with justification, may propose an alternative LSSS based on its particular set point methodology or license.

Conformance with Part 1 of ISA-S67.04-2006, provides a method for satisfying the NRC's regulations for ensuring that setpoints for safety-related instrumentation are established and maintained within the technical specification limits.

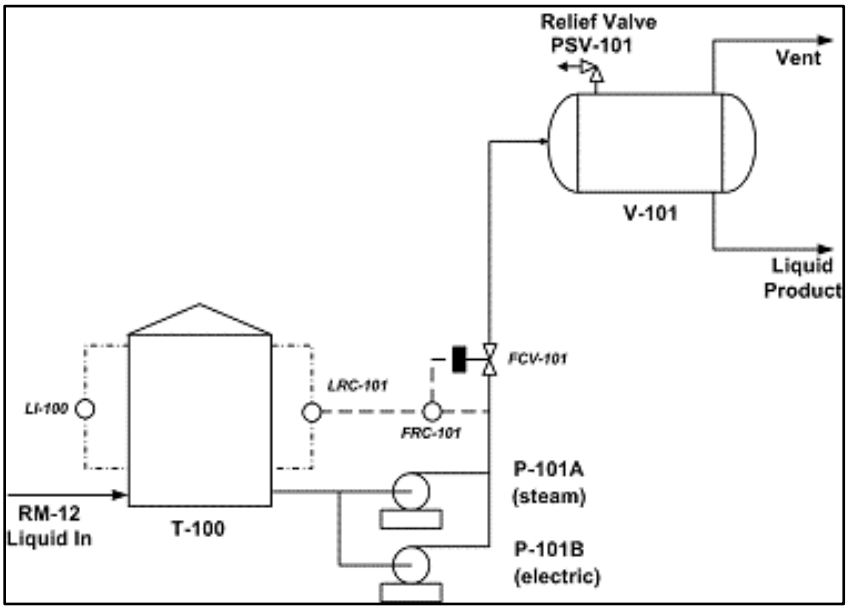
- Section 4 of ISA-S67.04-2006 specifies the methods, but not the criterion, for combining uncertainties in determining a trip set point and its allowable values. The 95/95 tolerance limit is an acceptable criterion for uncertainties. That is, there is a 95 percent probability that the constructed limits contain 95 percent of the population of interest for the surveillance interval selected.

- Sections 7 and 8 of part 1 of ISA-S67.04-2006 reference several industry codes and standards. If a referenced standard has been incorporated separately into the NRC's regulations, licensees and applicants must comply with that standard as set forth in the regulation. If the referenced standard has been endorsed in a regulatory guide, the standard constitutes a method of meeting a regulatory requirement as described in the regulatory guide. If a referenced standard has been neither incorporated into the NRC's regulations nor endorsed in a regulatory guide, licensees and applicants may consider and use the information in the referenced standard if appropriately justified, consistent with current regulatory practice.
- Section 4.3 of ISA-S67.04-2006 states that the LSSS may be maintained in technical specifications or appropriate plant procedures. However, 10 CFR 50.36 states that the technical specifications will include items in the categories of safety limits, LSSS, and LCSs. Thus, the LSSS may not be maintained in plant procedures. Rather, the LSSS must be specified as a technical-specification-defined limit to satisfy the requirements of 10 CFR 50.36. The LSSS should be developed in accordance with the set point methodology set forth in the standard, with the LSSS listed in the technical specifications.
- ISA-S67.04-2006 provides a discussion on the purpose and application of an allowable value. The allowable value is the limiting value that the trip set point can have when tested periodically, beyond which the instrument channel is considered inoperable and corrective action must be taken in accordance with the technical specifications. The allowable value relationship to the set point methodology and testing requirements in the technical specifications must be documented.

Process Safety Limits

The following is taken from Sutton Technical Books, *Process Safe Limits*.

Figure 58 shows a simple process sketch:



Source: Sutton Technical Books, Process Safe Limits

Figure 58. Simple process

Many aspects of process safety management require knowledge of safe limit values for process variables. For example, a hazard and operability study team needs to know the quantified meaning for terms such as “high temperature,” an inspector needs to know the corrosion allowance for vessels and pipes, an operator needs to know the maximum and minimum levels in tanks, and a management of change review team needs quantified information about the parameters that are being changed.

If the value of a variable moves outside its safe range then, by definition, a hazardous situation has been created.

Table 5 provides some examples for safe limit values for the equipment items in figure 58. Table 5 also provides some discussion to do with each value, showing where it came from, and what the impact of exceeding that value would be.

Table 5. Examples for safe limits

Item	Parameter	Units	Safe Upper Limit	Limit
T-100	Level	%	95	10
	The high limit is based on operating experience. It has been found that upsets rarely cause the level to deviate more than 2 or 3 percent. Therefore, keeping the level at 95 percent or less should minimize the change of tank overflow. Minimum flow protection for the pumps is not provided so a minimum level in the tank must be maintained to prevent pump cavitation leading to seal leaks			
p-101	Flow	kg/h	N/A	500
	The upper limit for flow is set by the capacity of the pumps. Even when they are pumping at maximum rates, no hazardous condition is created. Therefore no meaningful value for a safe upper limit of flow exists. Below the prescribed minimum flow rate, the pumps may cavitate.			
V-101	Pressure	bar(g)	12 (at 250ºC)	0
	The upper pressure limit is set by code. V-101 is not vacuum-rated, and there is uncertainty about lower pressure limit, so 0 barg (1 bar abs) has arbitrarily been set as the lower limit.			
V-101	Temperature	C	250º	-10
	The upper temperature limit is defined by code. Stress cracking may occur below the lower safe limit value.			

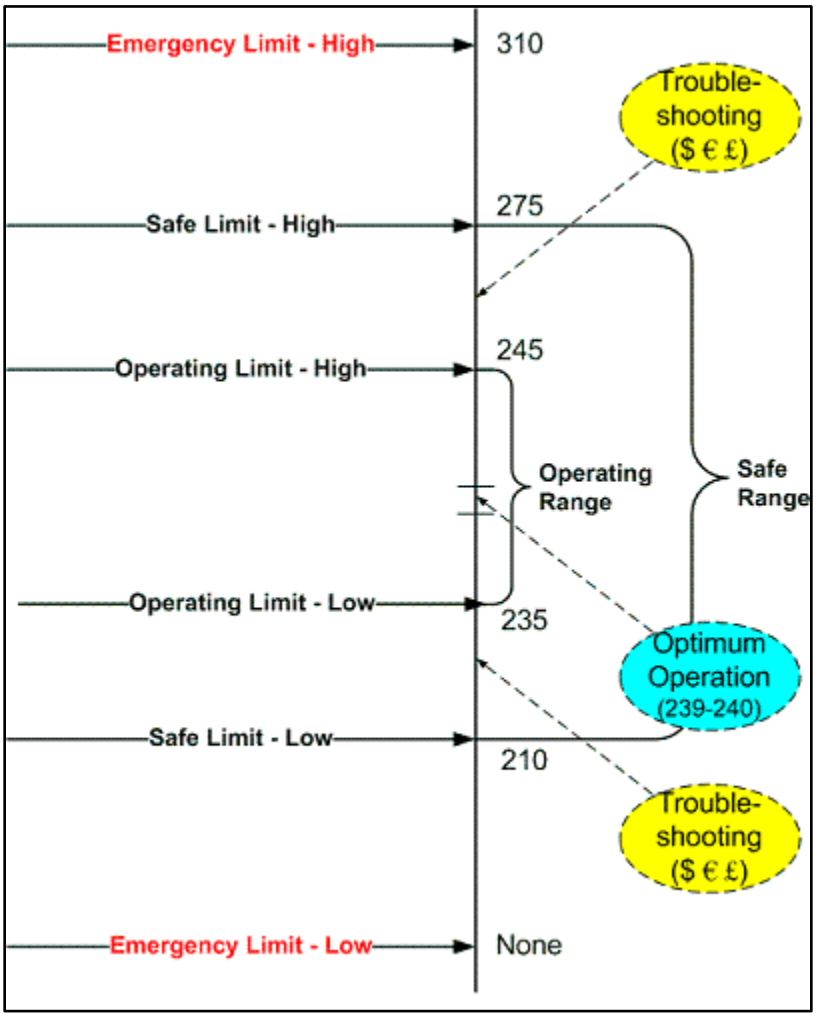
Source: Sutton Technical Books, Process Safe Limits

Figure 59 provides another illustration of the safe limit concept (the values shown in figure 59 could be for any process parameter such as pressure, temperature, level or flow).

Figure 59 shows three ranges for the process parameter in question. The first is the normal operating range; it lies between 218 and 245 (in the appropriate units of measurement). Normal operations are carried out within this envelope. If the value is allowed to go outside the range it is likely that production or quality problems will crop up. If an operating value goes outside the operating range, but stays within safe limits, then the facility is in “trouble”.

There is no perceived safety or environmental problem during this phase of the operation, but the facility may be losing money. Examples of trouble in this context include

- excessive steam consumption
- product quality problems
- unusually high consumption of spare parts
- production flow limitation problems



Source: Sutton Technical Books, Process Safe Limits

Figure 59. Example of safe limit range

The second range lies between the safe upper limit and the safe lower limit (210 - 275 in figure 59). These parameters are sometimes referred to as “Not to Exceed” limits. If the value of the parameter goes outside this range then the process is, by definition, unsafe, and action must be taken. The option of doing nothing is not an option. It is likely that, once these safe limits are breached, safety devices, particularly instrumentation systems, will be activated. Operations personnel should understand the consequence of exceeding the limits; they should also be provided with procedures and training as to what actions to take to bring the variable back into the safe range. If the operations team wishes to operate outside the safe range, say

to increase production rates, they can only do so after implementing the management of change process.

The third range shown in figure 59 defines emergency conditions. If a variable value goes outside the emergency limit range, urgent action is required. It is probable that an excursion outside the safe limits will lead to activation of emergency instrumentation and mechanical safety devices, such as pressure relief valves.

Some safe limits may have no meaningful value. For example, if a pressure vessel is designed for full vacuum operation, then that vessel has no safe lower limit for pressure. In table 5, no value for a safe upper limit for high flow is provided because the system is safe even when the pumps are running flat-out with all control valves wide open.

MAXIMUM ALLOWABLE WORKING PRESSURE (MAWP)

One particularly important safe limit value to understand is that of maximum allowable working pressure (MAWP) for pressure vessels. Since the concept of MAWP is so important, and since it is not always well understood, the following guidance, based on ASME terminology using V-101 in figure 58 as an example is provided.

As the process design is being developed, the process engineers require that V-101 be designed for a maximum pressure of 95.0 psig. This is the design pressure or pressure rating of the vessel (it is measured at the top of the vessel).

The process engineer's target values are transmitted to the vessel engineer. He or she designs the vessel using standard sizes for wall thickness and flange size, thus generating the MAWP, which is the maximum pressure at which the vessel can be operated. Generally MAWP is higher than the design pressure because wall thicknesses are in discrete sizes, and the designer will always choose the standard value greater than that called for. In the example, since it is unlikely that he/she can design for exactly 95.0 psig, the designer selects the next highest level, which turns out to give a MAWP of 120.0 psig. Once the vessel is in operation, the vessel can be operated at up to 120 psig without exceeding its safe limits. MAWP is the pressure that will be used for setting relief and interlock values.

The test pressure for the vessel is 1.5 times design pressure. Anytime the vessel is opened, it will be tested to that pressure before the process is restarted.

If the pressure goes above test pressure, the vessel walls are close to their yield point. Up to twice the MAWP value the vessel or associated piping may be slightly distorted, but any leaks are most likely to occur at gaskets. At 2 to 4 times MAWP, there will probably be distortion of the vessel, and it can be assumed that gaskets will blow out.

The vessel's burst pressure will typically be in the range of 3.5 to 4 times MAWP. Therefore, for this example, the burst pressure would be between 400 and 500 psig. (It is difficult to predict this value accurately because so few vessels actually fail, so there is not much field data.)

Because temperature affects the strength of a vessel (higher temperatures make the metal yield more easily), the MAWP has an associated temperature. The effect of high temperature

on equipment strength can be very deleterious. For example, the MAWP for a certain vessel may be 150 psig at a temperature of 600ºF. At 1000ºF, the same piece of equipment will fail at just 20 psig. On the other hand, at 100ºF, it may be able to handle nearly 300 psig. Hence, when temperatures are changing, the nominal pressure rating can be very misleading. (In this context, metal temperature refers to the average metal temperature through its entire depth.)

Although the MAWP should never be exceeded during normal operation, it may be acceptable for the operating pressure to go above the MAWP for brief periods of time, say during an emergency situation. However, following such an excursion, the vessel should be checked by a qualified vessel expert before being put back into service.

If equipment and piping are designed by rigorous analytical methods, such as finite element analysis, it is possible to operate with a lower safety margin than is required by the use of MAWP.

c. Explain the use of reset/rate/proportional controls used in process controls, feedback controls, control of system stability, etc.

Reset/Rate/Proportional Controls

The following is taken from Industrial-Electricity, *Understanding Gain-Reset-Rate*.

The terms gain, reset, and rate are functions that determine how fast a controller will change the output signal. They are also called modes of operation, and their functions were developed with the early pneumatic controllers and vacuum-tube controllers and later refined with op amp controllers. These basic modes of controller response were based on mathematical formulas (algorithms) that have been used for many years to solve complex problems. These formulas are derived from the calculus functions proportional, integral, and derivative. Today, companies that make process control equipment will use the terms gain, reset, and rate interchangeably with the terms proportional, integral, and derivative. This tends to make it more difficult for someone trying to learn process control theory. Table 6 shows the relationship of these terms. The terms gain, reset, and rate originally referred to controller operation. Proportional, integral, and derivative refer to the math functions used to make the controller perform the actions of gain, reset, and rate.

Table 6. Comparison of the PID terms proportional, integral, and derivative to the terms gain, reset, and rate.

proportional	gain
integral	reset
derivative	rate

Source: Industrial-Electricity, Understanding Gain-Reset-Rate

Another problem with the terms gain, reset, and rate, and the terms proportional, integral, and derivative has occurred with the advent of the microprocessor chip. Since the original calculation in the microprocessor uses formulas, these formulas can be changed slightly to provide different types of controller response when new models are produced each year. This means that several different responses may be found when using the gain function from

different brand names of controllers or from different models of the same controller from year to year because a different formula to calculate the gain may have been used.

This may not be a problem for someone learning process control for the first time, but it is definitely a problem for someone who learned how a proportional controller or integral controller operated with op amps or pneumatic controllers. The function of proportional control is rather fixed and limited with the op amp or pneumatic controller and people became familiar with this type of response. In modern microprocessor controllers, the response the manufacturer calls proportional may have enhancements to the calculation the microprocessor performs so that the controller response reacts differently than traditional proportional control. The enhancements were added through the years to make the controller provide better response and control. This means that the engineer will only need to understand the basic functions of gain, reset, and rate, or proportional, integral, and derivative to determine how this response will react. From these basic functions the engineer will be able to determine the specific detailed differences between brand names of controllers when they are used in the field.

The following is taken from Industrial-Electricity, *Using Gain for Control*

To make it easier to understand the function of gain, a microprocessor controller will be used in the coming examples. The simplest type of control to understand is called gain, where the controller uses gain as a multiplying factor. The controller uses a mathematical calculation called the algorithm to compute the amount of output for each change of error. This means that the processor is continually checking (sampling) the value from its sensor, which is the process variable (PV), and comparing this value to the set point (SP). This comparison takes place at the summing junction; the result is called error. It should be pointed out that the function of the summing junction is performed by a calculation; in older controllers this function was performed by op amps. The formula for error is as follows:

Error = Set point - Process Variable

or:

E = SP - PV

Note that some applications will use the formula E = PV – SP.

The error can be a positive number or a negative number, depending on the amount of the values; e.g., if the SP for a laboratory furnace is 450°F and the sensor indicates the actual temperature (PV) is 445°F, the error would be a positive 5°F. If the PV temperature is 455°F and the SP is 450°F, the error would be a negative 5°F. In this application, the controller is designed to change the output so that heat is added to the furnace if the error is positive, and to turn off the heat source if the error is negative.

The controller takes the error from the summing junction and uses the algorithm to calculate the amount of output. The algorithm can be a complex formula but it can be simplified as shown.

Output = Gain x Error

$$M_o = K_c \times E$$

In the formula, the output is referred to as M_o; the gain is referred to as K_c, which stands for controller (c) constant (K); and E is error. These terms have become standards for the ISA. ISA was formed to standardize and promote the process control and instrumentation industry. Some companies that design process control and motion control equipment may use slightly different designations for the variables in these formulas.

The following example will help explain how the error and gain are used by the controller to change the output to respond to the changes to the system. At the start of this example, the temperature (PV) inside a laboratory furnace is room temperature (75°F) and the SP is 75°F. The amount of error at this point is zero, and the controller sets the output to zero. The engineer starts the oven by entering a new SP at 100°F and sets the gain to a value of 2 in the controller. When the controller sees the new SP of 100°F, the error is calculated (100 - 75 = 25). The controller uses the error of 25 and multiplies it times the gain of 2 and the output is set to 50 percent. Remember that the output can only be set to values between zero and 100 percent.

When the output is set to 50 percent, the heating element begins to add heat to the furnace and the sensor continually sends the PV signal to the controller to indicate the increasing temperature. The controller is constantly recalculating the changing error and setting the new output. The following table shows a progression of these calculations as the controller samples the change in the PV and recalculates the output. The controller uses a sample time to determine how quickly to recalculate the output signal. The sample time may be fixed, or it may be adjustable in some controllers. Table 7 shows the calculations the controller makes.

Table 7. Calculations the controller makes to continually change the output as the PV changes

SP-VP = Error	Error × Gain = Output
100°F - 75°F = 25°F	25 × 2 = 50%
100°F - 80°F = 20°F	25× 2 = 40%
100°F - 85°F = 15°F	15× 2 = 30%
100°F - 90°F = 10°F	10× 2 = 20%

Source: Industrial-Electricity, Using Gain for Control

It should be noted that error is actually a percentage of the SP-PV over the total number of degrees (span) the system can control. For this example, the span is set for 100°F so the number of degrees of error is also the percentage of error.

From the calculations in table 7, notice that the controller continually reduces the percentage of output as the PV temperature inside the furnace increases and the temperature gets closer to the SP. The controller will need approximately 30% output to sustain the 85° temperature, and if the output is lowered below 30% the temperature will begin to decrease. This means that the controller will level out at some point and hold the output steady.

Video 25. Proportional controls

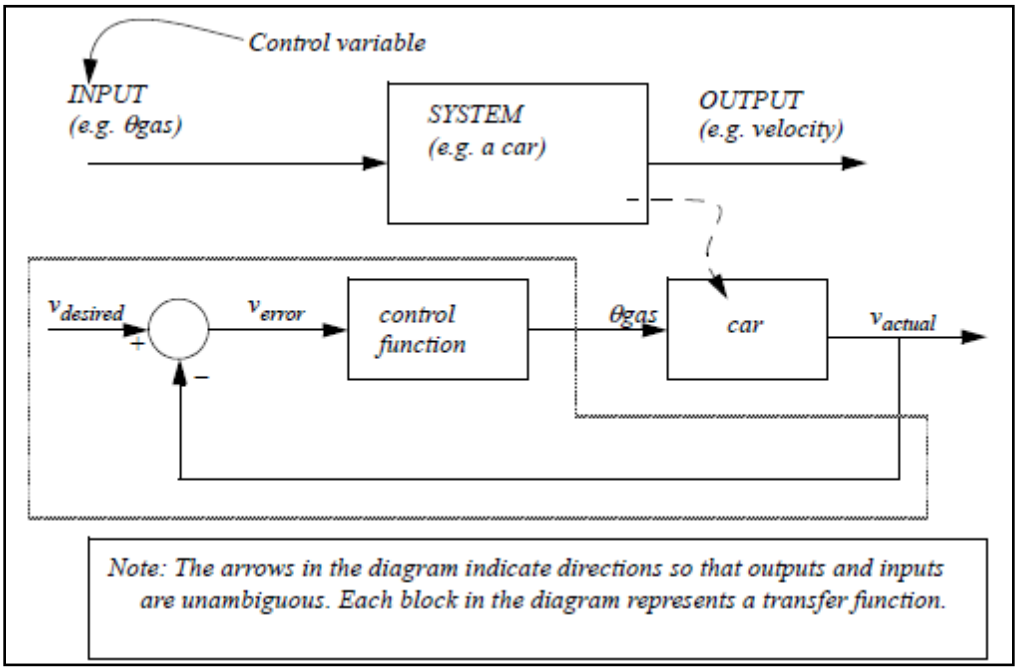
http://www.bing.com/videos/search?q=proportional+controls&view=detail&mid=FAA399F548BD80BAA95BFAA399F548BD80BAA95B&first=0

Feedback Controls

The following is taken from Grand Valley State University, *Feedback Control Systems.*

Figure 60 shows a transfer function block for a car. The input, or control variable, is the gas pedal angle. The system output, or result, is the velocity of the car. In standard operation, the gas pedal angle is controlled by the driver. When a cruise control system is engaged, the gas pedal must automatically be adjusted to maintain a desired velocity set point.

To do this, a control system is added. In the figure, it is shown inside the dashed line. In this control system, the output velocity is subtracted from the set point to get a system error. The subtraction occurs in the summation block (the circle on the left hand side). This error is used by the controller function to adjust the control variable in the system. Negative feedback is the term used for this type of controller.



Source: Grand Valley State University, Feedback Control Systems

Figure 60. An automotive cruise control system

There are two main types of feedback control systems: negative feedback and positive feedback. In a positive feedback control system, the set point and output values are added. In a negative feedback control, the set point and output values are subtracted. As a rule, negative feedback systems are more stable than positive feedback systems. Negative feedback also makes systems more immune to random variations in component values and inputs.

The control function in figure 60 can be defined many ways. A possible set of rules for controlling the system is given in figure 61. Recall that the system error is the difference

between the set point and actual output. When the system output matches the set point, the error is zero. Larger differences between the set point and output will result in larger errors. For example, if the desired velocity is 50 mph and the actual velocity 60 mph, the error is -10 mph, and the car should be slowed down. The rules in the figure give a general idea of how a control function might work for a cruise control system.

Human rules to control car (also like expert system/fuzzy logic):

- If v_{error} is not zero, and has been positive/negative for a while, increase/decrease θgas
- If v_{error} is very big/small increase/decrease θgas
- If v_{error} is near zero, keep θgas the same
- If v_{error} suddenly becomes bigger/smaller, then increase/decrease θgas.
- etc.

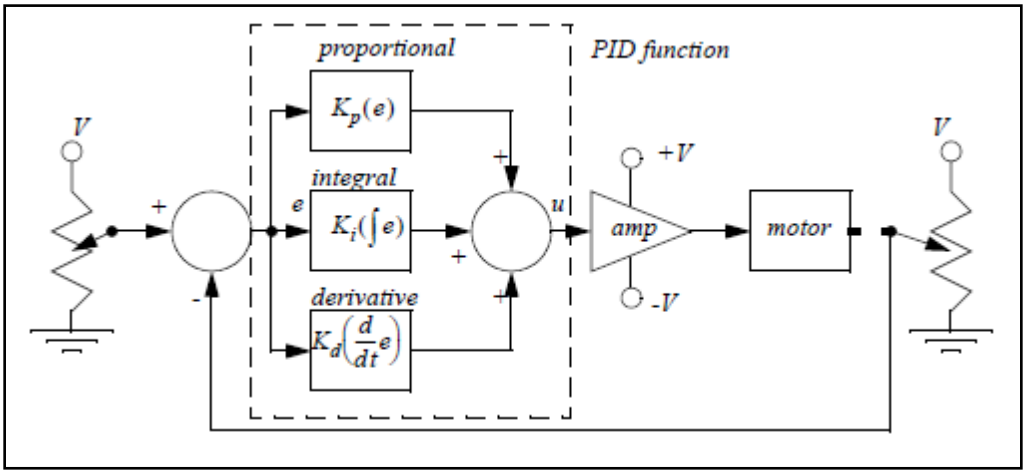
Source: Grand Valley State University, Feedback Control Systems

Figure 61. Example control rules

Proportional Integral Derivative Controls

The following is taken from Grand Valley State University, *Feedback Control Systems*.

The proportional integral derivative (PID) control function shown below is the most popular choice in industry. In the equation given, the 'e' is the system error, and there are three separate gain constants for the three terms. The result is a control variable value.



Source: Grand Valley State University, Feedback Control System

Figure 62. Basic PID controller

Figure 62 shows a basic PID controller in block diagram form. In this case the potentiometer on the left is used as a voltage divider, providing a set point voltage. At the output, the motor shaft drives a potentiometer, also used as a voltage divider. The voltages from the set point

and output are subtracted at the summation block to calculate the feedback error. The resulting error is used in the PID function. In the proportional branch, the error is multiplied by a constant to provide a long-term output for the motor. If an error is largely positive or negative for a while, the integral branch value will become large and push the system towards zero. When a sudden change occurs in the error value, the differential branch will give a quick response. The results of all three branches are added together in the second summation block. This result is then amplified to drive the motor. The overall performance of the system can be changed by adjusting the gains in the three branches of the PID function.

Video 26. Feedback controls

http://www.bing.com/videos/search?q=feedback+controls&view=detail&mid=34A5EB0BA8AF6939B19834A5EB0BA8AF6939B198&first=0

Control of System Stability

The following is taken from WikiBooks, *Control System/Stability*.

STABILITY

When a system becomes unstable, the output of the system approaches infinity (or negative infinity), which often poses a security problem for people in the immediate vicinity. Also, systems that become unstable often incur a certain amount of physical damage, which can become costly. The following paragraphs will deal with system stability, what it is, and why it matters.

BIBO STABILITY

A system is defined to be bounded input—bounded output (BIBO) stable if every bounded input to the system results in a bounded output over the time interval (t_o, ∞). This must hold for all initial times t_o. So long as we do not input infinity to the system, we will not get infinity output.

A system is defined to be uniformly BIBO stable if there exists a positive constant k that is independent of t_0 such that for all t_0 the following conditions apply:

$$\|u(t)\| \leq 1$$
$$t \geq t_0$$

implies that

$$\|y(t)\| \leq k$$

There are a number of different types of stability, and keywords that are used with the topic of stability. Some of the different types of stability are BIBO stable, marginally stable, conditionally stable, uniformly stable, asymptotically stable, and unstable. All of these words mean slightly different things.

DETERMINING BIBO STABILITY

One can prove mathematically that a system f is BIBO stable if an arbitrary input x is bounded by two finite but large arbitrary constants M and -M:

$$-M < x \leq M$$

Apply the input x, and the arbitrary boundaries M and -M to the system to produce three outputs:

$$y = f(x)$$
$$y = f(M)$$
$$y = f(-M)$$

Now, all three outputs should be finite for all possible values of M and x, and they should satisfy the following relationship:

$$y_{-M} \leq y_x \leq y_M$$

If this condition is satisfied, then the system is BIBO stable.

For a SISO linear time-invariant system is BIBO stable if and only if *g(t)* is absolutely integrable from [0,∞] or from

$$\int_0^\infty |g(t)|\,dt \leq M < \infty$$

EXAMPLE:
Consider the system

$$h(t) = \frac{2}{t}$$

Apply the test, selecting an arbitrarily large finite constant M, and an arbitrarty in put x such that -M < X < M.

As M approaches infinity (but does not reach infinity) it is shown that

$$y_{-M} = \lim_{M\to\infty} \frac{2}{-M} = 0^-$$

And

$$y_M = \lim_{M\to\infty} \frac{2}{M} = 0^+$$

So now the inequality is as follows:

$$y_{-M} \leq y_x \leq y_M$$
$$0^- \leq x < 0^+$$

This inequality should be satisfied for all possible values of x. However, when x is zero, the following is true:

$$y_x = \lim_{x\to 0} \frac{2}{x} = \infty$$

Which means that x is between -M and M, but the value y_x is not between y_{-M} and y_M. Therefore, this system is not stable.

Video 27. BIBO stability

http://www.bing.com/videos/search?q=system+stability&view=detail&mid=0F458C45C6C2667DA15F0F458C45C6C2667DA15F&first=0

POLES AND STABILITY

When the poles of the closed-loop transfer function of a given system are located in the right-half of the S-plane, the system becomes unstable. When the poles of the system are located in the left-half plane, the system is shown to be stable. A number of tests deal with this particular facet of stability: The Routh-Hurwitz Criteria, the Root-Locus, and the Nyquist Stability Criteria all test whether there are poles of the transfer function in the right-half of the S-plane.

If the system is multivariable, then the system is stable if and only if every pole of every transfer function in the transfer function matrix has a negative real part. For these systems, it is possible to use the Routh-Hurwitz, Root Locus, and Nyquist methods, but these methods must be performed once for each individual transfer function in the transfer function matrix.

POLES AND EIGENVALUES

The poles of the transfer function and the eigenvalues of the system matrix A are related. In fact, the eigenvalues of the system matrix A are the poles of the transfer function of the system. In this way, if the eigenvalues of a system are in the state-space domain, the Routh-Hurwitz, and Root Locus methods can be used as if the system was represented by a transfer function instead.

On a related note, eigenvalues, and all methods and mathematical techniques that use eigenvalues to determine system stability, only work with time-invariant systems. In systems which are time-variant, the methods using eigenvalues to determine system stability fail.

Video 28. Eigenvectors and eigenvalues

http://wn.com/eigenvalues#/videos

MARGINAL STABLITY

When the poles of the system in the complex S-Domain exist on the complex frequency axis (the vertical axis), or when the eigenvalues of the system matrix are imaginary (no real part), the system exhibits oscillatory characteristics, and is said to be marginally stable. A marginally stable system may become unstable under certain circumstances, and may be perfectly stable under other circumstances. It is impossible to tell by inspection whether a marginally stable system will become unstable or not.

Here are some rules concerning systems that are marginally stable. These theorems only apply to time-invariant systems:

- A time-invariant system is marginally stable if and only if all the eigenvalues of the system matrix A are zero or have negative real parts, and those with zero real parts are simple roots of the minimal polynomial of A.
- The equilibrium $x = 0$ of the state equation is uniformly stable if all eigenvalues of A have non-positive real parts, and there is a complete set of distinct eigenvectors associated with the eigenvalues with zero real parts.

- The equilibrium x = 0 of the state equation is exponentially stable if and only if all eigenvalues of the system matrix A have negative real parts.

CONDITIONALLY STABLE
A system with variable gain is conditionally stable if it is BIBO stable for certain values of gain, but not BIBO stable for other values of gain.

UNIFORM STABILITY
A uniform stability system is a system where an input signal in the range [0, 1] results in a finite output from the initial time until infinite time.

ASYMPTOTIC STABILITY
A time-invariant system is asymptotically stable if all the eigenvalues of the system matrix A have negative real parts. If a system is asymptotically stable, it is also BIBO stable. However, the inverse is not true: a system that is BIBO stable might not be asymptotically stable.

d. Explain the application of DOE-STD-1195-2011, Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities. This includes understanding of reliability analysis of safety instrumented systems, common mode/common cause failures, and life cycle management of I&C systems.

All the information for this KSA is taken from DOE-STD-1195-2011.

Reliability
To achieve the required reliability, the design can use industry standards developed for commercial nuclear power plant design for safety-related systems. These standards are listed in DOE G 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria Guide for Use with DOE O 420.1, Facility Safety*, for safety class instrumentation and control systems. However, the listed standards include some design requirements that are unwarranted for the design of safety significant (SS) SISs used in DOE nonreactor nuclear facilities.

An appropriate alternative means for meeting the reliability requirements for SS SISs is to use the processes outlined in ANSI/ISA 84.00.01-2004 – Part 1, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*. ANSI/ISA 84.00.01-2004 is used by the process industries for designing reliable SISs that are commensurate with the level of hazard mitigation or prevention strategy.

Common Cause Failures
The following is taken from DOE-STD-1195-2011.

Common cause failures (CCFs) can be either safe detected or undetected, or dangerous detected or undetected. The safety integrity level (SIL) verification calculation is concerned only with dangerous undetected failures. CCFs are influenced by physical and electrical separation, diversity, and the robustness of design of the component (ability to withstand environmental stressors).

ANSI/ISA 84.00.01-2004 uses the beta factor method to model common cause failures in a single SS SIS with redundant components. The beta factor normally falls within the range of 0 to 10 percent. When good engineering design is followed, the beta factor will generally fall within the range of 0 to 5 percent.

When physical and electrical separation is provided consistent with the intent of IEEE 384, *Standard Criteria for Independence of Class 1E Equipment and Circuits*, for two or more diverse SS SISs that are independent protection layers (IPLs) for a specific hazardous event, they may be considered as independent, and the addition of a CCF factor into the SIL verification calculation is not recommended.

A CCF factor should be included in the SIL verification calculation of an SS SIS when it is credited with another SS SIS IPL to reduce the risk of a specific hazardous event to a level defined in the safety basis documentation, the SS SISs have identical or similarly functioning components in any of the subparts of the systems, and when physical and electrical separation between SS SIS IPLs is not maintained.

