ATST
advanced technology solar telescope

Global Interlock System
Design Specification

Final Design Review

Tim Williams

July 25, 2011

What is Safety?

- Safety is freedom from unacceptable risk of physical injury or damage to the health of people either directly or indirectly, as a result of damage to property or to the environment.
- Functional Safety is part of safety which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction.

General Duty Clause

29 USC 654 § 5

(a) Each employer --

(1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees;

(2) shall comply with occupational safety and health standards promulgated under this Act.

More Importantly

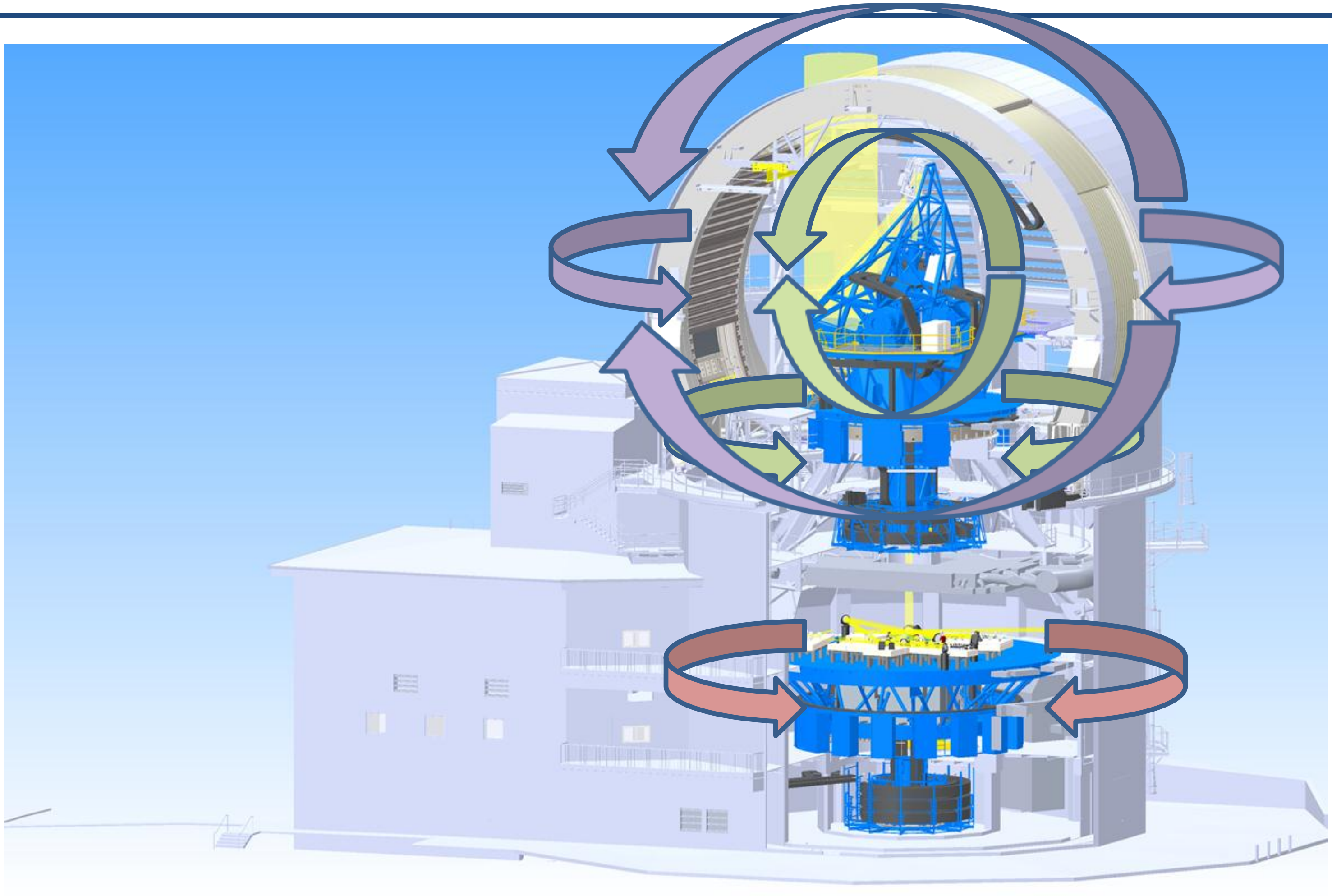
Applicable Codes and Requirements

- 29 CFR 1910 Occupational Safety And Health Standards (OSHA)
- NFPA 79 Electrical Standard For Industrial Machinery
- ANSI/RIA R15.06 Industrial Robots and Robot Systems - Safety Requirements

Industrial Robot

- “An automatically controlled, reprogrammable multipurpose manipulator programmable in three of more axes which may be either fixed in place or mobile for use in industrial applications.”

Multi-axis



The Three Laws of Robotics

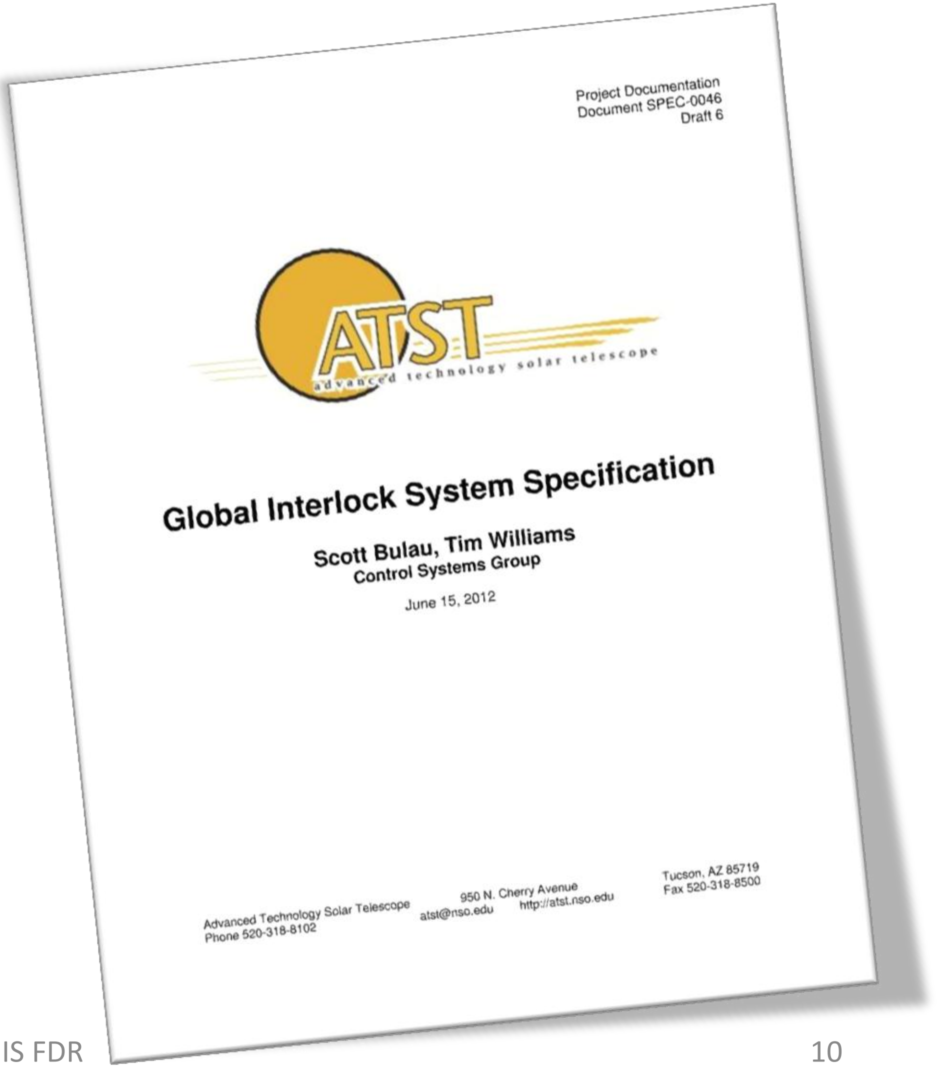
1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.
2. A robot must obey the orders given to it by human beings, except where such orders would conflict with the First Law.
3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.

