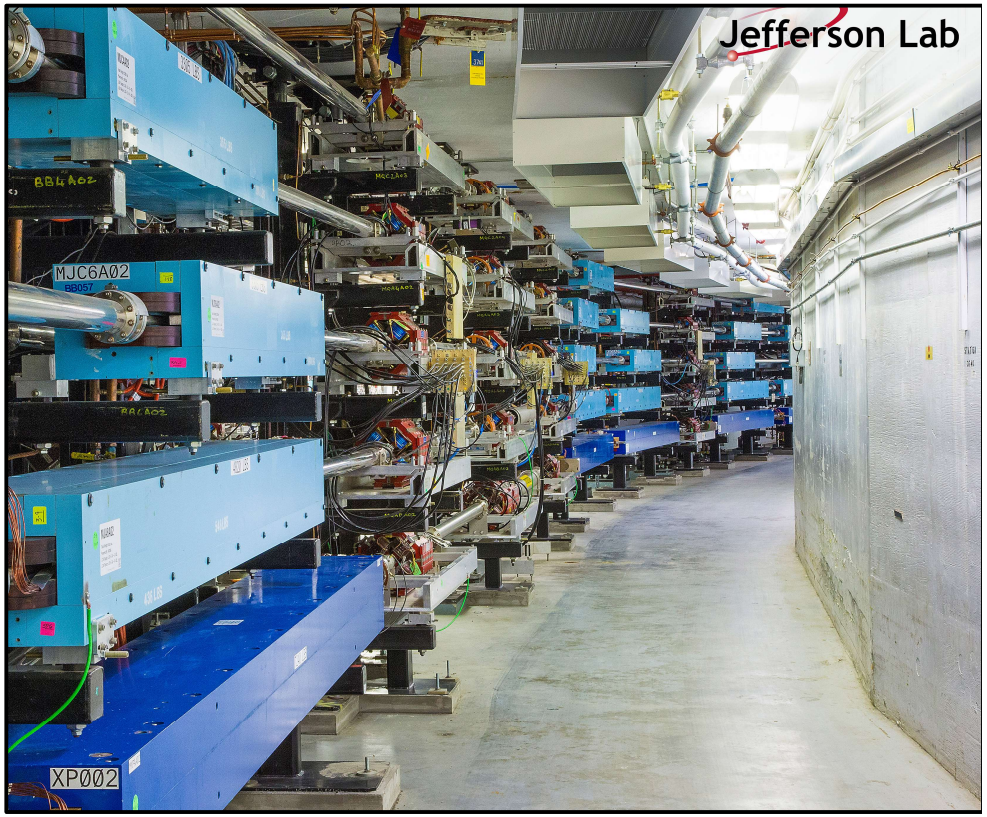
ASW 2021: Advanced Technology and Methods for Accelerator Activities

CEBAF Personnel Safety System Upgrades @ Jefferson Lab



Paul Metcalf

Wednesday, October 6, 2021
1244 – 1306 CST

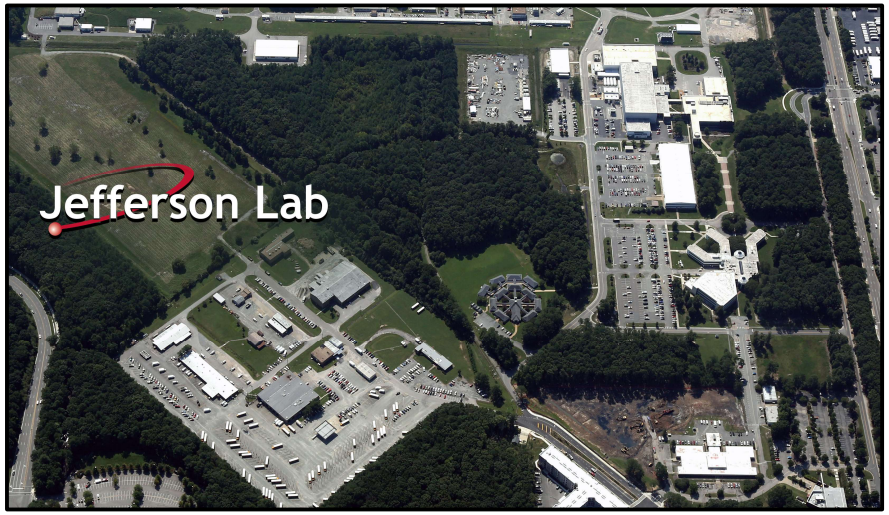
Jefferson Lab

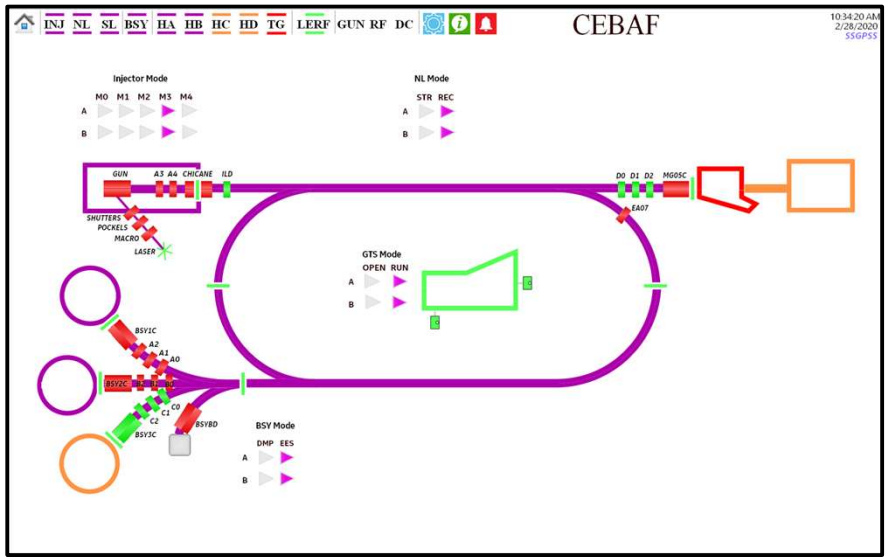
U.S. DEPARTMENT OF ENERGY | Office of Science