For example, if both SS SISs for a hazard event use identical valves as the final control element to shut off flow, then a beta factor times the average probability of failure on demand (PFDavg) of the valve should be added to the final PFDavg value in at least one of the SS SIS SIL verification calculations. If an individual SS SIS has redundant architecture within a subpart and has included a beta factor to address this architecture, then no additional beta factor is recommended for using identical components in similar SS SIS IPLs for a specific event because a beta factor is already addressed in the SS SIS SIL verification calculation of one of the IPLs.

The following CCF term should be added to the total PFDavg of the SIL verification calculation for each component/subsystem that is identical between two or more SS SISs credited for a single hazard:

- $CCF = \beta \times \lambda \times (TI/2)$.
- β is the fraction of failures that impact more than one component/subsystem in a redundant configuration.
- λ is the undetected dangerous failure rate of the component/subsystem.
- TI is the time interval between functional tests of the component/subsystem.

Common Mode Failure

According to DOE-STD-1195-2011, a common mode failure is the failure of two or more channels in the same way, causing the same erroneous result.

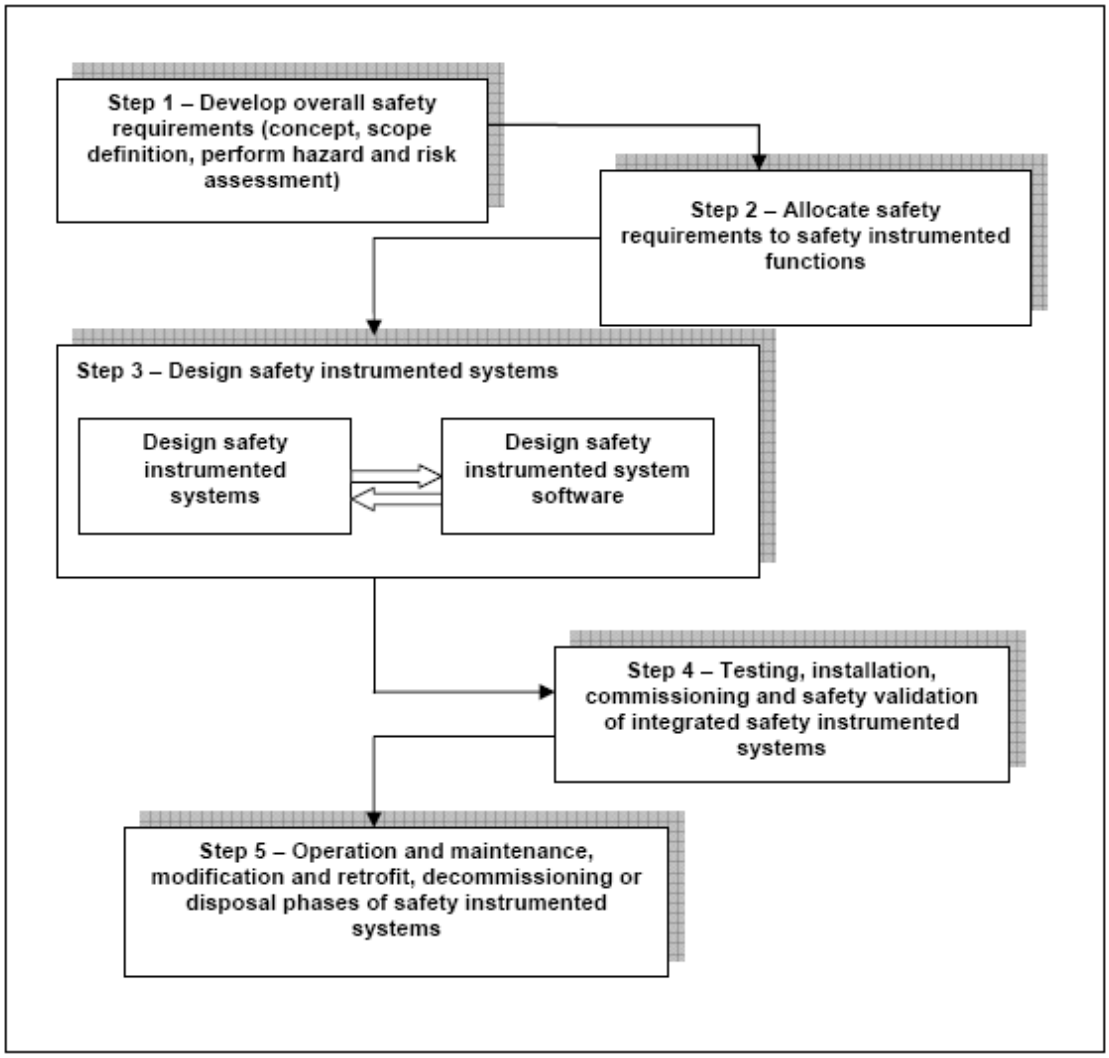
Life Cycle Management

A key aspect of the implementation of ANSI/ISA 84.00.01-2004 is effective control over each stage of the SIS life cycle to ensure proper initial design, proper installation, effective operation and maintenance, and configuration control. The processes for performing the life-cycle management for SIS should be defined, including identifying the organization(s) responsible for implementing them. The life-cycle stages outlined in ANSI/ISA 84.00.01-2004 can be fulfilled by conformance to the ANSI/ISA 84.00.01-2004 requirements or by

conformance to DOE orders, manuals, standards, and guides that provide equivalent processes and methods for the life-cycle stages of the safety instrumented functions.

The elements in the life cycle are hazards identification, safety requirements specification, design, installation, startup testing, management of change, operational testing, maintenance, operation, modification, and decommissioning of SIS. The life cycle also includes retention of the original documentation, including design criteria, procurement specification, commercial grade dedication files, and other relevant information for the life of the affected systems. Management of changes is applied in all steps of the life cycle.

This life-cycle approach is directed toward reducing the risks inherent in process facility operations. The ANSI/ISA 84.00.01-2004 approach can be summarized in five steps as depicted in figure 63.



Source: DOE-STD-1195-2011

Figure 63. Life cycle steps for SISs

STEP 1: DEVELOP OVERALL SAFETY REQUIREMENTS

This initial phase focuses on how much risk reduction will be required throughout the life cycle of the SIS. Some level of residual risk will always exist. The purpose of any safety system is to reduce the identified risk to an acceptable level as defined in the safety basis documentation.

Following the establishment of the conceptual requirements and scope definition, ANSI/ISA 84.00.01-2004 begins with a requirement to perform a hazard analysis, identification of hazards, and associated risks. The safety functions that are required to reduce the identified risks to an acceptable level are determined during this phase.

STEP 2: ALLOCATE SAFETY REQUIREMENTS TO SAFETY INSTRUMENTED FUNCTIONS

Acceptable risk is achieved by allocating safety requirements to various safety functions. The safety functions are then allocated to different systems, such as SC/SS mechanical or process systems, design features, SC or SS SISs, and other external hazard controls. When a safety function is allocated to an SIS, it is called a safety instrumented function (SIF). The allocation process also includes assigning an SIL to the SS SIF, which corresponds to the amount of risk reduction determined to be necessary in the hazard and risk analysis.

SILs can be expressed as either risk reduction factors (RRFs) or as a PFDavg. SILs have four discrete performance ranges and two kinds of controls; namely, those that respond on demand and those for continuous demand. The SIL is related to the average probability of the SIS failing when demanded to perform its safety function. In either case, ANSI/ISA 84.00.01-2004 applies. The SIL performance requirements in terms of the PFDavg and RRF are listed in table 8.

Table 8. SIL level and performance ranges for on-demand modes

SIL Level Designation	Probability of Failure On Demand-average (PFDavg)	Risk Reduction Factor (RRF)
SIL-1	$< 10^{-1}$ to $\geq 10^{-2}$ PFDavg	> 10 to ≤ 100 RRF
SIL-2	$< 10^{-2}$ to $\geq 10^{-3}$ PFDavg	> 100 to ≤ 1000 RRF
SIL-3	$< 10^{-3}$ to $\geq 10^{-4}$ PFDavg	> 1000 to ≤ 10,000 RRF
SIL-4	$< 10^{-4}$ to $\geq 10^{-5}$ PFDavg	> 10,000 to ≤ 100,000 RRF

Source: DOE-STD-1195-2011

SIL-1 represents the lowest risk-reduction level of performance; SIL-4 represents the highest risk-reduction level of performance. SIL-4 is not used in the process industry sector because it requires elaborate systems and is difficult to support due to the high level of reliability required of the hardware. SIL-4 systems are not expected to be used for SS controls in DOE facilities.

A number of methods (qualitative and quantitative) are available for assigning the SIL. Qualitative methods may be appropriate when the risk, implementing design, and the hardware are not well understood. Quantitative methods, such as fault tree or event tree

analysis, should be used when the design and hardware are well understood and supporting data are available.

Quantitative methods are required for verification that the final design and its installation meet the assigned SIL. Assigning the SIL links the design integrity of the SIS to the required level of risk reduction, and thereby closes the gap between the hazard analysis and safe process operation.

ANSI/ISA 84.00.01-2004 provides several methods for determining SIL, such as layer of protection analysis, which uses frequency of the event as a basis, or safety layer matrix, which uses available information of IPLs as a basis for selection of SIL for the SIS. For DOE's application, the accepted methodology is a deterministic method using the number of IPLs credited by hazard analysis.

STEP 3: DESIGN THE SIS AND SAFETY SOFTWARE

The SIL establishes a minimum required performance for the SIS, as measured by the PFDavg or RRF. The factors that affect the PFDavg or RRF are

- component failure rate
- redundancy/diversity of systems and components
- voting
- testing frequency
- diagnostic coverage
- common cause failure
- human factors
- technology
- software integrity

The user should design the SIS with hardware and software components considering the above factors to achieve the PFDavg or RRF related to the target SIL. The target SIL is an objective of design process decisions, component specification and procurement to ensure that the design is consistent with the target SIL. The design is verified at the end of the detailed design process to ensure that the design as installed and tested can achieve the assigned PFDavg or RRF.

STEP 4: TESTING, INSTALLATION, COMMISSIONING, AND SAFETY VALIDATION OF SIS

Testing is performed throughout the installation stages to enable validation and verification that SIS requirements are met. This phase of the life cycle addresses the policy that will be applied for the following:

- Integration of software and hardware
- Types of testing to be performed and data required to demonstrate functional adequacy and acceptance
- Environment necessary for conducting testing, along with the configuration that exists for testing
- Test criteria for which data will be collected and used to judge acceptability
- Physical locations (factory or site) for which the test will be performed

- Personnel requirements and qualifications required for performing the various activities related to the validation and verification functions
- Process for documenting and dispositioning non-conformances

In step 4, the SIS design is validated in its as installed configuration as achieving its assigned SIL.

STEP 5: OPERATION AND MAINTENANCE, MODIFICATION AND RETROFIT, DECOMMISSIONING OR DISPOSAL PHASES OF SISs

Long-term preservation of an SIS through startup, operation, maintenance, and management of change activities is as important as initial design and installation phases. The SIL is not just a design parameter; it is also an operational parameter. The selection made during conceptual or preliminary design phases, including design configuration, testing frequency, and so on, is maintained throughout the life of the facility. Therefore, it is essential that management of system change be maintained to ensure preservation of the SIS.

e. Explain the design considerations for sensors, logic solvers, and final control elements (e.g., structures, systems, and components diversity and redundancy, one-out-of- two/ two-out- of-three logic, etc.,) that are essential for reliable I&C systems design.

The following is taken from DOE-STD-1195-2011.

Three elements of safety software applications are as follows:

1. The sensor (may have internal logic; the primary function is to sense and transmit data or some form of aggregated data)
2. The logic device (processes information variables to determine their condition relative to a trip point, calculating transfer functions, or other process specific tasks)
3. The control element (an actuator, for example, performs a desired function based on the output results from the sensor or logic device).

The preceding elements are normally integrated using a network system with software of some type, such as an embedded program. Fieldbuses are also used for communication to field devices. Software development management control principles and software life-cycle elements apply to each of the above elements to the extent that the safety case can be verified for all safety subsystems and the overall safety system.

Prior to development of application software, an SIS software requirements specification should be developed that describes overall system operating requirements and functions, including applicable safety functions and safety requirements that form the safety basis for the system design. Safety software is designed to support one, or a combination of, the following:

- *Isolation.* Critical components are separated from each other in a manner to preclude undefined interactions. When applied to software design, the emphasis is on encapsulation, information hiding, and formal interfaces that preclude SIS failure due to unintended software execution or malfunction.
- *Independence.* The stimuli for actions originate from, and are handled by, separate components. This is generally implemented by redundant components, often with

different designs that support a safety-related task. As applied to software, independent hardware inputs are directed to independent software modules.

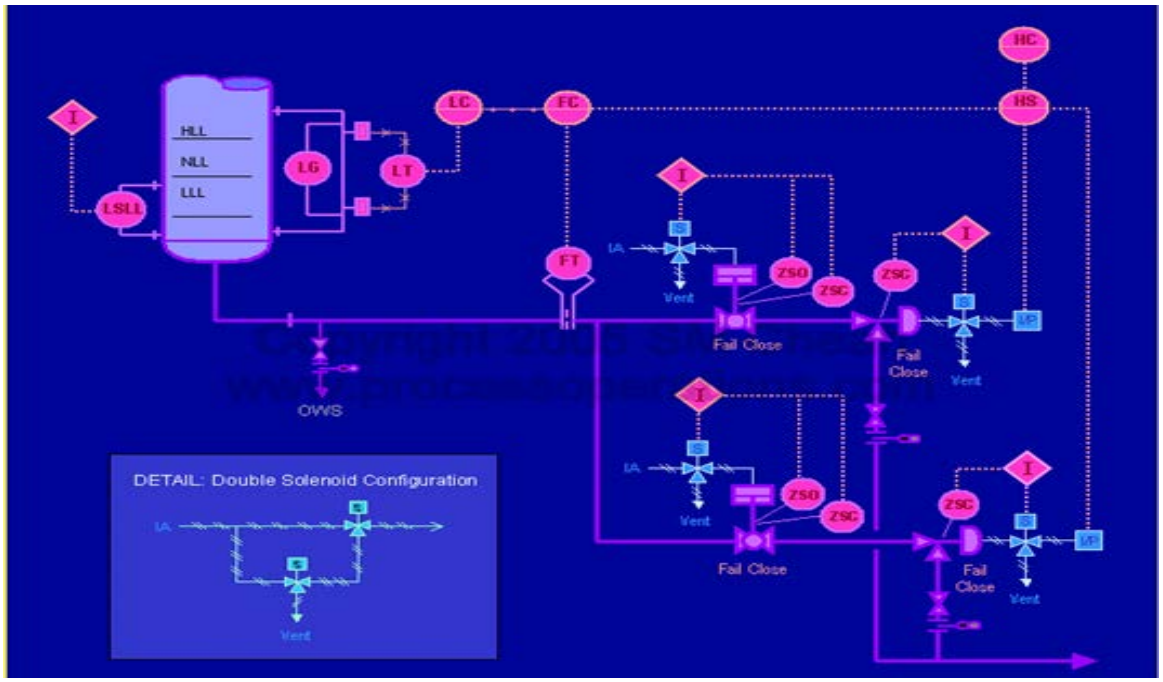
- *Inoperability.* Abnormal conditions cause a component to become inoperable in a safe, predictable manner and before any isolation features are compromised. As applied to software design, these criteria may be implemented through comprehensive exception handling and fail-safe designs in critical components.
- *Incompatibility*. Components in different parts of the system cannot operate together in a satisfactory manner. To avoid incompatibility, consider that sensors, a logic device, and control devices may have embedded software that needs to be integrated into a networked system. The acceptability of the integration needs to be validated.

Embedded software is generally used for software/hardware integration, and fieldbus is used for networking and communication purposes. Fieldbuses used to implement safety functions should follow the design considerations listed in ISA TR84.00.06, *Safety Fieldbus Design Considerations for Process Industry Sector Applications*.

Redundancy and Diversity of Components

The following is taken from Process Operations, *Redundancy and Diversity*.

Redundancy refers to the duplication of protective systems. If the failure of any sensor is of concern (i.e., a nuisance trip or a fail-to-function failure), then redundant or multiple sensors may be used. Ideally, the possibility of two sensors failing at the same time should be very remote.



Source: Process Operations, Redundancy and Diversity

Figure 64. Example of redundancy

An example of redundancy in field devices is shown in figure 64. Unfortunately, this does not account for common cause failures, which might impact multiple sensors at the same

time. If multiple sensors are used, they should be connected to the process using different taps and separate power supplies to avoid common plugging and power failures. Using different sensors from different manufacturers (diversity) or having different maintenance personnel work on the sensors may help to avoid the possibility of the same person incorrectly calibrating all the sensors.

SAFETY TRANSMITTERS AND TRANSMITTER REDUNDANCY

Most conventional transmitters are not inherently fail safe, catching only 30-35 percent of internal failures; therefore, they can adversely affect the overall reliability of an SIS. Even the so-called smart designs do not measure up for some critical applications.

Traditionally, the answer to this problem has been to have transmitter redundancy with more than one transmitter measuring the same variable. Separate taps are recommended to avoid common fault mode faults, such as plugged impulse lines. Each transmitter has a vote to shut down an SIS, but may not do that depending on the overall system architecture. Besides redundancy, another method of adding safety and reliability is to employ a combination of conventional transmitters and discrete switches. However, the benefit of being able to compare live readings of two analog instruments is lost.

Failure modes of conventional electronic transmitters usually, but not always, are downscale. In the case of a level control application, a downscale failure mode is quite undesirable. An indication of low level would cause the control system to continue adding liquid to a vessel and could cause a potentially hazardous overflow.

A safety-related transmitter uses the same kind of comprehensive diagnostics as a safety PLC to attain certifiable fail-safe operation.

Some of the key features of safety transmitters are

- a high level of self-diagnostics
- a high level of measurement diagnostics
- the ability to transmit diagnostics to the SIS's safety-related logic solver

Diverse redundancy uses a different technology, design, manufacture, software, etc., to reduce the influence of common cause failures.

Using two level measuring devices on a tank is an example of redundancy, while using a level measuring device combined with a device for measuring weight of liquid in the tank is an example of diversity.

Redundancy and diversity are effective when failures are random. They are less effective when failures are due to wear or when failures are systemic. For example, if failure is due to corrosion, two identical systems will corrode at the same rate. Two diverse systems, made from different materials of construction, may give extra protection, but they may both corrode. The ultimate example of a systemic failure is an error or ambiguity in an instruction.

DIVERSITY

As SIL values rise so does the need for diversity in the SIS. At SIL_3 the IEC standards expect redundant and diverse systems. At SIL_4 significant efforts should be made to avoid the risk of

common cause failures by having redundant and diverse sensing systems connected to redundant and diverse logic solvers, e.g., a solid state logic solver with a redundant programmable electronic system logic solver.

One-Out-of-Two and Two-Out of Three Logic Schemes

The following is taken from Control, *Safety Systems for Non-Engineers*.

SIS logic solvers use the input provided by the sensors and execute the program logic that eventually results in an automated emergency shut-down. For example, a one-out-of-two logic design monitors two inputs. If either of those inputs changes states, the logic solver executes the shut-down sequence. A two-out-of two logic design uses two inputs, and both must agree for the logic solver to initiate the shut-down. There are a number of different design types, one-out-of-one, one-out-of two, two-out-of two, two-out-of three, etc., and it is quite common to mix analog and discrete inputs. This is called using diverse technologies, and it is very useful in eliminating false or nuisance shut-downs resulting from common-cause failures.

f. Explain how human factors engineering criteria and requirements are used for safe and efficient operations (e.g., use of DOE-STD-1186-2004, *Specific Administrative Controls*, NUREG-0700, "Human-System Interface Design Review Guidelines," etc.).

The following is taken from DOE-STD-1186-2004.

Human actions, either taken in response to an event or taken proactively to establish desired conditions, are subject to errors of omission or commission. Experience shows that administrative controls are prone to common cause failure. The following attributes have proven value in improving worker performance in using administrative controls:

- Use of reader/worker/checker systems
- Independent verification
- Positive feedback systems
- Interlocks
- Warning signs and barriers
- Alarms and monitors
- Human factor analysis
- Operator training and certification
- Continuing training and re-qualification
- Abnormal event response drills
- Ergonomic considerations in procedures
- Dry runs for non-routine operations
- Use of double staffing or direct supervision for hazardous operations
- Human reliability assessment

Each of the listed attributes used to improve worker performance in using administrative controls should be carefully evaluated for improving the dependability of specific administrative controls (SAC). Implementation of each of these attributes may not be practical or necessary for every SAC.

The following is taken from the U.S. Nuclear Regulatory Commission, NUREG 0700.

The design of human-system interfaces (HSIs) should support the operating personnel's primary task of monitoring and controlling the plant, without imposing an excessive workload associated with using the HSI (window manipulation, display selection, and navigation, for example). The HSI also should support the recognition, tolerance, and recovery from any human errors. Human factors engineering guidelines for design review help to ensure that these goals are achieved. The high-level design-review principles discussed here represent the generic HSI characteristics necessary to support personnel performance. While these principles are not detailed review guidelines, they can be used to support the evaluation of aspects of the HSI not well defined by the detailed guidelines. Thus, for example, they can be used in reviewing novel HSI designs, such as display formats not identified in the guidelines. They can also support the evaluation of the significance of individual discrepancies in the guidelines.

The 18 principles are divided into four categories: general principles, primary task design, secondary task control, and task support (summarized in table 9). The categories and the principles that comprise them are described in the following paragraphs.

Table 9. Design review principles

Category	Principle
General	Personnel safety Cognitive compatibility Physiological compatibility Simplicity of design Consistency
Primary task design	Situation awareness Task compatibility User model compatibility Organization of HIS elements Logical/explicit structure Timeliness Controls/displays compatibility Feedback
Secondary task control	Cognitive workload Response workload
Task support	Flexibility User guidance and support Error tolerance and control

Source: U.S. Nuclear Regulatory Commission, NUREG-0700

General Principles

These principles ensure that the HSI design supports personnel safety, and is compatible with their general cognitive and physiological capabilities:

- *Personnel Safety*. The design should minimize the potential for injury and exposure to harmful materials.

- *Cognitive Compatibility*. The operator's role should consist of purposeful and meaningful tasks that enable personnel to maintain familiarity with the plant and maintain a level of workload that is not so high as to negatively affect performance, but sufficient to maintain vigilance.
- *Physiological Compatibility*. The design of the interface should reflect consideration of human physiological characteristics, including visual/auditory perception, biomechanics (reach and motion), characteristics of motor control, and anthropometry.
- *Simplicity of Design*. The HSI should represent the simplest design consistent with functional and task requirements.
- *Consistency.* There should be a high degree of consistency between the HSI, the procedures, and the training systems. At the HSI, the way the system functions and appears to the operating crew should always be consistent, reflect a high degree of standardization, and be fully consistent with procedures and training.

Primary Task Design

These principles support the operator's primary task of process monitoring, decision-making, and control to maintain safe operation:

- *Situation Awareness*. The information presented to the users by the HSI should be correct, rapidly recognized, and easily understood, and support the higher-level goal of user awareness of the status of the system.
- *Task Compatibility*. The system should meet the requirements of users to perform their tasks. Data should be presented in forms and formats appropriate to the task, and control options should encompass the range of potential actions. There should be no unnecessary information or control options.
- *User Model Compatibility*. All aspects of the system should be consistent with the users' mental models. All aspects of the system also should be consistent with established conventions.
- *Organization of HSI Elements*. The organization of all aspects of the HSI should be based on user requirements and should reflect the general principles of organization by importance, frequency, and order of use. Critical safety-function information should be available to the entire operating crew in dedicated locations to ensure its recognition and to minimize data search and response.
- *Logical/Explicit Structure*. All aspects of the system should reflect an obvious logic, based on task requirements or some other non-arbitrary rationale. The relationship of each display, control, and data-processing aid to the overall task/function should be clear. The structure of the interface and its associated navigation aids should make it easy for users to recognize where they are in the data space and should enable them to get rapid access to data not currently visible. The way the system works and is structured should be clear to the user.
- *Timeliness*. The system design should take into account users' cognitive processing capabilities as well as process-related time constraints to ensure that tasks can be performed within the time required. Information flow rates and control performance requirements that are too fast or too slow could diminish performance.
- *Controls/Displays Compatibility*. Displays should be compatible with the data entry and control requirements.

- *Feedback*. The system should provide useful information on system status, permissible operations, errors and error recovery, dangerous operations, and validity of data.

Secondary Task Control

These principles minimize secondary tasks, i.e., tasks that personnel perform when interacting with the human-system interface that are not directed to the primary task. Examples of secondary tasks include activities associated with managing the interface, such as navigation through displays, manipulating windows, and accessing data. Performing secondary tasks detracts from the crew's primary tasks, so the demands of secondary tasks must be controlled as follows:

- *Cognitive Workload*. The information presented by the system should be rapidly recognized and understood; therefore, the system should minimize requirements for making mental calculations or transformations and use of recall memory. Raw data should be processed and presented in directly usable form.
- *Response Workload*. The system should require a minimum number of actions to accomplish an action; e.g., single versus command keying, menu selection versus multiple command entry, single input mode versus mixed mode. In addition, the system should not require the entry of redundant data, nor the re-entry of information already in the system or information the system can generate from already resident data.

Task Support

These principles address the characteristics of the HSI that support its use by personnel, such as providing 1) HSI flexibility so tasks can be accomplished in more than one way, 2) guidance for users, and 3) mitigation of errors as follows:

- *Flexibility*. The system should give the user multiple means to carry out actions and permit displays and controls to be formatted in a configuration most convenient for the task. However, flexibility should be limited to situations where it offers advantages in task performance; it should not be provided for its own sake because there is a tradeoff with consistency and the imposition of interface management workload.
- *User Guidance and Support*. The system should provide an effective "help" function. Informative, easy-to-use, and relevant guidance should be provided on-line and off-line to help the user understand and operate the system.
- *Error Tolerance and Control*. A fail-safe design should be provided wherever failure can damage equipment, injure personnel, or inadvertently operate critical equipment. Therefore, the system should generally be designed such that a user error will not have serious consequences. The negative effects of errors should be controlled and minimized. The system should offer simple, comprehensible notification of the error, and simple, effective methods for recovery.

g. Explain the basic requirements for control room design, displays, annunciators, and operators' interface.

Control Room Design

The following is taken from Electric Energy Publications, *Proper Control Room Design Facilitates Critical Thinking and Situational Awareness*.

> In today's fast-paced electric utility, there are many forms of data available for analysis in a mission-critical control room. With the introduction of smart grid data such as outage management, geographic information systems, advanced metering infrastructure and substation automation data, the quantity of information is expected to grow exponentially.

Proper control room layout optimizes data visualization and interpretation for operations. As the electric industry is pushed to evolve, real-time visual analytics and three- and four-dimensional data will no longer be the exception, but the norm. Unless the operator work environment is enhanced, and the data presentation is streamlined and visually available for interpretation, an operator may be overwhelmed in an emergency. The proper planning, design, and control room components—including the proper ergonomic alignment and layout of each component—are crucial for optimal situation awareness and data interpretation.

WHAT ARE THE KEY COMPONENTS OF A CONTROL ROOM?

Key to the success of critical decision-making is the functional design of the control room itself. Integration firms specializing in mission-critical control room design are aware of the idiosyncrasies that contribute to a highly functional environment. Creating this environment begins with an information exchange with utility personnel who clearly understand the process, systems, and applications of the control center environment. In addition to the physical components (e.g., work station and office location, lighting, acoustics, etc.), the software and other tools used by the operator must also be considered carefully. The resultant design and solution set is one that best meets the needs of the operations staff and their unique operating environment.

Within this design, there are four critical factors or components to consider: spatial, ergonomic, environmental, and functional, each of which is summarized in the following.

Spatial considerations include room size, layout of the workspaces, number of users and functional requirements. When evaluating the room size, consideration should be given to the number of workstations, individual offices, shared or common spaces, display wall requirements, and any other required equipment. Proper placement of this equipment requires analysis for the total physical space of each component as well as the appropriate line of sight.

A sight line analysis is a critical piece of any control room design to assure each user is aware of any visual data required of their operational performance. This analysis should include, at a minimum, operator workstation viewing angles and display wall technologies. Combined, the proper placement of work station equipment and the most favorable visual viewing scenarios provide the optimal work environment for control room operators.

Ergonomics is the study of the relationship between workers and their work environment and is an integral piece of the control room design. Operator positioning and comfort contribute to proper data interpretation. With the emergence of computers into the work environment, individuals spend more time in static positions while undertaking repetitive tasks. Proper ergonomic design minimizes the inherent risks of repetitive tasks, awkward posture, and maintaining of a certain posture for a prolonged period of time.

Workspace design should allow the user to move and or change positions throughout the day. Useful ergonomic considerations include flexible mounting of fixtures for monitors, telephones, shelving and other accessories. Swivel arms allow movement, vertically and horizontally, for monitors to accommodate a wide range of sightlines. Proper height, width and depth of workspaces will comfortably accommodate the knee space up to the 95th percentile for male operators. Proper positioning of lighting reduces glare on the monitors, thus reducing operator eyestrain. Providing the proper work environment is proven to increase productivity, improve work quality, heighten worker satisfaction, and most importantly, reduce or eliminate human error.

When designing a control room, consideration should be given to the environmental impacts in the room. These include the acoustics, electrical/HVAC, and lighting. Proper design of the acoustics ideally suppresses all reverberant, mechanical, and other noises of the area. The room should ensure speech privacy while controlling ambient noise levels and containing the electronic system noises from adjacent spaces. Redundancy, power conditioning, power circuit delay and sequencing, and proper grounding and bonding of electronic system components contribute to proper electrical design.

The HVAC system should handle the heat load of the electronic systems and control the temperature and humidity levels to remain in compliance with the electronic system specifications. Ideal ambient room temperature is recommended between 70 and 72 degrees F. The relative humidity of the area should be 45-65 percent with air movement less than 4 inches to 6 inches per second. Lighting can bring some unique challenges. Most times, control rooms use indirect light where the ceiling is used to reflect the light downward.

The ceiling reflectance value should be 0.8 or greater. Ideally, walls should be covered with a matte finish with a reflectance value of 0.5 to 0.6 and be off-white in color. Floor coverings should have a reflectance value of 0.2 to 0.3 for carpet and 0.25 to 0.15 for tile. Adjustable task lighting is recommended at each operator work position. If the room includes a display wall, any lighting in front of this wall should be greater than 40 foot-candles.

Displays

Many control rooms are enhanced with the addition of display technologies. These technologies allow improved visual representation of data, which can accelerate insight and interpretation, particularly at crucial moments. Special consideration should be given to equipment used in mission-critical applications since not all video panels are manufactured for twenty four hours a day, seven days a week (24/7) operation.

Equipment such as liquid-crystal display panels can easily be tiled together to create a display wall. While this equipment is readily available and less expensive than rear or front-projection systems, these panels are not made for 24/7 operation.

Since these panels do not create a scalable image due to the larger mullion between panels, the operator is required to concentrate harder to interpret the data. Additionally, if static images are displayed for a prolonged period of time, the panel will create shadows of this image or suffer what is commonly referred to as “burn-in,” which is exacerbated by the persistence of the screen itself.

Front projectors – commonly used in boardrooms – are an option, but with some limitations. While they allow visualization of schematic, geographic, and other types of displays, not all are rated for 24/7 operating environments. Also, the cooling fans associated with projection-style displays can be an annoying distraction in the control room environment where concentration is of paramount importance. Front projectors will also require manual maintenance in the event of a malfunction, another potentially disruptive reality.

Video display cubes offer many attractive options including a range of technologies; multiple configurations and sizes; many resolutions; zero mullion design; and light, color and brightness management. These systems can be expanded to include audio and visual equipment, and can provide for inclusion of live video feeds such as news, weather, and security cameras. Maintenance advantages of video cube displays include redundancy of components and lamps, automatic color reconfiguration, and brightness modification.

To enhance the capabilities of the video display wall, software is often integrated to manage displays and provide flexible video feeds. This software offers advanced wall management control by interacting with the content sources to place the content on the wall. It also provides control of the data feeds for cameras, news, and other visual content. Optional features are available to provide “screen scraping” of displays from other systems or to assign areas of the wall to specific users.

Adding data visualization software — software that inter-operates with the video display wall and wall management software to further improve the quality of the content displayed — is a key component to a successful display wall solution. In fact, it is the content that aids the operator in decision-making; not the hardware or the software.

Rather than scaling the existing data to create a larger display, the data can be built and enhanced for better and quicker analysis, and may incorporate other tools such as graphics, charts, trends, and symbols.

Exercising proper placement and consideration of each individual control room component leads to a work environment that is free of obstacles, and that includes clear and unobstructed views of operational data while providing optimal situational awareness.

CRITICAL THINKING AND SITUATIONAL AWARENESS

Critical thinking is the skilled, active interpretation and evaluation of observations, communications, information, and argumentation. Situational awareness is the perception of environmental elements within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future. By applying these concepts and principles to the control room setting, operators are empowered to make decisions based on the information provided to them. For them to make effective decisions, it is imperative that

they are provided with the required information, that the information comes from all necessary sources, that the data is received in a timely manner, and that there isn't any question as to the quality of the data.