Global Interlock System

- “The GIS provides a redundant, stand-alone safety mechanism for personnel and equipment.”
  - Redundant: in addition to any safety functions implemented by the subsystem.
  - Stand-alone: separate and independent of the subsystem’s control system.

Design Specification

- ATST SPEC-0046



Project Documentation
Document SPEC-0046
Draft 6

Global Interlock System Specification

Scott Bulau, Tim Williams
Control Systems Group

June 15, 2012

Advanced Technology Solar Telescope
Phone 520-318-8102

950 N. Cherry Avenue
atst@nso.edu http://atst.nso.edu

Tucson, AZ 85719
Fax 520-318-8500

General Functional Requirements

- Provide control reliable safety functions
- Provide an Emergency Stop complementary safety function
- Provide continuous status of the GIS to the operator and the Observatory Control System (OCS).

What the GIS is not

- *It is not the responsibility of the GIS to maintain the status or general health of the subsystems or the facility. This is the responsibility of the individual subsystems controllers. The GIS is only concerned with the safety aspects of the subsystems.*

Control Reliable

- “Control reliable safety circuitry shall be designed, constructed and applied such that any single component failure shall not prevent the stopping action of the robot.”
- [A]nd include automatic monitoring at the system level
  - The monitoring shall generate a stop signal if a fault is detected. A warning shall be provided if the hazard remains after the cessation of motion;
  - Following detection of a fault, a safe state shall be maintained until the fault is cleared.
  - Common mode failures shall be taken into account when the probability of such a failure occurring is significant.
  - The single fault should be detected at time of failure. If not practicable, the failure shall be detected at the next demand upon the safety function.

Redundancy

Emergency Stop System

Architecture

Hard-wired

- Difficult to develop
- Difficult to maintain
- Limited distances

Programmable Network

- Easy to expand/modify
- Self-diagnostic
- Long distances possible

General Aspects

- Distributed
  - Subsystems located throughout observatory
  - Sensors in remote locations
- Programmable
  - Customizable for our unique environment
- High Reliability
- High Availability
- Meets or exceeds consensus standards

Safety Programmable Controller

- Safety-rated Allen-Bradley GuardLogix® Programmable Automation Controllers (PAC)
  - Based on ControlLogix series
- Safety-rated Guard I/O modules
- Safety-rated sensors
- Safety-rated control devices

GuardLogix PAC

- Full-function PAC that also provides safety control
- Dual processor solution for 1oo2 safety achieves SIL 3, CAT 4, PLe.

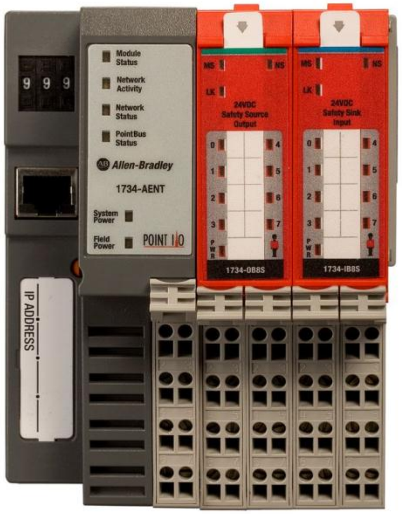
- Safety Task with restricted set of features and functions and TÜV-certified safety-specific instructions

Guard I/O Modules

- Provide integrated pulse testing
  - – Detect short circuits
    - 24V or GND
    - Between channels
  - – Detect wire continuity
- Detect discrepancies of dual channel inputs
- Detect loss of network connectivity
- Defaults to safe state in event of failure

Types of I/O modules

- Safety-rated Guard I/O modules
  - POINT I/O
    - Expandable
    - Configurable
    - Higher density
  - CompactBlock I/O
    - All-in-one design



Distributed System

- Independent Zones
  - Optical Support System
  - Telescope Mount Assembly
  - Coudé Floor
  - Instrumentation
  - Enclosure Thermal Control
  - Enclosure Motion Control
  - Facilities

Local Interlock Controller (LIC)

- One per zone
- A GuardLogix PAC safety controller and its partner controller
- A ControlLogix backplane and power supply
- An Ethernet bridge module for communication with the other GIS components

Global Interlock Controller (GIC)

- Only one in entire GIS
- A GuardLogix PAC safety controller and its partner controller.
- A ControlLogix backplane and redundant power supply.
- Two Ethernet bridge modules for communication with the GIS safety network and the OCS.

ATST advanced technology solar telescope

Independent Safety Network

GIS Review

- A distributed group of devices working together to form an overall safety system
- Safety-rated Allen-Bradley GuardLogix® Programmable Automation Controllers (PAC)
- Safety-rated I/O modules
- Safety-rated sensors
- Safety-rated control devices

Independent Safety Network

- TÜV approved safety protocol
- Redundant independent safety network
  - Redundant ring topology
  - Isolated from other networks
  - Virtual LANs

Common Industrial Protocol

- The Common Industrial Protocol (CIP™) encompasses a comprehensive suite of messages and services for the collection of manufacturing automation applications – control, safety, synchronization, motion, configuration and information.
- Network Independent
  - Ethernet, controlnet, devicenet,