JSA

Introduction

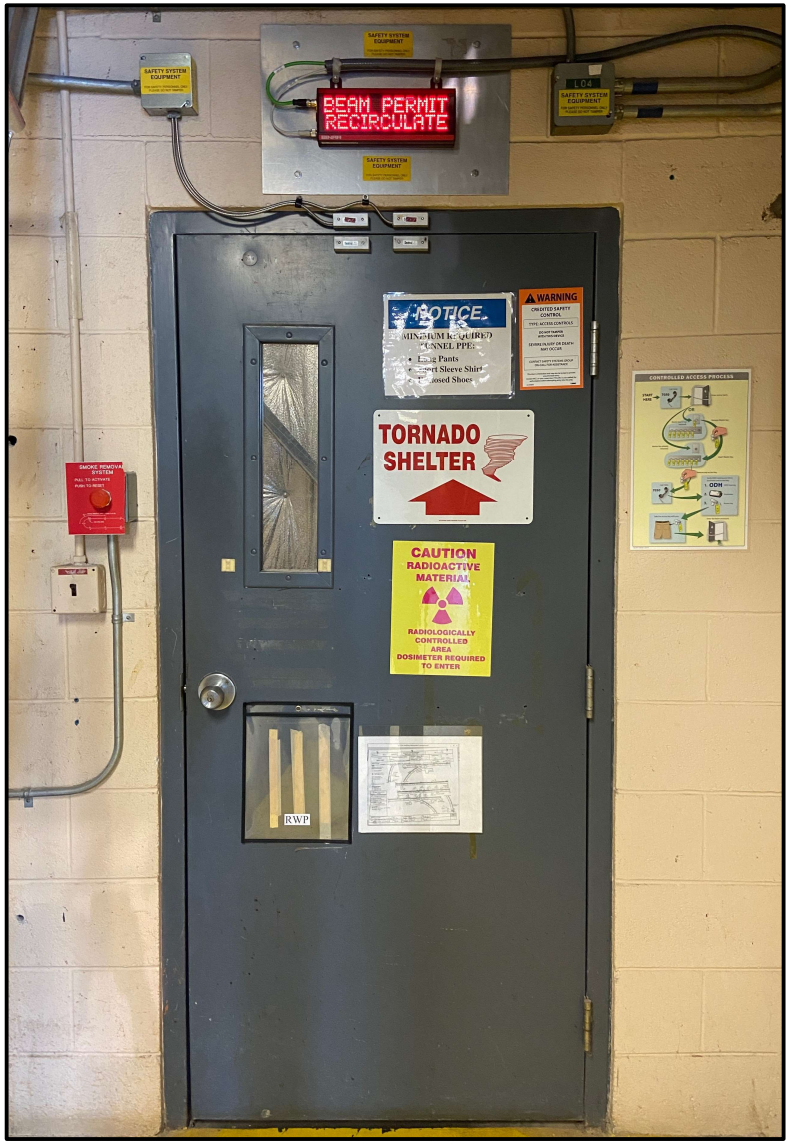
- Jefferson Lab operates the Continuous Electron Beam Accelerator Facility (CEBAF)
  - Circa 1995
  - Since upgraded to 12 GeV in 2012
- JLab aiming to increase CEBAF availability while at the same time address aging infrastructure
  - Significant investments being made to renew systems and address obsolescence.
- JLab Safety System Group (SSG) manages the engineered safety systems at CEBAF
  - Jerry Kowal (Group Leader)
  - Roger Araiza
  - Savvy Anbazhagan
  - Gabriela Aguilar
  - Paul Metcalf
  - Scott Bruhwell
  - Lawrence Hurt
  - Mike Beizer





Scope of Personnel Safety System

- Personnel Safety System
  - Electrical hazards
  - Beam transport to occupied segment
  - Protection of beam containment components
  - High radiation in occupied areas
    - Due to operation of beam or high power RF
- Machine Protection System
  - Beam loss within secured area
  - High radiation within secured area
  - Protection of beamline components
    - Excluding beam stoppers
- Beam Over Power
  - Beam Energy Limiting System
- Oxygen Deficiency Hazard
  - ODH Annunciation System (Administrative)
- Access to Low Oxygen Area
  - Training (Administrative)
- Access to High Radiation Area
  - RADCON, Training (Administrative)
- Laser Exposure Hazard
  - Local hard-wired interlocks



Jefferson Lab

Hazard Identification and Risk Reduction

- Hazard Analysis Review
  - CEBAF hazards are quite well understood from 20+ years of operation
  - PSS upgrade is not driven by safety deficiencies or new hazards/requirements
  - All extant safety functions maintained or improved
  - Hazard analysis mainly focused on the potential to introduce new hazards
- Other hazards, initiating events or contributors which were re-reviewed included
  - Annunciation of status of hazards
  - Medical emergency within PSS controlled segment
  - Fire within PSS controlled segment
  - Tornado
  - MCC unoccupied during shutdowns
- Some improvements to hardware and software design were identified and are being implemented

Overall PSS Safety Functions

- Existing documentation and requirements were reviewed thoroughly
- 16 Overall Safety Functions were identified which are now summarized
  - Hundreds of lower level requirements
- Access Control
  - OSF-01: Facilitate inspection of the accelerator enclosure to ensure all personnel are vacated prior to securing the enclosure
  - OSF-02: Prevent access to the accelerator enclosure when there exists an internal hazard to personnel safety
  - OSF-03: Shutdown the accelerator when a hazard to personnel safety exists due to an access control violation (separation of people from beam)
  - OSF-04: Allow disabling of access control system maglocks from within the accelerator to facilitate emergency exits
  - OSF-05: Allow access to the accelerator enclosure whenever required to mitigate an emergency
- Hazard Annunciation
  - OSF-06: Provide audible and visual warnings within the accelerator enclosure prior to transitioning to a powered state
  - OSF-07: Provide audible and visual warnings within the accelerator enclosure when hazards are present in unsecure areas
  - OSF-08: Display the status of accelerator hazards at external entry points and control centers

Overall PSS Safety Functions

- Personnel Safety
  - OSF-09: Maintain personnel safety inside the accelerator enclosure when the access control system allows access
  - OSF-10: Provide easily accessible emergency stop pushbuttons within the accelerator enclosure and at external control centers which can be used to make the accelerator safe
- Beam Containment
  - OSF-11: Shutdown the accelerator when a hazard to personnel safety exists due to loss of beam containment (separation of beam from people)
  - OSF-12: Shutdown the accelerator when required to protect beam containment components
- Radiation Containment
  - OSF-13: Shutdown the accelerator if radiation levels in accessible areas exceed operating limits
  - OSF-14: Shutdown the accelerator when a hazard to personnel safety exists due to removal of non permanently fixed radiation shielding
  - OSF-15: Shutdown radiation generating systems/sub-systems/components (high power RF) if radiation levels in accessible areas exceed operating limits
  - OSF-16: Shutdown radiation generating systems/sub-systems/components (high power RF) when a hazard to personal safety exists due to loss of radiation containment systems