ENHANCED DECISION MAKING AND SITUATIONAL AWARENESS

To enhance decision-making and improve situational awareness, map boards have traditionally been a useful control room component. As the need for more data moves into the control room, it is imperative that the operations staff has the proper tools available to improve processing and interpretation of this data.

Currently, control rooms use various kinds of display wall tools. These tools include metal or mosaic tile walls, large-scale paper drawings and maps, electronic panels, front projectors, and front- or rear-projection video systems. It is not uncommon for control rooms to incorporate some or all of the above in various combinations.

The large static display walls typically represent a schematic view of important service areas or an entire service territory. While this comprehensive view is useful, it does not offer real-time views or current system status. An operator still needs to interpret data from a workstation console and/or the wallboard, and then mentally combine this data prior to deciding on a proper response.

When a static wall incorporates LEDs or digital displays, it begins to add a situational awareness dimension. This added functionality contributes to the functionality of the system by adding a dynamic dimension to the schematic view of the system. However, simple indicators are often limited in purpose and may not change in real-time as system changes occur. That is, the operating staff is still required to process data provided from multiple sources, as previously explained.

By contrast, video display wall technologies can show multiple data images, providing a comprehensive real-time view of current system status. System schematics, geographic system representations, news and weather feeds, and video camera data can all be shown simultaneously. The operator is able to see, understand, analyze and then interpret the data quickly.

Today's software technologies allow 2-, 3- and 4-dimensional images and give the control room operations staff the ability to view displays from many different systems. This data can be integrated into one display to obtain an enterprise-wide area view of current system status. For example, geographic information system map data can be displayed with real-time updates from supervisory control and data acquisition (SCADA) and real-time weather maps to predict how an incoming storm may disrupt services. As Smart Grid data applications are introduced, and multiple forms of data are made available for analysis, the push for advanced display tools and technologies will likely accelerate. And, as technology is added to the grid, the expectation for improved customer service will likewise be heightened.

To enhance decision-making and improve situational awareness, map boards have traditionally been a useful control room component. As the need for more data moves into

the control room, it is imperative that the operations staff has the proper tools available to improve processing and interpretation of this data.

Annunciators

The following is taken from Wikipedia, *Annunciator Panel*.

In industrial process control, an annunciator panel is a system to alert operators of alarm conditions in the plant. Multiple back-lit windows are provided, each engraved with the name of a process alarm. Lamps in each window are controlled by hard-wired switches in the plant, arranged to operate when a process condition enters an abnormal state. Single point or multipoint alarm logic modules operate the window lights based on a preselected ISA 18.1 or custom sequence.

In one common alarm sequence, the light in a window will flash, and a bell or horn will sound to attract the operator's attention when the alarm condition is detected. The operator can silence the alarm with a button, and the window will remain lit as long as the process is in the alarm state. When the alarm clears, the lamps in the window go out.

Annunciator panels were relatively costly to install because they required dedicated wiring to the alarm initiating devices in the process plant. Since incandescent lamps were used, a lamp test button was always provided to allow early detection of failed lamps. Modern electronic distributed control systems usually require less wiring since the process signals can be monitored within the control system, and the engraved windows are replaced by alaphanumeric displays on a computer monitor.

Behavior of alarm systems, and colors used to indicate alarms, are standardized. Standards such as ISA 18.1 or BS EN (British Adopted European Standard) 60073, *Basic and Safety Principles for Man-Machine Interface, Marking, and Identification—Coding Principles for Indicators and Actuators*, simplify purchase of systems and training of operators by giving standard alarm sequences.

h. Explain the design requirements for safety class and safety significant I&C systems design.

Safety Class Systems Design

The following is taken from DOE-STD-6003-96.

The categorization of a safety-class SSC is a two-step process. The first step is to identify, early in the design, the SSCs whose failure would result in exceeding evaluation guidelines. This should be by a top down functional hazards analysis. The second step is to verify in the final stages of design that the safety-class SSCs are actually needed to be functional, as indicated by the safety analysis process. If the SSCs are verified as being needed in the safety analysis process, then the equipment would be designated as safety-class SSCs. These components also must perform the required safety functions. This design approach would be as follows:

- Identify all potential hazards associated with the facility
- Identify all SSCs needed to control those hazards

- Identify the safety-class SSCs necessary to ensure that evaluation guidelines are not exceeded
- Verify, through detailed safety analysis, the need for the systems to meet the evaluation guidelines provided in DOE-STD-6002-96, *DOE Standard: Safety of Magnetic Fusion Facilities: Requirements*

The safety-class SSCs should be designed such that a minimum number of active or passive mitigative systems, identified from and credited within the safety analysis, are available to ensure that the evaluation guidelines are not exceeded. Reliable SSCs are required to be employed to satisfy the requirements of safety-class items. Use of defense-in-depth principles such as redundancy, simplicity in design, independence, fail safe, fault tolerant, and multiple methods for increasing the reliability and reducing the consequence to acceptable levels is permitted and encouraged. In most cases, the use of passive methods of accomplishing the safety function is preferred over using active methods.

The next step in the process is to perform the required system safety analysis. The safety analysis results should verify the adequacy of the safety-class SSCs to mitigate the release of hazardous material to meet the evaluation guidelines specified in DOE-STD-6002.

Thus, the results of this evaluation determine which of the SSCs are required to satisfy the public safety function. It may result in multiple SSCs being required to satisfy the safety system requirements for a particular off-normal condition scenario. In most cases, the SSCs identified in the hazards assessment review would be the same as those verified by the safety analysis as being SSCs required to implement safety. In addition, the safety analysis would verify the adequacy of safety-significant SSCs in addressing the potential safety concerns. Worker protection and potential safety concerns associated with the public safety function are identified in DOE-STD-6002.

Descriptions of each SSC that provides safety functions are required in the DSA. A basic descriptive model of the facility and its equipment must be provided in which the required SSCs are addressed in detail commensurate with their preventive or mitigative role in meeting off-normal condition evaluation guidelines. For example, consider a facility that cannot meet evaluation guidelines, as discussed in DOE-STD-6002, unless credit is taken for system A. Besides being noted in the general facility description, system A, together with associated codes and standards, would be described in the section on safety-class SSCs. This system would typically be associated with a specific TSR, and would be described in detail commensurate with its importance to the safety basis. However, only the characteristics of the SSC that are necessary to perform the safety function are classified as part of the safety system. For example, if a valve in a system is only required to provide an external pressure boundary, then only the pressure boundary function would be classified as a safety system characteristic and all other functions, such as the valve operability, response time, etc., would not be included in the safety system definition.

Conversely, if the consequences of all hazardous releases or off-normal conditions examined meet the evaluation guidelines without relying on the safety-class function of process system B, then system B would not be considered to be a safety system performing a safety function. Detailed identification of its functional basis and construction is not necessary because it is

not a significant contributor to the overall facility safety basis. There would also be no need to discuss administrative provisions required to ensure the operability of system B, nor would there be a need for a specific TSR covering system B. If a system is designated as safety-significant, industry recognized codes and standards are to be applied and minimal, if any, TSRs are to be specified for the operation of the system components. A risk-based prioritization approach can be used to develop requirements for the safety-class and safety-significant SSCs. One of the dominant factors governing risk-based prioritization is the severity of the off-normal condition consequences associated with the facility, and the number and type of the SSCs needed to prevent evaluation guidelines from being exceeded. If, for example, the defense-in-depth principles are satisfied by providing other SSCs to mitigate the consequences, then added inspections and other quality pedigree requirements of the first system would not be as important as if the original SSCs were the only means of accomplishing the safety function. If the consequences of the off-normal condition exceed the evaluation guidelines by a large margin, and there is no other system that will mitigate or prevent the release for the off-normal condition, then special precautions should be taken in the design and in developing the inspection program to ensure that the system will be available to function when called upon. This may involve special inspections, alternate design approaches, or other actions that would significantly enhance system reliability. The rigor of compliance with the design and inspection requirements could be relaxed for systems that have multiple backups for preventing off-normal conditions or mitigating the off-normal condition consequences.

The design of the SSCs that perform the safety-class and safety-significant safety functions should meet the appropriate requirements established in table 10.

Table 10. Safety system functional requirements

Requirement	Safety-Class Safety Function	Safety-Significant Safety Function
System design	Reliable methods of accomplishing the required safety function should be provided. Some of the design techniques that would ensure system reliability would include redundancy, diversity, simplicity in design, independence, fail safe, and fault tolerant. Each method should be analyzed to identify potential failure mechanisms from performing the safety function in the system and to minimize those failures in the design.	Non-redundant systems are normally used to perform the worker safety function. The safety system should be analyzed to preclude failure mechanisms that could disrupt the system function. Multiple systems may be employed, at the discretion of the facility developer, to ensure that the system functions are performed.
Codes and Standards	Nationally accepted design codes should be used in the design. The applicability, adequacy, and sufficiency of the codes and standards used should be evaluated. These codes and standards should be supplemented or modified as necessary to ensure system performance in keeping with the importance of the safety functions to be performed.	The codes and standards used for these systems should be those that have been validated through satisfactory performance in commercial application.

Requirement	Safety-Class Safety Function	Safety-Significant Safety Function
Reliability	Safety systems should be demonstrated to have a high reliability. One of the ways to demonstrate this is by providing multiple, redundant, diverse systems/barriers to accomplish the safety function.	The safety system should be equivalent to that associated with commercial industrial safety practices.
Quality	The SSCs should require an appropriate level of quality for the design and construction to ensure the system function is performed. QA in accordance with the requirements of 10 CFR 830.120, "Scope" should be implemented.	The systems required should be designed in accordance with industrial quality requirements.
Testability/ surveillance	The SSCs should be tested/surveyed periodically to determine that the function can be provided. Acceptance criteria should be established to evaluate the test results that demonstrate when the system is performing its intended function. The test frequency should be established to ensure that the system demand and reliability requirements are achieved.	The SSCs should be tested/surveyed periodically to determine that the function can be provided.
Natural phenomena	The SSCs should be designed to withstand appropriate natural phenomena and continue to provide the required safety function. Design for natural phenomena should be in accordance with facility performance goals per DOE O 420.B, *Facility Safety*.	Design for natural phenomena should be in accordance with facility performance goals per DOE O 420.1B

Source: DOE-STD-6003-96

Safety Significant System Design

The following is taken from the Energy Facilities Contractor Group (EFCOG), *Safety System Design Adequacy*.

Table 11 lists the safety-significant design criteria.

Table 11. Safety-significant design criteria

Natural Phenomena Hazard Design • Evaluation basis earthquake • Evaluation basis wind/tornado • Probable maximum flood • Probable maximum precipitation	Safety functions must not be compromised by events for which they are credited.
Equipment Environment Conditions	Safety-significant items must be selected to function under expected limiting environmental conditions. Environmental conditions include temperature, pressure, radiation, and/or chemical exposures.
Industry or Consensus Codes and Standards	Piping, piping components and pressure vessels must satisfy applicable portions of the ASME piping or boiler and pressure vessel codes.

Specific Functional Requirements	SSC must be able to accomplish the specific safety action for which the SSC is credited. Evaluation of the ability of the SSC to perform the action in conjunction with the other applicable requirements in this table are necessary to demonstrate the safety function can be reliably preformed and under appropriate conditions.
Maintainability/Testability	Safety-significant items shall be designed to allow inspection, maintenance, periodic testing, and/or surveillance to ensure their continued functioning readiness for operation, and accuracy. Testing must be capable of being performed in place, on a regular schedule, and under simulated emergency conditions.

Source: EFCOG Safety System Design Adequacy

i. Explain the consideration of failure modes in I&C systems design, and how different failure modes influence the selection of motive power for the I&C system.

The following is taken from Santa Clara University, *Principles of Testing Electronic Systems*.

Failure modes manifest on the logical level as incorrect signal values. A fault is a model that represents the effect of a failure by means of the change that is produced in the system signal. Several defects are usually mapped to one fault model. It is a many-to-one mapping. But some defects may also be represented by more than one fault model. Table 12 lists the common fault models. Fault models have the advantage of being a more tractable representation than physical failure modes.

Table 12. Most commonly used fault models

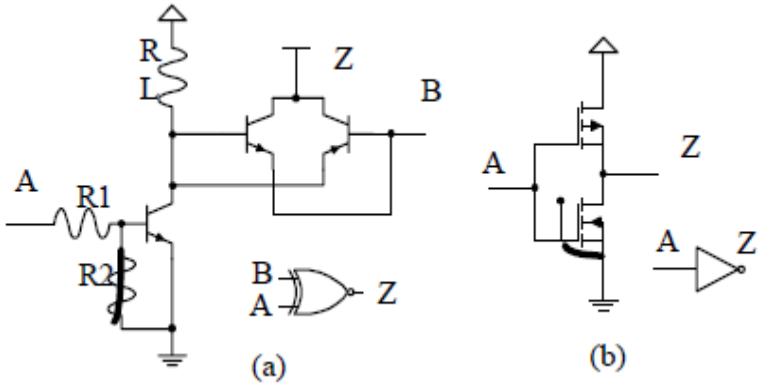
Fault Model	Description
Single stuck-at faults	One line takes the value 0 or 1.
Multiple stuck-at faults	Two or more lines have fixed values, not necessarily the same.
Bridging faults	Two or more lines that are normally independent become electrically connected.
Stuck-open faults	A failure in a pull-up or pull-down transistor ins a CMOS logic device causes it to behave like a memory element.
Delay faults	A fault is caused by delays in one or more paths in the circuit.

Intermittent faults	Caused by internal parameter degradation. Incorrect signal values occur for some but not all stages of the circuit. Degradation is progressive until permanent failure occurs.
Transient faults	Incorrect signal values caused by coupled disturbance. Coupling may be via power vs. capacitive or inductive coupling. Includes internal and external sources as well as particle irradiation.

Source: Santa Clara University, Principles of Testing Electronic Systems

As a model, the fault does not have to be an exact representation of the defects, but rather, to be useful in detecting the defects. For example, the most common fault model assumes single stuck-at (SSA) lines even though it is clear that this model does not accurately represent all actual physical failures. The rationale for continuing to use the stuck-at-fault model is the fact that it has been satisfactory in the past. Also, test sets that have been generated for this fault type have been effective in detecting other types of faults. However, as with any model, a fault cannot represent all failures, and a stuck-at fault is no longer sufficient for present circuits and technologies. With the advent of MOS technology, it has become evident that other fault models are needed to represent more accurately the failure modes in this technology.

Single Stuck-at Faults

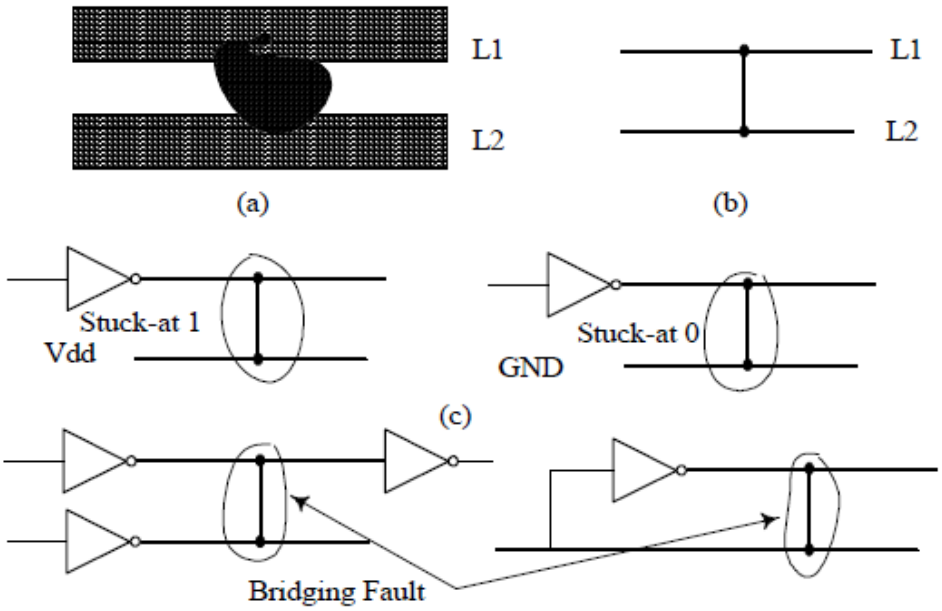


An SSA fault represents a line in the circuit that is fixed to logic value 0 or 1. One may think of it as representing a short between the faulty line and the ground or V_{dd} rail. Examples of failure modes that manifest themselves as stuck-at faults are shown in figure 65.

Source: Santa Clara University, Principles of Testing Electronic Systems

Figure 65. Stuck-at faults: (a) A bipolar XNOR gate, (b) A CMOS inverter

The first example shows how a defective resistance caused the input of the bipolar XOR gate to short to ground. This is represented by a stuck-at-0 fault. Similarly, in the CMOS gate, the breakdown in gate oxide causing a resistive short between gate and source results in a stuck-at-0 fault on the input. Another example is shown in figure 66, which resulted from extra metal shorting the output of a gate to the power or ground rail.



Source: Santa Clara University, Principles of Testing Electronic Systems

Figure 66. Mapping Physical Defects onto Faults a) metal mask with dust causing extra metal, b) failure mode—a short c) faults on the logic level—stuck-at faults d) bridging faults

Multiple Stuck-at Faults

A defect may cause multiple stuck-at faults. That is, more than one line may be stuck-at high or low simultaneously. With decreased device geometry and increased gate density on the chip, the likelihood is greater that more than one SSA fault can occur simultaneously. It has been recommended to check m-way stuck-at faults up to m = 6 This is particularly true with present technology circuits because of the high device density. The number of faults increases exponentially with m as indicated in table 13. A set of m lines has 2m combinations of SA faults.

Table 13. Number of multiple stuck-at faults in an n-line circuit

	Number of Faults		
Number of Nodes	**Single**	**Double**	**Triple**
N	2N	4C(N,2)	8C(N,3)
10	20	180	960
100	200	19,800	1.3×10^{6}
1000	2,000	1,998,000	$>10^{9}$
10000	20,000	199,980,000	$>10^{12}$

Source: Santa Clara University, Principles of Testing Electronic Systems

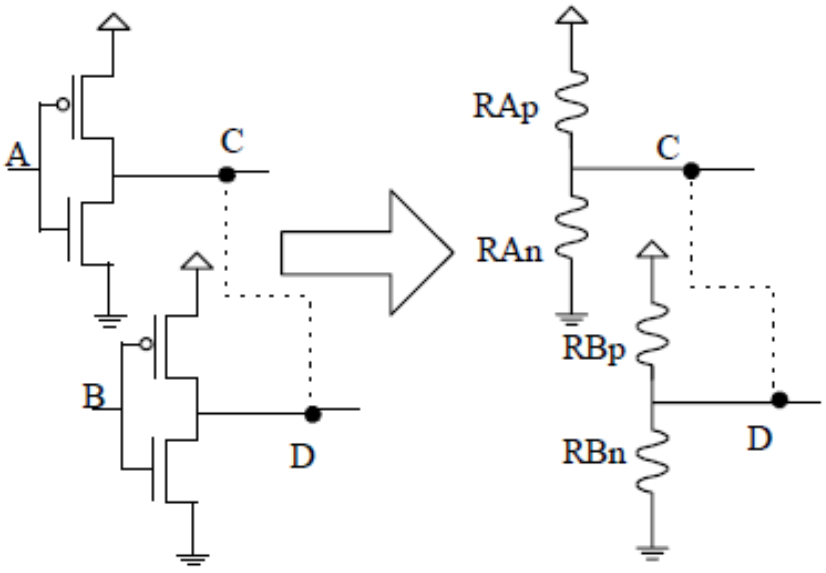
In detecting multiple stuck-at faults, it is always possible to use exhaustive and pseudoexhaustive testing. However, this is not practical for large circuits. It has been shown that using an SSA fault test yields high fault coverage in detecting multiple stuck-at faults. The most important factors that affect the detectability of multiple stuck-at faults are the number of primary outputs and the reconverging fanouts. Comparing a multiple-output

circuit such as an arithmetic logic unit to a parity tree, the multiple fault coverage of a stuck-at fault test decreased from 99.9 to 83.33 percent. The high reconverging-path nature of a parity tree causes fault masking, but the fault coverage increased to 96 percent when the test was increased.

Bridging Faults

Bridging faults occur when two or more lines are shorted together and create wired logic. When the fault involves r lines with $r \geq 2$, it is said to be of multiplicity r; otherwise, it is a simple bridging fault. Multiple bridging faults are more likely to occur at the primary inputs of a chip. Bridging faults are becoming more predominant because the devices are becoming smaller and the gate density higher. The total number of all possible simple bridging faults in an m-line circuit is C(m, 2). However, in reality most pairs of lines are not likely to be shorted. Thus the actual number is much smaller than theoretically calculated and is layout dependent.

The behavior of the circuit in the presence of bridging faults is dependent on the technology. The short between the outputs of two inverters as shown in figure 66 can be modeled as a wired logic. If the implementation is in TTL technology, it is a wired AND; in the case of Electrochemiluminescence technology, it is a wired-OR. In the case of CMOS technology, the wired logic depends on the type of gate driving the shorted lines and the input on these gates.



Source: Santa Clara University, Principles of Testing Electronic Systems

Figure 67. Bridging faults voting model

Figure 67 illustrates these effects. The two CMOS inverters are represented by their pull-up and pull-down resistances.

Of course, the value of these resistances will depend on the inverters' input signals. For example, if A = 0, the N-type metal-oxide-semiconductor transistor is off, and its corresponding resistance, RA_n, is infinite while the P-type metal-oxide-semiconductor is on, and RA_p assumes the value of the on resistance. The circuit may then be represented as a voltage divider, and the value of the output will depend on the on resistance of the various transistors, as listed in table 14.

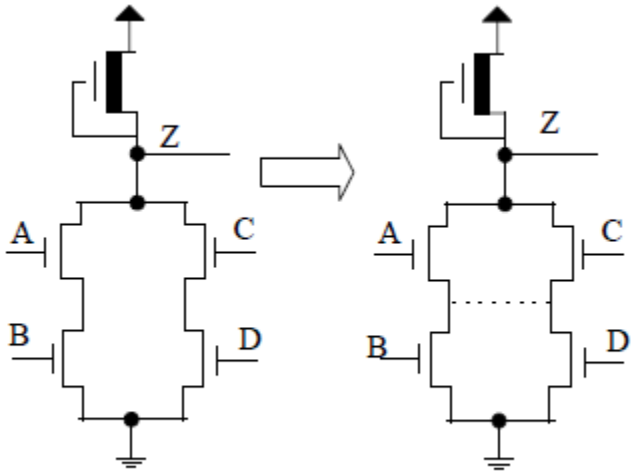
Table 14. Bridging faults models for the circuit in figure 67

Input Condition	Relative Drive	Output Values	Wired Logic
A=B	Any ratio	C=D=A' =B'	AND, OR
A=0, B=1	$RA_p > RB_u$ $RA_p < RB_u$	C=D=0 C=D=1	AND OR
A=1, B=0	$RA_n > RB_p$ $RA_n > RB_p$	C=D=1 C=D=0	OR AND

Source: Santa Clara University, Principles of Testing Electronic Systems

If the input signals are the same for both gates, the output will be the same for both gates and the fault will not be detected. Now if A = 0 and B = 1, the output will depend on RA_p and RB_n. If $RA_p > RB_n$, the output is 0, as if the two outputs, C and D, are wired ANDed. Following the same reasoning, one can understand the remainder of the entries in table 14.

Bridging faults may cause a change in the functionality of the circuit that cannot be represented by a known fault model. An example of this type of fault is shown in figure 68, where the function of the good NMOS circuit is AB + CD, while the bridging fault changes the functionality of the gate to (A + C)(B + D). Another important consequence of bridging faults is observed where the bridged wires are the input and the output of the same gate. Called a feedback bridging fault, this is illustrated on the right in figure 66. The fault transforms a combinational circuit into a sequential circuit and increases the number of states in a sequential circuit.



Source: Santa Clara University, Principles of Testing Electronic Systems

Figure 68. Change in functionality due to bridging faults

SSA fault test sets have been used to detect bridging faults. They yield 100 percent fault detection for some special circuits. The approach is to alter the order of the patterns. It is also possible to use exhaustive test sets.

j. Explain alarm management.

The following is taken from PAS, *Understanding and Applying the ANSI/ISA 18.2 Alarm Management Standard*.

Alarm management has become an ever-increasing topic of discussion in the power and processing industries. In 2003, ISA started developing a standard around this subject. After six years of hard work, the ANSI/ISA-18.2-2009 *Management of Alarm Systems for the Process Industries* standard was published. The following paragraphs review the scope, regulatory impact, requirements, recommendations, alarm definitions, and other details of the standard.

Over the last several years, alarm management has become a highly important topic, and the subject of a number of articles, technical symposia, and books.

The issuance of ISA-18.2 is a significant event for the chemical, petrochemical, refining, power generation, pipeline, mining and metals, pharmaceutical, and similar industries using modern control systems with alarm functionality. It sets forth the work processes for designing, implementing, operating, and maintaining a modern alarm system in a life cycle format. It will also have considerable regulatory impact.

Purpose and Scope

The basic intent of ISA-18.2 is to improve safety. Ineffective alarm systems have often been documented as contributing factors to major process accidents. The alarm system problems that ISA-18.2 addresses have been well known for nearly two decades.

There are several common misconceptions about standards. Standards intentionally describe the minimum acceptable; not the optimum. By design, they focus on the "what to do" rather than the "how to do it." By design, standards do not have detailed or specific "how-to" guidance. ISA-18.2 does not contain examples of specific proven methodologies or of detailed practices. The standard focuses on both work process requirements ("shall") and recommendations ("should") for effective alarm management.

Readers familiar with alarm management literature should not expect to learn new or different information when reading the ISA-18.2. The key difference is that ISA-18.2 is a standard, not a guideline or a recommended practice, developed in accordance with stringent ANSI methodologies. As such, it will be regarded as a "recognized and generally accepted good engineering practice" by regulatory agencies. ISA-18.2 is in the process of being adopted as an International IEC standard.

Who Does ISA-18.2 Apply To?

The focus of ISA-18.2 is on alarm systems that are part of modern control systems, such as distributed control systems, SCADA systems, PLCs, or safety systems. It applies to plants with operators responding to alarms depicted on a computer-type screen and/or an annunciator.

This includes the bulk of all processes operating today, specifically

- petrochemical
- chemical

- refining
- platform
- pipelines
- power plants
- pharmaceuticals
- mining & metals

Additionally, it applies whether the process is continuous, batch, semi-batch, or discrete. The reason for this commonality is that alarm response is really not a function of the specific process being controlled; it is a human-machine interaction. The steps for detecting an alarm, analyzing the situation, and reacting are steps performed by the operator.

There is little difference if gasoline, plastics, megawatts, or aspirin are being made (or moved). While many industries feel they are different, that is simply not the case when it comes to alarm response. Many different industries participated in the development of ISA-18.2, recognized this, and the resulting standard has overlapping applicability.

ISA-18.2 indicates the boundaries of the alarm system relative to terms used in other standards, such as basic process control systems, SISs, etc. Several exclusions are listed to not contradict existing content in other standards.

Regulatory Impact

The regulatory environment is complex and overlapping for some industry segments. Many industries are clearly covered by 29 CFR 1910.119 “Process Safety Management of Highly Hazardous Chemicals,” which makes a few specific mentions of alarms.

The important thing is that regulatory agencies have “general duty” clauses and interpretations. Codes, standards, and practices are usually considered recognized and generally accepted good engineering practices (RAGAGEP). In the Occupational Safety and Health Administration (OSHA) interpretation letter to ISA, a National Consensus Standard, such as ISA-18.2, is a RAGAGEP.

There is little question ISA-18.2 is an example of RAGAGEP, and companies should expect the regulatory agencies to take notice. Generally, a regulated industry can be expected to either comply with RAGAGEP or explain and show they are doing something just as good or better.

Indeed, OSHA has sought and received permission from ISA to internally distribute ISA-18.2 to its inspectors. This was with the specific intent to be able to easily cite it in investigations and use it for enforcement reasons.

The U.S. Chemical Safety Board will also be using ISA-18.2 as a resource in its investigations. Other regulatory agencies are also becoming aware of ISA-18.2. The American Petroleum Institute (API) released API RP-1167, *Pipeline SCADA Alarm Management*, in 2010. This API document is in full alignment with ISA-18.2, and the Pipeline and Hazardous Materials Safety Administration generally adopts API recommended practices in their regulatory language.

Alarm State Transitions

ISA-18.2 includes a moderately complex diagram depicting the alarm states and sub-states of "Normal", "Unacknowledged", "Acknowledged", "Returned-to-Normal", and "Latched". Of particular interest are the states of "Shelved", "Suppressed by Design", and "Out of Service". These have specific meanings as follows:

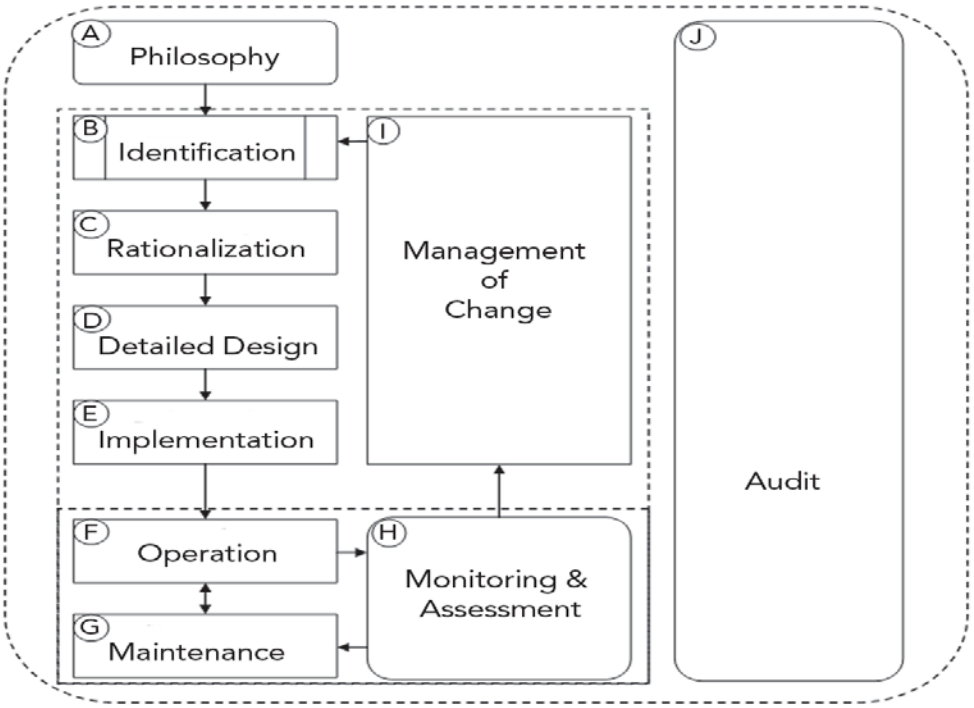
- "Shelved" is an alarm that is temporarily suppressed, usually via a manual initiation by the operator, using a method meeting a variety of administrative requirements to ensure the shelved status is known and tracked.
- "Suppressed By Design" is an alarm intentionally suppressed due to a designed condition. This is a generic description that includes such items as simple logic-based alarms and advanced state-based alarming techniques.
- "Out of Service" is a non-functioning alarm, usually for reasons associated with the maintenance stage of the life cycle. An "Out of Service" alarm is also tracked via similar administrative requirements to a shelved alarm.

The terms "suppress" and "alarm suppression" are intentionally generic and not specific to a type of DCS. They are used to indicate when the alarm functionality is not working. It is possible, and unfortunately common, to suppress an alarm outside of the proper work practices, and the detection of such undesirable situations is part of the monitoring life cycle stage.

The Alarm Management Life Cycle

ISA-18.2 is written with a life cycle structure comprised of ten stages (see figure 69). They are as follows:

A. Alarm Philosophy—documents the objectives of the alarm system and the work processes to meet those objectives.
B. Identification—determines which alarms are necessary.
C. Rationalization—ensures an alarm meets the requirements set forth in the alarm philosophy, including the tasks of prioritization, classification, settings determination, and documentation.
D. Detailed Design—designs the aspects of the alarm so that it meets the requirements determined in rationalization and in the philosophy. This includes some human-machine interface (HMI) depiction decisions and can include the use of special or advanced techniques.
E. Implementation—brings alarm into operational status. This may involve commissioning, testing, and training activities.
F. Operation—functions as designed. This stage includes refresher training, if required.
G. Maintenance—makes the alarm non-functional, due to either test or repair activities. (Do not equate this life cycle stage with the maintenance department or function.)
H. Monitoring and Assessment—monitors and reports the alarm system's performance continuously against the goals in the alarm philosophy.
I. Management of Change—changes to the alarm system follow a defined process.
J. Audit—reviews periodically to maintain the integrity of the alarm system and alarm management work processes.