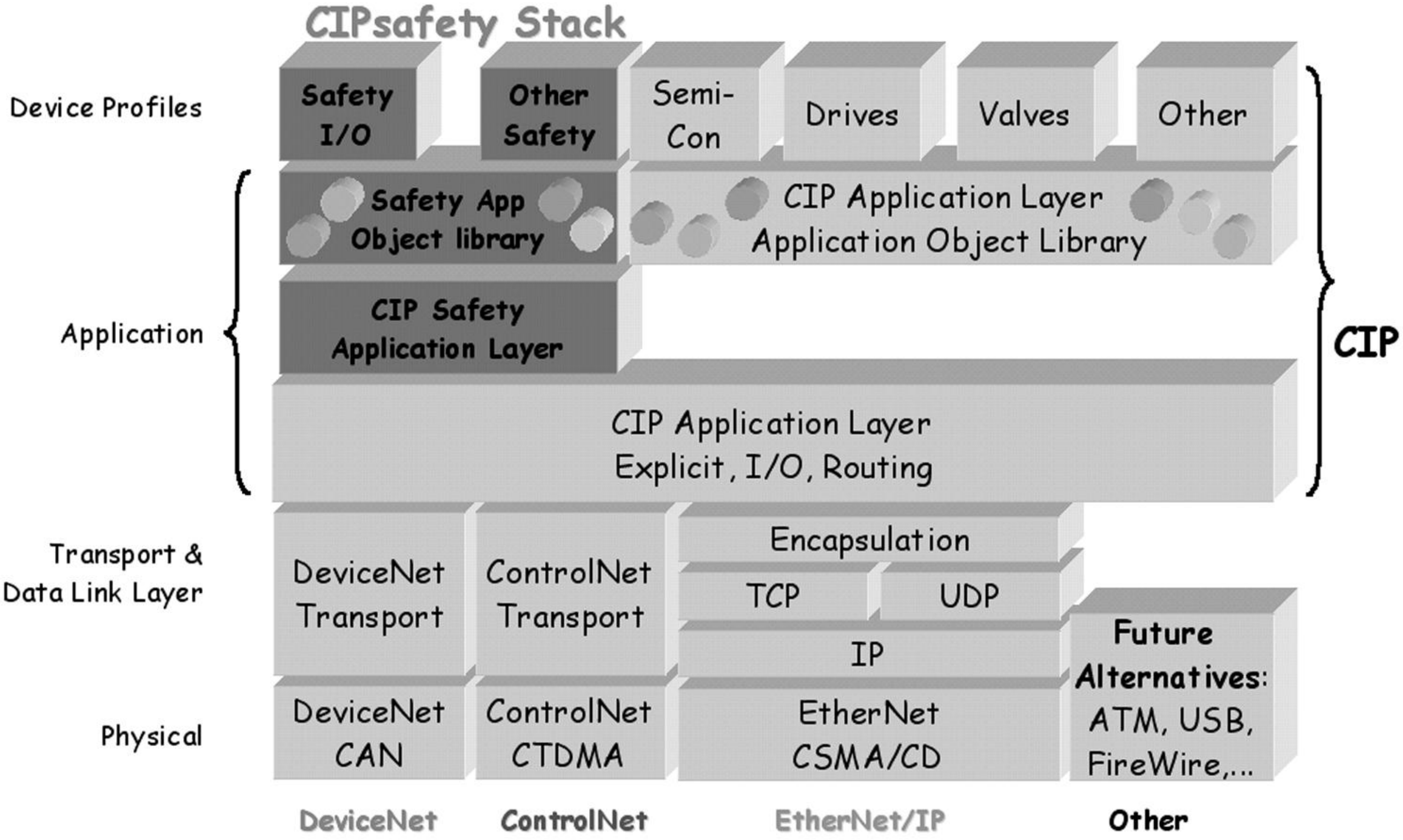
CIP Safety

- TÜV approved extension to Standard CIP
  - Time expectation via timestamp
  - Production Identifier
  - Safety CRC (Cyclic Redundancy Check)
  - Redundancy and Crosscheck
  - Diverse Measures for Safety and Standard CIP

Short Data Section					Time Stamp Section	
Actual Data	Mode Byte		Actual CRC	Comp. CRC	Data	CRC
1-2 Bytes			CRC-S1	CRC-S1	Time Stamp	CRC-S1

Long Data Section						Time Stamp Section	
Actual Data	Mode Byte		Actual CRC	Complemented Data	Comp. CRC	Data	CRC
3-250 Bytes			CRC-S1	3-250 Bytes	CRC-S1	Time Stamp	CRC-S1

OSI Model


CIPsafety Stack
Device Profiles
Safety I/O
Other Safety
Semi-Con
Drives
Valves
Other
Application
Safety App Object library
CIP Application Layer Application Object Library
CIP Safety Application Layer
CIP Application Layer Explicit, I/O, Routing
CIP
Transport & Data Link Layer
DeviceNet Transport
ControlNet Transport
Encapsulation
TCP
UDP
IP
Future Alternatives: ATM, USB, FireWire,...
Physical
DeviceNet CAN
ControlNet CTDMA
EtherNet CSMA/CD
DeviceNet
ControlNet
EtherNet/IP
Other