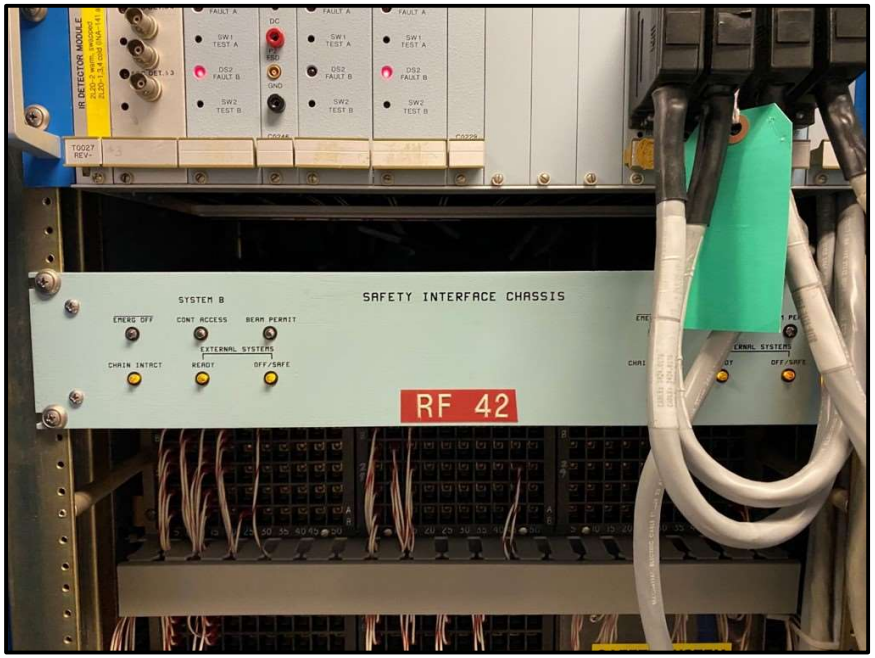
Mission, Scope and Timeframe

- Mission
  - Upgrade all CEBAF PSS PLC hardware to address obsolescence and reliability concerns
  - Extend PSS Proof Test Interval thereby improving beam time availability
- Scope
  - Replace all legacy PLC hardware
    - Includes
      - PLC's
      - I/O Interfaces
      - Power Supplies
      - Network Switches
    - Excludes
      - (Most) field I/O (sensors and actuators)
      - Uninterruptible Power Supplies
    - Some field I/O being upgraded on a case by cases basis
      - New IP based annunciator displays
      - Upgraded combined horns/sirens (24V)
      - Light curtains to replace door micro-switches inside fire door push to escape bar's
  - Opportunity to incorporate latest standards and best practices
    - Engineering according to IEC 61508
- Timeframe to complete is 4-5 years
  - Replacement hardware necessitates a complete software re-write
  - Installation work must be scheduled during major shutdowns
  - Recently completed Injector and North Linac segments
  - Approximately 50% completed

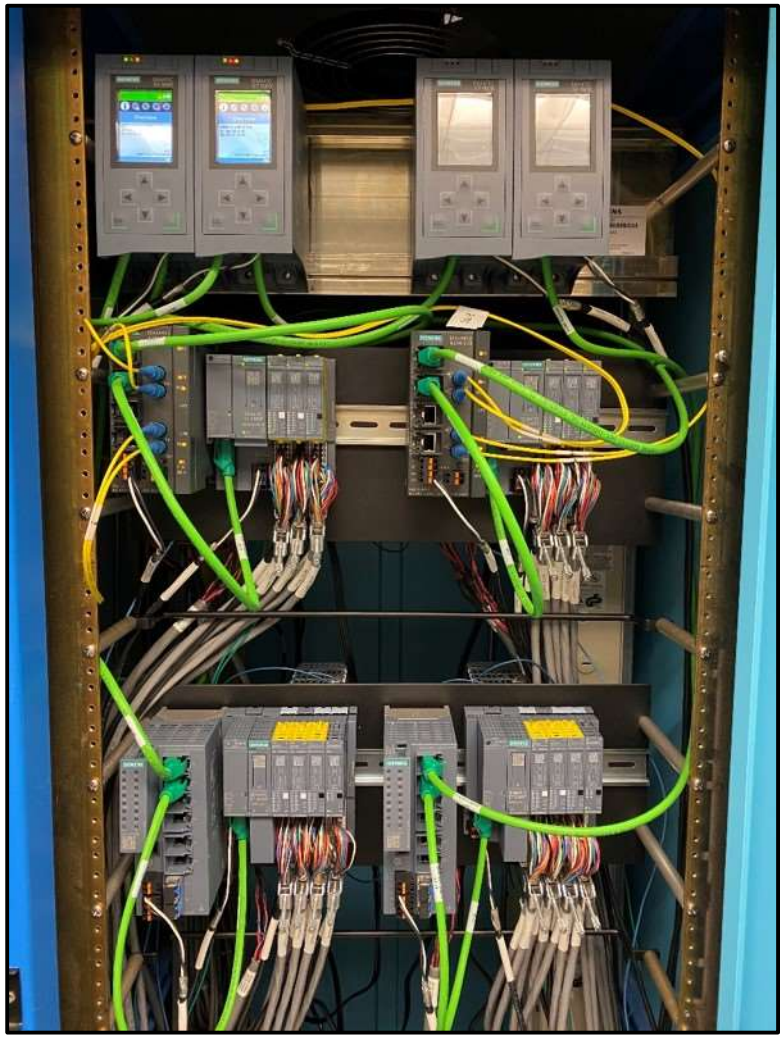
Mission 1: Replace PSS PLC Hardware

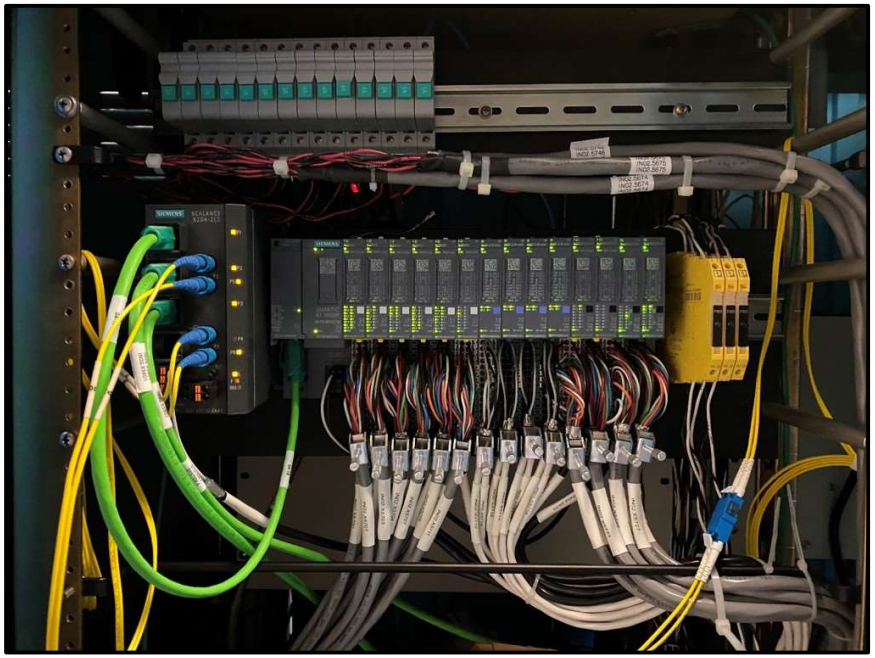
- Hardware Assessment
  - Legacy Hardware
    - Non-safety rated Schneider Modicon PLC's circa 1990's
    - Fieldbus Communication
      - Non safety rated Modbus+ over combination of older generation multi-mode fibers and Coax
  - First segments upgraded using Siemens S7 300 F CPU's
    - Has (with few exceptions) been reliable
- Replacement Hardware Selection
  - Redundant PLC's maintained on a per-segment basis
  - Siemens S7 1500 F series safety rated PLC's
  - Siemens ET-200 SP distributed I/O interfaces
  - Siemens modular power supplies and networking switches
  - Phoenix Contact safety relays used for relay outputs
  - Fieldbus and Inter-PLC communication
    - Safety rated Profinet communication over replacement single mode fibers and Cat 6A Ethernet