Source: PAS,

Understanding and Applying the ANSI/ISA 18.2 Alarm Management Standard

Figure 69. Alarm management life cycle

The Alarm Philosophy Life Cycle Stage

ISA-18.2 recognizes that an alarm philosophy document is a key requirement for effective alarm management. A table lists topics that are noted as either mandatory or recommended for inclusion. A standard describes the minimum acceptable, not the optimum.

The major mandatory contents of the alarm philosophy include roles and responsibilities, alarm definition, the basis for alarm prioritization, HMI guidance, performance monitoring, management of change, training, etc.

There are no surprises in the list except for two concepts not previously included in the Alarm Management lexicon, “alarm classification” and “highly managed alarms”.

ALARM CLASSIFICATION

Alarm classification is a method for assigning and keeping track of various requirements for alarms, mostly administrative ones. For example, some alarms may require periodic refresher training, while others may not. The same could be true for testing, maintenance, reporting, HMI depiction, and similar aspects. Alarm classes are defined and used to keep track of these requirements. It is mandatory in ISA-18.2 to define alarm classes.

This is a slightly unusual thing for a standard. Normally, standards tell what to do but not how to do it, or to require a specific method. For example, the standard could have simply stated, “Identify and track alarms that require periodic testing.” There are a variety of methods to successfully do this; a classification structure is only one of them. However, the committee elected to require a classification structure, though it need not be an onerous one.

There are no specific class requirements and no minimum number of class definitions specified.

HIGHLY MANAGED ALARMS

The committee thought it desirable to explicitly define one class of alarms. A variety of designations were considered, from “critical” to “vital” to “special” to “super-duper.” Highly managed alarms (HMA) was chosen as the term. The intent is to identify the alarms that must have a considerably high level of administrative requirements.

The various mandatory requirements for HMAs are spread over several sections throughout ISA-18.2. These include

- specific shelving requirements, such as access control with audit trail;
- specific out of service alarm requirements, such as interim protection, access control, and audit trail;
- mandatory initial and refresher training with specific content and documentation;
- mandatory initial and periodic testing with specific documentation;
- mandatory training around maintenance requirements with specific documentation; and
- mandatory audit requirements.

The Alarm System Requirements Specification (ASRS)

This non-mandatory section basically says that when buying a new control system, it is a good idea to write down the requirements and evaluate vendor offerings and capabilities against them. Specific deficiencies in the chosen system can drive the acquisition or creation of third-party or custom solutions. The ASRS then becomes a useful document for system testing and acceptance.

The Alarm Identification Life Cycle Stage

This section of ISA-18.2 notes that different methods are used to initially identify the need for some alarms. All modern control systems have a lot of built-in alarm capability; perhaps more than a dozen types of alarms are available for some point types.

In some cases, the need for use of one of those types or the creation of a specific alarm via custom logic or calculation may be driven by a variety of process-related sources. These are the usual list of studies such as a process hazard analysis, layer of protection analysis, Failure Mode and Effects Analysis (FMEA), etc.

The Alarm Rationalization Life Cycle Stage

This life cycle stage consists of several activities. Most people familiar with alarm management concepts think of rationalization as the specific activity of a team reviewing an alarm system and making decisions about usage, priority, setpoints, etc. In ISA-18.2, the word is used to indicate a collection of activities that may be done in a variety of ways. The activities are as follows:

- Ensuring alarms meet the criteria set forward in the alarm philosophy
- Justifying the need for the alarm
- Marking for deletion alarms that should not exist
- Determining the appropriate alarm type

- Determining the appropriate alarm set point or logical condition
- Determining the proper priority
- Documenting any special design considerations for an alarm
- Documenting any advanced alarming capabilities desired for an alarm
- Documenting relevant information such as operator action, consequences, etc.
- Determining the alarm's classification

All of the activities listed include the cases of review of already existing alarms or consideration of potential new alarms. The major mandatory contents of the rationalization stage are for specific alarm documentation and alarm classification.

The Basic Alarm Design Life Cycle Stage

This section of ISA-18.2 describes the common capabilities of control system alarm functionality and how they relate to the alarm state diagram. There is some non-mandatory advice about the proper usage of some alarm types and some alarm configuration capabilities, such as deadband and delay time.

HMI Design for Alarm Systems

This section of ISA-18.2 describes the desired functionality for indicating alarms to the operator. Some items discussed include the following:

- Depiction of alarm states, priorities, and types
- Alarm silencing and acknowledgement
- Alarm shelving, designed suppression, and out of service conditions and depiction
- Alarm summary display functionality
- Other alarm-related similar displays and functionality
- Alarm sounds
- Alarm information and messages
- Alarm annunciators

Many functionality items are listed as mandatory or recommended. The major mandatory items are for specific depiction of various alarm-related conditions, and specifically required HMI screens and functionality. These items are typically within the capabilities of most modern control systems.

Enhanced and Advanced Alarm Methods

This section of ISA-18.2 provides an overview of alarm features and capabilities that are usually a bit beyond the standard capability of a control system. This section notes that usage of such advanced capabilities may require additional design work and support. These types of advanced methods briefly discussed include the following:

- Information linking
- Logic-based alarming
- Model-based alarming
- Alarm attribute modification
- Externally enabled systems
- Logical alarm suppression/attribute modification
- State-based alarming
- Model-based alarming

- Non-control room considerations such as remote alarm notification
- Paging, e-mailing, and remote alerting systems
- Supplementary alarm systems
- Continuously variable alarm thresholds
- Batch process alarm considerations
- Training, testing, and auditing systems
- Alarm attribute enforcement

The Implementation Life Cycle Stage

This section of ISA-18.2 covers the activities and requirements involved in implementing a new alarm system or implementing desired changes to an existing one. The areas covered generally have mandatory requirements and non-mandatory recommendations. They are as follows:

- Planning
- Training for new systems and modifications
- Testing and validation for new systems and modifications
- Documentation of training and testing

The Operation Life Cycle Stage

This section of ISA-18.2 deals with mandatory requirements and non-mandatory recommendations for in-service and operating alarms. The areas addressed are

- alarm response procedures
- alarm shelving, including documentation
- operator refresher training, including documentation

The Maintenance Life Cycle Stage

This section of ISA-18.2 is about the condition where an alarm has been removed from service specifically for testing or repair. The section covers mandatory requirements and non-mandatory recommendations for the following:

- Procedures for moving alarms in and out of the maintenance stage of the life cycle, including notification, tracking, and documentation
- Interim procedures for when alarms are out of service
- Periodic testing of alarms, including record-keeping
- Refresher training for personnel involved with alarm repair or testing
- Alarm validation in regard to equipment replacement

The Monitoring and Assessment Life Cycle Stage

This is the stage in which alarm system performance is measured and reported. The intent is to verify that the other life cycle stages are successful in creating an alarm system that is effective.

It is mandatory that alarm system performance be measured and compared against goals identified in the alarm philosophy. Four clearly defined terms are used in this section: “monitoring”, “assessment”, “audit”, and “benchmark”.

Several analyses are described and recommended for alarm system performance measurement. A non-mandatory table indicating recommended performance goals and metrics is provided. The numbers allow for possible modifications, and are as follows:

> The target metrics in the following sections are approximate and depend upon many factors (e.g., process type, operator skill, HMI, degree of automation, operating environment, types, and significance of the alarms produced). Maximum acceptable numbers could be significantly lower or perhaps slightly higher depending upon these factors. Alarm rate alone is not an indicator of acceptability.

The analyses described are as follows:

- Average annunciated alarm rate per operating position
- Peak annunciated alarm rates per operating position
- Alarm floods (calculation methods and recommendations)
- Frequently occurring alarms
- Chattering and fleeting alarms
- Stale alarms
- Annunciated alarm priority distribution (alarm occurrences)
- Alarm attributes priority distribution (alarm configuration)
- Unauthorized alarm suppression
- Alarm attribute monitoring (for unauthorized change)

In deciding the particular measures and performance numbers, the committee did considerable research to achieve consensus. Several analyses with problematic concerns were intentionally left out. Recommendations for the reporting of alarm system analyses are provided.

The Management of Change Life Cycle Stage

This section of ISA-18.2 deals with mandatory requirements and non-mandatory recommendations for change of the alarm system. The items covered are as follows:

- Changes subject to management of change
- Change review process requirements, including the consideration of technical basis, impact, procedure and documentation modifications, review, and authorization
- Changes are in accordance with the alarm philosophy
- Temporary changes
- Implementation of changes
- Change documentation requirements and recommendations
- Alarm decommissioning recommendations
- Alarm attribute modification requirements and recommendations

The Audit Life Cycle Stage

The audit stage involves a more comprehensive review of not only the performance of the alarm system itself, but also of the various work processes associated with it. This section covers the nature of audits, items to be examined, and some recommendations around practices, such as interviews and action plans.

ISA-18.2 is an important standard and will undoubtedly result in a significant safety enhancement for the process industries. It validates and embodies practices that industry

experts and leading manufacturing companies have advocated for many years. The publication of ISA-18.2 has significant regulatory consequences, and TQP participants are advised to become familiar with its contents.

9. I&C personnel must demonstrate a working level knowledge of procurement, installation, and testing.

a. Explain the key elements of the procurement process for I&C structures, systems and components as defined in DOE O 414.1D, Quality Assurance. This includes quality assurance requirements for both hardware and software.

The following is taken from DOE G 414.1-4.

Most software projects will have procurement activities that require interactions with suppliers regardless of whether the software is level A, B, or C. Procurement activities may be as simple as the purchase of compilers or other development tools for custom developed software, or as complicated as procuring a complete safety program software control system. Thus, there are a variety of approaches for software procurement and supplier management based on

- the level of control DOE or its contractors have on the quality of the software or software service being procured
- the complexity of the software

Procurement documentation should include the technical and quality requirements for the safety software. Some of the specifications that should be included are

- specifications for the software features, including requirements for safety, security, functions, and performance;
- process steps used in developing and validating the software, including any document to be delivered;
- requirements for supplier notification of defects, new releases, or other issues that impact the operation; and
- mechanisms for the users of the software to report defects and request assistance in operating the software.

These requirements should be assessed for completeness and to ensure the quality of the software being purchased. There are four major approaches for this assessment:

1. Performing an assessment of the supplier
2. Requiring the supplier to provide a self-declaration that the safety software meets the intended quality
3. Accepting the safety software based on key characteristics
4. Verifying the supplier has obtained a certification or accreditation of the software product quality or software quality program from a third party

The following is taken from DOE G 414.1-2B.

The procurement process should ensure that items and/or services provided by suppliers meet the requirements and expectations of the end user. The procurement process should be planned, implemented, and controlled to ensure that

- supplier QA program requirements are identified using a grading process;
- proper flow down takes place and the supplier/vendor clearly understands all procurement requirements;
- the end user's requirements are accurately, completely, and clearly communicated to the supplier;
- supplier, designer, and end user requirements are met during the production phase;
- the product is delivered on time; and
- special handling and storage requirements are specified at time of delivery.

The selection of procurement requirements should be commensurate with the importance of the end use of the purchased item or service. Management controls exist for DOE procurement and subcontracts through applicable DOE Orders, the Department of Energy Acquisition Regulation in 48 CFR, subchapters A through H, and the Federal Acquisition Regulation in 48 CFR 970, "DOE Management and Operating Contracts."

The procurement process of DOE nuclear facility contractors should include a determination of the applicability of the QA Rule, 10 CFR 830.121, "Quality Assurance Program." If applicable, procurement documents and contracts for items and services provided to facilities covered by the QA Rule should include a statement informing the supplier/vendor or subcontractor of the QA Rule requirements and of the potential for enforcement actions under 10 CFR 820, "Procedural Rules for DOE Nuclear Activities." DOE O 414.1D, *Quality Assurance*, requires that contractors be responsible for ensuring proper flow down of all applicable requirements, including the adopted standards to suppliers/vendors and subcontractors. DOE should ensure proper oversight of the flow down of requirements by their contractors to subcontractors, vendors, and suppliers. The DOE contractor is responsible for determining methods to ensure that procured items and services meet requirements and perform as expected, including the prevention and control of the introduction of suspect/counterfeit items. The selection of prospective suppliers should be based on specified criteria. Suppliers/vendors should be evaluated to verify their capability to meet performance and schedule requirements.

Procurement processes should be established and implemented to ensure that approved suppliers continue to provide acceptable items and services. Suppliers/vendors should be monitored to ensure that acceptable items or services are produced within the specified schedule.

b. Explain the importance of quality assurance requirements for safety software used in design, analysis, and controls (e.g., requirements of O 414.1D, *Quality Assurance,* and additional guidance of DOE G 414.1-4, *Safety Software Guide for use with 10 CFR 830 Subpart A, Quality Assurance Requirements*, and DOE O 414.1D.

The following is taken from DOE G 414.1-4.

The use of digital computers and programmable electronic logic systems has increased significantly since 1995, and their use is evident in safety applications at nuclear facilities across the DOE complex. The commercial industry has increased attention to QA of safety software to ensure that safety systems and structures are properly designed and operate correctly. Recent DOE experience with safety software has led to increased attention to the safety-related decision making process, the quality of the software used to design or develop safety-related controls, and the proficiency of personnel using the safety software.

The Department has recognized the need to establish rigorous and effective requirements for the application of QA programs to safety software. In evaluating the Defense Nuclear Facilities Safety recommendation 2002-1 and through assessing the current state of safety software, the Department concluded that an integrated and effective software quality assurance (SQA) infrastructure must be in place throughout the Department's nuclear facilities. This is being accomplished through the Implementation Plan for Defense Nuclear Facilities Safety Board Recommendation 2002-1, *Quality Assurance for Safety Software at Department of Energy Defense Nuclear Facilities.*

To ensure the quality and integrity of safety software, DOE directives have been developed and revised based on existing SQA industry or Federal agency standards. This resulted in the development and issuance of DOE O 414.1D, which includes specific SQA requirements, DOE G 414.1-4 and the DOE STD-1172-2003, *Safety Software Quality Assurance Functional Area Qualification Standard*.

DOE promulgated the safety software requirements and DOE G 414.1-4 to control or eliminate the hazards and associated postulated accidents posed by nuclear operations, including radiological operations. Safety software failures or unintended output can lead to unexpected system or equipment failures and undue risks to the DOE/NNSA mission, the environment, the public, and the workers. Thus DOE G 414.1-4 has been developed to provide guidance on establishing and implementing effective QA processes tied specifically to nuclear facility safety software applications. DOE also has guidance for the overarching QA program, which includes safety software within its scope. DOE G 414.1-4 includes software application practices covered by appropriate national and international consensus standards and various processes currently in use at DOE facilities. DOE G 414.1-4 is also considered to be of sufficient rigor and depth to ensure acceptable reliability of safety software at DOE nuclear facilities.

DOE G 414.1-4 should be used by organizations to help determine and support the steps necessary to address possible design or functional implementation deficiencies that might exist, and to reduce operational hazards-related risks to an acceptable level. Attributes such as the facility life-cycle stage and the hazardous nature of each facility's operations should be

considered when using DOE G 414.1-4. Alternative methods to those described in DOE G 414.1-4 may be used provided they result in compliance with the requirements of 10 CFR 830, Subpart A, and DOE O 414.1D.

c. Explain the importance of adequately identifying I&C requirement specifications to ensure that system functional and performance requirements used for design, procurement, installation, and operation are appropriate for the selected equipment, and identify potential consequences of improperly classifying equipment.

Functional Requirements

The following is taken from DOE G 200.1-1, Chapter 5.

The functional design process maps the "what to do" of the software requirements specification into the "how to do it" of the design specifications.

During this stage, the overall structure of the software product is defined from a functional viewpoint. The functional design describes the logical system flow, data organization, system inputs and outputs, processing rules, and operational characteristics of the software product from the user's point of view. The functional design is not concerned with the software or hardware that will support the operation of the software product; the physical organization of the data; or the programs that will accept the input data, execute the processing rules, and produce the required output.

The focus is on the functions and structure of the components that comprise the software product. The goal of this stage is to define and document the functions of the software product to the extent necessary to obtain the system owner and user's understanding and approval to the level of detail necessary to build the system design.

Prototyping of system functions can be helpful in communicating the design specifications to the system owner and users. Prototypes can be used to simulate one function, a module, or the entire software product. Prototyping is also useful in the transition from the functional design to the system design.

Performance Requirements

The following is taken from DOE G 200.1-1, Chapter 4.

Performance requirements define how the software product must function (e.g., hours of operation, response times, and throughput under detailed load conditions). The information gathered in defining the project objectives can translate into very specific performance requirements. Also, government and DOE policy can dictate specific availability and response times.

SSC Classification

The following is taken from IAEA DS367.

REQUIREMENTS FOR A SAFETY CLASSIFICATION PROCESS

The basic requirements for a safety classification system are established in International Atomic Energy Agency, (IAEA) Safety Standards Series No. SSR-2/1, *Safety of Nuclear Power Plants*: *Design*, and are repeated in the following paragraphs.

A systematic approach shall be taken to identify the items important to safety that are necessary to fulfill the fundamental safety functions, and to identify the inherent features that are contributing to or affecting the fundamental safety functions, for the first four levels of defense in depth.

All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance.

The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methodologies complemented where appropriate by probabilistic methods, with account taken of factors such as

- the safety function(s) to be performed by the item;
- the consequences of failure to perform the safety function;
- the frequency at which the item will be called upon to perform a safety function; and
- the time following a postulated initiating event at which, or the period for which, it will be called upon to operate.

The design shall be such as to ensure that any interference between items important to safety shall be prevented. In particular, any failure of items important to safety in a system classified in a lower class will not propagate to a system classified in a higher safety class.

Equipment that performs multiple functions shall be classified consistent with the most important function performed.

Fulfillment of the following fundamental safety functions shall be ensured for all plant states:

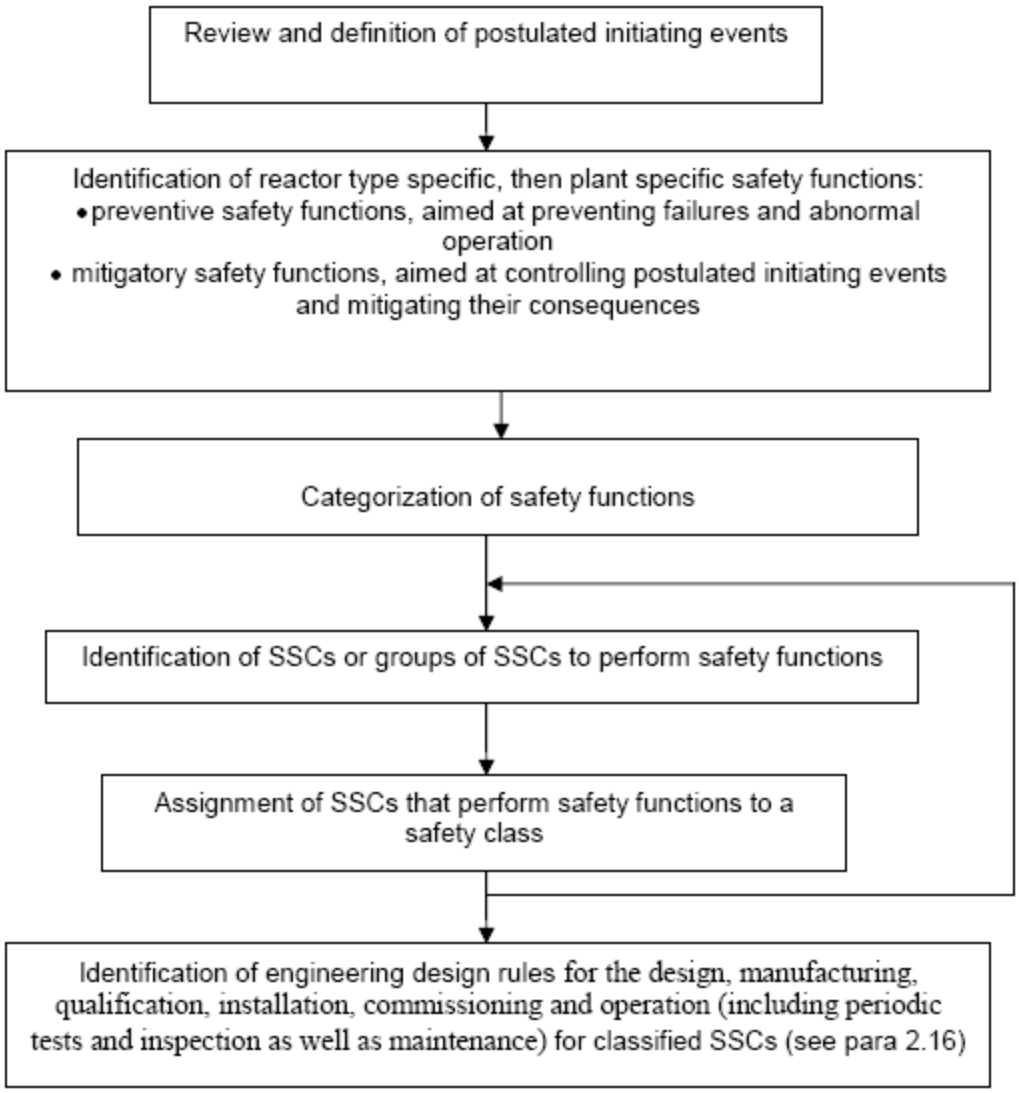
- Control of reactivity
- Removal of heat from the core and from spent fuel
  Confinement of radioactive material, shielding against radiation, and control of planned radioactive releases, as well as limitation of accidental radioactive release

The recommended approach to safety classification involves categorization of safety functions followed by classification of the SSCs. The main steps involved are shown in figure 70.

For a specific plant, prerequisites for classifying all SSCs according to their safety significance should be based on the following:

- A list of all postulated initiating events considered in the plant design basis
- The identification of the safety functions needed to achieve the fundamental safety functions for the different plant states

As part of the design process, the postulated initiating events should be arranged in groups in which attributes or features of the initiating events are the same. Where this simplifies the analysis, one or more postulated initiating events should be selected from the group that bound all aspects of the event that are important to safety.



Source: IAEA, DS367

Figure 70. Main steps in classifying SSCs

The safety functions that prevent and mitigate these postulated initiating events should be derived at an adequate level of detail to identify SSCs to perform these safety functions. These safety functions will be specific to each plant.

These plant specific safety functions should then be categorized into a limited number of categories on the basis of their safety significance, with account taken of aspects such as the following:

- The consequences of the failure of the safety function
- The frequency of occurrence of the postulated initiating events they prevent or mitigate
- The time following a postulated initiating event at which they will be required to perform
- the period following a postulated initiating event they will be required to perform

The SSCs or groups of SSCs that work together to perform the plant specific safety functions should then be identified.

The SSCs are subsequently classified, mainly on the basis of the category of the safety functions they perform. Preliminary safety classifications of SSCs should then be verified, applying an appropriate confirmation process. Three classes of SSCs are recommended in IAEA DS367, based on experience in member states. However, a larger or smaller number of classes may be used if warranted.

The safety classification process described in IAEA DS367 highlights the significant linkage that exists between design, analysis of postulated initiating events and the consequences of failure of safety functions, and the classification of SSCs. In the design process, the aims of safety classification are to determine the appropriate engineering design rules for all SSCs and to ensure that SSCs are then designed, manufactured, qualified, constructed, installed, commissioned, quality assured, maintained, tested, and inspected to standards appropriate to their safety significance.

The basis for the classification and the results of the classification should be documented in an auditable record.

Safety classification is an iterative process that should be carried out throughout the design process. Any preliminary assignments of SSCs to particular safety classes should be justified using deterministic safety analysis, and complemented, where appropriate, by probabilistic safety analysis and engineering judgment.

Safety classification should be performed during the plant design, system design, and equipment design phases and should be reviewed for any relevant changes during construction, commissioning, commercial operation, and subsequent stages of the plant's lifetime.

The safety classification process recommended in IAEA DS367 is consistent with the concept of defense in depth that is required in the design process. The preventive safety functions may be associated with defense in depth level 1 and the mitigatory safety functions with defense in depth levels 2 to 4.

Although the precise nature of the steps taken at each stage could vary according to regulatory requirements and the plant design, the safety classification process should include the steps outlined in the following paragraphs. Various methods for the safety classification of SSCs have been used for different types of reactors and in different member states for operating nuclear power plants and for new designs. These differences in approach have, for instance, led to a different number of classes or different grouping of safety functions.

ESTABLISHING THE INPUT TO THE CLASSIFICATION PROCESS: REVIEW OF POSTULATED INITIATING EVENTS

To establish the inputs required to start the classification process, the safety objective for the design should be analyzed and the specific safety challenges associated with the specific reactor type (or technology) and with the specific plant should be identified, as well as the philosophy for prevention of these challenges and mitigation of their effects. The list of

postulated initiating events applicable to the reactor type should be reviewed and adapted to the particular plant. This list should take into consideration the relevant internal and external hazards affecting the plant in accordance with the requirements. Grouping or bounding of postulated initiating events should be performed and assessed during the design and prior to the safety classification process, using deterministic safety analysis and where appropriate, probabilistic safety assessments. For plant modifications, the newly identified or modified postulated initiating events should be assessed, with account taken of interfaces with existing safety functions and safety classes of SSCs that may be affected.

IDENTIFICATION OF PLANT SPECIFIC SAFETY FUNCTIONS

At the early stage of design, reactor type safety functions, which are necessary to fulfill the fundamental safety functions in all plant states, should be identified in accordance with the safety objectives for the design. These will comprise preventive safety functions and mitigatory safety functions.

Items that are necessary for performing the fundamental safety functions should be defined to an adequate level of detail to allow the identification of the required SSCs. Therefore, the reactor type safety functions should be broken down to plant specific safety functions, which are related to the individual plant location, design, and operation.

Each plant specific safety function should be linked to a particular bounding postulated initiating event, and should be refined in the design process to establish and fulfill the fundamental safety functions. Some plant specific safety functions can be defined to cover more than one postulated initiating event.

For existing nuclear power plant designs, lists of plant specific safety functions are usually available. In some safety classification schemes, reactor type safety functions are detailed enough that they can be used as plant specific safety functions and immediately allocated to bounding postulated initiating events.

The plant specific safety functions that are required to fulfill the fundamental safety functions during normal operation should be identified. These preventive measures are aimed at avoiding failures of SSCs that may cause initiating events and abnormal operation, and at maintaining the integrity of the main confinement barriers. Failures of SSCs can originate from malfunctions and from the effects of external and internal hazards or human induced events. For practical purposes, specific failures can be eliminated from the plant design basis provided suitable provisions have been implemented or relevant requirements and criteria met.

These preventive plant specific safety functions should ensure that the fundamental safety functions are fulfilled in normal operation. Most preventative plant specific safety functions support the three fundamental safety functions only indirectly by preventing operating conditions for which the mitigatory plant specific safety functions could be ineffective. Preventive plant specific safety functions identified during the early stage of the design should be reviewed.

Mitigatory plant specific safety functions should be identified at an adequate level of detail to identify the SSCs that control and mitigate the consequences of initiating events such that the relevant safety acceptance criteria are met for all anticipated operational occurrences and design basis accidents, and the consequences of designed extension conditions are appropriately reduced.

Safety functions for the mitigation of anticipated operational occurrences detect and intercept deviations from normal operation in order to prevent anticipated operational occurrences from escalating to an accident condition.

Safety functions for the mitigation of design basis accidents control accidents within the safety acceptance criteria of the plant's design basis. Mitigatory safety functions for design basis accidents can be subdivided into two levels, depending on the potential consequences of the accident and the time needed to achieve a controlled or safe shutdown state.

The two levels are based on the definition of plant states as follows:

- Level A mitigatory safety functions for design basis accidents should establish a controlled state following a design basis accident. A controlled state should be reached as soon as possible.
- Level B mitigatory safety functions for design basis accidents should
  - achieve and maintain a safe shutdown state following a design basis accident after a controlled state is reached; and
  - minimize the challenge to the remaining barriers from the design basis accident.

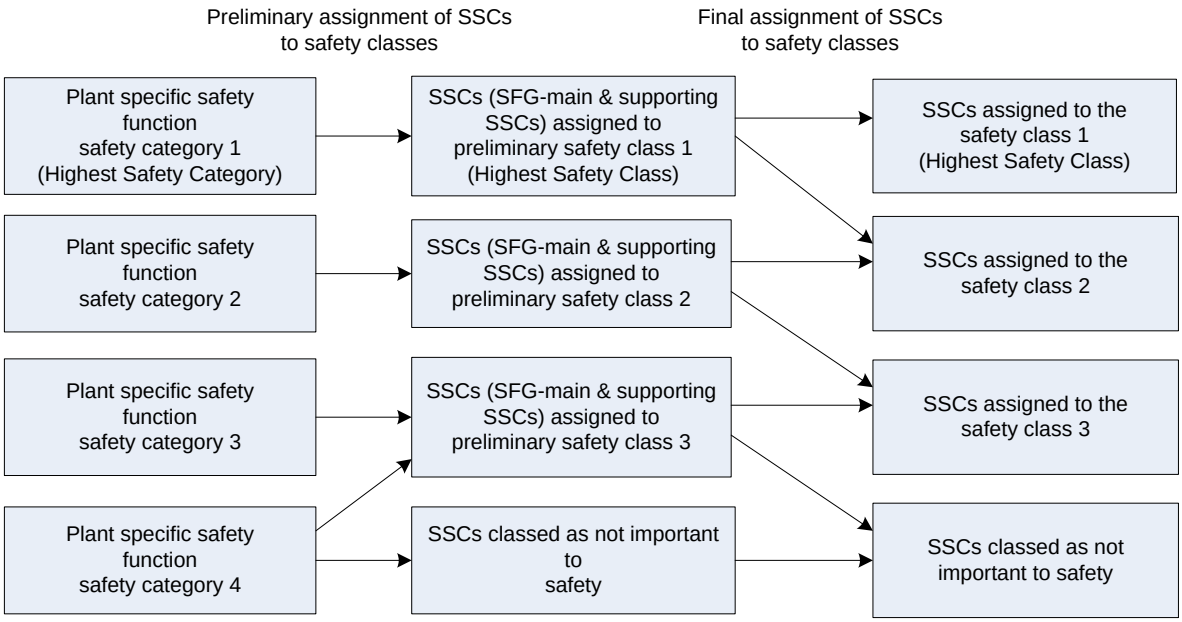
Level A and B mitigatory safety functions can be achieved by active or passive safety systems and features, or potentially by means of operator actions, to control reactivity, heat removal, and radioactive releases to the environment to within prescribed regulatory limits. In the safe shutdown state achieved by Level B mitigatory safety functions, plant parameters are well below the design limits for components and structures, the reactor remains sub-critical, decay heat is removed for as long as necessary, and radiological releases do not exceed those of normal operation.

Safety functions for the mitigation of design extension conditions are intended to limit accident progression and to mitigate the consequences of a severe accident.

CLASSIFICATION OF STRUCTURES, SYSTEMS AND COMPONENTS

The recommended approach to safety classification uses three safety classes. Initially, SSCs should be assigned to the safety class corresponding to the safety category of the plant specific safety function that they fulfill.

These correspondences are shown in figure 71. However, because not all SSCs within a safety functional group may make an equal contribution towards achieving the desired safety function, some SSCs may then be assigned to a lower safety class.



Source: IAEA DS367

Figure 71. Assignment of SSCs to safety classes

If justified by an appropriate safety analysis, a safety class lower than the safety class initially assigned can be proposed for an SSC. For example, an SSC could be assigned to a lower safety class (generally one level lower) in the following cases:

- The SSC does not directly support the accomplishment of the plant specific safety function in the corresponding safety category.
- The SSC would already be in operation at the moment the postulated initiating event occurs, and its safety function(s) would not be affected by it.
- The corresponding plant specific safety function is fulfilled by more than one SSC, the safety class could be lowered if
  - the SSC to be assigned to a lower safety class is less likely to be used than other SSCs in the safety functional group; or
  - it will be possible to deploy the safety function in time for it to be effective.

If there are main SSCs within certain safety functional groups whose failure cannot be accepted because the conditional probability for unacceptable consequences is approximately 1, then these SSCs should be allocated to the highest safety class, and additional engineering design rules should be specified on a case by case basis.

Supporting SSCs should initially be assigned to the same class as that of the main SSCs in the safety functional group. The class of a supporting SSC could, however, be lowered later.

If an SSC contributes to the performance of several plant specific safety functions of different categories, it should be assigned to the class corresponding to the highest of these categories.

In the classification of SSCs, no account should be taken of whether the operation of the SSC is active or passive, or a mixture.

Any SSC that is not part of a safety functional group but whose failure could adversely affect that safety functional group in accomplishing its plant specific safety function should be classified in accordance with the safety category of that safety functional group. The SSC may later be assigned to a lower safety class depending on the conditional probability of the consequential failure of the safety functional group.

Where the safety class of connecting or interacting SSCs is not the same, interference between the SSCs should be prohibited by means of a device classified in the higher safety class, to ensure that there will be no effects from a failure of the SSC in the lower safety class. An exception may be made where there is no identified mechanism to propagate a failure to the higher safety class.

By assigning each SSC to a safety class, a set of common engineering design rules can be identified that will ensure that an appropriate quality and reliability is achieved.

d. Explain the methods for establishing I&C structures, systems, and components storage, installation, and acceptance criteria for testing and calibration.

