Instrumentation and Control (I&C) Systems in Nuclear Power Plants: A Time of Transition

I&C systems are the nervous system of a nuclear power plant. They monitor all aspects of the plant's health and help respond with the care and adjustments needed.

Progress in electronics and information technology (IT) has created incentives to replace traditional analog instrumentation and control (I&C) systems in nuclear power plants with digital I&C systems, i.e. systems based on computers and microprocessors. Digital systems offer higher reliability, better plant performance and additional diagnostic capabilities. Analog systems will gradually become obsolete in the general IT shift to digital technology. About 40% of the world's operating reactors have been modernized to include at least some digital I&C systems. Most newer plants also include digital I&C systems.

Digital I&C systems have posed new challenges for the industry and regulators, who have had to build up the methods, data and experience to assure themselves that the new systems meet all reliability and performance requirements. In general, countries with more new construction of nuclear reactors have had greater incentives and opportunities to develop the needed capabilities. Other countries are still in the process of doing so.

A. Status and examples of digital I&C systems in nuclear power plants

Nuclear power plants (NPPs) rely on I&C systems for protection, control, supervision and monitoring. A typical unit has approximately 10 000 sensors and detectors and 5000 km of I&C cables. The total mass of I&C related components is on the order of 1000 tonnes. This makes the I&C system one of the heaviest and most extensive non-building structures in any nuclear power plant.

No globally comprehensive statistics are available on the numbers of plants with fully analog, fully digital or hybrid I&C systems. However, approximately 40% of the world's 439 operating power reactors, accounting for nearly all of the 30 countries with operating NPPs, have had some level of digital I&C upgrade to, at least, important safety systems. From another perspective, 90% of all the digital I&C installations that have been done have been modernization projects at existing reactors. 10% have been at new reactors. Of the 34 reactors currently under construction around the world, all of those for which construction began after 1990 have some digital I&C components in their control and safety systems.

In Japan, the first fully digital I&C system was integrated into the Kashiwazaki-Kariwa-6 advanced boiling water reactor (ABWR) in 1996, followed shortly by Kashiwazaki-Kariwa-7 (see Fig. V-1). Similar digital I&C systems are used in Hamaoka-5. Tomari-3, which will feature the first all-digital reactor control room, is scheduled to begin operation in 2009.

In China, Qinshan Phase III, with two 700 MW(e) CANDU reactors, and Tianwan-1 and -2, with two 1000 MW(e) VVERs, have fully digital I&C systems, including both the safety and control systems, and partly computerized, i.e. hybrid, human-system interfaces (HSIs). China's high-temperature gas-cooled experimental reactor, the HTGR-10, also has fully digital safety and control I&C systems, plus a hybrid human-system interface in its main control room.

In the UK at Sizewell B, a 1250 MW(e) PWR, all automatic functions of the safety I&C systems are digital, and in the main control room, all the qualified displays used in the human-system interface are computerized.[1]

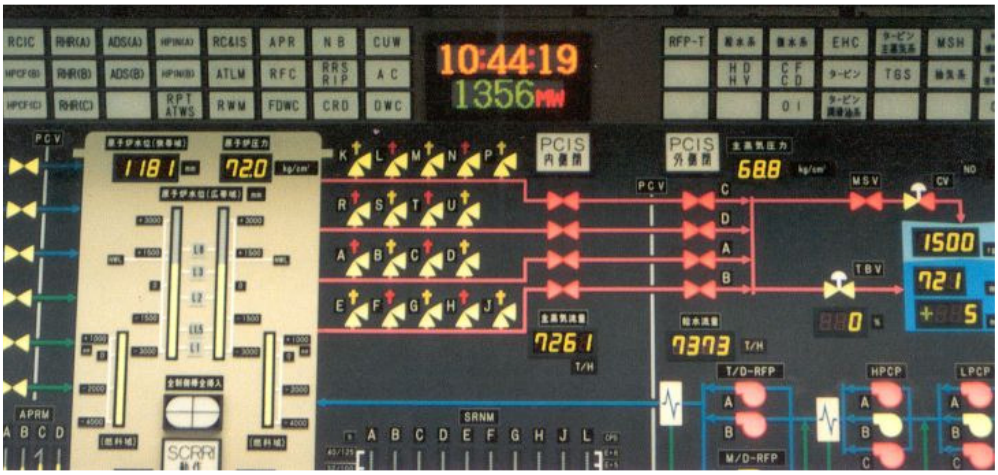

FIG. V-1. Section of main control panel in the Kashiwazaki-Kariwa-6 and -7 Advanced Boiling Water Reactor (1350 MW(e)).