Old Hardware: CPU, I/O and Interface Chassis



New Hardware: CPU and Distributed I/O





New Hardware: Magnet / RF Interface Chassis

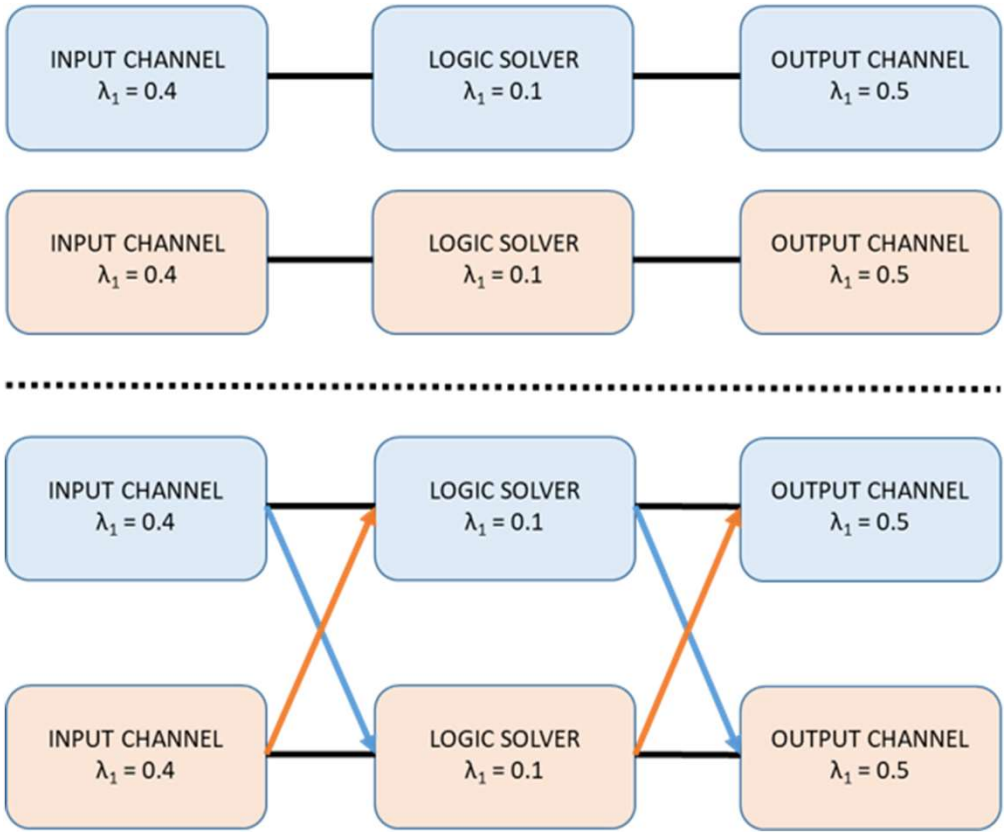
Mission 2: Extend Proof Test Interval

- Problem: Extending PTI will decrease safety
  - First we need to find ways to increase safety

$$PFD_{avg} = \frac{\lambda_{d_u}^2 T^2}{3}$$

- Options to Increase Safety and Availability
  - Install More Hardware (more I/O channels i.e. 2oo3, 2oo4)
    - Very high cost and high complexity
  - Install Better Hardware (i.e. more reliable hardware)
    - Very high cost but low complexity
  - Modify Existing Architecture and Install Diagnostics
    - Low cost and medium complexity
    - Minimal additional hardware required
      - Additional network switches and cables required
    - Requires
      - Inter-PLC Communication
      - Voting implemented in software
      - Programming of Diagnostic Alarms
- Revised architecture will improve safety hence provides additional risk reduction for the extant safety functions
  - Some but not all of this additional safety margin will be “consumed” by extending the Proof Test Interval
    - Win-Win: Improvements made to Reliability, Availability, Maintainability and Safety

Solution Part 1: Modernize Architecture



$$\lambda_G = (\lambda_1 + \lambda_2 + \lambda_3)^2$$

~2X

$$\lambda_G = (\lambda_1)^2 + (\lambda_2)^2 + (\lambda_3)^2$$

Solution Part 2: Add Diagnostics

- Original system did not allow for any diagnostics at all
  - Diagnostic coverage was essentially zero
  - This creates a high risk of Fault Accumulation
  - Also creates a high burden of Proof Testing
- Replacement system developed with online diagnostics and non-destructive testing as priorities
- With communication links installed between the redundant PLC, it is now possible to perform online diagnostics and implement fault control

$$PFD_G = 2.t_{CE}.t_{GE}.(\lambda_{DD} - \beta_D.\lambda_{DD} + \lambda_{DU} - \beta.\lambda_{DU})^2 + \beta_D.\lambda_{DD}.MTTR + \beta.\lambda_{DU}.\left(MRT + \frac{T}{2}\right)$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}.\left(\frac{T}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}.MTTR \qquad t_{GE} = \frac{\lambda_{DU}}{\lambda_D}.\left(\frac{T}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}.MTTR$$

- Examples
  - Redundant Channel Monitor
  - Beam Valve Monitor
  - Laser Shutter Monitor