The following is taken from the U.S. Nuclear Regulatory Commission, Appendix A to Part 50—"General Design Criteria for Nuclear Power Plants."

Overall Requirements

Criterion 1—Quality standards and records: Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency, and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A quality assurance program shall be established and implemented to provide adequate assurance that these SSCs will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of SSCs important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

Criterion 2—Design bases for protection against natural phenomena: Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions. The design bases for these structures, systems, and components shall reflect 1) appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated; 2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena; and 3) the importance of the safety functions to be performed.

Criterion 3—Fire protection: Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. Noncombustible and heat resistant materials shall be used wherever practical throughout the unit, particularly in locations such as the containment and

control room. Fire detection and fighting systems of appropriate capacity and capability shall be provided and designed to minimize the adverse effects of fires on SSCs important to safety. Firefighting systems shall be designed to assure that their rupture or inadvertent operation does not significantly impair the safety capability of these SSCs.

Criterion 4—Environmental and dynamic effects design bases: Structures, systems, and components important to safety shall be designed to accommodate the effects of, and to be compatible with, the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These SSCs shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit. However, dynamic effects associated with postulated pipe ruptures in nuclear power units may be excluded from the design basis when analyses reviewed and approved by the Commission demonstrate that the probability of fluid system piping rupture is extremely low under conditions consistent with the design basis for the piping.

Criterion 5—Sharing of SSCs: Structures, systems, and components important to safety shall not be shared among nuclear power units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, in the event of an accident in one unit, an orderly shutdown and cooldown of the remaining units.

Criteria for Testing and Calibration

Instrumentation and control: Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

Inspection and testing of electric power systems: Electric power systems important to safety shall be designed to permit appropriate periodic inspection and testing of important areas and features, such as wiring, insulation, connections, and switchboards, to assess the continuity of the systems and the condition of their components. The systems shall be designed with a capability to test periodically 1) the operability and functional performance of the components of the systems, such as onsite power sources, relays, switches, and buses; and 2) the operability of the systems as a whole and, under conditions as close to design as practical, the full operation sequence that brings the systems into operation, including operation of applicable portions of the protection system, and the transfer of power between the nuclear power unit, the offsite power system, and the onsite power system.

10. I&C personnel must demonstrate a familiarity level knowledge of operations and maintenance of I&C systems.

a. Explain the maintenance management requirements as defined in DOE O 433.1B, admin chg 1, *Maintenance Management Program for DOE Nuclear Facilities*, and DOE G 433.1-1A, *Nuclear Facility Maintenance Management Program Guide for use with DOE O 433.1B.*

The following requirements are taken from DOE O 433.1B.

DOE G 433.1-1A provides acceptable approaches for meeting the requirements of DOE O 433.1B. Using a graded approach, DOE G 433.1-1A references Federal regulations, DOE directives, and industry best practices regarding implementation of requirements for maintaining DOE-owned government property. Guidance for applying the graded approach is provided in DOE G 433.1-1A.

All hazard category 1, 2, or 3 nuclear facilities, as defined in DOE STD-1027-92, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*, must conduct all maintenance of SSCs that are part of the safety basis in compliance with an approved nuclear maintenance management program (NMMP).

NMMPs for government-owned contractor operated (GOCO) facilities must demonstrate compliance with the requirements contained in the contractor requirements document of DOE O 433.1B and must be approved by the respective field office manager; approval consists of reviewing NMMP description documentation and evaluating its compliance with attachment 1. NMMPs for government-owned government-operated (GOGO) facilities must demonstrate compliance with the requirements.

NMMPs for GOGO facilities must demonstrate compliance with the requirements contained in attachment 2 of DOE O 433.1B and must be approved by the respective Secretarial Officer (SO) or designee; approval consists of reviewing NMMP description documentation and evaluating its compliance.

Approval of NMMP description documentation is required prior to startup of new hazard category 1, 2, and 3 nuclear facilities and at least every three years for all hazard category 1, 2, and 3 nuclear facilities.

Changes to NMMPs must be reviewed under the unreviewed safety question (USQ) process to ensure that SSCs are maintained and operated within the approved safety basis, as required by 10 CFR 830, "Nuclear Safety Management." Changes which would result in a USQ must be approved prior to the change taking effect.

Assessments of NMMP implementation must be conducted at least every three years, or less frequently, if directed by the SO, in accordance with DOE O 226.1B, *Implementation of Department of Energy Oversight Policy*, to evaluate whether all CRD requirements are appropriately implemented.

Periodic self assessments in accordance with DOE O 226.1B must be conducted to evaluate the effectiveness of oversight of NMMPs.

A single maintenance program may be used to address the requirements of DOE O 433.1B and the requirements of DOE O 430.1B, *Real Property Asset Management*.

The following requirements are taken from DOE G 433.1-1A.

Nuclear Maintenance Management Program

DOE O 433.1B requires DOE facility operators to develop and implement an NMMP for hazard category 1, 2, and 3 nuclear facilities under DOE cognizance. In accordance with DOE O 433.1B, the NMMP must describe the safety management program for maintenance, and the reliable performance of SSCs that are part of the safety basis at hazard category 1, 2 and 3 DOE nuclear facilities. In accordance with DOE O 433.1B, the NMMP must clearly address the 17 elements of maintenance identified in section 2 of attachment 2 of DOE O 433.1B.

Beyond the administrative requirements regarding 1) the scope of and areas to be addressed by the NMPP and 2) the timeframes for implementation and review, DOE O 433.1B provides broad latitude for operating organizations in defining their NMMP to best suit their mission and organizational environment.

Nuclear Maintenance Management Program Description Documentation

DOE O 433.1B requires NMMP description documentation to be, at a minimum, an applicability matrix or a combination of multiple documents that covers 1) correlation of the requirements to the applicable facilities; 2) correlation of the implementing documents to the specific requirements; and 3) documentation of the basis for applying a graded approach, if applicable.

DOE O 433.1B requires each organization to develop an NMMP-Description Document (DD) that addresses the topics listed in DOE O 433.1B, and that the NMMP-DD be submitted to DOE for review and approval. Re-submission for review and approval is required at least every three years.

Sites with more than one nuclear facility and/or contractor may develop a consolidated NMMP that can accommodate the facility differences without losing effectiveness.

DOE O 433.1B states that the NMMP-DD can be anything from a manual to a combination of multiple documents, to an applicability matrix, at a minimum. The maintenance implementation plan (MIP) that was required by the previous revision of DOE O 433 served a similar purpose to the NMMP-DD. In practice, MIPs varied from a very thick manual with much detail to an applicability matrix that simply listed the procedure documents associated with each element of maintenance. Most MIPs included an applicability matrix; some MIPs also included a description of the overall maintenance program.

MIPs can be converted into NMMP-DD, and compliance with the current Order can be achieved with an NMMP-DD that is only an applicability matrix so long as it identifies the document(s) that report 1) the basis for applying the graded approach; and 2) the

implemented (or planned) site-specific methods for satisfying the Order's requirements for each of the 17 elements of maintenance.

An applicability matrix is a table listing a set of applicable procedures and other associated documents and sometimes listing the applicable paragraph numbers of sections of the documents. An applicability matrix does not contain any narratives or explanations of the listed documents.

It is recommended that the applicability matrix include/list a single document that provides an overall summary of the NMMP. This summary should be written at a level that comprehensively describes the big picture of the implemented (or planned) site-specific methods for satisfying the Order's requirements for each of the 17 elements of maintenance. An appropriate title for this document is NMMP Summary-Level Description or NMMP Summary. A recommended practice is for this NMMP Summary to contain an assessment of strengths and weaknesses along with a listing and explanation of the planned continuous improvements (if any).

Application of Graded Approach

Attachment 2 of DOE O 433.1B requires Federal and contractor organizations to submit an NMMP-DD that provides documentation of the basis for applying a graded approach, if applicable. The graded approach methodology ensures the level of rigor for implementing the Order's 17 maintenance management elements is based on their importance/significance and associated consequences.

Graded approach, as defined in 10 CFR 830, means the process of ensuring that the level of analysis, documentation, and actions used to comply with a requirement are commensurate with the following:

- The safety, safeguards, and security function provided
- The magnitude of any hazard involved
- The life-cycle stage of a facility
- Programmatic mission of a facility
- Particular characteristics of a facility
- The relative importance of radiological and non-radiological hazards
- Any other relevant factor

DOE contractors should use knowledge of their nuclear facilities and sound engineering judgment to determine the depth of detail and magnitude of resources required for implementing each of the Order's 17 maintenance management elements.

The method of, and basis for, applying the graded approach should be documented and address the following:

- How the graded approach defined in 10 CFR 830 was used
- Where it was applied
- Why it was used and how it ensures an adequate level of safety for this SSC

b. Explain safety-related maintenance requirements.

Refer to item "a" in this competency for an explanation of safety-related maintenance requirements.

c. Explain the relationship between maintenance and conduct of operations, quality assurance, and configuration management.

The following is taken from DOE G 433.1-1A.

The safety management program is designed to ensure a facility is operated in a manner that adequately protects workers, the public, and the environment by covering topics such as quality assurance; maintenance of safety systems; personnel training; conduct of operations; inadvertent criticality protection; emergency preparedness; fire protection; waste management; or radiological protection of workers, the public, and the environment.

To perform the planning function correctly and efficiently, the maintenance activity should be evaluated to determine the necessary worker skills along with the necessary level of detail in procedures to support the activity. The requirements to provide procedures to maintain SSCs important to facility safety are defined in DOE O 433.1B, DOE O 422.1, *Conduct of Operations,* 10 CFR 830, and the facility TSR.

In accordance with DOE O 433.1B, the NMMP must include incorporation of the configuration management program to control approved modifications and to prevent unauthorized modifications to safety SSCs. Implementation of configuration management (CM) programs shall be in accordance with requirements of DOE O 420.1B.

The NMMP should address the following:

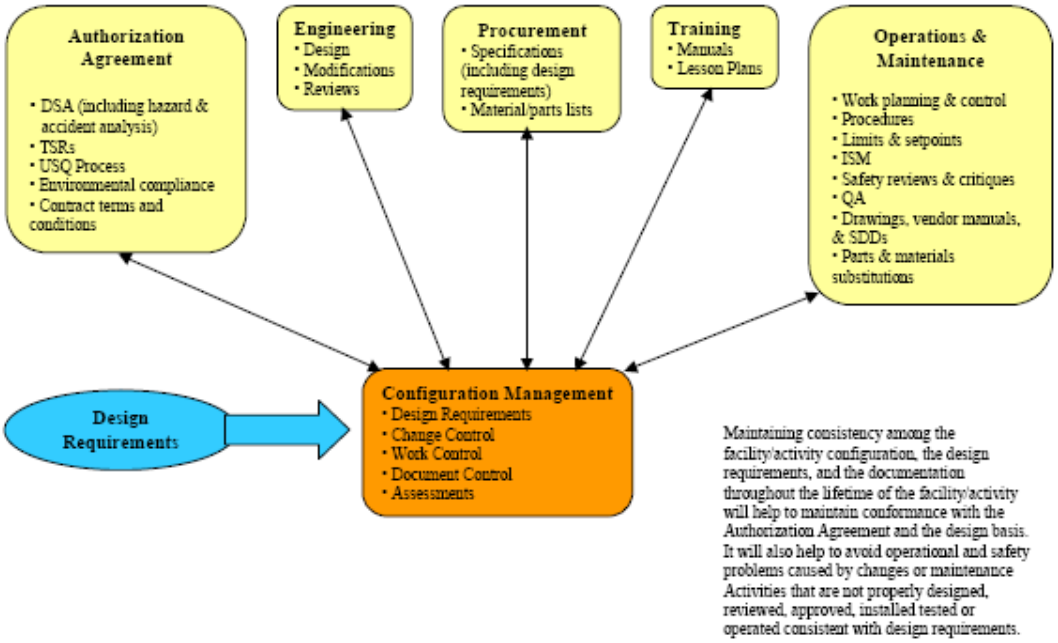
- The process to document and maintain plant configuration and handle desired changes, while maintaining the facility safety basis and without increasing risk to personnel, facility equipment, or the environment
- The process to authorize the use of equivalent repair parts, and a method for workers to verify this approval
- The role of the cognizant systems engineer in CM, according to DOE O 420.1B
- A method to ensure that planners and workers are familiar with the need for engineering review and approval if maintenance will not result in returning SSCs to their design configuration

11. I&C personnel must demonstrate a working level knowledge of the configuration management process applied to I&C systems documentation.

a. Explain the importance of the configuration management process as it applies to I&C systems (e.g., documenting, controlling, revising, and issuing I&C drawings, as-built configuration, software, calculations, and analyses).

The following is taken from DOE-STD-1073-2003.

Configuration management supports a number of contractor organizations and initiatives by ensuring conformance with the established design requirements. Figure 72 illustrates some of these interfaces.



Source: DOE-STD-1073-2003

Figure 72. Configuration management interfaces

DOE-STD-1073-2003, *Configuration Management*, recognizes the need for configuration management of software used to perform functions or analysis related to safe operations, but it does not provide detail on the special considerations related to software configuration management. For example, DOE-STD-1121-2008, *Internal Dosimetry*, states that dosimetry codes should be subject to configuration management, including records of the version of the code, the user's manual, instructions for running the code, limitations of the code, hardware requirements, acceptance testing records, and a copy of the code itself. Contractors should refer to DOE G 200.1-1, *Software Engineering Methodology*, or other standards on software configuration management, to supplement the guidance in DOE-STD-1073-2003 for software.

DOE O 430.1B requires a configuration management process to ensure the integrity of physical assets and systems, and configuration integrity in designs and acquisitions. DOE G 430.1-5, *Transition Implementation Guide*, encourages the use of configuration management and configuration control during transition from the operational to the disposition phase of a facility/activity life to ensure accurate and up-to-date drawings are used in the transition process.

b. Explain the change control process described in DOE-STD-1073-2003, Configuration Management Program and DOE O 414.1D, Quality Assurance.

The following is taken from DOE-STD-1073-2003.

Contractors must establish and use a formal change control process as part of the configuration management process. The objective of change control is to maintain consistency among design requirements, the physical configuration, and the related facility documentation, even as changes are made. The change control process is used to ensure changes are properly reviewed and coordinated across the various organizations and personnel responsible for activities and programs at the nuclear facility.

Through the change control process, contractors must ensure that

- changes are identified and assessed through the change control process;
- changes receive appropriate technical and management review to evaluate the consequences of the change;
- changes are approved or disapproved;
- waivers and deviations are properly evaluated and approved or denied and the technical basis for the approval or the denial is documented;
- approved changes are adequately and fully implemented or the effects of the partial implementation are evaluated and accepted;
- implemented changes are properly assessed to ensure the results of the changes agree with the expectations; and
- documents are revised consistent with the changes and the revised documents are provided to the users.

Identifying Change Mechanisms

The contractor must ensure that each proposed change to the facility, activity, or operation is considered for processing through the change control process. To ensure that all changes are controlled as appropriate, the contractor must identify all mechanisms that can lead to temporary or permanent changes in

- the design requirements
- the physical configuration
- the documentation

For any facility, activity, or operation there are typically multiple mechanisms for initiating change. Changes may be initiated through any of a variety of organizations, such as design, operations, maintenance, procurement, procedures, training, and security. Changes can include physical, document, procedural, operations, software, or design changes. Contractors should assess each type of change to determine the mechanisms for initiating changes and link them to the change control process. Contractors should integrate the change control process into the work processes for all potential mechanisms of changes by requiring workers and organizations to use the change control process, as appropriate, when a change is to be made. The identification of change mechanisms is often the most critical step to achieving effective change control. Change mechanisms that are not identified cannot be controlled.

Once change mechanisms are defined, contractors should ensure that the change control process is properly integrated into the procedures and other work processes for that change mechanism. Contractors should consider eliminating or combining change mechanisms to make changes easier to control.

Considering the Impact of Minor Changes

It is important to identify and consider even subtle changes under the configuration management process. Changes that are perceived to be minor or insignificant can significantly impact the functions of SSCs required to maintain safe operation or to achieve mission objectives. They can also result in operation outside the approved safety basis. A well-designed change control process should include a screening process to determine if seemingly insignificant changes should have at least a cursory review by an interdisciplinary group to confirm that there will be no significant impacts from the proposed change. In addition, the contractor must ensure that the USQ process is invoked and applied to changes, consistent with the requirements of 10 CFR 830 and the DOE-approved USQ process, to maintain the integrity of the safety basis.

Making Equivalent Changes

Changes that are shown to be equivalent changes do not need to be evaluated under the change control process. Equivalent changes are hardware changes that

- continue to meet the design requirements for the equipment
- meet all interface requirements
- do not impact the safety basis

An example of an equivalent change would be replacement of a failed part with the same make and model number part. However, as vendors sometimes change materials or design of components without changing the model number, the contractor should ensure that the design requirements continue to be met by the replacement part.

Using a Consistent Configuration Management Process

If multiple change control processes are used, they should be consolidated into a single, consistent change control process that is useful and effective. Unique change control processes for specific types of changes, such as software changes, should be integrated into the overall change control process for the activity. The change control process may provide provisions for varying levels of review based on a documented graded approach, as well as graded schedules for updating documents based upon their relative importance. Facility managers should ensure that vendors and subcontractors use the established process. All personnel in design, operations, and support organizations that do work for the facility or activity should

- be trained on the change control process
- follow the associated procedures closely
- be alert to activities that may not be planned or may occur without following appropriate procedures

Developing Efficient Configuration Management Processes

The change control process should be efficient to ensure that it is used effectively. Forms and procedures should be easy to use and understand, particularly as the change control process will need to be used by individuals from a number of organizations with varied backgrounds and experience. To be effective, forms and procedures should

- facilitate complete and timely change identification and control
- be easy to use and encourage participants to use them
- provide for management tracking and reporting

c. Explain the purpose and objectives of the operational configuration management program, and explain how it relates to I&C systems.

The following is taken from DOE-STD-1073-2003.

To assess the impact a change will have on an activity, the contractor must understand the design requirements of the activity. These design requirements must be identified and documented, and changes to them must be controlled.

The contractor should identify and document the set of SSCs for an activity that will be managed through the configuration management process. This set is referred to as the CM SSCs. The CM SSCs are compiled from several sets of SSCs. These sets may overlap.

The first set of SSCs that must be included in the CM SSCs for hazard category 1, 2, and 3 nuclear facilities is the set of safety SSCs identified in the DSA as required by 10 CFR 830. Safety SSCs are defined as the combination of SC SSCs and SS SSCs, and they include those SSCs whose preventive or mitigative functions are considered to be major contributors to defense-in-depth and worker safety. The safety SSCs identified in the DSA constitute the baseline set of SSCs that must be included in the configuration management process.

In addition, contractors should include in the set of CM SSCs the SSCs whose functions are considered to be important to defense-in-depth or worker safety, but are not already included in the safety SSCs. The combination of the safety SSCs and the other defense-in-depth SSCs should encompass the vital safety systems. The vital safety systems include the SS systems, the SC systems, and other systems that perform an important defense-in-depth safety function.

The contractor should also review the activity to determine if it is appropriate to include other SSCs in the set of CM SSCs. Other categories of SSCs that should be considered include the following:

- Mission critical SSCs—SSCs whose failure could cause substantial interruption to the mission of the facility or activity
- Environmental protection SSCs—SSCs that could have a significant impact on the environment if they failed to perform their function
- Costly SSCs—SSCs that would be expensive to fix or replace or whose failure could result in problems that could be expensive to fix
- Critical Software—software whose proper performance is critical to the expected performance of a safety SSC, a defense-in-depth SSC, or the safety of the nuclear facility
- Master Equipment List SSCs—SSCs that are included in the maintenance program
- Adjacent SSCs—SSCs that are located adjacent to the safety or defense-in-depth SSCs such that changes to these SSCs could negatively impact the safety or mission of the activity

Figure 73 illustrates the various sets of SSCs that should be considered by the contractor when compiling the set of CM SSCs. The design authority should define the SSCs that fall under each type. Some SSCs will fall under multiple designations.

Source: DOE-STD-1073-2003

Figure 73. Compiling the set of CM SSCs

Identified systems must have defined system boundaries and component lists. Defined systems should contain those components necessary to accomplish the system's function and meet the system's design requirements. Applicable design codes and standards often define system boundaries. In addition, the following considerations may help to define system boundaries for some facilities or activities:

- Location of piping class breaks
- Location of isolation valves
- Location of seismic class breaks
- Location of test features

Some supporting features may be outside the system boundary, such as electrical power, instrument air, lubricating oil, and ventilation. In addition, some complete systems, such as ventilation systems, may cross multiple facility and activity boundaries.

Identifying and Documenting Design Requirements

Once the set of CM SSCs is identified, the contractor must identify and document the design requirements for this set of SSCs. The contractor must assess the effects of changes to the design requirements of CM SSCs through the configuration management process. Furthermore, the contractor must maintain the design requirements for CM SSCs throughout the life of the nuclear activity.

The documentation should identify which of the design requirements are required for safety and which are necessary for cost, environmental, or other considerations, so the impacts of changes can be better assessed.

The design requirements to be documented include those that affect

- function
- installation
- performance
- operation
- maintenance

12. I&C personnel must demonstrate a working level knowledge of life cycle management.

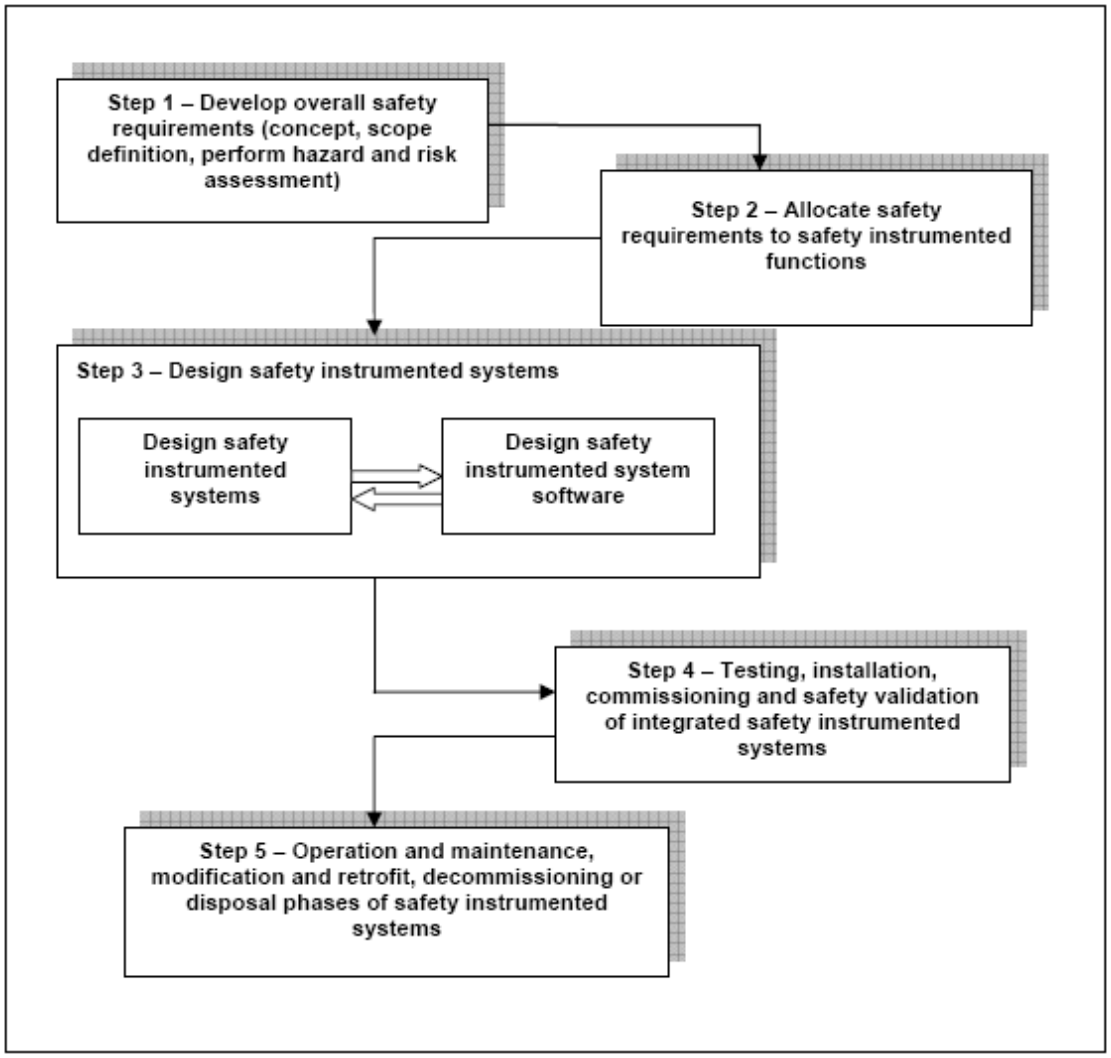
a. Explain the importance of life cycle management to I&C systems.

The following is taken from DOE-STD-1195-2011 and is repeated from competency statement 8 for convenience.

A key aspect of the implementation of ANSI/ISA 84.00.01-2004 is effective control over each stage of the SIS life cycle to ensure proper initial design, proper installation, effective operation and maintenance, and configuration control. The processes for performing the life-cycle management for SIS should be defined, including identifying the organization(s) responsible for implementing them. The life-cycle stages outlined in ANSI/ISA 84.00.01-2004 can be fulfilled by conformance to the ANSI/ISA 84.00.01-2004 requirements or by conformance to DOE orders, manuals, standards, and guides that provide equivalent processes and methods for the life-cycle stages of the safety instrumented functions.

The elements in the life cycle are hazards identification, safety requirements specification, design, installation, startup testing, management of change, operational testing, maintenance, operation, modification, and decommissioning of SIS. The life cycle also includes retention of the original documentation, including design criteria, procurement specification, commercial grade dedication files, and other relevant information for the life of the affected systems. Management of changes is applied in all steps of the life cycle.

This life-cycle approach is directed toward reducing the risks inherent in process facility operations. The ANSI/ISA 84.00.01-2004 approach can be summarized into five steps as depicted in figure 74.



Source: DOE-STD-1195-2011

Figure 74. Lifecycle steps

STEP 1: DEVELOP OVERALL SAFETY REQUIREMENTS

This initial phase focuses on how much risk reduction will be required throughout the life cycle of the SIS. Some level of residual risk will always exist. The purpose of any safety system is to reduce the identified risk to an acceptable level as defined in the safety basis documentation.

Following the establishment of the conceptual requirements and scope definition, ANSI/ISA 84.00.01-2004 begins with a requirement to perform a hazard analysis and identification of hazards and associated risks. The safety functions that are required to reduce the identified risks to an acceptable level are determined during this phase.

STEP 2: ALLOCATE SAFETY REQUIREMENTS TO SAFETY INSTRUMENTED FUNCTIONS

Acceptable risk is achieved by allocating safety requirements to various safety functions. The safety functions are then allocated to different systems, such as SC/SS mechanical or process

systems, design features, SC or SS SISs, and other external hazard controls. When a safety function is allocated to an SIS, it is called a safety instrumented function (SIF). The allocation process also includes assigning a safety integrity level (SIL) to the SS SIF, which corresponds to the amount of risk reduction determined to be necessary in the hazard and risk analysis.

SILs can be expressed as either risk reduction factors (RRFs) or as a PFDavg. SILs have four discrete performance ranges and two kinds of controls; namely, those that respond on demand and those for continuous demand. The SIL is related to the average probability of the SIS failing when demanded to perform its safety function. In either case, ANSI/ISA 84.00.01-2004 applies. The SIL performance requirements in terms of the PFDavg and RRF are listed in table 15.

Table 15. SIL level and performance ranges for on demand modes

SIL Level Designation	Probability of Failure On Demand-average (PFDavg)	Risk Reduction Factor (RRF)
SIL-1	$< 10^{-1}$ to $\geq 10^{-2}$ PFDavg	> 10 to ≤ 100 RRF
SIL-2	$< 10^{-2}$ to $\geq 10^{-3}$ PFDavg	> 100 to ≤ 1000 RRF
SIL-3	$< 10^{-3}$ to $\geq 10^{-4}$ PFDavg	> 1000 to ≤ 10,000 RRF
SIL-4	$< 10^{-4}$ to $\geq 10^{-5}$ PFDavg	> 10,000 to ≤ 100,000 RRF

Source: DOE-STD-1195-2011

SIL-1 represents the lowest risk-reduction level of performance; SIL-4 represents the highest risk-reduction level of performance. SIL-4 is not used in the process industry sector because it requires elaborate systems and is difficult to support because of the high level of reliability required of the hardware. SIL-4 systems are not expected to be used for SS controls in DOE facilities.

A number of methods (qualitative and quantitative) are available for assigning the SIL. Qualitative methods may be appropriate when the risk, implementing design, and the hardware are not well understood. Quantitative methods, such as fault tree or event tree analysis, should be used when the design and hardware are well understood and supporting data are available.

Quantitative methods are required for verification that the final design and its installation meet the assigned SIL. Assigning the SIL links the design integrity of the SIS to the required level of risk reduction, and thereby closes the gap between the hazard analysis and safe process operation.

ANSI/ISA 84.00.01-2004 provides several methods for determining SIL, such as layer of protection analysis, which uses frequency of the event as a basis, or safety layer matrix, which uses available information of IPLs as a basis for selection of SIL for the SIS. For DOE's application, the accepted methodology is a deterministic method using the number of IPLs credited by hazard analysis.

STEP 3: DESIGN THE SIS AND SAFETY SOFTWARE

The SIL establishes a minimum required performance for the SIS, as measured by the PFDavg or RRF. The factors that affect the PFDavg or RRF are

- component failure rate
- redundancy/diversity of systems and components
- voting
- testing frequency
- diagnostic coverage
- common cause failure
- human factors
- technology
- software integrity

The user should design the SIS with hardware and software components considering the previously mentioned factors to achieve the PFDavg or RRF related to the target SIL. The target SIL is an objective of design process decisions, component specification, and procurement to ensure that the design is consistent with the target SIL. The design is verified at the end of the detailed design process to ensure that the design as installed and tested can achieve the assigned PFDavg or RRF.

STEP 4: TESTING, INSTALLATION, COMMISSIONING, AND SAFETY VALIDATION OF SIS

Testing is performed throughout the installation stages to enable validation and verification that SIS requirements are met. This phase of the life cycle addresses the policy that will be applied for the following:

- Integration of software and hardware
- Types of testing to be performed and data required to demonstrate functional adequacy and acceptance
- Environment necessary for conducting testing along with the configuration that exists for testing
- Test criteria for which data will be collected and used to judge acceptability
- Physical locations (factory or site) for which the test will be performed
- Personnel requirements and qualifications required for performing the various activities related to the validation and verification functions
- Process for documenting and dispositioning non-conformances

In step 4, the SIS design is validated in its as installed configuration as achieving its assigned SIL.

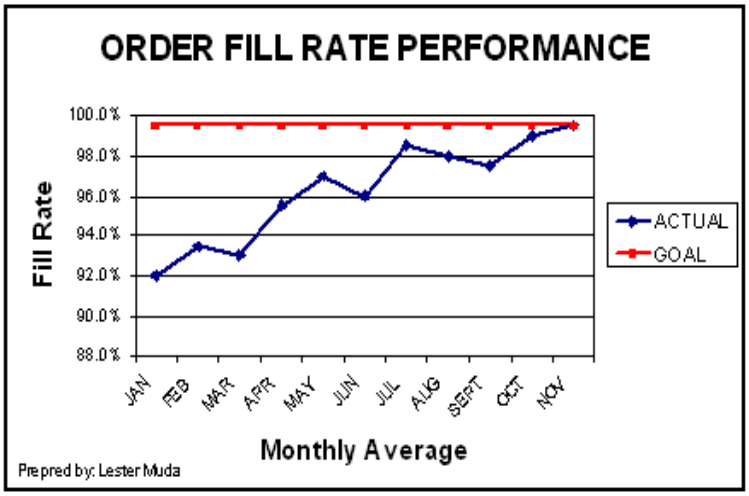
STEP 5: OPERATION AND MAINTENANCE, MODIFICATION AND RETROFIT, DECOMMISSIONING OR DISPOSAL PHASES OF SISs

Long-term preservation of an SIS through startup, operation, maintenance, and management of change activities is as important as initial design and installation phases. The SIL is not just a design parameter; it is also an operational parameter. The selection made during conceptual or preliminary design phases, including design configuration, testing frequency, and so on, is maintained throughout the life of the facility. Therefore, it is essential that management of system change be maintained to ensure preservation of the SIS.

b. Explain the mechanisms for feedback of relevant information, such as trend analysis and instrumentation performance reliability data, to identify necessary program modifications.

Trend Analysis

The following is taken from MoreSteam.com, *Trend Chart*.