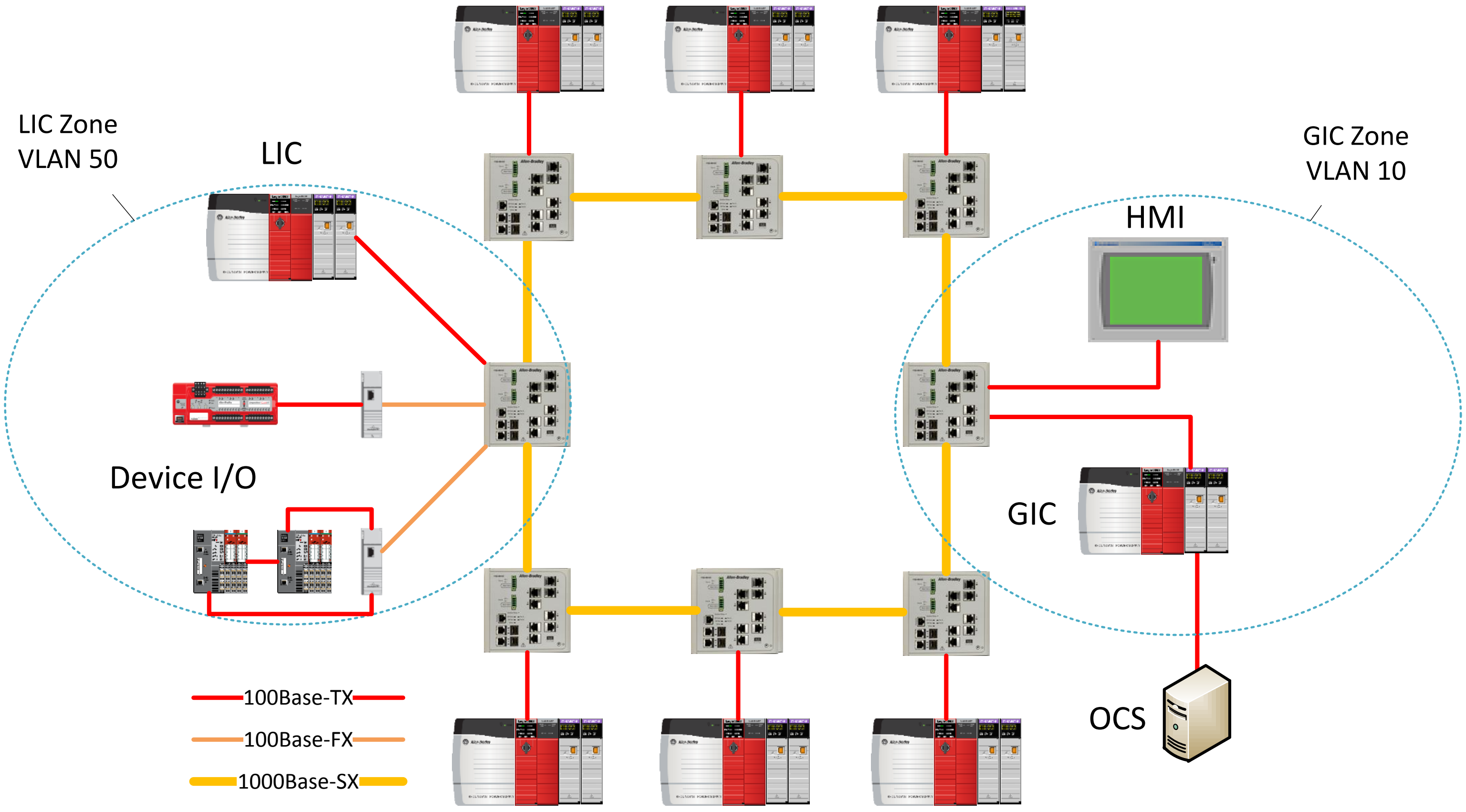
Ethernet / IP

- Uses existing IEEE standards (IEEE 802.3) for Ethernet physical and data link layers
- TCP and UDP connections

Independent Safety Network

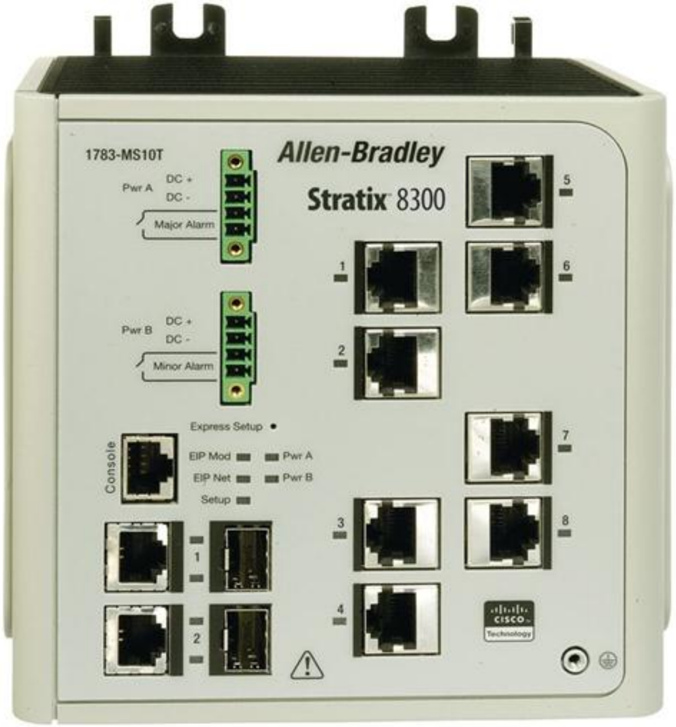
- Eight Stratix 8300 Level 3 managed switches
  - One for each zone plus one for the GIC
- Redundant ring topology using 1Gb fiber optics (1000Base-SX)
- Additional Device Level Rings using 1783-ETAP and embedded switches

Network Topology



Stratix 8300

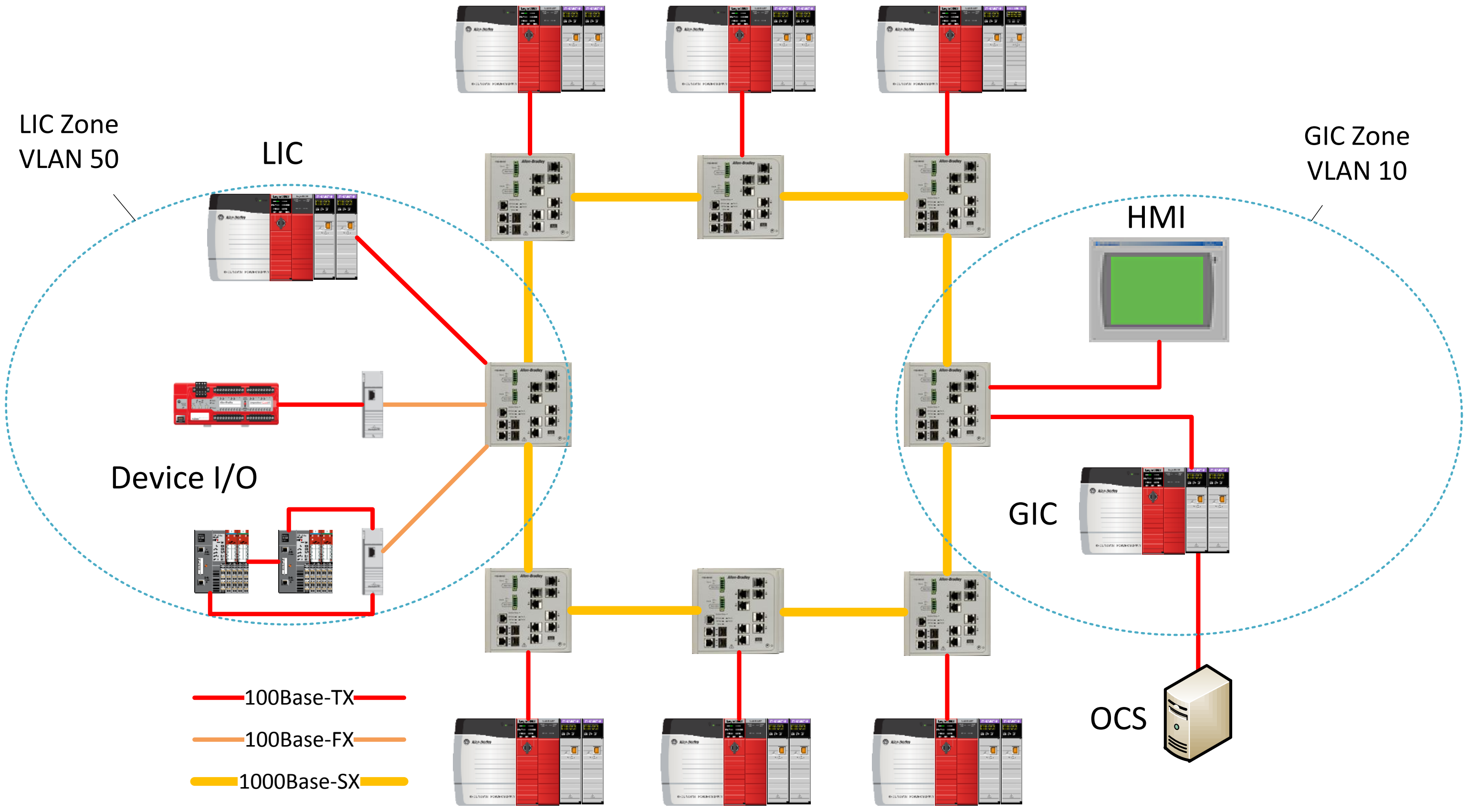
- Layer 3 Industrial Ethernet Switch
- Cisco IOS
- 2 uplink ports
- 8 data ports (expandable to 24)



Ethernet Media

- 1000Base-SX Multimode Fiber Optic
  - – Between network switches
- 100Base-FX Multimode Fiber Optic
  - – From network switch to Ethernet tap
- 100Base-TX CAT 5e UTP
  - – From network switch to remote I/O
  - – From Ethernet Tap to remote I/O

Network Topology



Virtual LANs

- Each zone will be isolated as a virtual LAN
- One network switch will be configured for spanning traffic.