In Russia, Kalinin-3, which was commissioned in 2004, is the first VVER-1000 equipped with digital I&C safety systems and digital process control systems. In addition, both its main and emergency control rooms have hybrid human-system interfaces (Fig. V-2.a). A dynamic simulator was also installed (Fig. V-2.b) for the purpose of testing control functions.

FIG.V-2a. Main control room of Kalinin Unit 3

FIG.V-2b. Dynamic simulator of Kalinin Unit 3

In the Republic of Korea, three 1000 MW(e) PWRs are under construction (Shin-Kori-1 and -2 and Shin-Wolsong-1), all with fully digital I&C safety and control systems and hybrid human-system interfaces in the control rooms.

In the USA, 1978 was the last year in which construction started on a reactor that eventually came on line. The US Nuclear Regulatory Commission (NRC) has therefore not had the same experience with digital I&C systems as have regulators in China, India, Japan and the Republic of Korea, where the

---

[1] The phrase "qualified displays" refers to dedicated display equipment with the high performance and dependability needed for safety applications.

expansion of nuclear power is centred. Partly as a result, digital systems have not yet been approved for use as safety systems in operating US NPPs. Figure V-3 is a simplified illustration of a US case where the I&C systems for controlling the plant, on the left side of the figure, are digital (computers, digital data networks, automatic calculations, and microprocessor-based sensors), and the I&C systems for safety, labelled "protection" on the right side of the figure, are analog. The figure also illustrates the features of independence, redundancy, and diversity that are essential in I&C systems and are outlined below.