Solution Part 2: Add Diagnostics

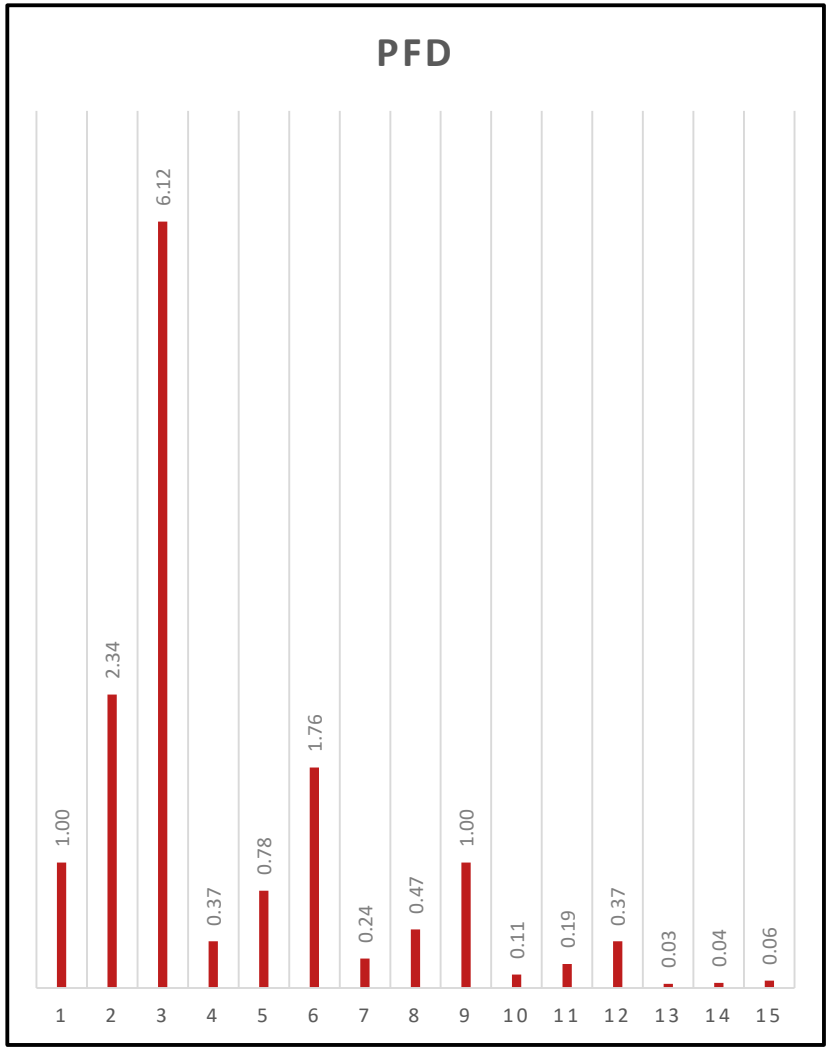
- Improving the Diagnostic Coverage Fraction makes a huge impact to safety by increasing the Safe Failure Fraction

$$DCF = \frac{\lambda_{D_d}}{\lambda_{D_d} + \lambda_{D_u}} \qquad SFF = \frac{\Sigma\lambda_S + \Sigma\lambda_{D_d}}{\Sigma\lambda_S + \Sigma\lambda_{D_d} + \Sigma\lambda_{D_u}}$$

- We are conservatively assuming only 60% coverage will be achieved but in reality we should achieve well over 75% coverage and probably over 90% coverage
- When combined with the architectural improvements made above, the additional diagnostics coverage will add significantly to the safety margins available
- These safety margins can be used to offset the planned extension to the Proof Test Interval
- Proof Testing need only detect faults which cannot be detected online. Future Proof Testing will be
  - Shorter In Duration
  - Less Frequent
  - Non Destructive

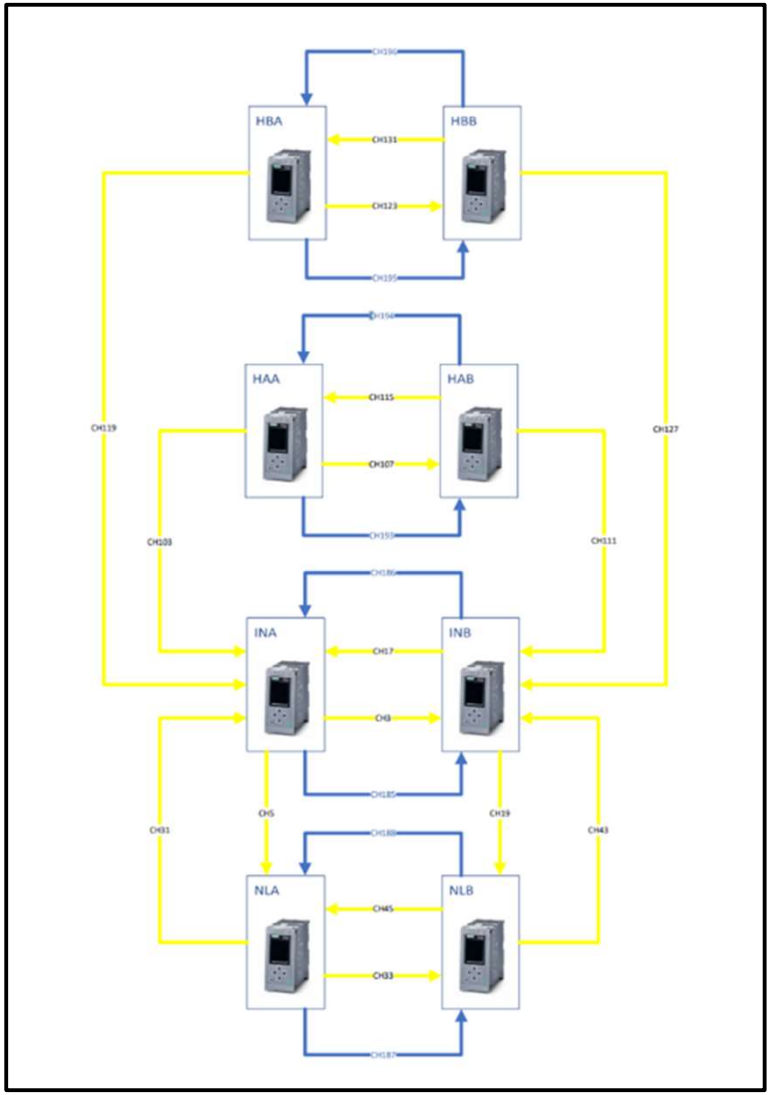
Effect of Diagnostics

DCF	SFF	ID	PTI	PFD
0%	60%	1	6	1.00
		2	12	2.34
		3	24	6.12
60%	84%	4	6	0.37
		5	12	0.78
		6	24	1.76
75%	90%	7	6	0.24
		8	12	0.47
		9	24	1.00
90%	96%	10	6	0.11
		11	12	0.19
		12	24	0.37
99%	99.6%	13	6	0.03
		14	12	0.04
		15	24	0.06