Subsystem	VLAN	Addresses
GIS	10	x.y.1.0/24
OSS	20	x.y.2.0/24
Mount Base	30	x.y.3.0/24
Coudé floor	40	x.y.4.0/24
Instrumentation	50	x.y.5.0/24
Enclosure Thermal	60	x.y.6.0/24
Enclosure Motion	70	x.y.7.0/24
Facilities	80	x.y.8.0/24

Reaction Time

- Goal: reaction time ≤ 200mS
- AB Safety Estimator tool
  - Best case 32mS
  - Worst case 122ms
  - Single fault/delay 176mS
- Prototype
  - Typically 45-70mS

Local Interlock Controllers

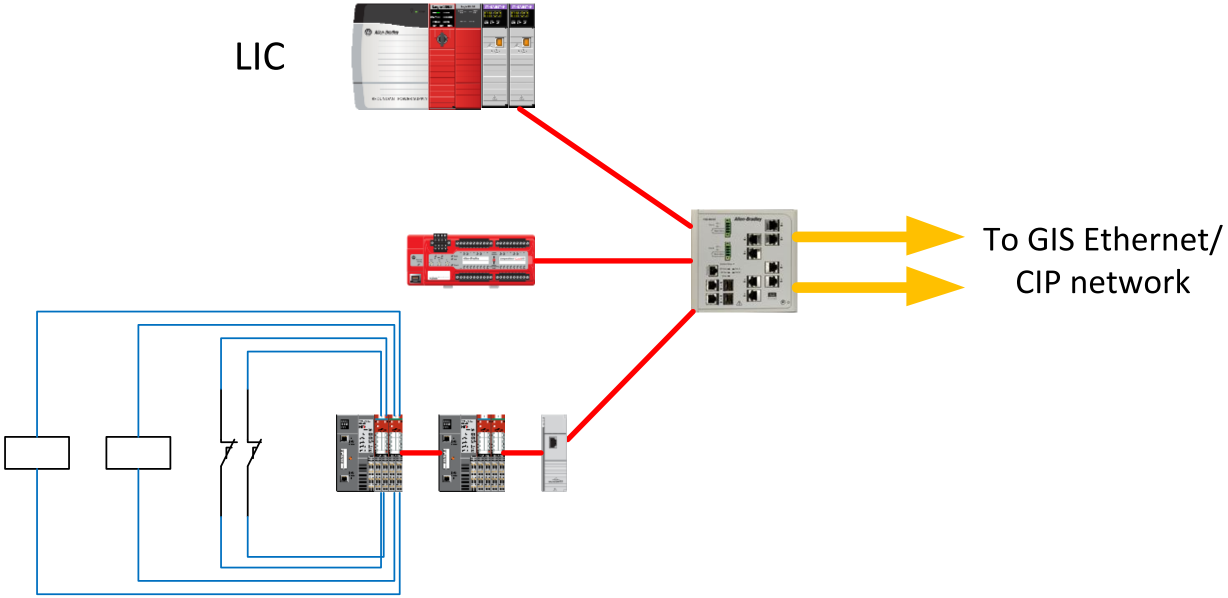
Local Interlock Controller

- One per zone
- A GuardLogix PAC safety controller and its partner controller.
- A ControlLogix backplane and power supply.
- An Ethernet bridge module for communication on the Independent Safety Network

LIC Functions

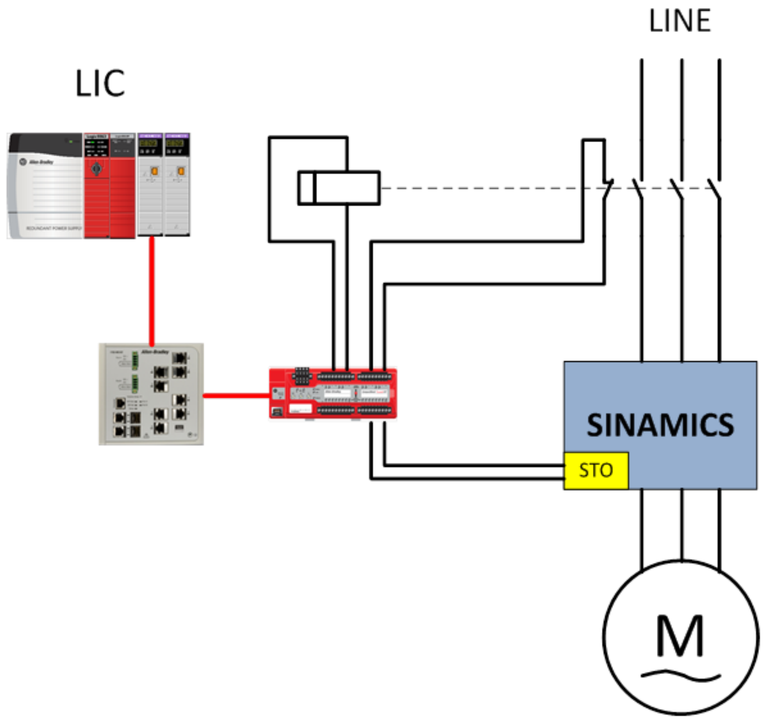
- Monitor safety I/O of the subsystem
- Communicate status of subsystem with the GIC
- Apply interlocking safety functions based on local safety I/O and status received from GIC

Typical Remote I/O Arrangement



Example Drive for SIL3

- Siemens Sinamics S700
  - SIL 2 Rated
- Redundant Safety Function
  - Pulse Blocking
  - Power Removal



Global Interlock Controller

Global Interlock Controller

- Only one in entire GIS
- A GuardLogix PAC safety controller and its partner controller.
- A ControlLogix backplane and redundant power supply.
- Two Ethernet bridge modules for communication with the Independent Safety Network and the OCS.