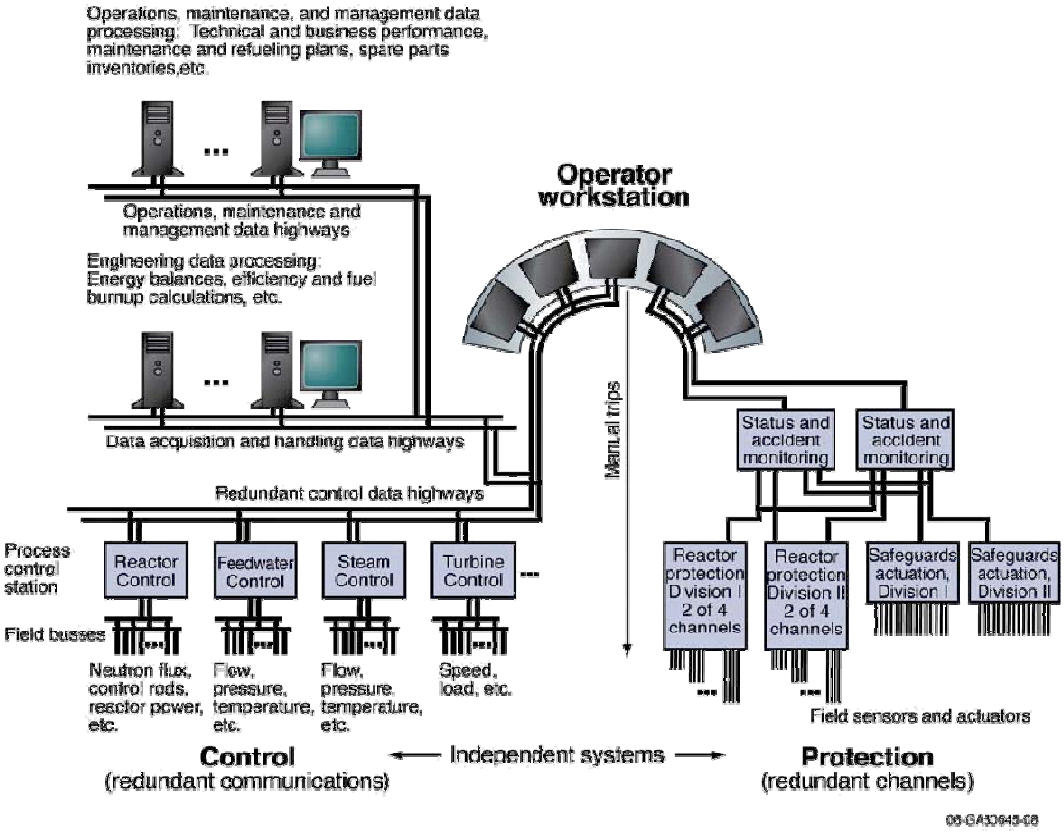

FIG.V-3. Typical I&C architecture for a plant with a digital I&C system for control and an analog I&C system for safety (labelled "protection" in the figure)[2]*. (Source: US National Research Council).*

B. I&C basics and the reasons for shifting from analog to digital I&C systems

I&C systems are installed throughout a nuclear power plant and are vital parts of normal, abnormal and emergency operations. Typically plants have both main and secondary (emergency) control rooms from which most I&C systems are operated. Some I&C functions are critical for assuring nuclear safety (e.g. reactor shutdown systems). Others influence safety to varying degrees. And still others, which are more related to production and maintenance, may have no impact on nuclear safety (e.g. I&C functions for turbine diagnostics, fluid level controllers in the turbines, or the turbine hall crane).

---

[2] US National Research Council, *Digital Instrumentation and Control Systems in Nuclear Power Plants (Safety and Reliability Issues),* 1997

I&C systems are the nervous system of the plant, and they affect every aspect of plant operation. Their components and functions include the following:

- Sensors interfacing with the physical processes within a plant and continuously taking measurements of plant variables such as neutron flux, temperature, pressure and flow.
- Control, regulation and safety systems that process measurement data to manage plant operation, optimize plant performance and keep the plant in a safe operating envelope.
- Communication systems for data and information transfer through wires, fiber optics, wireless networks or digital data protocols.
- Human-system interfaces to provide information and allow interaction with plant operating personnel.
- Surveillance and diagnostic systems that monitor sensor signals for abnormalities.
- Actuators (e.g. valves and motors) operated by the control and safety systems to adjust the plant's physical processes.
- Status indicators of actuators (e.g. whether valves are open or closed, and whether motors are on or off) providing signals for automatic and manual control.

In the control room, the I&C systems and the plant operators meet at the human-system interface (HSI). The designs of HSIs, whether digital (e.g. digital displays and touch screens), analog (gauges, knobs, switches, and push-buttons) or hybrid (some of both), must go beyond IT electrical engineering to include human factors engineering and assure both that the operators get the most out of the I&C system and, in a sense, the I&C system gets the most out of the human wisdom of the operators. The next section below elaborates on HSI technologies.

Perhaps faster than any other part of nuclear power plants, I&C technology is continuously advancing. Yet the majority of instrumentation and control equipment in nuclear power plants was designed more than 30 years ago with analog and relay components, and in some cases rudimentary digital technology. Although analog I&C systems have served the above functions satisfactorily for many decades, a substantial amount of this original I&C equipment already is or soon will be obsolete. Much is approaching or has exceeded its original life expectancy.

Approaching obsolescence means a decreasing availability of replacement parts, decreasing supplier support (or even the loss of the supplier to the nuclear industry), a lack of functional capabilities needed to satisfy current and future needs, and a lack of experienced staff for maintenance and engineering. This can lead to degraded reliability and availability, and a compensatory increase in operation and maintenance (O&M) costs to maintain acceptable performance. Older technology also limits possibilities for adding new beneficial capabilities to the plant. New technology, in contrast, provides opportunities to improve plant performance, HSI functionality, and reliability; to enhance operator performance and reliability; and to address difficulties in finding young professionals with education and experience with older analog technology.

Aging, by itself, can also reduce performance. If the I&C system has a high failure rate, especially if the consequences are unacceptable or unnecessarily challenge protection systems, then it should have high priority for modernization. In addition, the need for ever higher reliability and availability may require newer technologies with capabilities not possible or practical with older technology.

Approaching obsolescence and aging may thus make the effort to maintain or increase the reliability and useful life of existing I&C systems greater in the long run than that of modernizing or replacing them completely with new digital or hybrid systems. Finally, potential regulatory updates might require modernization.