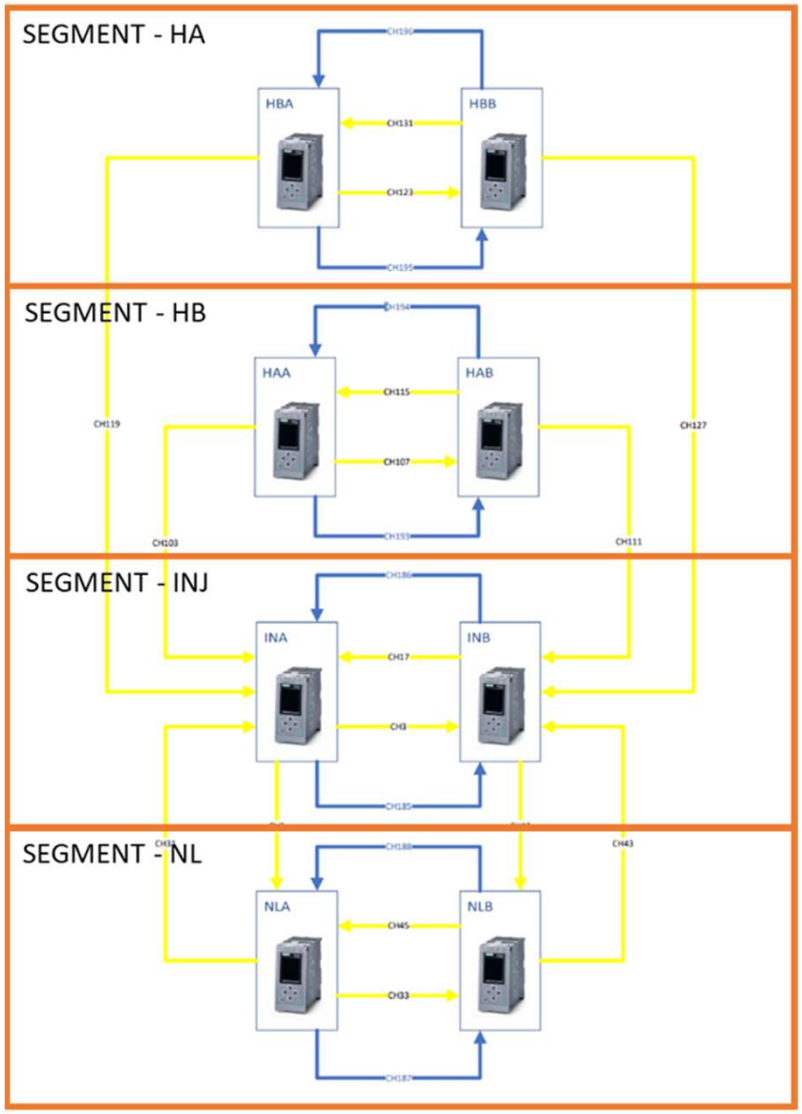


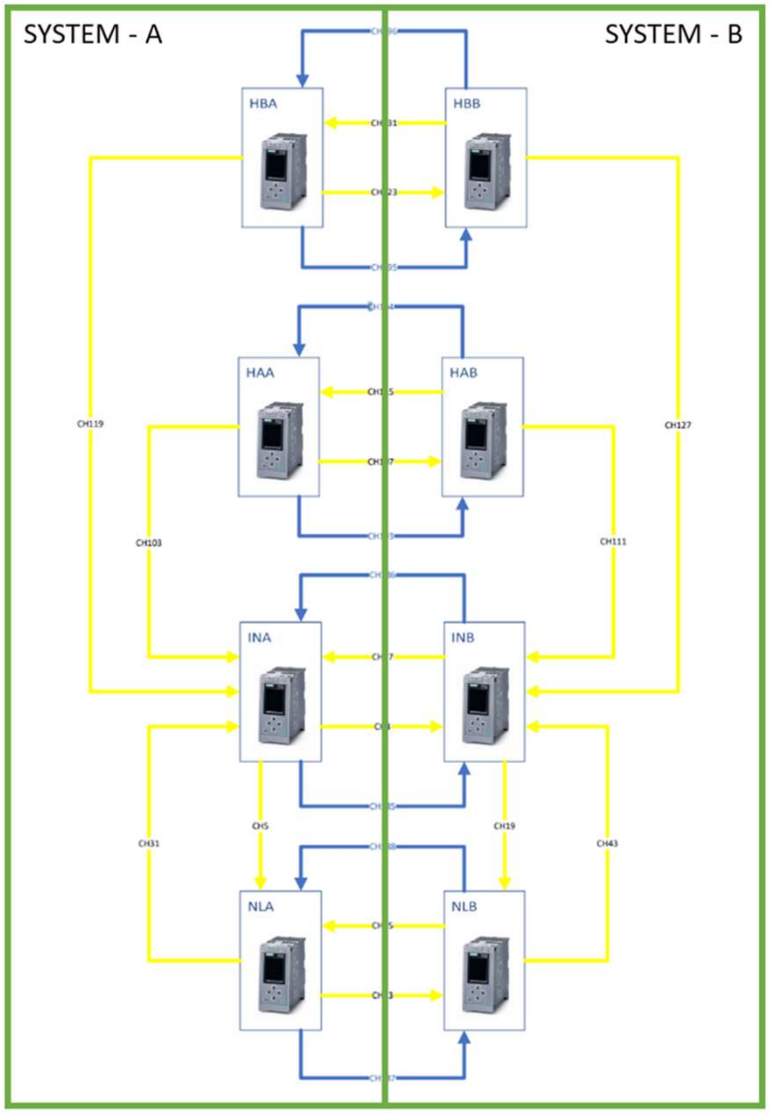
Networking Architecture

- Implementing Inter-PLC communication necessitated a re-design of the process network architecture
- The process network was divided into segments and systems. Communication is only possible for devices within the same segment or system
- Inter-PLC Communication is therefore allowed
  - Between systems within the same segment
  - Between segments within the same system
- Inter-System and Inter-Segment communication are functionally independent
  - Faults with Inter-Segment communication on System A cannot effect System B and vice versa
  - Similarly faults with Inter-System communication within a particular segment cannot effect any other segment
  - Furthermore communication between System A and System B is electrically isolated with fiber optics