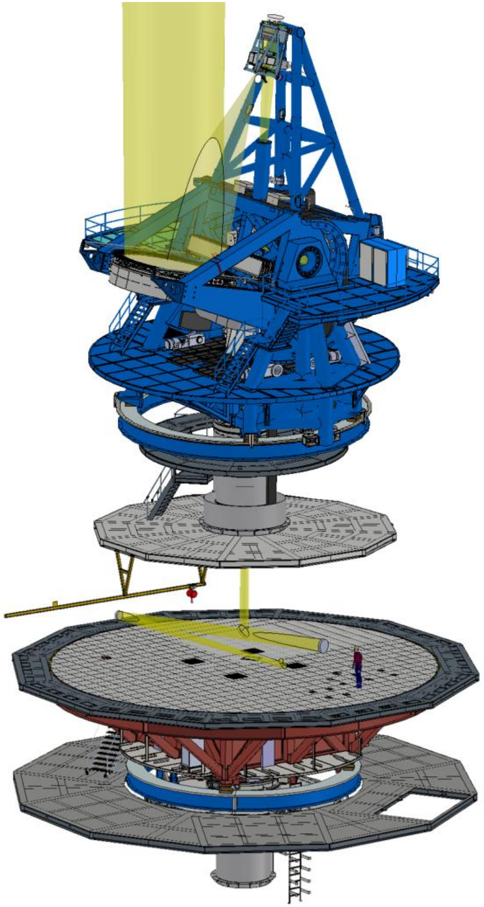
GIC Functions

- It provides the coordination of safety functions between all subsystems and applies global safety functions.
- It provides the status of the entire GIS to the OCS and all HMI

Global Safety Functions

- Emergency Stop
- Fire Alarm
- Seismic Alarm

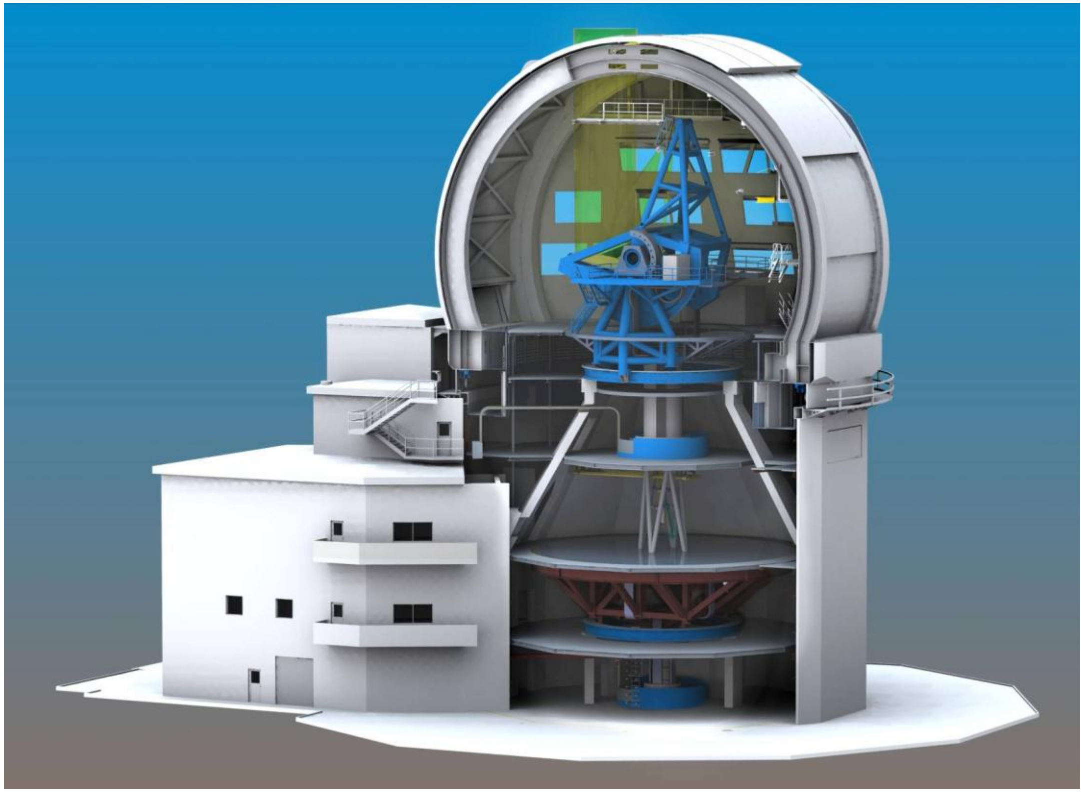
E-stop Locations on TMA



- Sides telescope mount
- Mount platforms +X, -X
- M2 assembly
- On OSS (near Gregorian focus)
- Fixed locations on pier, coudé floor
- Opposite sides mezzanine level
- Rotator structure, mezzanine level
- Inside pier at ground level, coudé AZ wrap

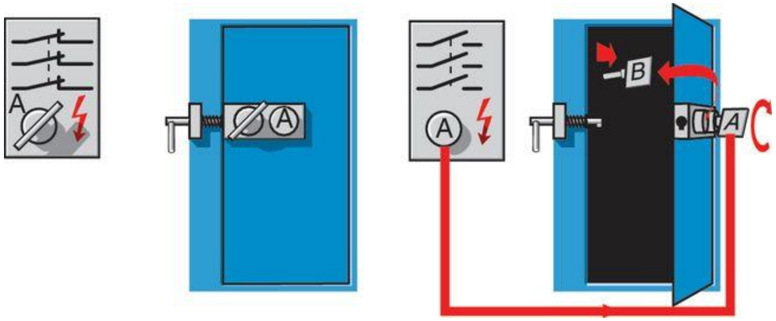
E-stop Locations on Enclosure & Operations Building

- Carousel entrance aperture
- Rear access door, in/out
- Bridge crane pendant
- Level access doors
- +X, -X Upper access platforms
- TEOA access platform
- X, Y Shutter drives, back/front
- Bogie inspection area
- AZ utility transfer system, front/back
- Control room
- Instrument prep lab



Trapped Key System

- Control Interlocking
  - Removing key disables hazardous motion
    - Key can then be used to enter a hazardous area, or
    - used to enable contradictory or limited motion
  - Does **not** remove hazardous energy
    - OSHA lockout/tagout alternative means for minor servicing only.



System Interconnects

- UPS Power
  - Generator back-up
- Coolant
  - T_a -4 for electronics racks

GIS Hazard Analysis

- Hardware Failure
- Programming Error
- System Integrity
- Hazardous Voltages

Hardware Failure

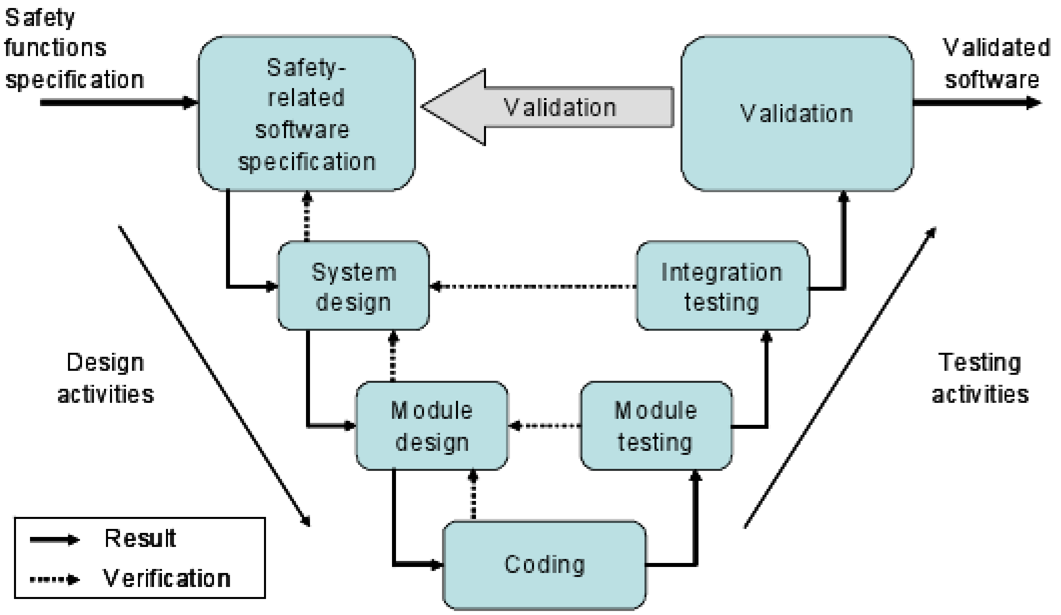
- High-reliability safety-rated components
  - Mean time to dangerous failure ($MTTF_d$)
- Diagnostic coverage
  - Self-monitoring
  - Plausibility testing
- Good engineering practice
  - Installation per manufacturers specifications