I&C modernization should be performed in the context of, and in support of, the overall plant goals, objectives, and internal and external commitments. These include commitments to licensing

authorities, staff and other stakeholders. The goals and objectives of the plant will be driven substantially by utilities' long-term and short-term business plans.

An adequate assessment of the expected length of a plant's remaining lifetime is crucial. In extreme cases, the decision is obvious. If a unit is to be shut down and decommissioned very soon, there is no justification to modernize any of its significant systems, including I&C. On the other hand, when the plant's lifetime is extended through licence renewal and the existing systems cannot continue to support the plant, modernization is required. A nuclear power plant that operates for 60 years, as 48 reactors in the USA are now licensed to do, could outlive its original I&C system by a factor of three, shifting first from analog to digital I&C systems, and then subsequently to even more advanced digital I&C systems.

In between the extremes, those making the decision can benefit from the experience of other plants that have already modernized their I&C systems. Such experience covers cost-benefit analyses, design and selection of equipment, licensing requirements, qualification methods and project management. Importantly, O&M experience from other plants is valuable for determining the goals for a new system, the scope of the project and the system's design.

C. Control rooms and human-system interface (HSI) technologies

The HSI in the control room is where plant information is translated into required operator action. It is critical to safe operation. Computerizing an HSI means incorporating features such as computerized procedures, digital displays, touch-screen interfaces, pointing devices (like mice), and large-screen overview displays. Computerization allows more tasks to be done by operators sitting at their workstations without moving about the control room.

HSI modernization is an integral part of I&C modernization in general. Because computerization is phased, control rooms at plants that have been modernized are hybrid, incorporating some analog features and some digital features (Figures V-4.a and V-4.b).

HSI computerization offers advantages similar to those of digital I&C systems. It allows more efficient operations and maintenance due to the HSI providing operators with a more comprehensive and detailed understanding of operating conditions. This leads to improved power plant availability and safety and reduced operating costs through the avoidance of transients, forced outages, and unnecessary shutdowns. More precise controls and modelling allow increased power plant efficiency and output. New digital systems also have additional capabilities including self-diagnostic capabilities, simple recalibration, screening and validation of input signals.

Shifting to an increasingly computerized HSI requires retraining operators and revising operating and maintenance procedures. However, it is also an opportunity to take advantage both of certain features of digital systems and of improved understanding of human cognitive processing. Control rooms and their HSIs can be designed, operated, and maintained to better match with human cognitive processing abilities and thus increase performance and reduce the likelihood of human errors.

To this end, it is important that control room modernization be a continuous and iterative process with feedback from intended users, who should be involved in all phases. Human factors verification and validation play an important role both in the design and development of individual sub-systems and in their integration and installation in the complete system. Human factors verification refers to the comparison of detailed design features against those given in specifications. Human factors validation refers to overall performance testing to check for safe, error-free, and efficient performance.

FIG. V-4a. Sweden's Oskarshamn unit 1 MCR before modernization in 2003

FIG. V-4b. Sweden's Oskarshamn unit 1 MCR after modernization

D. Classification of I&C systems

I&C systems are classified based on the safety importance of the functions and systems they support. The nuclear industry's graded approach to safety stipulates that greater attention is given to systems and equipment that are important to safety than to systems that have less or no safety impact. In practice, this principle is implemented using a classification or categorization document which lists every system and component and assigns it to a safety class or category. Different countries and international organizations use different categorization schemes. For example, the International Electrotechnical Commission (IEC) categorization defines three safety categories, A, B and C, while the US Institute of Electrical and Electronics Engineers (IEEE) only distinguishes between safety and non-safety systems. The IAEA has generally adopted a three-level distinction between safety systems, safety related systems and non-safety systems. Table 1 illustrates how categories used in different classification systems overlap. All classification systems essentially provide the same guidance concerning priorities for I&C modernization, for assuring that safety is never compromised and for allocating resources for testing, verification and validation.