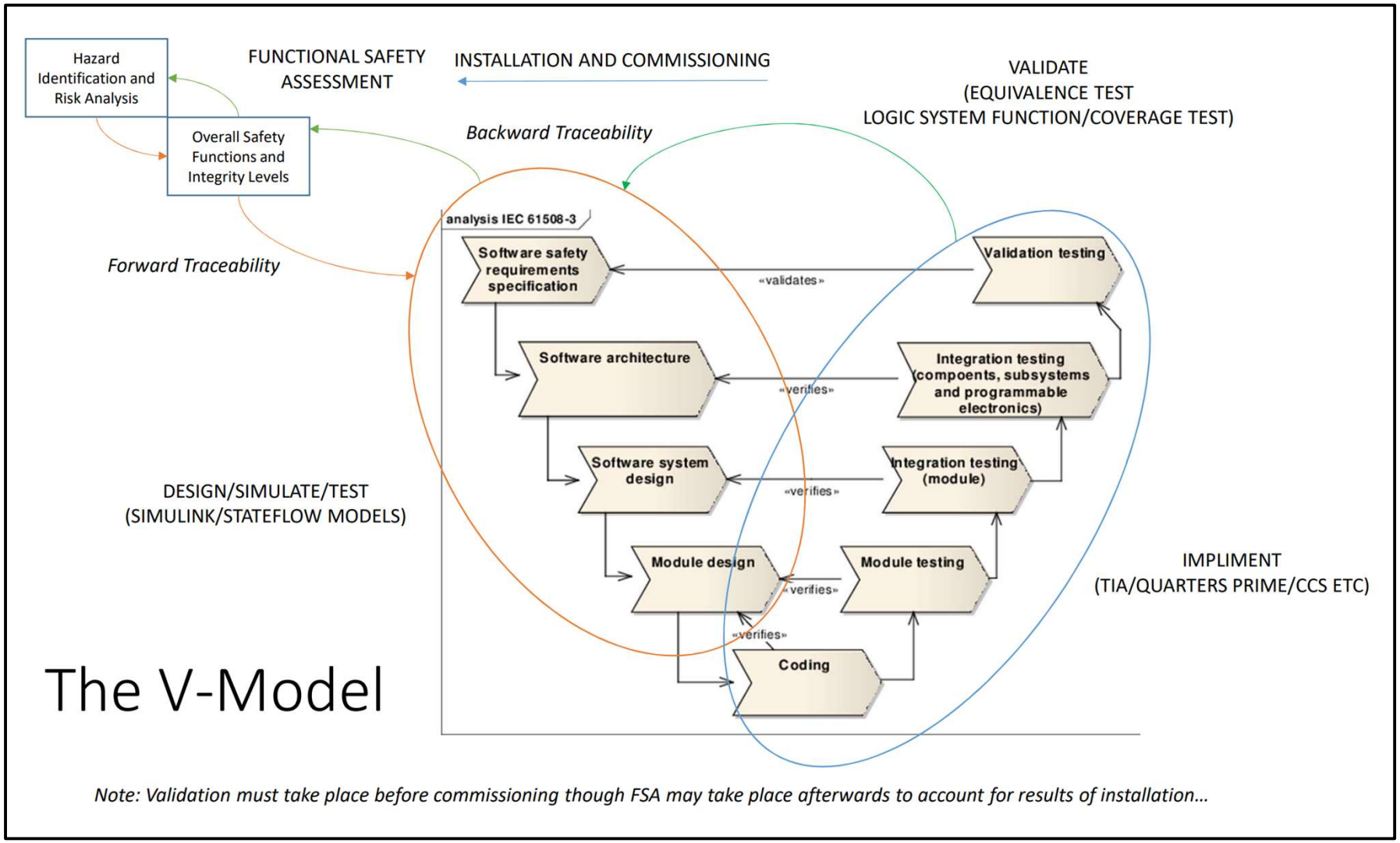


Networking Implementation



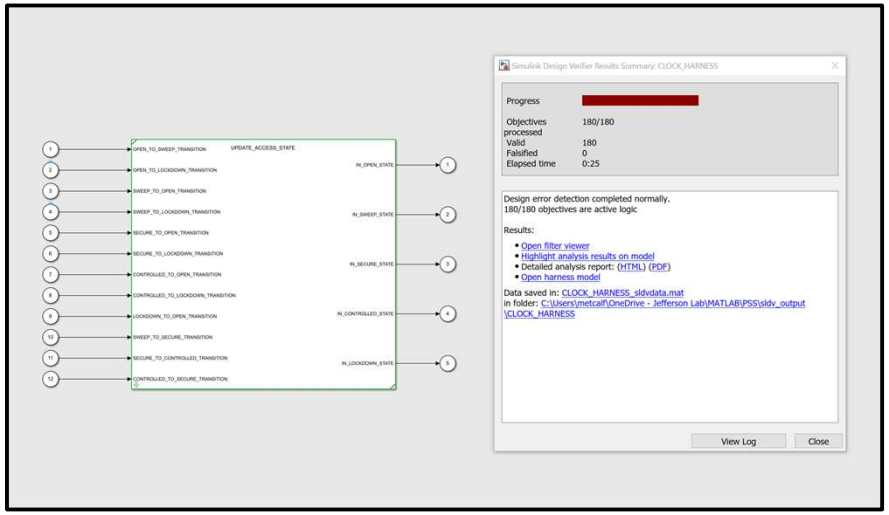


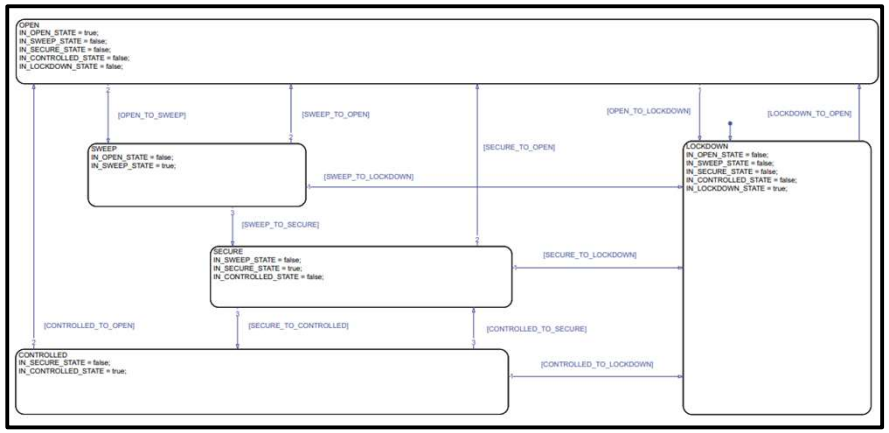
V-Model


Hazard Identification and Risk Analysis
Overall Safety Functions and Integrity Levels
FUNCTIONAL SAFETY ASSESSMENT
INSTALLATION AND COMMISSIONING
VALIDATE (EQUIVALENCE TEST LOGIC SYSTEM FUNCTION/COVERAGE TEST)
Backward Traceability
Forward Traceability
analysis IEC 61508-3
Software safety requirements specification
Validation testing
«validates»
Software architecture
Integration testing (compoents, subsystems and programmable electronics)
«verifies»
Software system design
Integration testing (module)
«verifies»
DESIGN/SIMULATE/TEST (SIMULINK/STATEFLOW MODELS)
Module design
Module testing
«verifies»
«verifies»
Coding
IMPLIMENT (TIA/QUARTERS PRIME/CCS ETC)
The V-Model
Note: Validation must take place before commissioning though FSA may take place afterwards to account for results of installation…