Control Software

- Developed using RSLogix 5000, version 19
- Ladder Logic
  - Limited Variability Language
- GuardLogix Safety Application Instruction Set
  - Safety-certified subset of standard ladder logic
- Software V-model

Development Model

Development model: simplified V-model
Objective: readable, comprehensible, testable and maintainable software



System Integrity

- Physical Security
- Network Security
- Computer Hardening
- Application Security
- Device Hardening

Network Security

- Only components of the GIS will be connected to the Independent Safety Network
  - MAC filtering
  - Block-out and Lock-in devices will be used
- Configuration will password protected
- Default configurations (addresses, ports, VLANs, etc.) will not be used

Verification and Validation

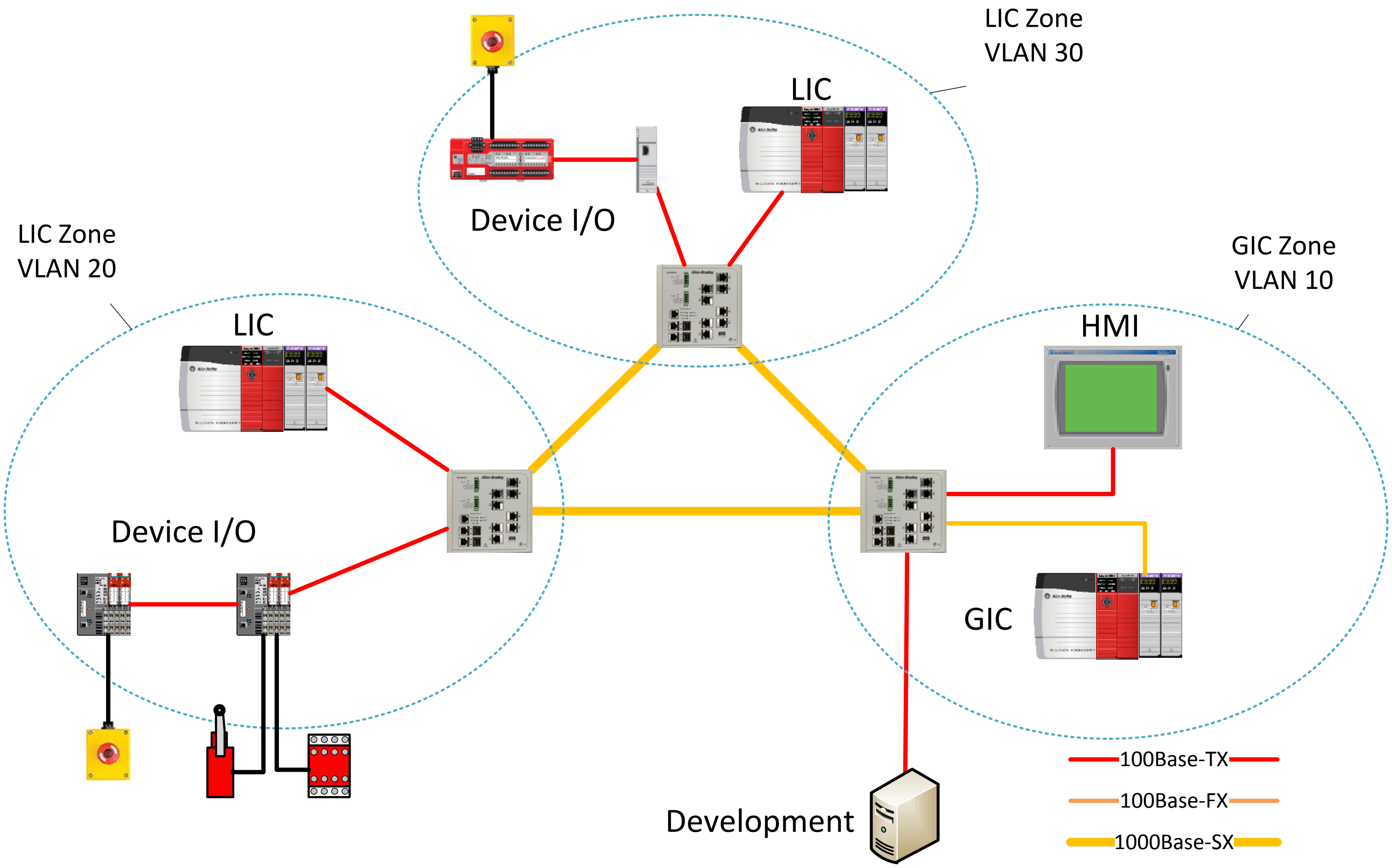
- Functional Verification
- Project Verification
- Safety Validation