Table 1: A comparison of different classification systems

National or International Standard	Classification to the Importance to Safety			
IAEA	Systems Important to Safety			Systems Not Important to Safety
	Safety System	Safety Related System		
IEC 61226	Category A	Category B	Category C	Unclassified
France N4	1E	2E	IFC/NC	
European Utility Requirements	F1A (Automatic)	F1B (Automatic and Manual)	F2	Unclassified
Russia	Class 1 (beyond DBA*)	Class 2 (Safety System, DBA)	Class 3	Class 4
UK	Category 1	Category 2	Unclassified	
USA (IEEE)	1E	Non-nuclear Safety		

* DBA = design basis accident

Examples of systems important to safety, using the IAEA classification, are:

- reactor protection systems,
- engineered safety features actuation systems (ESFAS), e.g. emergency core cooling and feedwater,
- safe shutdown systems, e.g. for the fast insertion of absorber rods or injection of neutron absorbing liquid,
- emergency power supply and diesel generator control systems,
- information systems important to safety, e.g. displays in the main control room or the neutron flux in-core monitoring system,
- interlock systems important to safety,
- reactor control systems and access control systems,
- some data communications systems, and
- essential auxiliary supporting systems, e.g. heating, ventilation, and air conditioning.

E. Challenges of digital I&C systems

Digital equipment with improved performance has had an important influence on I&C systems design in many major industries. However, in nuclear power plants digital technology has been adopted more slowly, especially for safety I&C systems. For good reason, the nuclear industry has an inherently conservative approach to safety, and substantial effort is required to provide the necessary evidence and analysis to assure that digital I&C systems can be used in safety-critical and safety-related applications. That effort has been made in countries where it has been justified by recent new construction and by national policies supportive of expanding nuclear power. In other countries industry and regulatory approval of digital safety I&C is less advanced. In both cases, designers and regulators will need to make continuing mutual adjustments at least until digital I&C systems become

the universal norm, and probably longer as the technology keeps developing. Designers have to design to existing regulations, which are often still based on analog systems. Regulators have to adjust to the new technology to make sure a country benefits, efficiently and safely, from any advantages it offers in terms of greater reliability, lower costs or greater safety.

For industry adoption and regulatory approval, three features of digital I&C systems are distinctive. First, a digital I&C system has more connections among its many components and is simply more complex than its analog predecessor. Second, the digital system is more dependent on software. Third, the overall dependence on computers raises the importance of cyber security.

The first two of these features, complexity and software-dependence, introduce new possibilities for common cause failures.

E.1. Common cause failures

The greater complexity of digital I&C systems, and the greater interaction among subsystems, increase the possibility that a latent fault can exist in the system that could be triggered and propagate, thus causing the system to not perform as expected. The fact that the generation of software can be prone to failures, and the possibility that copies of the same software might be used in redundant channels of a safety system, create an additional potential for common cause failures.

For a potentially unsafe common cause failure to occur a number of developments must happen at once, as illustrated in Figure V-5. The system must have a fault; a triggering event must activate the fault; channels that are supposed to be independent must be affected concurrently; the result must have an affect on safety; and multiple systems must share the same fault(s) and be susceptible to the same trigger concurrently.

Concern about similar common cause failures did not exist for earlier analog safety systems because it was assumed that any common cause failure that did occur would be due to slow distinct processes like corrosion or a part prematurely wearing out. The same cannot be assumed for systems dependent on software.

There are three complementary ways to prevent common cause failures, all of which contribute to defence in depth. They are diversity, redundancy and independence. Diversity means that, for a particular function, two or more redundant systems or components with different attributes are included in the design. In practice, it may mean using different components based on different designs and principles, from different vendors. Redundancy means that alternative systems and components are included, so that any one can perform the required function if the others fail. Independence prevents the propagation of failures and common cause failures due to common internal plant hazards. Independence is achieved by electrical isolation, physical separation and independence of communications between systems.[3]