Source: MoreSteam.com, Trend Chart

Figure 75. Typical trend chart

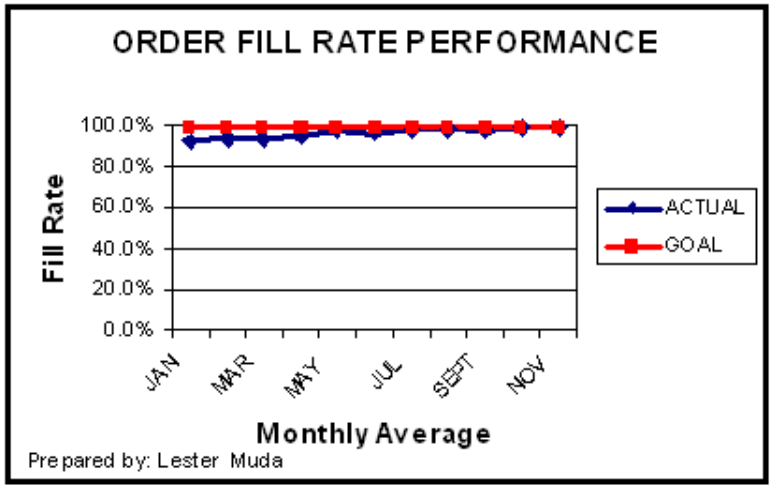
Trend charts are also known as run charts, and are used to show trends in data over time. All processes vary, so single point measurements can be misleading. Displaying data over time increases understanding of the real performance of a process, particularly with regard to an established target or goal. Figure 75 is an example of a trend chart of order fill rate performance.

A good trend chart has the following characteristics:

- A clear title to describe the subject of the chart
- Labels on the vertical Y-axis and horizontal X-axis to describe the measurement and the time period
- A legend to differentiate the plotted lines—in this case, the actual vs. the goal
- Appropriate scales that are narrow enough to show variation
- Limited characteristics on each chart to avoid confusion from too many lines
- An appropriate time frame.
- Notations on any major spikes
- Targets or goals should be noted on the chart for reference.
- Note who prepared the chart in case there are questions about the chart or the data.

Two common errors in chart construction are shown in figures 76 and 77.

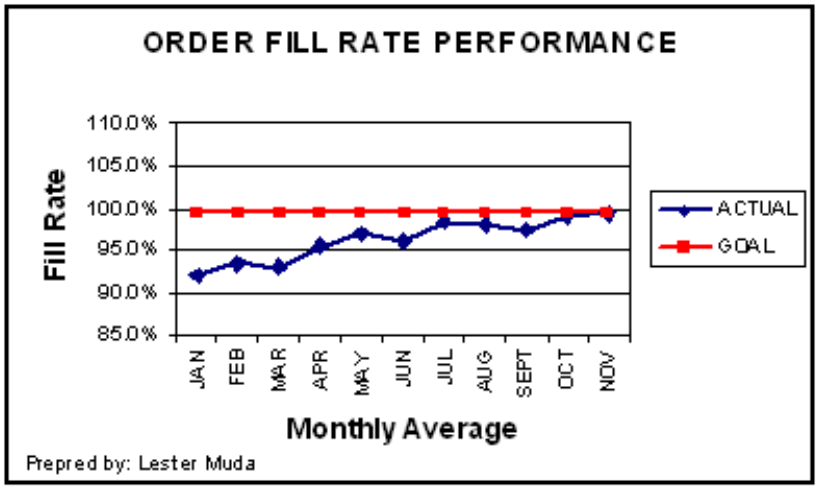
The chart in figure 76 has a scale that is so wide that little variation can be seen. The data are correct (and are the same as in figure 75), but the chart is not very useful because the scale is so wide (0-100%).



Source: MoreSteam.com, Trend Chart

Figure 76. Chart with little variation

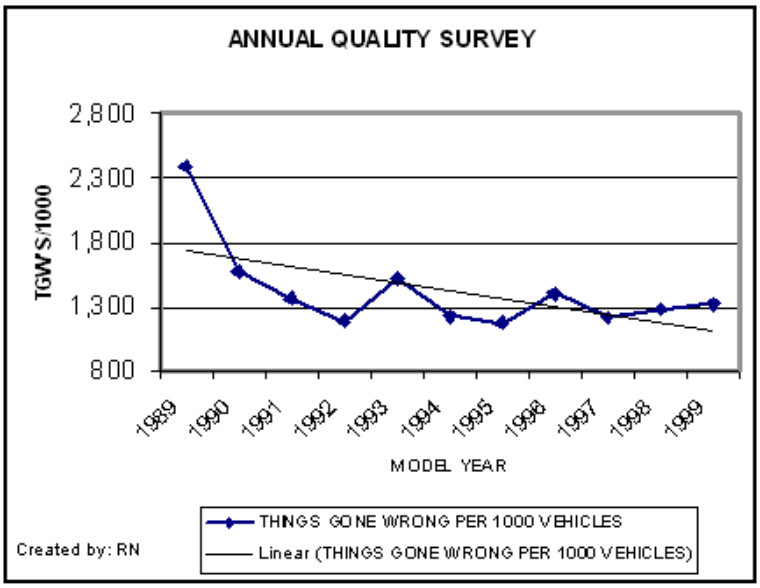
The chart in figure 77 has a scale that includes impossible numbers based on the definition of the metric being charted. In this case, fill rate cannot be higher than 100 percent, so a scale that goes to 110 percent is misleading. Again, this chart uses the same data as figure 75 and 76 but conveys a different message.



Source: MoreSteam.com, Trend Chart

Figure 77. Impossible numbers

A third problem arises from using long time scales and inappropriate trend line plots. Sometimes this practice is helpful for a long term perspective, but it can be confusing if it diverts attention from more recent events—especially when a trend line is plotted through the data. Consider figure 78, a chart of quality complaints, or things gone wrong (TGWs):



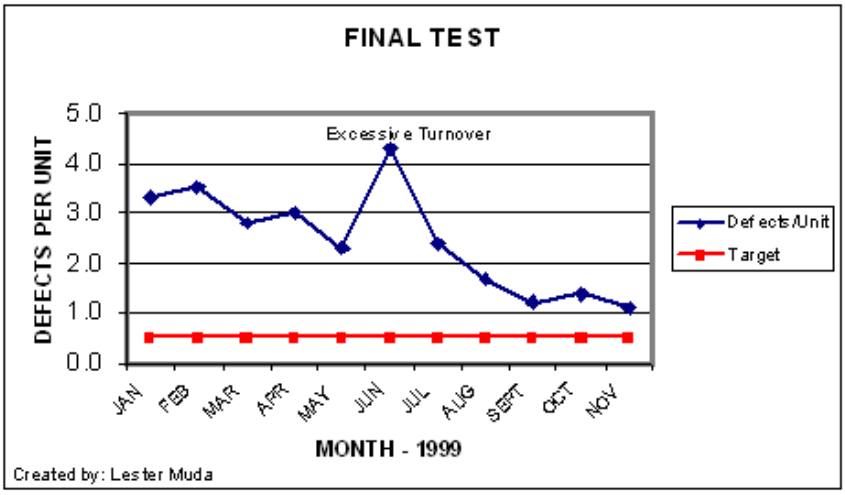
Source: MoreSteam.com, Trend Chart

Figure 78. Things gone wrong

It is a fact that the TGW level in 1999 (1,320) is 44.5 percent lower than it was in 1989 (2,378). The trend line appears to indicate continuous improvement over time. However, the process is relatively stable since 1990, with little sustained improvement since that time, and an increase in TGWs over the last two years.

The presentation of the chart can tell two different stories, and the trend line is not appropriate in this instance. See the following discussion and Figure 80 on the use of reference bars.

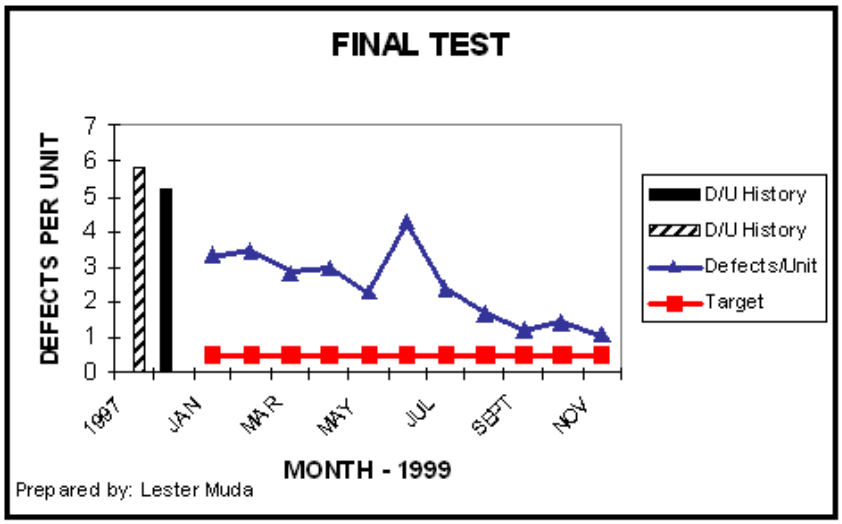
Many times a chart will exhibit an apparently abnormal fluctuation, or spike, as seen in figure 79. Since such spikes always raise questions, a good rule of thumb is to pro-actively answer the question by putting a note on the chart as shown. This practice also provides documentation of the history of a process and helps to connect cause with effect.



Source: MoreSteam.com, Trend Chart

Figure 79. Trend with an abnormal spike

It is not always obvious when a spike occurs. Control charts use statistical rules to establish control limits that give indication of a statistically significant change in the process.



Source: MoreSteam.com, Trend Chart

Figure 80. Reference bars

Whenever using data to make decisions, remember to question the quality of the measurement. A well-constructed chart made with poor quality data is not a valuable tool.

A further improvement to aid understanding of a trend chart is to add reference bars. Figure 80 is the same as that represented by figure 79, but has reference bars added to show the performance in prior years. The addition broadens the reader's perspective by showing the extent of improvement over a longer time horizon.

Trend charting enables process improvement teams to identify changes in process outputs over time. The chart can be used as a measurement tool to understand how a process is currently performing and also to track any changes in the process over time.

Instrumentation Performance Reliability Data

The following is taken from SA Instrumentation and Control, *Enhanced Reliability for Final Elements.*

Application of IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, in the process industry is mandatory. Based on an analysis of possible hazards and risks, safety measures have to be defined and implemented with the goal to bring the risk down to an acceptable level. SIFs are implemented to counter individual hazards. These SIFs typically comprise a sensor, monitoring the state of the process; a deciding logic, responsible for triggering the required action; and a final element, blocking a pipeline or venting it, which is comprised of a valve, an actuator, and a solenoid valve. A quantitative analysis of the whole loop is mandatory. The reliability performance of the loop can be calculated based on the performance and reliability data of the single components. Therefore, manufacturers are increasingly getting more requests to provide

reliability data, mainly the so-called dangerous failure rate, divided into detected and undetected failures and the safe failure fraction.

It is generally assumed that the performance of a typical loop is dominated by actuator and valve performance. The best numbers, and therefore the least risk, are created by the logic solver, followed by the sensor/transmitter element. The actuator/valve combination is rated worst. This might be astonishing at first glance, as a logic solver incorporating many electronic parts and even software seems to be more sophisticated and therefore more prone to error than the few pieces of metal making up a valve or actuator. The problem comes from the interaction with the process. Logic solvers, as complicated as they are, have been evaluated for a long time as being reliable; all of the components and subsystems have a known performance. The key to the success of this research, however, is that the logic solver operates in a known environment, the control room. By contrast, the final element is exposed not only to the environment, but also to the process. Due to the huge variety of materials, processes, phase states, and other conditions that can be found in a chemical plant, it is very hard to gather enough data to make a sound statistical statement for a given material or substance or process.

If someone uses, for example, the well-known EXIDA library to check out instrumentation for a loop, he/she will find plenty of equipment within the categories of logic solvers and transmitters, and also barriers. But the valve section is much less populated: only three manufacturers and three valve types are listed, and of these, only the SAMSON valve is an instrument for general service. Checking into the performance level of the rated product, the valve series 3241 gives surprising figures of reliability. What is the background of these figures, and can they be relied upon?

IEC 61508 opens two ways for defining reliability data: failure modes, effects, and diagnostic analysis (FMEDA), or prior use. FMEDA is the analysis of the design to calculate reliability data. But, as the use in the process industry can lead to process conditions and problems not foreseen, the second approach of employing prior use data seems to be more favorable. Prior use calls for recording and subsequent analysis of all failures for a given population in the field. There are also stringent requirements of the hours in use, which call for a large sample under investigation. It is not easy to achieve both at the same time; large population as well as complete and comprehensive records on all failures. To address this issue, SAMSON AG and Infraserv (former Hoechst AG) have run an investigation at their site in Frankfurt in a long-term project that seems to be the most comprehensive study on the market.

The future might bring a closer monitoring of safety loops in the plant, supported by new functionalities of field instruments. This monitoring should enable the generation of data on trip performance and test performance. Close cooperation between suppliers and end users should ensure the expansion of databases and generation of dependable safety figures.

PARTIAL STROKE TESTING

The total performance of the safety loop depends on instrument performance and the frequency of testing. The well-known formula is

$$PFD_{avg} = \lambda^{DU} TI/2$$

Where

PFD: Probability of failure on demand
λ^{DU}: Undetected dangerous failure rate
TI: Proof test interval

Therefore, the test interval is crucial for gaining a specific PFD value. Many chemical plants run on a basis of an annual shutdown. During this shutdown, the instrumentation, including the safety valves, is tested. However, in the petrochemical industry, operating times of five years between shutdowns are common. According to a simplified calculation, this requires a PFD value five times lower than that needed for a plant with annual shutdowns.

In order to avoid this stringent requirement, more frequent testing without interrupting operation of the plant is required.

One technology being proposed and already in use is the so-called partial stroke testing (PST). This involves a movement of 10 percent of a shutdown valve from 100 percent open to 90 percent open and then back to 100 percent. The actual movement has to be recorded. From the proof that the valve is able to move, the conclusion is made that the valve would shut down the pipeline completely in case of a demand. The PST procedure is described in many papers.

Issues still remain: what is the precise diagnostic coverage of this procedure? Due to the large variations in process conditions, there is certainly no general answer. A correct way to address this question could only start at the FMEDA of a shutdown system. It must be determined which failure modes could be detected by PST technology. A failure table might look like table 16.

Table 16. Failure table

Problem	Effect	Detectable at occurrence by PST	Detectable in advance by PST
Valve stem seized	Valve will not move	Yes	
Spring of actuator broken.	Valve will not move	Yes	
Corrosion of valve ball/plug		Probably	Possible
Crystallising media	Valve will not move after first stroke	Effects of PS dependent on individual process	

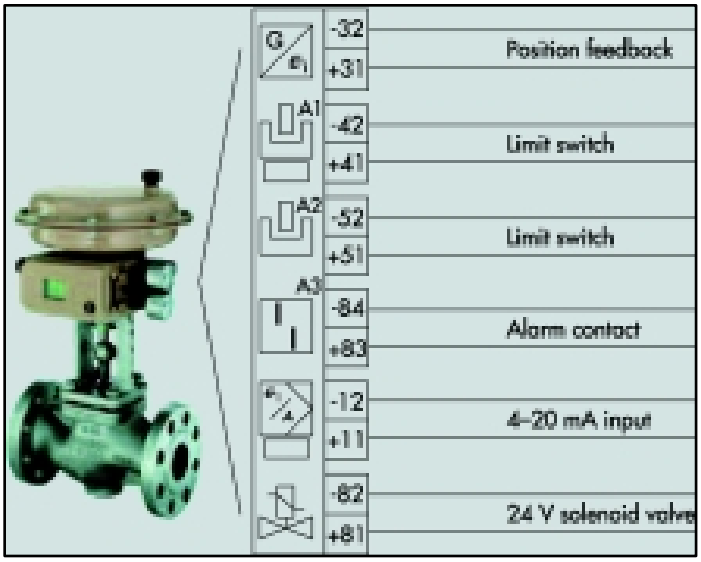
Source: SA Instrumentation and Control, Enhanced Reliability for Final Elements

Only by making this specific breakdown can the benefits of PST be made clear for a given process. Therefore, the conclusion to the test is similar to the use of valves. The manufacturer can provide general data; the customer is responsible for analyzing his/her process and making correct use of the data. A general statement like "...partial stroke can extend your process run time to..." makes no sense. Furthermore, a packaged bundle from one supplier consisting of positioner, actuator, and valve should be more advantageous in regard to precise statements on diagnostic coverage than a combination of valve and positioner from different suppliers mounted first on site of the user.

HOW IS A PARTIAL STROKE APPROACH VALIDATED?

Assume, based on implementation of a PST, the inspection interval of an SIF is extended. How can it be proved that a partial stroke has been performed? A detailed look into the documentation of the instrument of a leading manufacturer reveals that the approval for SIL use of a PST positioner is only valid for the ability to shut down the process. The diagnostic functions are not evaluated and consequently not approved. It is easy to understand this attitude, as it is very hard to approve the positioner software with all its functions. But, is it therefore possible to use the diagnostic information in a context for extending the safety review of a plant?

A different solution might be found in using a combination of a hard- and software packages like the positioner outlined in figure 81, as is provided by Samson AG. This package provides a positioner with process shutdown system functionality as well as a solenoid valve, Pepperl+Fuchs (P&F) switches, and alarm output.



Source: SA Instrumentation and Control, Enhanced Reliability for Final Elements

Figure 81. Positioner

A configuration of this positioner, wired to an HIMA safety PLC, was tested. The positioner did perform the PST when triggered manually or automatically by timer. The event of the PST was recorded internally, and diagnosis was performed. The diagnostic data allowed the monitoring of graduation of valve performance over time. Key to the configuration was the recording of the PST by the HIMA safety PLC by means of P&F switches through the path

- P&F switch
- Input channel HIMA safety PLC
- Logic on HIMA for event recording

The PS was recorded with a precise time stamp in a chain of approved devices. There could be no doubt that the event had taken place.

This configuration makes another interesting monitoring capability possible. The diagnostic package of the positioner contains a datalogger. This datalogger is a monitoring function, recording valve movement and input signal over time. It can be triggered by the solenoid valve inside the positioner. Therefore, during shutdown or spurious trips, the complete closing run of the valve can be recorded.

This makes the proof and recording of valve testing very efficient, as any valve equipped with this feature can automatically generate a protocol on valve performance during shutdown testing.

Not only closing of the valve can be approved; it is also possible to draw conclusions from parameters like dead time, closing time, closing speed, and others which might lead to early recognition of valve failures. Spurious trips can be documented and used as valve tests as well. These capabilities lead to a proposal for use of a positioner at an electrostatic discharge valve.

c. Explain the purpose and importance of maintenance history.

The following is taken from DOE-STD-1068-94.

The objective of a maintenance history program is to document SSC maintenance and performance data as a basis for improving facility reliability. This history should assist in ensuring that root causes of failures are determined and corrected, and used in future work planning. This may be accomplished by a thorough review and analysis of maintenance performed, diagnostic monitoring data, and industry experience reports.

This file should be an electronic system maintained centrally, with individual groups responsible for collecting data and populating the system, to be an effective method for maintenance history control.

The derived database should be readily accessible in a READ ONLY mode facility-wide.

13. I&C personnel must demonstrate a working level knowledge of surveillance and assessment techniques, reporting, and follow up actions for I&C systems and programmatic elements.

a. Describe the role of I&C personnel in performance oversight of government-owned, contractor-operated (GOCO), and government-owned, government-operated (GO-GO) facilities.

The following is taken from DOE O 226.1B.

Oversight processes implemented by applicable DOE line management organizations must do the following:

- Evaluate contractor and DOE programs and management systems, including site assurance systems, for effectiveness of performance (including compliance with requirements). Such evaluations must be based on the results of operational awareness activities; assessments of facilities, operations, and programs; and assessments of the contractor's assurance system. The level and/or mix (i.e., rigor or frequency in a particular area) of oversight may be tailored based on considerations of hazards, and the maturity and operational performance of the contractor's programs and management systems.
- Include written plans and schedules for planned assessments, focus areas for operational oversight, and reviews of the contractor's self-assessment of processes and systems. Address the role of the Central Technical Authorities and their support staff for core nuclear safety functions.
- Include DOE Headquarters line organizations' conduct of oversight processes that are focused primarily on their DOE Field Elements, including reviewing contractor activities to the extent necessary to evaluate the implementation and effectiveness of the Field Element's oversight of its contractors.
- Include an issues management process that is capable of categorizing findings based on risk and priority, ensuring relevant line management findings are effectively communicated to the contractors, and ensuring that problems are evaluated and corrected on a timely basis. The issues management process must ensure for issues categorized as high significance findings:
  a) A thorough analysis of the underlying causal factors is completed.
  b) Corrective actions that will address the cause(s) of the findings and prevent recurrence are identified and implemented.
  c) After completion of a corrective action or a set of corrective actions, the conduct of an effectiveness review using trained and qualified personnel that can verify the corrective action/corrective action plan has been effectively implemented to prevent recurrences.
  d) The analysis process and results described in a) and maintenance tracking to completion of plans and schedules for the corrective actions and effectiveness reviews described in b) and c) above are documented in a readily accessible system.
  e) When findings and/or corrective actions apply to more than one Secretarial Office, a lead office is appointed by mutual agreement between the affected SOs.

- Be tailored according to the effectiveness of contractor assurance systems, the hazards at the site/activity, and the degree of risk, giving additional emphasis to potentially high consequence activities.

DOE line management must establish and communicate performance expectations to contractors through formal contract mechanisms. Such expectations must be established on an annual basis, or as otherwise required or determined appropriate by the field element.

DOE line management must have effective processes for communicating oversight results and other issues in a timely manner up the line management chain, and to the contractor as appropriate, sufficient to allow senior managers to make informed decisions.

For activities and programs at Government-owned and Government-operated facilities and sites that are not under the cognizance of a DOE Field Element, DOE Headquarters program offices must establish and implement comparably effective oversight processes consistent with requirements for the contractor assurance system and DOE line management oversight processes.

b. Describe the assessment requirements and limitations associated with the interface of I&C personnel and contractor employees.

As assessment requirements and limitations associated with the interface of I&C personnel and contractor employees vary from site to site, the local qualifying official will evaluate the completion of this competency.

c. Describe how planning, observations, interviews, and document research are used during an assessment.

The following is taken from DOE G 414.1-1B.

Planning

Planning management assessments is an organization-specific effort that should be integrated with other assessment processes. No single method is appropriate for every situation. Either quantitative or qualitative assessment methods may be used as appropriate for the assessment scope. Managers are challenged to make the assessment a value-added process that will lead to improvement in organizational performance, safety, meeting customer expectations, and achieving mission goals in full compliance with regulatory and DOE requirements. It is important to remember that while management assessments have some commonalities with audits, they should focus on evaluating organizational performance and identifying barriers that hinder improved performance.

Observations

Observation (the viewing of actual work activities) is often considered the most effective technique for determining whether performance is in accordance with requirements. Assessors should understand the effect their presence has on the person being observed and convey an attitude that is helpful, constructive, positive, and unbiased. The primary goal during observation is to obtain the most complete picture possible of the performance, which should then be put into perspective relative to the overall program, system, or process.

Interviews

Interviews provide the means of verifying the results of observation, document review, inspection, and performance testing; allow the responsible person to explain and clarify those results; help to eliminate misunderstandings about program implementation; and provide a venue where apparent conflicts or recent changes can be discussed and organization and program expectations can be described.

Document Research

Document reviews provide the objective evidence to substantiate compliance with applicable requirements. A drawback is that the accuracy of the records cannot be ascertained by review alone. This technique should be combined with interviews, observation, inspection, and/or performance testing to complete the performance picture. Records and documents should be selected carefully to ensure that they adequately characterize the program, system, or process being assessed.

d. Explain the essential elements of a performance-based assessment, including investigation, fact-finding, and reporting.

The following information is taken from DOE G 414.1-1B.

Performance-based assessments focus first on the adequacy of the process that produced a product or service, and then on the product itself. If problems are found in the product or work processes, the assessor evaluates the methods and procedures used to implement the applicable requirements in an effort to find the failure that led to the problems. The assessor is expected to determine whether a non-compliance or series of non-compliances with procedures could result in a failure to satisfy top-level requirements. Results of prior compliance assessments may help the assessor in determining the focus areas for planning performance-based assessments.

Investigation and Fact-Finding

In performance-based assessments, great emphasis is placed on getting the full story on a problem before coming to a conclusion. If an assessor sees a problem with the execution of a welding process, the next step should determine the extent of the problem. Is it limited to one welder? Is it limited to one process? Can the problem be traced to the qualification program for the welder or to the qualification program for the welding process? Or is there a problem with the weld material itself, indicating a problem in an area such as engineering or procurement?

While the assessor should be familiar with requirements and procedures, in performance-based assessments, the assessor's experience and knowledge play an integral part in determining whether requirements are satisfied. Therefore, participants in performance-based assessments should be technically competent in the areas they are assessing. For example, if an assessor is evaluating a welding process, the assessor relies heavily on his or her knowledge of welding codes, welding processes, and metallurgy, rather than just verifying simple procedure compliance.

Performance-based assessments usually provide the most useful information to management; however, they require a much higher level of competence on the part of the assessment team.

Results of performance-based assessments may provide useful insight for management's pursuit of excellence.

Reporting

Assessment reports are required for documentation of assessment results. Assessment team leaders have the overall responsibility for preparing the report and obtaining appropriate approval for its release as applicable. The report may be formal (e.g., distributed by memorandum) or informal (e.g., letter to file or email), depending on the level of assessment performed, but should provide a clear picture of the results in terms of the programs, systems, and processes assessed. The assessment report should be clear, concise, accurate, and easy to understand, and should include only facts that directly relate to assessment observations and results. It should include sufficient information to enable the assessed organization to develop and implement appropriate improvement plans.

Specific report formats may vary considerably from one organization to the next. An independent assessment report usually includes the following sections:

- Executive summary
- Assessment scope
- Identification of team members
- Identification of personnel contacted
- Documents reviewed
- Work performance observed
- Assessment process and criteria (e.g., criteria review and assessment documents)
- Results of the assessment, including identification of areas for improvement, and/or strengths

A management assessment report may not require all of the listed sections and may only require an executive summary.

e. Describe the methods by which noncompliance is determined and communicated to the contractor and departmental management.

The following is taken from DOE G 414.1-1B.

Site/facility protocols should be followed for what to do if an imminent danger situation or a reportable noncompliance or violation is encountered during the course of an assessment. Any assessment schedules or specific protocols established during the pre-assessment meeting are used to ensure that the assessment is conducted effectively and safely. Assessors should keep their points of contact informed of their activities to preclude surprises during the post-assessment conference. This may include requests for additional assistance or the communication of concerns that require immediate action on the part of the assessed organization. Timely communication, oral and written, will allow the assessed organization to verify the accuracy of observations and provide relevant facts and background on the issues. One way to accomplish this is to meet periodically (daily or every other day) with the organization being assessed to convey questions/concerns and provide a status update.

Daily team meetings may be helpful in ensuring continuity and overall focus by providing assessment team leaders with information about the completion status of the assessment checklists, and offering the opportunity for inquiry into issues requiring additional action (e.g., clearances, access, requests for personnel or material, and impasse resolution). These meetings also provide the setting for advising other team members of issues that may be of interest in their assigned scope, or for integrating data gathered by the various assessors. The meetings should be brief so that they do not significantly reduce the team members' field time with the processes they are to assess and the people they are to interview.

It is important that sufficient information be gathered during the assessment to determine whether an activity meets the performance criteria established. The assessor should be able to clearly state the criterion impacted by the activity and whether identified findings impact the mission/goals of the organization. To accomplish this, the assessor may deviate from the assessment schedule to determine the extent and significance of an issue. Deviations that affect the assessor's ability to complete the assessment team's interview schedule should immediately be made known to the organization being assessed and the team leader.

Mandatory Performance Activities:

a. **Develop an assessment report.**

b. **Demonstrate the ability to communicate technical issues (both orally and by written report) when working or interacting with contractors, stakeholders, and other internal and external organizations.**

c. **Evaluate an I&C system to support review and approval of a new or revised facility documented safety analysis (DSA) and/or TSR. The scope of the review will be dictated by the changes associated with the I&C system (e.g., new I&C system design, modification of an existing design, addition of instrument loops to a PLC or DCS, set point modification, etc.).**

d. **Evaluate a safety function specified in a new or revised facility DSA and/or TSR for satisfactory identification and classification of I&C needed to fulfill and/or support that safety function. The scope of the review will be dictated by the change in the safety function (e.g. new facility, newly identified safety function, modification of a previously identified safety function, added performance criteria, etc.)**

KSAs a through d are performance-based KSAs. The Qualifying Official will evaluate their completion.

14. I&C personnel must demonstrate a working level knowledge of problem analysis principles, and the ability to apply techniques as necessary to identify problems, determine potential causes of problems, and identify potential corrective actions.

Mandatory Performance Activities:

a. Demonstrate the application of problem analysis techniques including the following:
- **Failure modes and effects analysis (FMEA)**
- **Fault tree analysis (FTA)**
- **Root cause analysis (RCA)**

This is a performance-based KSA. The Qualifying Official will evaluate its completion. The following information may be helpful.

Failure Modes and Effects Analysis

The following is taken from DRM Associates, *New Product Development Solutions*, "Failure Modes and Effects Analysis."

Failure modes and effects analysis (FMEA) is methodology for analyzing potential reliability problems early in the development cycle when it is easier to take actions to overcome these issues, thereby enhancing reliability through design. FMEA is used to identify potential failure modes, determine their effects on the operation of the product, and identify actions to mitigate the failures. A crucial step is anticipating what might go wrong with a product. While anticipating every failure mode is not possible, the development team should formulate as extensive a list of potential failure modes as possible.

The early and consistent use of FMEA in the design process allows the engineer to design out failures and produce reliable, safe, and customer pleasing products. FMEA also captures historical information for use in future product improvement.

FMEA provides the engineer with a tool that can supply reliable, safe, and customer pleasing products and processes. Since FMEA helps the engineer identify potential product or process failures, it can be used to do the following:
- Develop product or process requirements that minimize the likelihood of product or process failures.
- Evaluate the requirements obtained from the customer or other participants in the design process to ensure that those requirements do not introduce potential failures.
- Identify design characteristics that contribute to failures and design them out of the system or at least minimize the resulting effects.
- Develop methods and procedures to generate and test the product/process to ensure that the failures have been successfully eliminated.
- Track and manage potential risks in the design. Tracking the risks contributes to the development of corporate memory, and the success of future products.
- Ensure that any failures that could occur will not injure or seriously impact the customer of the product/process.

FMEA PROCEDURE

The process for conducting an FMEA is straightforward. The basic steps are outlined in the following:

- Describe the product/process and its function. It is important to clearly articulate an understanding of the product or process under consideration. This understanding simplifies the process of analysis by helping the engineer identify those product/process uses that fall within the intended function, and which ones fall outside. It is important to consider both intentional and unintentional uses since product failure often ends in litigation, which can be costly and time consuming.
- Create a block diagram of the product or process. This diagram shows major components or process steps as blocks connected together by lines that indicate how the components or steps are related. The diagram shows the logical relationships of components and establishes a structure around which the FMEA can be developed. Establish a coding system to identify system elements. The block diagram should always be included with the FMEA form.
- Complete the header on the FMEA form worksheet: product/system, subsys./assy., component, design lead, prepared by, date, revision (letter or number), and revision date. Modify these headings as needed.
- Use the example diagram as shown in figure 82 to begin listing items or functions. If items are components, list them in a logical manner under their subsystem/assembly based on the block diagram.
- Identify Failure Modes. A failure mode is defined as the manner in which a component, subsystem, system, process, etc. could potentially fail to meet the design intent. Examples of potential failure modes include
  - corrosion
  - hydrogen embrittlement
  - electrical short or open
  - torque fatigue
  - deformation
  - cracking
- A failure mode in one component can serve as the cause of a failure mode in another component. Each failure should be listed in technical terms. Failure modes should be listed for the function of each component or process step. At this point the failure mode should identify whether or not the failure is likely to occur. Looking at similar products or processes and the failures that have been documented for them is an excellent starting point.