Maintenance Plan

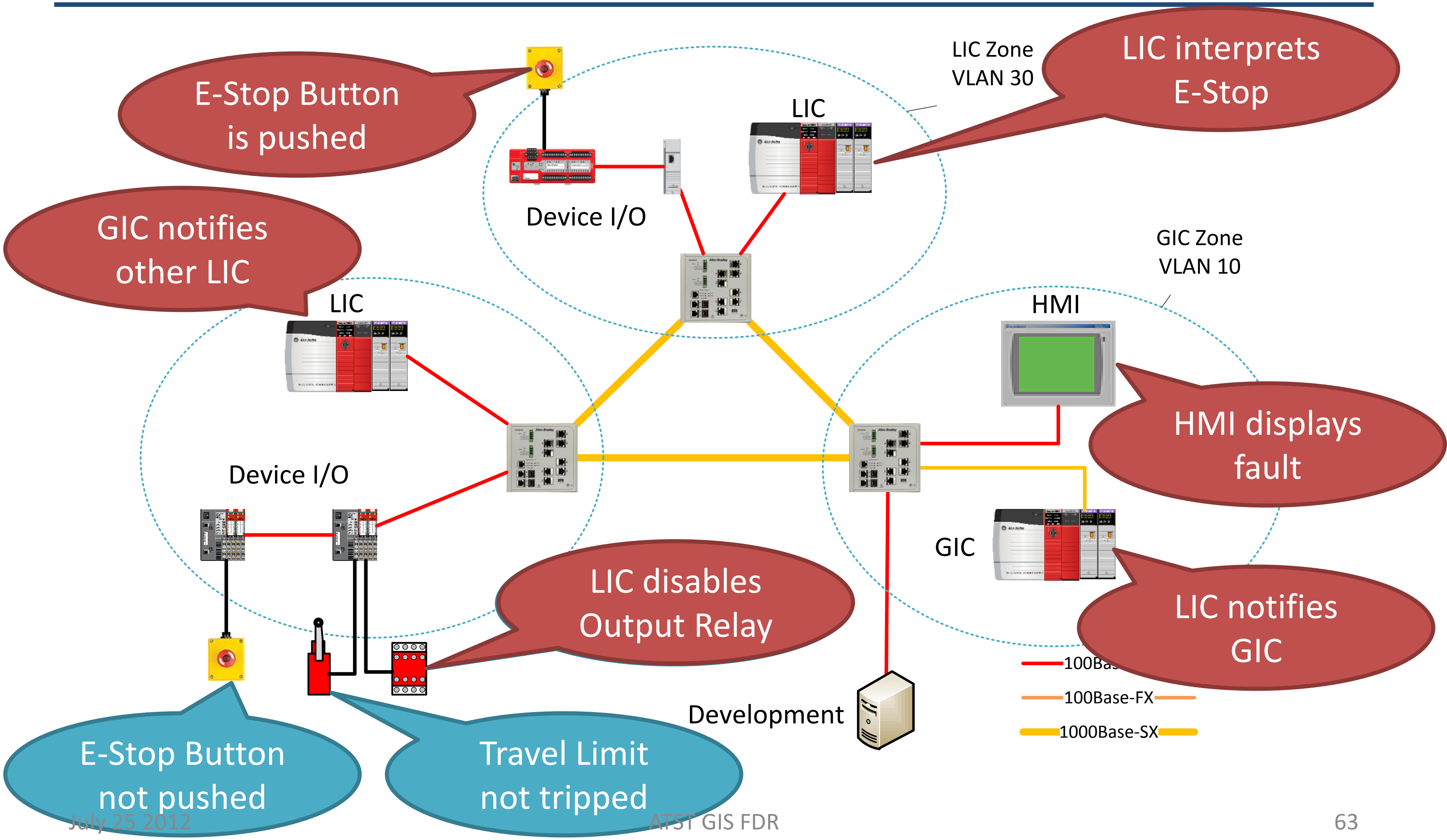
- Connecting a computer
- Patch Management
- Replacing a failed component
- Changes to control programs
- By-passing an interlock

GIS Testbed

GIS Prototype



GIS Prototype



E-Stop Button is pushed

LIC interprets E-Stop

GIC notifies other LIC

HMI displays fault

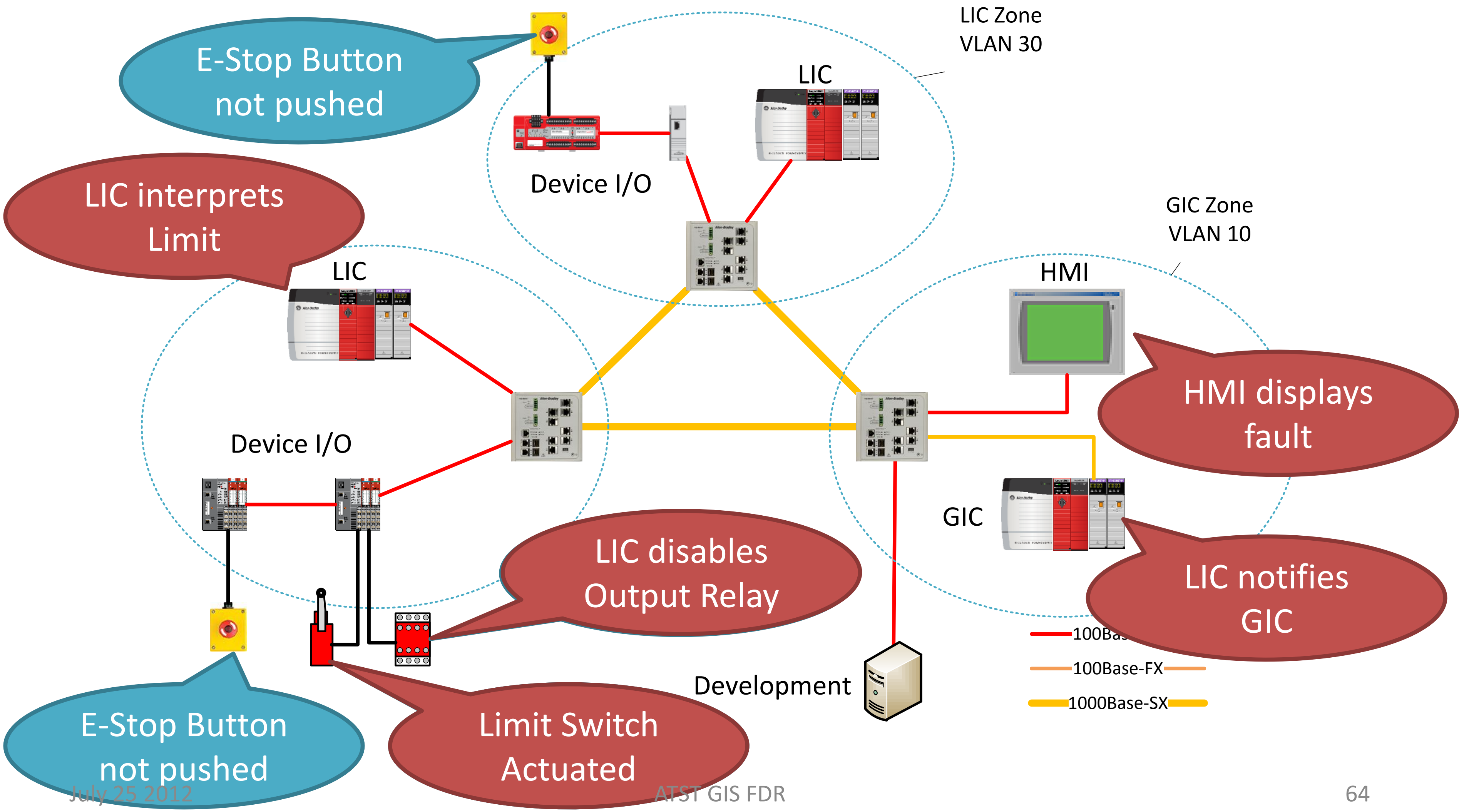
LIC disables Output Relay

LIC notifies GIC

E-Stop Button not pushed

Travel Limit not tripped

GIS Prototype



E-Stop Button not pushed

LIC interprets Limit

HMI displays fault

LIC disables Output Relay

LIC notifies GIC

E-Stop Button not pushed

Limit Switch Actuated

Why Automation Safety?

Why Automation Safety?