[3] IAEA Safety Guide No. NS-G-1.3

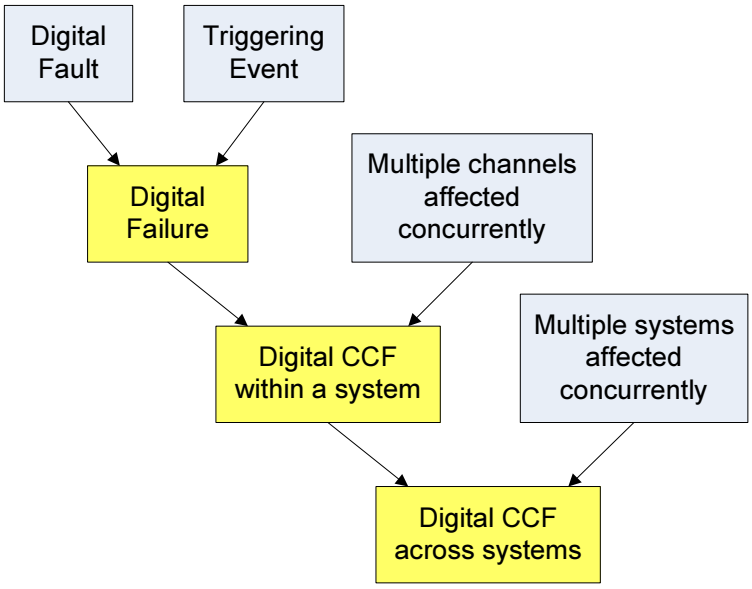

FIG. V-5. Conditions for a common cause failure in a digital I&C system.

Additional diversity, redundancy and independence, however, also increase a system's complexity and raise the possibility that the additional complexity may pose a larger risk of human errors in design, operation, and maintenance than the common cause failure they were intended to avoid. To compensate, one way to simplify the design, manufacture and use of digital I&C systems is to use pre-qualified 'commercial off-the-shelf' (COTS) hardware and software components that have been thoroughly tested and evaluated for nuclear power plant applications.

Whichever mix of these approaches is taken to reducing possible failures, the overall risk of a digital I&C system needs to be assessed, quantified, and managed using probabilistic safety assessment (PSA) methods. This will become increasingly straightforward as experience with digital I&C systems grows, as the data on their performance in all conditions expand, and as associated PSA models are further developed.

E.2. Cyber security

Nuclear power plant I&C systems are generally isolated from external communication systems. Nonetheless, particularly the computers used in safety and safety-related systems must be very well protected from possible intrusions. But other computers must be protected as well. The computers used to control the plant are essential to assure the continuity of power production. The computers used to control access to sensitive areas are needed both to prevent unauthorized access that might be part of an attack, and to assure authorized access both for safety and security reasons. Computers that store important and sensitive data have to be protected to assure that those data are not erased or stolen.

Possible cyber attacks could be associated with business espionage, technology theft, a disgruntled employee, a recreational hacker, a cyber activist, organized crime, a nation state, or a terrorist organization. Four categories of possible cyber attacks have to be considered: (1) unauthorized access to information (loss of confidentiality), (2) interception and change of information, software, hardware (loss of integrity), (3) blocking data transmission lines and/or shutting down systems (loss of availability), and (4) unauthorized intrusion in data communication systems or in computers (loss of reliability).

Computer security is built from a consideration of these possible threats and the development of a design basis threat (DBT), defined within the context of computer security, that typically involves both

insiders and outsiders. A significant difficulty is that the complexity of computer systems sometimes makes it difficult to identify possible sequences that could introduce important threats. The tools for identifying threats and building barriers include both technical tools, such as intrusion detection, virus scanners and encryption, and administrative tools such as the application of security zones, security management systems, passwords and biometric identification.

Experience gained from cyber security in other sensitive fields, such as the military, national security, banking, and air-traffic control is valuable both for improving cyber security at nuclear power plants with digital I&C systems and for demonstrating that cyber defences can consistently stay ahead of cyber attacks. But, as with safety and other areas of security, cyber security is an area where no-one can rest on his laurels. Continued success requires continuous vigilance and continuous improvement.

F. Emerging technologies

Digital I&C systems are expected to continue as an area of rapid technological development. Future designs of NPPs will require new solutions both in sensing technologies and in digital control. Advanced sensors, detectors, transmitters, and data transmission lines are needed to meet the requirements imposed by the operating conditions of new designs (e.g. high temperatures and high flux) and the harsh environment of ‘beyond design basis’ conditions. Additional monitoring and diagnostic systems will need to be developed, making use of on-line condition monitoring techniques, reactor noise analysis for incipient failure detection, wireless sensor networks and communication, and integrated remote operation.