System	LTN2001 GPS SSU	Potential Failure Mode and Effects Analysis (Design FMEA)	Revision	B
Subsystem	Receiver Card		Prepared By	Robert Crow
Part Number	468230-100		FMEA Date	8/18/1992
Design Lead	J. Davies		Revision Date	

Item / Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Design Controls	Det	RPN	Recommended Action(s)	Responsibility & Target Completion Date	Action Results: Actions Taken	New Sev	New Occ	New Det	New RPN
Circuit Block 4.1.1	Output loss from pre-amp	Receiver & output data loss; track loss; GPS shut-down	5	C1 short	1	PR-20 & HW-5	2	10	QA Proc 20-6	R. Jones, 11/30/92	Added to control plan	2	1	1	2
			5	C88 short	2		2	20	QA Proc 20-6	R. Jones, 11/30/92	Added to control plan	2	1	1	2
			5	L1 open/short	3		2	30	QA Proc 20-3	R. Jones, 11/30/92	Added to control plan	2	2	1	4
			5	U21 function	4		2	40	Test 147	R. Jones, 11/30/92	Added to control plan	2	3	1	6
								0							0
Circuit Block 4.1.2	Undetected & insignificant component failure mode	No noticeable system effect	1	C1open/chg val.	2	None	8	16	None						0
			1	C88open/chg val	2		8	16	None						0
								0							0
Circuit Block 4.2.1	Loss of signal from 2nd RF amplifier & 1st down converter	Loss of position, velocity & time output data; track loss; GPS shut-down	4	C2 short	1	PR-20 & HW-5	2	8	QA Proc 20-6	B. Howell 10/15/92	Added to control plan				0
			4	C3 short	1	PR-20 & HW-5	2	8	QA Proc 20-6	B. Howell 10/15/92	Added to control plan	2	1	1	2
			4	C4 open/short	2	PR-20 & HW-5	2	16	QA Proc 20-6	B. Howell 10/15/92	Added to control plan	2	1	1	2
			4	C5 short	2	PR-20 & HW-5	2	16	QA Proc 20-6	B. Howell 10/15/92	Added to control plan	2	1	1	2
			4	C66 open/short	2	PR-20 & HW-5	2	16	QA Proc 20-6	B. Howell 10/15/92	Added to control plan	2	1	1	2
			4	C99 short	3	PR-20 & HW-5	2	24	QA Proc 20-6	B. Howell 10/15/92	Added to control plan	2	2	1	4
			4	FL1 short/open	5	None	2	40	100% Insp.	B. Howell 10/15/92	Added to control plan	2	2	2	8
			4	FL2 short/open	5	None	2	40	100% Insp.	B. Howell 10/15/92	Added to control plan	2	2	2	8
			4	R2open/chg val	2		2	16	None						0
			4	R18 open/chg val	2		2	16	None						0

Source: DRM Associates, New Product Development Solutions, Failure Modes and Effects Analysis

Figure 82. FMEA form example

- Describe the effects of those failure modes. For each failure mode identified, the engineer should determine what the ultimate effect will be. A failure effect is defined as the result of a failure mode on the function of the product/process as perceived by the customer. It should be described in terms of what the customer might see or experience should the identified failure mode occur. Keep in mind the internal as well as the external customer. Examples of failure effects include
  - injury to the user
  - inoperability of the product or process
  - improper appearance of the product or process
  - odors
  - degraded performance
  - noise

  Establish a numerical ranking for the severity of the effect. A common industry standard scale uses 1 to represent no effect and 10 to indicate a very severe effect with failure affecting system operation and safety without warning. The intent of the ranking is to help the analyst determine whether a failure would be a minor nuisance or a catastrophic occurrence to the customer. This enables the engineer to prioritize the failures and address the big issues first.

- Identify the causes for each failure mode. A failure cause is defined as a design weakness that may result in a failure. The potential causes for each failure mode should be identified and documented. The causes should be listed in technical terms and not in terms of symptoms. Examples of potential causes include
  - improper torque applied
  - improper operating conditions
  - contamination
  - erroneous algorithms
  - improper alignment
  - excessive loading
  - excessive voltage
- Enter the probability factor. Each cause should be assigned a numerical weight that indicates how likely that cause is. A common industry standard scale uses 1 to represent not likely and 10 to indicate inevitable.
- Identify current controls. Current controls are the mechanisms that prevent the cause of the failure mode from occurring or which detect the failure before it reaches the customer. The engineer should now identify testing, analysis, monitoring, and other techniques that can or have been used on the same or similar products/processes to detect failures. Each of these controls should be assessed to determine how well it is expected to identify or detect failure modes. After a new product or process has been in use, previously undetected or unidentified failure modes may appear. The FMEA should then be updated and plans made to address those failures to eliminate them from the product/process.
- Determine the likelihood of detection. Detection is an assessment of the likelihood that the current controls will detect the cause of the failure mode or the failure mode itself, thus preventing it from reaching the customer. Based on the current controls, consider the likelihood of detection.
- Review risk priority numbers (RPN). The risk priority number is a mathematical product of the numerical severity, probability, and detection ratings.

  $$RPN = (Severity) \times (Probability) \times (Detection)$$

  The RPN is used to prioritize items than require additional quality planning or action.
- Determine recommended action(s) to address potential failures that have a high RPN. These actions could include specific inspection, testing, or quality procedures; selection of different components or materials; de-rating; limiting environmental stresses or operating range; redesign of the item to avoid the failure mode; monitoring mechanisms; performing preventative maintenance; and inclusion of back-up systems or redundancy.
- Assign responsibility and a target completion date for these actions. This makes responsibility clear-cut and facilitates tracking.
- Indicate actions taken. After these actions have been taken, re-assess the severity, probability, and detection and review the revised RPNs. Are any further actions required?
- Update the FMEA as the design or process changes, the assessment changes, or new information becomes known.

Video 29. Failure modes and effects analysis

http://www.bing.com/videos/search?q=Failure+Modes+and+Effects+Analysis&view=detail&mid=36C7ECDD3C5B9F470A1636C7ECDD3C5B9F470A16&first=0

Fault Tree Analysis

The following is taken from Wikipedia, *Fault Tree Analysis*.

Many different approaches can be used to model an FTA, but the most common and popular way can be summarized in a few steps. A single fault tree is used to analyze one and only one undesired event or top event, which may be subsequently fed into another fault tree as a basic event. Though the nature of the undesired event may vary dramatically, an FTA follows the same procedure for any undesired event; be it a delay of 0.25 msec for the generation of electrical power, an undetected cargo bay fire, or the random, unintended launch of an ICBM. Due to labor cost, FTA is normally only performed for more serious undesired events.

FTA analysis involves five steps:

1. Define the undesired event to study. Definition of the undesired event can be very hard to catch, although some of the events are very easy and obvious to observe. An engineer with a wide knowledge of the design of the system or a system analyst with an engineering background is the best person to help define and number the undesired events. Undesired events are used then to make the FTA, one event for one FTA; no two events will be used to make one FTA.
2. Obtain an understanding of the system. Once the undesired event is selected, all causes with probabilities of affecting the undesired event of 0 or more are studied and analyzed. Getting exact numbers for the probabilities leading to the event is usually impossible because it may be very costly and time consuming to do so. Computer software is used to study probabilities; this may lead to less costly system analysis. System analysts can help with understanding the overall system. System designers have full knowledge of the system and this knowledge is very important for not missing any cause affecting the undesired event. For the selected event, all causes are then numbered and sequenced in the order of occurrence and then are used for the next step which is drawing or constructing the fault tree.
3. Construct the fault tree. After selecting the undesired event and having analyzed the system so that we know all the causes (and if possible their probabilities) we can now construct the fault tree. Fault tree is based on AND and OR gates which define the major characteristics of the fault tree.
4. Evaluate the fault tree. After the fault tree has been assembled for a specific undesired event, it is evaluated and analyzed for any possible improvement; or in other words, the risk management is studied and ways to improve the system are found. This step is as an introduction to the final step which will be to control the hazards identified. In short, in this step all possible hazards affecting the system in a direct or indirect way are identified.
5. Control the hazards identified. This step is very specific and differs largely from one system to another, but the main point will always be that after identifying the hazards, all possible methods are pursued to decrease the probability of occurrence.

Root Cause Analysis

The following is taken from Envision Software, *Root Cause Analysis*.

Root cause analysis (RCA) is a management process that seeks to locate the ultimate cause or causes behind performance or process-related problems in a business or engineering environment, and then proceeds to resolve the problem by treating these underlying causes.

The advantage of RCA as a failure-management method over troubleshooting, for example, is that the latter is a knee-jerk reaction to the occurrence of some critical problem or failure. Some fire-fighting is carried out in order to handle and recover immediately. Since this expeditious approach deals with patching up symptoms quickly, the problem seems temporarily solved. Over time, the problem is likely to recur, resulting in a similar knee-jerk troubleshooting process, racking up huge costs along the way.

The benefit of RCA is deeper investigation into the reason for the occurrence in the first place. The root cause or causes might be much deeper than outward symptoms reveal, and several layers may have to be pushed aside to reach the root cause. So, the focus is on analyzing this fabled root cause that propagated forward and manifested in the form of the problem at hand, rather than on exclusively treating the symptoms, as troubleshooting does.

Having identified the root cause, proceed to treat the cause(s) within the organizational perspective, thereby eliminating or reducing the anomalous impact such as maintenance cost. The critical importance of RCA is prevention of recurring failures.

Summarized, the goals of RCRA are

- failure identification—determining what exactly went wrong
- failure analysis—discovering the root cause, why it happened
- Failure resolution—providing a solution that prevents recurrence

While training to perform RCA, the analyst should learn to identify the following causes during their investigations:

- *Causal factor*. This is a condition or an event that made some effect take place, or may have shaped or influenced the outcome in some way. For example, a leaking overhead oil pipe on the factory floor is a causal factor that may lead to fire in that area.
- *Direct cause*. This is the cause that resulted in the occurrence. For instance, in the case of the overhead pipe which oozed oil on the factory floor, the actual leakage is the direct cause.
- *Contributing cause*. This is a cause that indirectly affected the outcome or occurrence. On its own, the cause might not have the sufficient power to result in the event taking place. In the example of the overhead pipe leakage, selection of a supplier—who supplies low-quality pipes—by the purchase manager is a contributing cause.
- *Causal factor chain*. This is simply a chain of events, one leading to another. Some specific action creates some condition that results in an event. This event on its own creates yet another set of conditions, which lead to another event, and the chain of cause and effect continues. In this sequence or chain, the earlier events or conditions

are known as upstream factors. The fishbone chart is often utilized to assist in this process.
- *Root cause*. This is finally the cause that, if corrected, would prevent the occurrence of the particular event or phenomenon. It is the most fundamental aspect of the causal chain that can be logically identified.

Root cause analysis training teaches students to phase the analysis process into the following, which closely matches the goals identified above:
- Collection of data—Phase I
- Event Investigation—Phase II
- Resolution of occurrence—Phase III

Root cause analysis phase I, data collection, should ideally begin as soon as possible after the occurrence of the event or phenomenon. This ensures that no data is lost. If possible, data may be collected even while the event or phenomenon progresses. All information pertaining to the occurrence should get noted — including conditions before, during, and after the occurrence; what current actions were taken by the personnel involved; environmental factors, if any; and so on.

While collecting data, it is critical to investigate what actually happened, rather than focusing on what could have happened. To this end, data collection should be a fact-finding investigation, and not a fault-finding mission. Objectivity, as opposed to subjectivity, is critical.

Data collection techniques include interviewing personnel most familiar with and directly or indirectly involved in the incident. The first contact with them may be restricted to hearing their perspective on the failure. Records pertaining to the incident are another excellent source for data collection. These may include correspondence between the key players, minutes of meetings, operation logs, maintenance records, equipment history records, and the like. As is obvious from this list, data collection methods may be as varied as the scenarios where the analysis is being performed.

Root cause analysis phase II, event/phenomenon investigation, involves an objective evaluation of the data collected, in order to identify any causal factor chain that may have led to the occurrence of the failure. Usually, one or several of the following categories of causes are involved:
- *Failures related to malfunctioned equipment or material*. This could also be due to non-availability of such equipment or sub-standard material.
- *Failures related to procedural issues*. Either the procedures have been short-circuited by personnel, or new circumstances have made established procedures inadequate or obtrusive.
- *Failures caused by personnel*. This could be from improper training, or distraction caused by environmental factors while operating equipment and such.
- *Failures related to equipment design*. Perhaps some ergonomic factor was overlooked when designing the equipment or one component failed to align with the rest of the equipment.

- *Failures related to management policies*. Perhaps management shortsightedness is one of the root causes.
- *Failures related to external phenomena*. Perhaps some external or uncharacteristic events caused an unforeseen occurrence.

ROOT CAUSE ANALYSIS METHODS

There are a number of methods available at this stage of analysis. The ultimate RCA training would provide in-depth knowledge and awareness of all root cause analysis methods. This rounded training is critical, so that determination of the root of the failure is quite thorough, leading to the right conclusions being reached. A few popular methods are discussed as follows:

- The Events and cause and effect analysis method is used when the data collected in the investigation phase points to a long chain of causal factors, or when the failure at hand apparently has several dimensions.
- The change analysis method is a simple process of six steps, and is especially useful for evaluation of failure of equipment. The method, due to its superficial nature, may not be able to identify all the root causes of the occurrence, and can at best be used as a supplement to a larger investigation activity.
- The barrier analysis method provides a systematic approach to identifying failures of equipment and/or any procedural or administrative failures. It is quite powerful in the hands of someone who is familiar with the details of the processes involved.
- The MORT (Management Oversight and Risk Tree) method can be deployed when there are few experts who know the right kind of questions to ask, and the failure is a recurring one, with no let up. Visually oriented, this method involves drawing a tree with the left side listing all factors that are relevant to the occurrence, and the right side listing deficiencies in management that led those factors to come into existence. For each factor, a set of questions is included that need to be addressed. This method helps prevent omissions, and ensures that all causal factors that have the potential to be part of the chain leading to the occurrence are considered.
- The human performance evaluation (HPE) method comes into play when the data collection phase clearly points to the role of personnel as a contributory node in the causal chain within a system. Thus, its focus is on man-machine interface studies, and on system operability and work environment. Psychological insight on the part of the analyst, along with training in ergonomics, is required to carry out HPE effectively.
- The Kepner-Tregoe method is a highly-structured method that looks into all the aspects of the occurrence. This method provides a systematic framework for gathering, organizing, and evaluating data. A formal training in K-T method may be required in order to be able to adopt this approach.

Root Cause Analysis Phase III, Occurrence Resolution, is a realistic assessment of the viability of the corrective action that the previous phase has revealed, followed by application of said corrective action. The phenomenon must then be monitored periodically to verify resolution and effective recurrence prevention.

b. Using event and/or occurrence data, apply problem analysis techniques and demonstrate the ability to identify problems and how they could be resolved.

This is a performance-based KSA. The Qualifying Official will evaluate its completion.

15. I&C personnel must demonstrate a working level knowledge of process and instrumentation diagrams (P&IDs), logic diagrams, electrical schematics, loop diagrams for I&C systems, construction drawings, as-built drawings, and wiring diagrams.

a. Discuss the origin and purpose of "as-built" drawings.

The following is taken from Answers, *What is an As-Built Drawing*?

The phrase "as-built" in construction is equivalent to "as-is." Drawings deemed "as-built" are drawings that show the existing conditions as they are, or "as-is." These are the actual existing conditions as opposed to designs or proposed conditions, which are more common for the content of drawings.

As-built drawings can be documented either after or during construction. When it is after construction, a qualified technician collects accurate data to reconstruct the drawings. When it is during construction, the design drawings are red marked for editing.

For example, if a contractor is installing sewer pipe in the road at a buried depth of 5 feet and suddenly encounters an abandoned pipe and must change the buried depth to 6.50 feet, then the contractor should be responsible for the as-built conditions. The installing contractor should red mark the set of drawings to show how the sewer line was actually installed so that a draftsman can later edit the drawings into an "as-built" set.

<u>Mandatory Performance Activities:</u>

a. Using P&IDs, identify I&C devices by symbology and explain their functions.

b. Using logic diagrams, loop diagrams, and electrical schematics describe the effect of an action taken.

c. Using construction drawings, identify instrument sensing lines, instrument valve manifold and instrument mounting details, and verify compliance with instrument installation requirements.

d. Walk down a facility to demonstrate the ability to verify that installation conforms to P&IDs and other relevant documentation.

KSAs a through d are performance-based KSAs. The Qualifying Official will evaluate their completion.

16. I&C personnel must demonstrate a working level knowledge of DOE and industry codes and standards and their applicability as they relate to I&C systems design, procurement, installation, testing, operations, and maintenance. I&C personnel must also demonstrate the ability to evaluate compliance with applicable DOE and industry codes and standards. If listed documents have been superseded or replaced, the latest version should be used.

a. Discuss the purpose and content of the Documented Safety Analysis (DSA).

The following is taken from DOE G 421.1-2A.

Purpose and Content

The DSA for a DOE hazard category 1, 2, or 3 nuclear facility in accordance with 10 CFR 830.204, "Documented Safety Analysis," must, as appropriate for the complexities and hazards associated with the facility or activity, describe the facility, activities, and operations; provide a systematic identification of both natural and manmade hazards associated with the facility; evaluate normal, abnormal, and accident conditions, including consideration of natural and manmade external events, identification of energy sources or processes that might contribute to the generation or uncontrolled release of radioactive and other hazardous materials, and consideration of the need for analysis of accidents that may be beyond the design basis of the facility; derive the hazard controls necessary to ensure adequate protection of workers, the public, and the environment; demonstrate the adequacy of these controls to eliminate, limit, or mitigate identified hazards, and define the process for maintaining them current at all times and controlling their use; define the characteristics of the safety management programs necessary to ensure the safe operation of the facility, including quality assurance, procedures, maintenance, personnel training, conduct of operations, emergency preparedness, fire protection, waste management, and radiation protection; and with respect to a nonreactor nuclear facility with fissionable material in a form and amount sufficient to pose a potential for criticality, define a criticality safety program that

- ensures that operations with fissionable material remain subcritical under all normal and credible abnormal conditions;
- identifies applicable nuclear criticality safety standards; and
- describes how the program meets applicable nuclear criticality safety standards.

b. Discuss the purpose and content of Technical Safety Requirements (TSR).

The following is taken from DOE G 423.1-1A.

Purpose

10 CFR 830.205 requires DOE contractors responsible for hazard category 1, 2, and 3 DOE nuclear facilities to develop TSRs. These TSRs identify the limitations to each DOE-owned, contractor-operated nuclear facility based on the DSA and any additional safety requirements established for the facility.

Content

There are three types of limits identified by 10 CFR 830: SLs, LCSs, and LCOs. The intent of these limits is to ensure that the operating regime is restricted to the bounds of safe operation as defined by the safety analyses.

SPECIFICATION OF SAFETY LIMITS

SLs are limits on important process variables needed for the facility function that, if exceeded, could directly cause the failure of one or more of the passive barriers that prevent the uncontrolled release of radioactive materials, with the potential of consequences to the public above specified evaluation guidelines.

SPECIFICATION OF LIMITING CONTROL SETTINGS

LCSs define the settings on safety systems that control process variables to prevent exceeding an SL. LCSs for reactors should include reactor trip system instrumentation set points. The reactor trip set-point limits are the nominal values at which the reactor trips are set and should be selected to provide sufficient allowances between the trip set point and the SL. This allowance will ensure the core and the reactor coolant system are prevented from exceeding SLs during normal operation and anticipated operational occurrences.

SPECIFICATION OF LIMITING CONDITIONS FOR OPERATION

LCOs define the limits that represent the lowest functional capability or performance level of safety SSCs required to perform an activity safely. LCOs should include the initial conditions for those design basis accidents or transient analyses that involve the assumed failure of, or present a challenge to, the integrity of the primary radioactive material barrier. Identification of these variables should come from a search of each transient and accident analysis documented in the DSA. The LCO should be established at a level that will ensure the process variable is not less conservative during actual operation than was assumed in the safety analyses.

LCOs should also include those SSCs that are part of the primary success path of a safety sequence analysis, and those support and actuation systems necessary for them to function successfully. Support equipment for these SSCs would normally be considered to be part of the LCO if relied on to support the SSCs function.

c. Discuss the purpose and content of 10 CFR Part 830, "Nuclear Safety Management."

The following is taken from the Federal Register, 1810.

Purpose

The safety basis requirements of 10 CFR 830 require the contractor responsible for a DOE nuclear facility to analyze the facility, the work to be performed, and the associated hazards, and to identify the conditions, safe boundaries, and hazard controls necessary to protect workers, the public, and the environment from adverse consequences.

These analyses and hazard controls constitute the safety basis upon which the contractor and DOE rely to conclude that the facility can be operated safely. Performing work consistent

with the safety basis provides reasonable assurance of adequate protection of workers, the public, and the environment.

The safety basis requirements are intended to further the objective of making safety an integral part of how work is performed throughout the DOE complex. Developing a thorough understanding of a nuclear facility, the work to be performed, the associated hazards, and the needed hazard controls is essential to integrating safety into management and work at all levels.

Performing work in accordance with the safety basis for a nuclear facility is the realization of that objective.

Content

The following is taken from10 CFR 830.

Subpart A of 10 CFR 830 establishes quality assurance requirements for contractors conducting activities, including providing items or services that affect, or may affect, nuclear safety of DOE nuclear facilities.

Subpart B of 10 CFR 830 establishes safety basis requirements for hazard category 1, 2, and 3 DOE nuclear facilities. Subpart B includes requirements related to the safety basis, DSAs, preliminary DSAs, TSRs, and USQs.

d. Discuss the purpose and content of DOE O 414.1D, *Quality Assurance*, 05-18-13.

The following is taken from DOE O 414.1D.

Purpose

The purpose of DOE O 414.1D is

- to ensure that DOE products and services meet or exceed customers' requirements and expectations;
- to achieve quality for all work based on the following principles:
  - all work, as defined in DOE O 414.1D, is conducted through an integrated and effective management system;
  - management support for planning, organization, resources, direction, and control is essential to QA;
  - performance and quality improvement require thorough, rigorous assessments and effective corrective actions;
  - all personnel are responsible for achieving and maintaining quality;
  - risks and adverse mission impacts associated with work processes are minimized while maximizing reliability and performance of work products; and
  - establish additional process-specific quality requirements to be implemented under a QA program for the control of suspect/counterfeit items, and nuclear safety software.

Content

DOE O 414.1D includes requirements for the following:

- Quality assurance program development and implementation

- Quality assurance program approval and changes
- Federal technical capability and qualifications

e. Discuss the purpose and content of DOE G 414.1-4, *Safety Software Guide for use with 10 C.F.R 830 Subpart A, Quality Assurance Requirements*, and DOE O 414.1D, admin chg 1, *Quality Assurance*, 05-18-13.

The following is taken from DOE G 414.1-4.

Purpose

DOE G 414.1-4 provides information plus acceptable methods for implementing the safety SQA requirements of DOE O 414.1D. Requirements of DOE O 414.1D supplement the QA program requirements of 10 CFR 830 for DOE nuclear facilities and activities. The safety SQA requirements for DOE and its contractors are necessary to implement effective QA processes and achieve safe nuclear facility operations.

DOE promulgated the safety software requirements and DOE G 414.1-4 to control or eliminate the hazards and associated postulated accidents posed by nuclear operations, including radiological operations. Safety software failures or unintended output can lead to unexpected system or equipment failures and undue risks to the DOE/NNSA mission, the environment, the public, and the workers. Thus DOE G 414.1-4 has been developed to provide guidance for establishing and implementing effective QA processes tied specifically to nuclear facility safety software applications. DOE also has guidance for the overarching QA program, which includes safety software within its scope. DOE G 414.1-4 includes software application practices covered by appropriate national and international consensus standards and various processes currently in use at DOE facilities. DOE G 414.1-4 is also considered to be of sufficient rigor and depth to ensure acceptable reliability of safety software at DOE nuclear facilities.

DOE G 414.1-4 should be used by organizations to help determine and support the steps necessary to address possible design or functional implementation deficiencies that might exist and to reduce operational hazards-related risks to an acceptable level. Attributes such as the facility life-cycle stage and the hazardous nature of each facility's operations should be considered when using DOE G 414.1-4.

Another objective of DOE G 414.1-4 is to encourage robust software quality methods to enable the development of high quality safety applications.

Content

DOE G 414.1-4 includes requirements and guidance related to the following:

- Safety software types and grading
- System quality and safety software
- Guidance for software safety design methods and software work activities
- Guidance for assessment and oversight

f. Discuss the purpose and content of DOE O 420.1C, *Facility Safety*, 12-04-2012.

The following is taken from DOE O 420.1B, Chg 1.

Purpose

The purpose of DOE O 420.1B, Chg. 1 is to establish facility and programmatic safety requirements for DOE for

- nuclear and explosives safety design criteria
- fire protection
- criticality safety
- natural phenomena hazards (NPH) mitigation
- the system engineer program

Content

Each chapter of DOE O 420.1B defines specific facility or programmatic safety requirements.

g. Discuss the purpose and content of DOE G 420.1-1A, *Nonreactor Nuclear Safety Design Criteria for Use with DOE O 420.1C, Facility Safety*, 12-04-2012.

The following is taken from DOE G 420.1-1A.

Purpose

DOE G 420.1-1 provides an acceptable approach for satisfying the requirements of DOE O 420.1B. The objective of DOE G 420.1-1 is to provide a methodology for selecting industry codes and standards for nuclear safety aspects of nonreactor nuclear facility design. DOE G 420.1-1 stresses that safety design should be driven by safety analysis, and provides interpretive guidance on the performance-level requirements of DOE O 420.1B. A successful safety design depends on the quality of the safety analysis and on engineering judgment in the transformation of this guidance to the final design.

Content

DOE G 420.1-1 provides guidance related to the following:

- Safety analysis and design process
- Elements of design for nuclear safety
- Functional design criteria
- Design criteria for SSCs

h. Discuss the purpose and content of DOE O 433.1B, admin chg 1, *Maintenance Management Program for DOE Nuclear Facilities*, 4-21-2010.

The following is taken from DOE O 433.1B.

Purpose

The purpose of DOE O 433.1B is to define the safety management program required by 10 CFR 830.204 for maintenance and the reliable performance of SSCs that are part of the safety basis required by 10 CFR 830.202, “Safety Basis,” at hazard category 1, 2, and 3 DOE nuclear facilities.

Content

DOE O 433.1B includes the following requirements related to maintenance management:

- All hazard category 1, 2, or 3 nuclear facilities, as defined in DOE STD-1027-92, must conduct all maintenance of SSCs that are part of the safety basis in compliance with an approved NMMP.
- NMMPs for GOCO facilities must demonstrate compliance with the requirements contained in the CRD of DOE O 433.1B and must be approved by the respective field office manager; approval consists of reviewing NMMP-DD and evaluating its compliance. NMMPs for GOGO facilities must demonstrate compliance with the requirements contained in DOE O 433.1B and must be approved by the respective SO or designee; approval consists of reviewing NMMP-DD and evaluating its compliance. Approval of NMMP-DD is required prior to startup of new hazard category 1, 2, and 3 nuclear facilities and at least every three years for all hazard category 1, 2, and 3 nuclear facilities.
- Changes to NMMPs must be reviewed under the USQ process to ensure that SSCs are maintained and operated within the approved safety basis, as required by 10 CFR 830. Changes that would result in USQ must be approved prior to the change taking effect.
- Assessments of NMMP implementation must be conducted, at least every three years, or less frequently if directed by the SO, in accordance with DOE O 226.1A, to evaluate whether all CRD requirements are appropriately implemented.
- Periodic self assessments in accordance with DOE O 226.1B must be conducted to evaluate the effectiveness of oversight of NMMPs.
- A single maintenance program may be used to address the requirements of this Order and the requirements of DOE O 430.1B.
- Full implementation of the requirements in DOE O 433.1B must be accomplished within 1 year of its issuance, unless a different implementation schedule is approved by the SO with concurrence of the central technical authorities.

i. Discuss the purpose and content of DOE G 433.1-1A, *Nuclear Facility Maintenance Management Program Guide for use with DOE O 433.1B*, 9-12-11.

The following is taken from DOE G 433.1-1A.

Purpose

DOE G 43.1-1A has been prepared to assist maintenance managers in understanding and meeting the requirements of DOE O 433.1B. DOE G 433.1-1A also helps DOE employees in the approval and oversight of DOE NMMPs. It is especially useful for review and approval authorities as a benchmark for determining if alternate methods used are justified and demonstrate compliance with DOE O 433.1B requirements.

DOE O 433.1B requires DOE facility operators to develop and implement an NMMP for hazard category 1, 2, and 3 nuclear facilities under DOE cognizance. An acceptable NMMP consists of processes to ensure that SSCs are capable of fulfilling their intended function as identified in the facility safety basis. DOE G 433.1-1A provides guidance for implementing program NMMP elements in a manner that would be acceptable to DOE for meeting the requirements of DOE O 433.1B.

DOE G 433.1-1A may also be used for development of the maintenance program required in DOE O 430.1B, *Real Property Asset Management*, for facilities not covered by DOE O 433.1B. The requirements of DOE O 430.1B also apply to nuclear facilities. The NMMP may serve as the single program to satisfy the requirements of both Orders. The NMMP-DD can be used to document the implementation of maintenance requirements in DOE O 430.1B and the implementation of maintenance for SSCs that are not part of the safety basis of a nuclear facility.

DOE O 433.1B requires DOE and contractor personnel to perform assessments. Guidance is provided for the various types of assessments and associated scopes. DOE G 433.1-1A may also be used for contractor assurance systems. The approved NMMP-DD provides a description of the locally implemented maintenance program and should be the basis for assessing program execution.

Content

DOE G 433.1-1A provides acceptable, but not mandatory methods for meeting requirements.

DOE G 433.1-1A is divided into two sections to provide guidance on general requirements and maintenance program elements of DOE O 433.1B. These sections are followed by three appendices.

Section II of DOE G 433.1-1A covers the general requirements and includes guidance for the application of the graded approach. General requirements are covered in section I.

Section III provides guidance on each of the 17 maintenance program elements that are identified as specific requirements in DOE O 433.1B. The topics are organized and numbered following the same structure outlined in DOE O 433.1B:

1. Integration with regulations and DOE Orders and manuals
2. Maintenance organization and administration
3. Master equipment list
4. Planning, scheduling, and coordination of maintenance
5. Types of maintenance
6. Maintenance procedures
7. Training and qualification
8. Configuration management
9. Procurement
10. Maintenance tool and equipment control
11. Suspect and counterfeit items
12. Maintenance history
13. Aging degradation and technical obsolescence
14. Seasonal facility preservation
15. Performance measures
16. Facility condition inspection
17. Post maintenance testing

Each sub-section for the 17 maintenance program elements includes the following:

- *Order implementation guidance*. A statement of DOE O 433.1B requirements followed by guidance for the items that the NMMP should address.

- *Additional background/guidance supporting implementation and procedure development*. More detailed guidance useful in supporting development of the NMMP.

Some sections also include example forms and checklists.

j. Discuss the purpose and content of DOE-STD-1073-2003, *Configuration Management Program.*

The following is taken from DOE-STD-1073-2003.

Purpose

The purpose of DOE-STD-1073-2003 is to define the objectives of a configuration management process for DOE nuclear facilities, and to provide detailed examples and supplementary guidance on methods of achieving those objectives. Configuration management is a disciplined process that involves management and technical direction to establish and document the design requirements and the physical configuration of nuclear facilities and to ensure that they remain consistent with each other and the documentation.

The size, complexity, and missions of DOE nuclear facilities vary widely, and configuration management processes may need to be structured to individual facilities, activities, and operations. It would generally be inappropriate to apply the same configuration management standards to widely different activities; for example, a reactor facility and a small, simple laboratory. The detailed examples and methodologies in DOE-STD-1073-2003 are provided to aid those developing their configuration management processes; however, they are provided for guidance only and may not be appropriate for application to all DOE nuclear activities. The individuals defining the configuration management process for a particular nuclear activity will need to apply judgment to determine if the examples and methods presented in DOE-STD-1073-2003 are appropriate for the activity.

Content

Chapters 3 through 7 in DOE-STD-1073-2003 address each of the key elements of configuration management and provide additional details on how they can be implemented.

The contractor must have a formal policy that endorses the use of configuration management and defines key roles and responsibilities. The contractor must also ensure that sufficient resources are provided to adequately implement the configuration management process. The contractor should establish and document the configuration management requirements at the earliest practical time prior to facility operation or initiation of the activity. Configuration must be controlled for the life of the facility or the duration of the activity. Prior to the end of life of the facility or activity, the contractor, in coordination with DOE, must determine if configuration management should be applied to post-operation activities, such as decontamination and deactivation. If there is a contractor change at the end of operation, the operating contractor should work with the post-operation contractor to determine how the configuration management effort should be relayed to the new contractor.

The contractor must formally document and implement the configuration management process to be used for the activity in a configuration management plan. The configuration management plan must address

- how each of the key elements of configuration management will be implemented (See chapters 3 through 7);
- what SSCs will be included in the configuration management process and what is the basis/justification for the selection (See CM SSCs in Chapter 3);
- what configuration management training will be provided;
- who will be assigned key responsibility and authority for configuration management;
- how interfaces will be controlled (for control of interfaces for documentation, see Section 6.5); and
- what programs and procedures must incorporate configuration management.

k. Discuss the purpose and content of DOE-STD-1189-2008, *Integration of Safety into the Design Process.*

The following is taken from DOE-STD-1189-2008.

Purpose

A fundamental element that is necessary to achieve the DOE goal for capital asset acquisition is the integration of safety throughout the DOE acquisition management system. DOE-STD-1189-2008 supports the DOE objective by providing guidance on those actions and processes important for integrating safety into the acquisition process for DOE hazard category 1, 2, and 3 nuclear facilities. Integrating safety into design is more than just developing safety documents that are accepted by the design function and organization: it requires that safety be understood by, and integrated into, all functions and processes of the project. Therefore, DOE-STD-1189-2008 identifies interfaces, methodologies, and documentation strategies that might support proper integration. In addition, DOE-STD-1189-2008 provides format and content guidance for the development of safety documentation required by DOE O 413.3B, *Program and Project Management for the Acquisition of Capital Assets*, and 10 CFR 830.

Content

Some of the key concepts that are included in DOE-STD-1189-2008 are the following:

- The importance of the integrated project teams, Federal and contractor, including a contractor safety design integration team (SDIT), and effective coordination among these teams. The SDIT comprises safety and design subject matter experts and is the heart of the safety and design integration effort.
- The development of a safety design strategy (SDS) that provides a roadmap for how important safety issues will be addressed in the design, tailoring, and development of key safety documentation. The SDS should be initiated based on a statement of DOE expectations for safety-in-design developed during the pre-conceptual stage, and should be submitted during the conceptual design stage and updated and refined through the design process.
- The development, in the conceptual design stage, of facility-level design basis accidents that provide the necessary input to the identification and classification of important safety functions. These classifications provide design expectations for SSCs.

- The development of objective radiological criteria for safety and design classification of SSCs. These criteria relate to public and collocated worker-safety design considerations.
- The identification and application of nuclear safety design criteria as provided by DOE O 420.1B and its associated guides.
- The development of guidance for the preparation of a conceptual safety design report, a preliminary safety design report, and the preliminary DSA. These reports are required by DOE O 413.3B, for hazard category 1, 2, and 3 nuclear facilities, and they must be approved by DOE as part of the project approvals to proceed to the next design or construction phase. The intent of these reports and their approval is to ensure that the directions and decisions made regarding project safety are explicitly identified and dealt with in early stages of design. The objective is to reduce the likelihood of costly late reversals of design decisions involving safety.

I. Discuss the purpose and content of DOE-STD-1195-2011, *Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities.*

The following is taken from DOE-STD-1195-2011.

Purpose

DOE-STD-1195-2011 provides requirements and guidance for the design, procurement, installation, testing, maintenance, operation, and quality assurance of SISs that may be used at DOE nonreactor nuclear facilities for SS functions.

The focus of DOE-STD-1195-2011 is on how the process industry standard, ANSI/ISA 84.00.01-2004, can be used to support design of reliable SS SISs.

Content

DOE-STD-1195-2011 provides requirements for SISs, with section 2.1 providing general requirements and identifying two industry standards options for SIS design, and sections 2.2 through 2.9 identifying detailed requirements.

Appendices A through I provide the following guidance or requirements related to ANSI/ISA 84.00.01-2004 implementation.

- Appendix A provides a general overview of ANSI/ISA 84.00.01-2004.
- Appendix B provides requirements of the approved method for the determination of SILs.
- Appendix C provides guidance on SIL verification.
- Appendix D provides an example of SIL determination and verification.
- Appendix E provides guidance for obtaining failure rate data.
- Appendix F provides guidance related to quality assurance for safety software used in SISs.
- Appendix G provides guidance on human factors engineering.
- Appendices H and I provide references, abbreviations, acronyms, and definitions.

m. Discuss the purpose and content of DOE-STD-3024-2011, *Content of System Design Descriptions.*

The following is taken from DOE-STD-3024-2011.

Purpose

DOE-STD-3024-2011 provides criteria and guidance for the technical content and organizational structure of SDDs at DOE facilities.

Content

The main body of DOE-STD-3024-2011 describes the objective of SDDs and provides higher level criteria and guidance for SDD development (section 4 and 5).

Appendices A through C provide the following general supporting and background information:

- Appendix A—"Glossary"
- Appendix B—"Abbreviations and Acronyms"
- Appendix C—"Developmental Resources"
- Appendix D—"Format of SDDs"
- Appendix E—"Technical Content Criteria and Guidance"
- Appendix F—"Compiling Technical Information for the Development of SDDs"
- Appendix G—"Application of the Graded Approach to the Development of SDDs"
- Appendix H—"Preparation of Facility Design Descriptions"

n. Discuss the purpose and content of ISA-18.1-1979 (R2004), *Annunciator Sequences and Specifications.*

The following is taken from ISA-18.1-1979.

Purpose

The purpose of ISA-18.1-1979 is to establish uniform annunciator terminology, sequence designations, and sequence presentation, and to assist in the preparation of annunciator specifications and documentation.

ISA-18.1-1979 is intended to improve communications among those that specify, distribute, manufacture, or use annunciators.

Content

The content covers electrical annunciators that call attention to abnormal process conditions by the use of individual illuminated visual displays and audible devices. Sequence designations provided can be used to describe basic annunciator sequences and also many sequence variations.

o. Discuss the purpose and content of ANSI/ISA-18.2-2009 (R2004), *Management of Alarm Systems for the Process Industries.*

The following is taken from ISA-18.2-2009.

Purpose

ANSI/ISA-18.2-2009 addresses the development, design, installation, and management of alarm systems in the process industries. Alarm system management includes multiple work processes throughout the alarm system lifecycle. ANSI/ISA 18.2-2009 defines the terminology and models to develop an alarm system, and it defines the work processes recommended to effectively maintain the alarm system throughout the lifecycle.

Content

ANSI/ISA-18.2-2009 was written as an extension of existing ISA standards with due consideration of other guidance documents that have been developed throughout industry. Ineffective alarm systems have often been cited as contributing factors in the investigation reports following major process incidents. ANSI/ISA-18.2-2009 is intended to provide a methodology that will result in the improved safety of the process industries.

p. Discuss the purpose and content of ISA-67.01.01-2002 (R2007), *Transducer and Transmitter Installation for Nuclear Safety Applications.*

The following is taken from ISA-67.01.01-2002.

Purpose

ISA-67.01.01-2002 covers the installation of transducers for nuclear safety-related applications. ISA-67.01.01-2002 establishes requirements and recommendations for the installation of transducers and auxiliary equipment for nuclear applications outside of the main reactor vessel.

Content

ISA-67.01.01 discusses the following elements associated with the installation of transducers and auxiliary equipment for nuclear applications:

- Safety classification
- Equipment mounting
- Location of equipment
- Environmental considerations
- Interface connections
- Service, calibration, and test facilities
- Quality assurance

q. Discuss the purpose and content of ISA-S67.02.01-1999, *Nuclear-Safety-Related Instrument Sensing Line Piping and Tubing Standard for Use in Nuclear Power Plants.*

The following is taken from ISA-S67.02.01-1999.

Purpose

ISA-S67.02.01-1999 establishes the applicable code requirements and code boundaries for the design and installation of instrument-sensing lines interconnecting nuclear safety-related power plant processes with nuclear safety-related and nonnuclear safety-related instrumentation. ISA-S67.02.01-1999 also establishes the applicable requirements and limits for the design and installation of sample lines interconnecting nuclear safety-related power plant processes with sampling instrumentation.

ISA-S67.02.01-1999 addresses the pressure boundary integrity of an instrument-sensing line and sampling line in accordance with the appropriate parts of ASME B31.1, *Power Piping*, as applicable, and the assurance that the safety function of the nuclear safety-related instruments and process sampling is available.

Content

ISA-S67.02.01-1999 covers the pressure boundary requirements for sensing lines up to and including one inch outside diameter or three-quarter inch nominal pipe. The boundaries of ISA-S67.02.01-1999 for instrument-sensing lines span from the root valve/piping class change up to, but not including, the manufacturer-supplied instrument connection. The boundaries of ISA-S67.02.01-1999 for sampling lines span from the process tap to the upstream side of the sample panel, bulkhead fitting, or analyzer shutoff valve, and include in-line sample probes.

r. Discuss the purpose and content of ANSI/ISA-67.04.01-2006 (R2011), *Setpoints for Nuclear Safety-Related Instrumentation.*

The following is taken from ANSI/ISA-67.04.01-2006.

Purpose

The purpose of ANSI/ISA-67.04.01-2006 is to define the bases for establishing safety-related and other important instrument setpoints associated with nuclear power plants and nuclear reactor facilities.

Content

ANSI/ISA-67.04.01-2006 includes the following elements associated with instrument setpoints associated with nuclear power plants:

- Establishment of setpoints
- Documentation of uncertainty calculations
- Maintenance of safety-related setpoints

s. Discuss the purpose and content of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector* – Part 1: "Framework, Definitions, System, Hardware and Software Requirements"

The following is taken from ANSI/ISA-84.00.01-2004.

Purpose

ANSI/ISA-84.00.01-2004 gives requirements for the specification, design, installation, operation, and maintenance of an SIS, so that it can be confidently entrusted to place and/or maintain the process in a safe state. ANSI/ISA-84.00.01-2004, has been developed as a process sector implementation of IEC 61508.

Content

ANSI/ISA-84.00.01-2004 includes requirements related to the following elements of a SIS:

- Management of functional safety
- Safety life-cycle requirements
- Verification
- Process hazard and risk assessment
- Allocation of safety functions to protection layers
- SIS safety requirement specifications
- SIS design and engineering
- Requirements for application software
- Factory acceptance testing
- SIS installation and commissioning
- SIS safety validation
- SIS operation and maintenance
- SIS modification
- SIS decommissioning
- Information and documentation requirements

t. Discuss the purpose and content of ISA-TR84.00.06, *Safety Fieldbus Design Considerations for Process Industry Sector Applications.*

The following is taken from ISA-TR84.00.06.

Purpose

ISA-TR84.00.06 provides the following:

- guidance on implementing safety fieldbus protocols and devices in safety instrumented systems in the process industries
- recommendations for additional considerations and practices for the implementation of safety fieldbus protocols that are not currently included in ANSI/ISA-84.00.01-2004.

ISA-TR84.00.06 addresses safety fieldbus design and management. It does not provide detailed implementation guidance, which would be different for each fieldbus technology.

Content

ISA-TR84.00.06 includes the criteria for the following:

- Safety requirements
- Speed of response
- Interoperability and integration
- Fault tolerance
- Security
- Operation
- Diagnostics
- Documentation
- Testability

u. Discuss the purpose and content of IEEE Std 7-4.3.2-2003, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.*

[Note: IEEE Std 7-4.3.2-2003 has been superseded by IEEE Std 7-4.3.2-2010.]

The following is taken from the ANSI Standard Store, IEEE Std 7-4.3.2-2010.

Purpose and Content

Additional computer specific requirements to supplement the criteria and requirements of IEEE Std 603-2009, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*, are specified. Within the context of IEEE Std 7-4.3.2-2010, the term computer is a system that includes computer hardware, software, firmware, and interfaces. The criteria contained herein, in conjunction with criteria in IEEE Std 603-2009, establish minimum functional and design requirements for computers used as components of a safety system.

v. Discuss the purpose and content of IEEE Std 323-2003, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.*

The following is taken from IEEE Std 323-2003.

Purpose and Content

IEEE Std 323-2003 describes the basic requirements for qualifying safety related, Class 1E, and/or important to safety electrical equipment and interfaces that are to be used in nuclear power generating stations and nuclear facilities. The principles, methods, and procedures described are intended to be used for qualifying equipment, maintaining and extending qualification, and updating qualification, as required, if the equipment is modified. Meeting the qualification requirements demonstrates and documents the ability of equipment to perform safety function(s) under applicable service conditions including design basis events, thereby minimizing the risk of common-cause equipment failure.

w. Discuss the purpose and content of IEEE Std 344-2004, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.*

The following is taken from IEEE Std 344-2004.

Purpose and Content

Recommended practices are provided for establishing procedures that will yield data to demonstrate that the Class 1E equipment can meet its performance requirements during and/or following one safe shutdown earthquake event proceeded by a number of operating basis earthquake events. This recommended practice may be used to establish tests, analyses, or experienced based evaluations that will yield data to demonstrate Class 1E equipment performance claims, or to evaluate and verify performance of devices and assemblies as part of an overall qualification effort. Common methods currently in use for seismic qualification by test are presented. Two approaches to seismic analysis are described, one based on dynamic analysis and the other on static coefficient analysis. Two approaches to experienced-based seismic evaluation are described, one based on earthquake experience and the other based on test experience.

x. Discuss the purpose and content of IEEE Std 379-2000, *IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,* 2001.

The following is taken from IEEE Std 379-2000.

Purpose and Content

Application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power generating safety systems is covered in IEEE Std 379-2000.

y. Discuss the purpose and content of IEEE Std 384-2008, *IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits.*

The following is taken from IEEE Std 384-2008.

Purpose and Content

The independence requirements of the circuits and equipment comprising or associated with Class 1E systems are described. Criteria for the independence that can be achieved by physical separation and electrical isolation of redundant circuits and equipment are set forth. The determination of what is to be considered redundant is not addressed.

z. Discuss the purpose and content of IEEE Std 1023-2004, *IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and other Nuclear Facilities.*

The following is taken from IEEE Std 1023-2004.

Purpose and Content

IEEE Std 1023-2004 provides recommended practices for applying human factors engineering to systems and equipment that have significant human interfaces in nuclear power generating stations and other nuclear facilities.

aa. Discuss the purpose and content of NUREG-0700, "Human-System Interface Design Review Guidelines," Revision 2, Nuclear Regulatory Commission, 2002.

The following is taken from NUREG-700.

Purpose

The NRC staff reviews the human factors engineering (HFE) aspects of nuclear power plants in accordance with NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition." Detailed design review procedures are provided in NUREG-0711, "Human Factors Engineering Program Review Model, Revision 2." As part of the review process, the plant's human-system interfaces (HSIs) are evaluated.

The HSIs are the parts of a nuclear power plant with which personnel interact in performing their functions and tasks. Major HSIs include alarms, information displays, and controls. These other types of HSIs are described in NUREG-0700. Each type of HSI is made up of hardware and software components and is characterized in terms of its important physical and functional characteristics. The review guidelines contained in NUREG-0700 address the physical and functional characteristics of HSIs. Since these guidelines only address the HFE aspects of design and not other related considerations, such as instrumentation and control and structural design, they are referred to as HFE guidelines.

Personnel use of HSIs is influenced directly by 1) the organization of HSIs into workstations; 2) the arrangement of workstations and supporting equipment into facilities such as a main control room, remote shutdown station, local control station, technical support center, and emergency operations facility; and 3) the environmental conditions in which the HSIs are used, including temperature, humidity, ventilation, illumination, and noise. HFE guidelines are provided in NUREG-0700 for the review of these design considerations as well.

As per the review procedures described in NUREG-0711, the guidelines contained in NUREG-0700 can be used to review the design of HSIs and review a design-specific HFE guidelines document or style guide.

Content

The HFE guidelines are organized into four basic parts, which are divided into sections. Part I contains guidelines for the basic HSI elements: information display, user-interface interaction and management, and controls. These elements are used as building blocks to

develop HSI systems to serve specific functions. The guidelines address the following aspects of these HSI elements:

- *Information display.* This section provides HFE guidelines for the review of visual displays. Following a section of general guidelines, guidelines are provided in top-down fashion, beginning with display formats, display format elements, data quality and update rate, and display devices.
- *User-interface interaction and management.* This section provides HFE guidelines for the review of the modes of interaction between plant personnel and the HSI. Topics include dialogue formats, navigation, display controls, entering information, system messages, and prompts. This section also contains guidelines concerning methods for ensuring the integrity of data accessed through the user interface. Guidelines cover prevention of inadvertent change or deletion of data, minimization of data loss due to computer failure, and protection of data, such as setpoints, from unauthorized access.
- *Controls.* This section provides HFE guidelines for the review of information entry, dialogue types, display control, information manipulation, and system response time. Review guidelines are also provided for conventional control devices such as pushbuttons and various types of rotary controls. Considerations of display-control integration are also included here.

Part II contains the guidelines for reviewing the following seven systems:

1. Alarm system
2. Safety function and parameter monitoring system
3. Group-view display system
4. Soft control system
5. Computer-based procedure system
6. Computerized operator support system
7. Communication system

The guidelines include the functional aspects of the system, as well as any unique considerations for display, user-system interaction, and control that may be needed to review the system.

Selected Bibliography and Suggested Reading

Code of Federal Regulations

10 CFR 20.1501, "General." January 1, 2012.
10 CFR 50, "Domestic Licensing of Production and Utilization Facilities." January 2012.
10 CFR 50.36, "Technical Specifications." January 1, 2012.
10 CFR 50.36a, "Technical Specifications on Effluents from Nuclear Power Reactors." January 1, 2012.
10 CFR 50.48, "Fire Protection." January 1, 2012.
10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants." January 1, 2012.
10 CFR 820, "Procedural Rules for DOE Nuclear Activities." January 1, 2012.
10 CFR 830, "Nuclear Safety Management." January 1, 2012.
10 CFR 830.120,"Scope." January 1, 2012.
10 CFR 830.121, "Quality Assurance Program." January 1, 2012.
10 CFR 830.202, "Safety Basis." January 2012.
10 CFR 830.204, Documented Safety Analysis." January 1, 2012.
10 CFR 830.205, "Technical Safety Requirements." January 1, 2012.
10 CFR 835.502, "High and Very High Radiation Areas." January 1, 2012.
29 CFR 1910.119, "Process Safety Management of Highly Hazardous Chemicals." July 1, 2012.
48 CFR 970, "DOE Management and Operating Contracts." October 1, 2012.

All About Circuits

Ammeter.
Programmable Logic Controllers.
Resistors.
Time Delay Relays.

American National Standards Institute

ANSI C2, *National Electrical Safety Code*. 2007.
ANSI-N13.1, *Sampling and Monitoring Releases of Airborne Radioactive Substances From the Stacks and Ducts of Nuclear Facilities*. 2011.
ANSI-N42.18, American *National Standard Specification and Performance of On-Site Instrumentation for Continuously Monitoring Radioactivity in Effluents*. 2004.
ANSI-N320, *Performance Specifications for Reactor Emergency Radiological Monitoring Instrumentation*. 1979.

ANSI/American Nuclear Society. ANSI/ANS-8.3, *Criticality Accident Alarm System*. 2012.

ANSI/Institute for Electrical and Electronic Engineers

ANSI/IEEE-141, *IEEE Recommended Practice for Electric Power Distribution for Industrial Plants*. 1986.
ANSI/IEEE-142, *IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems*. 2007.
ANSI/IEEE-242, *IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems (IEEE Buff Book)*. 2001.

ANSI/IEEE-Std-323, *Qualifying Class 1E Equipment for Nuclear Power Generating Stations*. 2003.
ANSI/IEEE-336, *Recommended Practice for Installation, Inspection, and Testing for Class 1E Power, Instrumentation, and Control Equipment at Nuclear Facilities*. 2010.
ANSI/IEEE-338, *Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems*. 2012.
ANSI/IEEE-Std-344, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*. 2004.
ANSI/IEEE-379, *Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.* 2000.
ANSI/IEEE-384, *Criteria for Independence of Class 1E Equipment and Circuits.* 2008.
ANSI/IEEE-493, *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*. 2007.
ANSI/IEEE-1050, *Guide for Instrumentation and Control Equipment Grounding in Generating Stations*. 1996.
ANSI/ISA-18.2, *Management of Alarm Systems for the Process Industries*. 2009.
ANSI/ISA-67.04.01-2006, *Setpoints for Nuclear Safety-Related Instrumentation*. 2006.
ANSI/ISA 84.00.01-2004 – Part 1, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*. 2004.
ANSI Standard Store, IEEE Std 7-4.3.2-2010.

American Petroleum Institute. API RP-1167, *Pipeline SCADA Alarm Management.* 2010.

American Society for Mechanical Engineers
ASME B 31.1, *Power Piping*. 2012.
ASME NQA-1-2008, *Quality Assurance Requirements for Nuclear Facility Applications*. March 14, 2008.
ASME NQA-1a-2009, addenda to *Quality Assurance Requirements for Nuclear Facility Applications*. August 31, 2009.

American Society for Testing and Materials (ASTM). E230, *Standard Specification and Temperature-Electromotive Force (EMF) Tables for Standardized Thermocouples.* 2011.

Answers. *What is an As-Built Drawing*?

Bird, John. *Electrical and Electronic Principles and Technology*, Elsevier Limited. 2010.

Bright Hub Engineering. *Pneumatic vs. Electronic Control Mechanisms*. January 10, 2011.

BS EN 60073, Basic and Safety Principles for Man-Machine Interface, Marking and Identification—Coding Principles for Indicators and Actuators. September 6, 2002.
(BSEN = British Adopted European Standard)

California Department of Transportation. *Transportation- and Construction-Induced Vibration Guidance Manual*. June 2004.

Control. *Safety Systems for Non-Engineers*. August 7, 2009.

DesignAerospace LLC. *Hydraulic Fluid—Properties*. 2010.

diydata.com. Ball *(or float) Valves*.

DRM Associates. *New Product Development Solutions*, "Failure Modes and Effects Analysis." 2002.

eHow
Advantages and Disadvantages of Hydraulic Systems.
Advantages and Disadvantages of Wireless Media.
Difference Between Potential Transformer & Current Transformer.
How Does a Fluid System Work?
How do Pneumatic Controls Work?
Types of Vibration Sensors.
What is a Motor Control Center?
What is an Ohmmeter?

Electric Energy Publications. *Proper Control Room Design Facilitates Critical Thinking and Situational Awareness*. 2012.

Energy Facilities Contractor Group. (EFCOG) *Safety System Design Adequacy*. August 2004.

Envision Software Inc. *Root Cause Analysis*. February 8, 2012.

Federal Register. 1810, 10 CFR Part 830, January 10, 2010.

Fluke. *Electrical Calibration*, "Why Calibrate Test Equipment?" 2004.

Georgia State University, *Hyperphysics*
"Voltage."
"Electric Current."

GlobalSpec. *Humidity Measurement Instruments Information.*

Grand Valley State University. *Feedback Control Systems*.

Gray, David M. *Improved Technology for Dissolved Oxygen Measurement*. March 2002.

Hydraulicmania.com. *The Workings of a Hydraulic Lift,* "Various Uses for Hydraulic Lifts." 2010**.**

Industrial-Electricity.com
Understanding Gain, Reset, and Rate
Using Gain for Control

Information Point Technologies. *Wireless Networking, Advantages and Disadvantages to Wireless Networking*.

Institute of Electrical and Electronic Engineers

IEEE\ANSI 91-1984, *Graphic Symbols for Logic Functions*. 1984.

IEEE Std 7-4.3.2-2010, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*. 2010.

IEEE Std 323-2003, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations*. 2004.

IEEE Std 344-2004, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*. 2004.

IEEE Std 379-2000, *IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*. 2001.

IEEE 384, *Standard Criteria for Independence of Class 1E Equipment and Circuits*. 2008

IEEE Std 603-2009, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*. 2009.

IEEE Std 1023-2004, *IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and other Nuclear Facilities*. 2004

Instrumentation and Process Control

Motor Operated Valve (MOV).

Valve Manifold for Pressure Instrument.

International Atomic Energy Agency

IAEA DS367, *Safety Classification of Structures, Systems and Components in Nuclear Power Plants*. February 4, 2011.

IAEA Safety Standards Series No. SSR-2/1, *Safety of Nuclear Power Plants: Design.* 2012.

International Electrotechnical Commission

IEC 61158, *Industrial Communication Networks—Fieldbus Specifications*. 2010.

IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.* 2010.

IEC 61511, *Functional Safety—Safety Instrumented Systems for the Process Industry Sector—Part 1: Framework, Definitions, System, Hardware and Software Requirements*. March 12, 2003.

International Society of Automation

ISA-18.1-1979 (R2004), *Annunciator Sequences and Specifications*. 2004.

ISA-67.01.01-2002 (R2007), *Transducer and Transmitter Installation for Nuclear Safety Applications*. 2007.

ISA-S67.02.01-1999, *Nuclear-Safety-Related Instrument Sensing Line Piping and Tubing Standard for Use in Nuclear Power Plants*. 1999.

ISA-S67.04-2006, *Setpoints for Nuclear Safety-Related Instrumentation*. 2006.

ISA TR84.00.06, *Safety Fieldbus Design Considerations for Process Industry Sector Applications*. 2006.

International Organization for Standardization. ISO 7027, *Water Quality: Determination of Turbidity*. 1999.

Los Alamos National Laboratory. *LANL Engineering Standards Manual ISD 341-2,* "Appendix D, Installation & Calibration of Instruments." October 27, 2006.

MoreSteam.com. *Trend Chart*.

MyChemE. *Design Guides*, "Designing Compressed Air Systems."

National Center for Biotechnology Information. *Vision 2020: Computational Needs of the Chemical Industry.* 1999.

National Fire Protection Association
NFPA-70, *National Electrical Code*. 2011.
NFPA-110, *Standard for Emergency and Standby Power Systems*. 2010.

National Institute of Standards and Technology. *Microsystems for Harsh Environment Testing*. October 22, 2012.

National Research Council, *Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability*. 1997.

NDT Resource Center
Alternating Current.
Impedance.

Newcastle University. *Overview of Measurement Systems and Devices*.

Oak Ridge National Laboratory. *Electrical Signal Analysis (ESA).*

Omega Engineering. *pH Control: A Magical Mystery Tour*. September 1984.

Online Article-Openticle.com. *Head Flow Meters*, Dall Flow Tube.

OpAmp-Electronics. *Chapter 6. Ladder Logic*, "Ladder Diagrams." May 2003.

PAControl. Com. *Final Control Elements–Control Valves*. 2012.

PAS. *Understanding and Applying the ANSI/ISA 18.2 Alarm Management Standard*. 2010.

Piping-Designer. *Instrument Air*. March 4, 2010.

Power Engineering. *Seismic Instrumentation and Nuclear Power Plants*. June 1, 2012.

Process Operations. *Redundancy and Diversity*.

Pumps-in-Stock. *Centrifugal Pump Design*.

Radiometer Analytical. *Conductivity Theory and Practice*. 2004

Rensselaer Polytechnic Institute. *Positive-Displacement Pumps*.

SA Instrumentation and Control
Compressor Optimization and Surge Elimination. January 2001.
Enhanced Reliability for Final Elements. May 2006.

Sadar, Mike. *Turbidity Instrumentation—An Overview of Today's Available Technology.* May 2, 2002

Santa Clara University. *Principles of Testing Electronic Systems*. 2005.

Spiraxsarco. *Control Value Actuators and Positioners*. 2012.

Sutton Technical Books. *Process Safe Limits*.

The Engineering ToolBox
Thermocouples.
Types of Fluid Flow Meters.

U.S. Department of Energy Directives (Guides, Manuals, Orders, and Policies)
DOE Guide 200.1-1, *Software Engineering Methodology*. May 21, 1997.
DOE Guide 200.1-1, *Chapter 4, Requirements Definition Stage*. May 21, 1997.
DOE Guide 200.1-1, *Chapter 5, Functional Design Stage*. May 21, 1997.
DOE Guide 414.1-1B, *Management and Independent Assessments Guide for Use with 10 CFR Part 830, Subpart A, and DOE O 414.1C, Quality Assurance; DOE M 450.4 -1, Integrated Safety Management System Manual; and DOE O 226.1A, Implementation of DOE Oversight Policy.* September 27, 2007.
DOE Guide 414.1-2B, *Admin Chg 1, Quality Assurance Program Guide.* August 16, 2011.
DOE Guide 414.1-4, *Safety Software Guide for use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance*. June 17, 2005.
DOE Guide 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide for use with DOE O 420.1, Facility Safety*. March 28, 2000.
DOE Guide 421.1-2A, *Implementation Guide for use in Developing Documented Safety Analyses to Meet Subpart B OF 10 CFR 830*. December 19, 2011.
DOE Guide 423.1-1A, *Implementation Guide for use in Developing Technical Safety Requirements*. November 3, 2010.
DOE Guide 430.1-5, *Transition Implementation Guide.* April 24, 2001.
DOE Guide 433.1-1A, *Nuclear Facility Maintenance Management Program Guide for Use with DOE O 433.1B.* September 12, 2011.
DOE Order 226.1B, *Implementation of Department of Energy Oversight Policy*. April 25, 2011.
DOE Order 413.3B, *Program and Project Management for the Acquisition of Capital Assets.* November 29, 2010.
DOE Order 414.1D, *Quality Assurance*. April 25, 2011.
DOE Order 420.1B, Chg. 1, *Facility Safety*. April 19, 2010.
DOE Order 422.1, *Conduct of Operations.* June 29, 2010.
DOE Order 430.1B, *Real Property Asset Management.* February 24, 2003.

DOE Order 433.1B, *Maintenance Management Program for DOE Nuclear Facilities*. April 21, 2010.

U.S. Department of Energy Handbooks and Standards

DOE-HDBK-1013-92, Volumes 1 and 2, *DOE Fundamentals Handbook: Instrumentation and Control*. June 1992.
DOE-HDBK-1016-93, Volumes 1 and 2, DOE *Fundamentals Handbook: Engineering Symbology, Prints, and Drawings.* January 1993.
DOE-HDBK-1122-99, *Radiological Control Technician Training*. February 2009.
DOE STD-1027-92, Chg. 1, *DOE Standard*: *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*. September 1997.
DOE-STD-1068-94, *DOE Standard: Guideline to Good Practices for Maintenance History at DOE Nuclear Facilities*. June 1994.
DOE-STD-1073-2003, *DOE Standard: Configuration Management*. October 2003.
DOE-STD-1098-99, Chg. 1, *DOE Standard: Radiological Control*. March 2005.
DOE-STD-1121-2008, *DOE Standard: Internal Dosimetry*. October 2008.
DOE STD-1172-2003, *DOE Standard: Safety Software Quality Assurance Functional Area Qualification Standard.* December 2003.
DOE-STD-1186-2004, *DOE Standard: Specific Administrative Controls*. August 2004.
DOE-STD-1189-2008, *Integration Of Safety Into The Design Process*. March 2008.
DOE-STD-1195-2011, *DOE Standard: Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities*. April 2011.
DOE-STD-3009-94, Chg. 3, *DOE Standard: Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*. March 2006.
DOE-STD-3024-2011, *DOE Standard: Content of System Design Descriptions*. August 2011.
DOE-STD-6002-96, *DOE Standard: Safety of Magnetic Fusion Facilities: Requirements*. May 1996.
DOE-STD-6003-96, *DOE Standard: Safety of Magnetic Fusion Facilities: Guidance. May 1996.*

U.S. Environmental Protection Agency

EPA 180.1, *Determination of Turbidity by Nephelometry*. August 1993.

U.S. Nuclear Regulatory Commission

Appendix A to Part 50—"General Design Criteria for Nuclear Power Plants." November 6, 2012.
Background Information on NRC Effluent and Environmental Monitoring Requirements.
Nuclear Regulatory Guide 1.12, *Nuclear Power Plant Instrumentation for Earthquakes*. March 1997.
Nuclear Regulatory Guide 1.105, *Setpoints for Safety-Related Instrumentation.* December 1999.
Nuclear Regulatory Guide 8.8, *Information Relevant to Ensuring that Occupational Radiation Exposures at Nuclear Power Stations Will Be As Low As Reasonably Achievable*. June 1978.
NUREG-0700, "Human-System Interface Design Review Guidelines." March 2002.

NUREG-0711, “Human Factors Engineering Program Review Model, Revision 2.” February 2004.
NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition.” March 2007.
NUREG 1.209, “Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants.” March 2007.
Radiological Assessment Branch Technical Position, Revision 1. November 1979, *An Acceptable Radiological Environmental Monitoring Program.*

Whatis.com. *Interface Devices*. December 2010.

Wikibooks. *Control System/Stability*. June 12, 2012.

Wikipedia

Accuracy and Precision. November 8, 2012.
Analog Switch. August 30, 2012.
Annunciator Panel. November 18, 2012.
Battery. September 27, 2010.
Butterfly Valve. October 20, 2012.
Check Valve. October 27, 2012.
Chlorine. November 1, 2012.
Circuit Breaker. October 22, 2012.
Dampers. August 13, 2012
Density. October 21, 2012.
Diaphragm Valve. June 15, 2012.
Diesel Generator. October 13, 2012.
Digital Electronics. November 20, 2012.
Digital Signal Processors. November 11, 2012.
Direct Current. October 12. 2012.
Electric Generator. October 16, 2012.
Electric Motor. October 24, 2012.
Electrical Reactance. October 20, 2012.
Fault Tree Analysis. November 7, 2012.
Fieldbus. November 26, 2012.
Functional Requirements. July 18, 2012.
Fuse. October 17, 2012.
Gate Valve. October 12, 2012.
Globe Valve. September 6, 2012.
HEPA. October 21, 2012.
Hydraulics. October 23, 2012.
Hydrogen. November 27, 2012.
Inductor. July 30, 2013.
Input/Output. June 26, 2012.
Laws of Thermodynamics. October 25, 2012.
Orifice Plate. October 17, 2012.
Pitot Tube. November 26, 2012.

Pressure. October 22, 2012.
Pressure Regulator. August 21, 2012.
Relief Valve. September 20, 2012.
Relays. October 21, 2012.
Residual Gas Analyzers. January 23, 2012.
Resistance Thermometer. October 28, 2012.
Safety Instrumented System. October 22, 2012.
Sight Glass. May 6, 2012.
Switchgear. October 8, 2012.
Temperature Measurements. October 27, 2012.
Traditional Handled Refractometer. December 13, 2010.
Transformer. October 19, 2012.
Turbine. October 27, 2012.
Uninterruptible Power Supply. November 10, 2012.
Viscosity. November 25, 2012.
Voltmeter. October 14, 2012.
Volumetric Flow Rate. October 14, 2012.

Wolf Automation, *Communication Modules*.

Instrumentation and Control
Reference Guide
June 2013