Software Tools

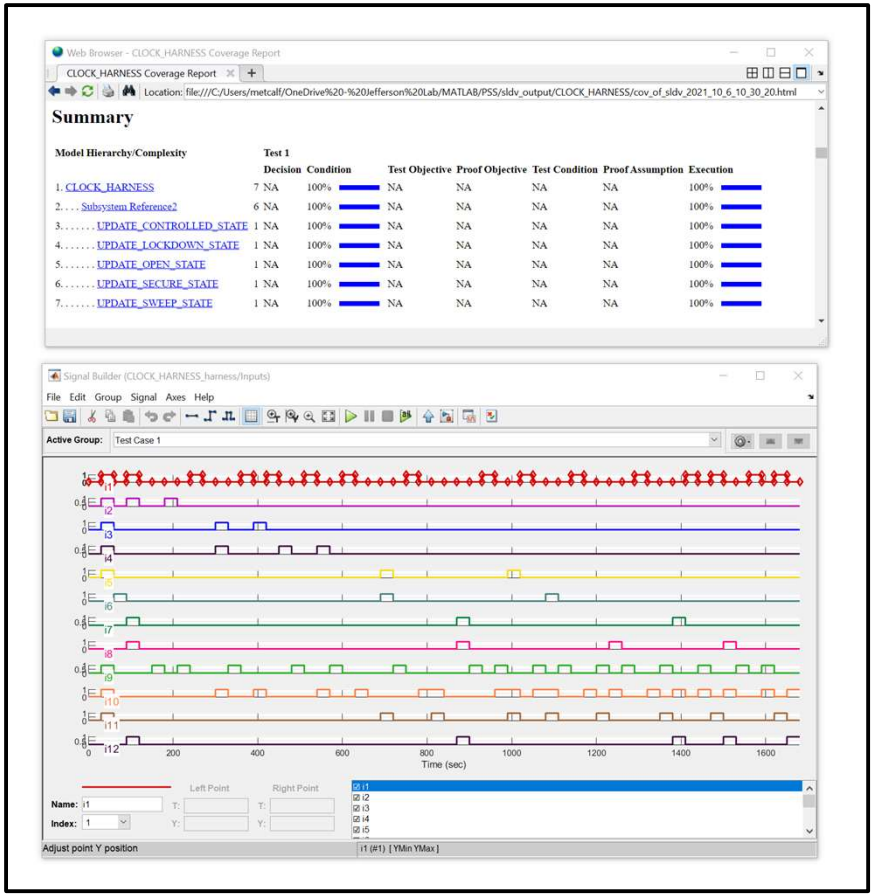
- Implementation of a CAE workflow is considered best practice and is highly recommended by IEC 61508 for SIL 3
  - Model Based Systems Engineering
  - Graphical: Function Block Diagramming (FBD)
  - Fully described logical and functional requirements
  - Modular and hierarchical
  - Executable and testable
- Design
  - Simulink
  - Stateflow
  - Fixed Point Designer
- Verification
  - Simulink
  - Simulink Check
  - Simulink Coverage
  - Simulink Design Verifier
- Implementation
  - TIA Portal v16/17
    - Step 7 Professional
    - Step 7 Safety Advanced
- Validation and Certification
  - Existing certification procedures were re-used
  - This ensures the upgrades do not invalidate the extant safety functions or introduce unintended functionality





Increasing Systematic Capability

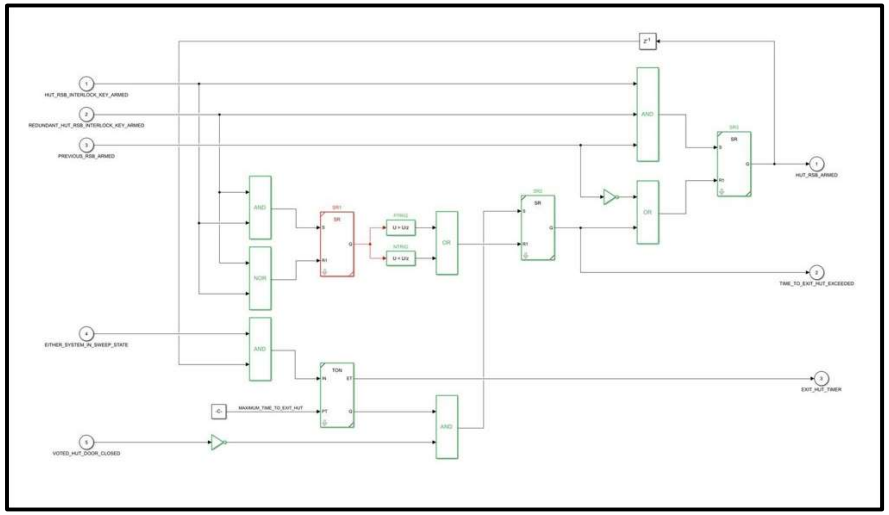
- Fixed Point Designer
  - Optimize custom fixed point data types
  - Measure min/max signal ranges throughout code
  - Determine precision achievable for fixed point designs
- Simulink Check
  - Compliance checks with IEC 61508 modelling guidelines
- Simulink Coverage
  - Verification of model and code coverage against objectives
  - Uses standard methods such as MCDC
  - Measure coverage provided by manually authored procedures
- Simulink Design Verifier
  - Implements advanced error detection using formal methods proving the absence of
    - Dead (un-executable) code and logic
    - Memory access violations
    - Integer Overflows
    - Parameter Underflows
    - Divide by zero
  - Automatic test case generation to measure maximum code coverage achievable

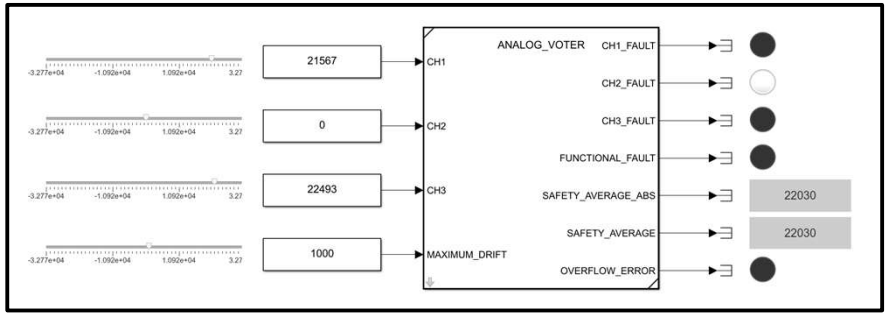


Jefferson Lab

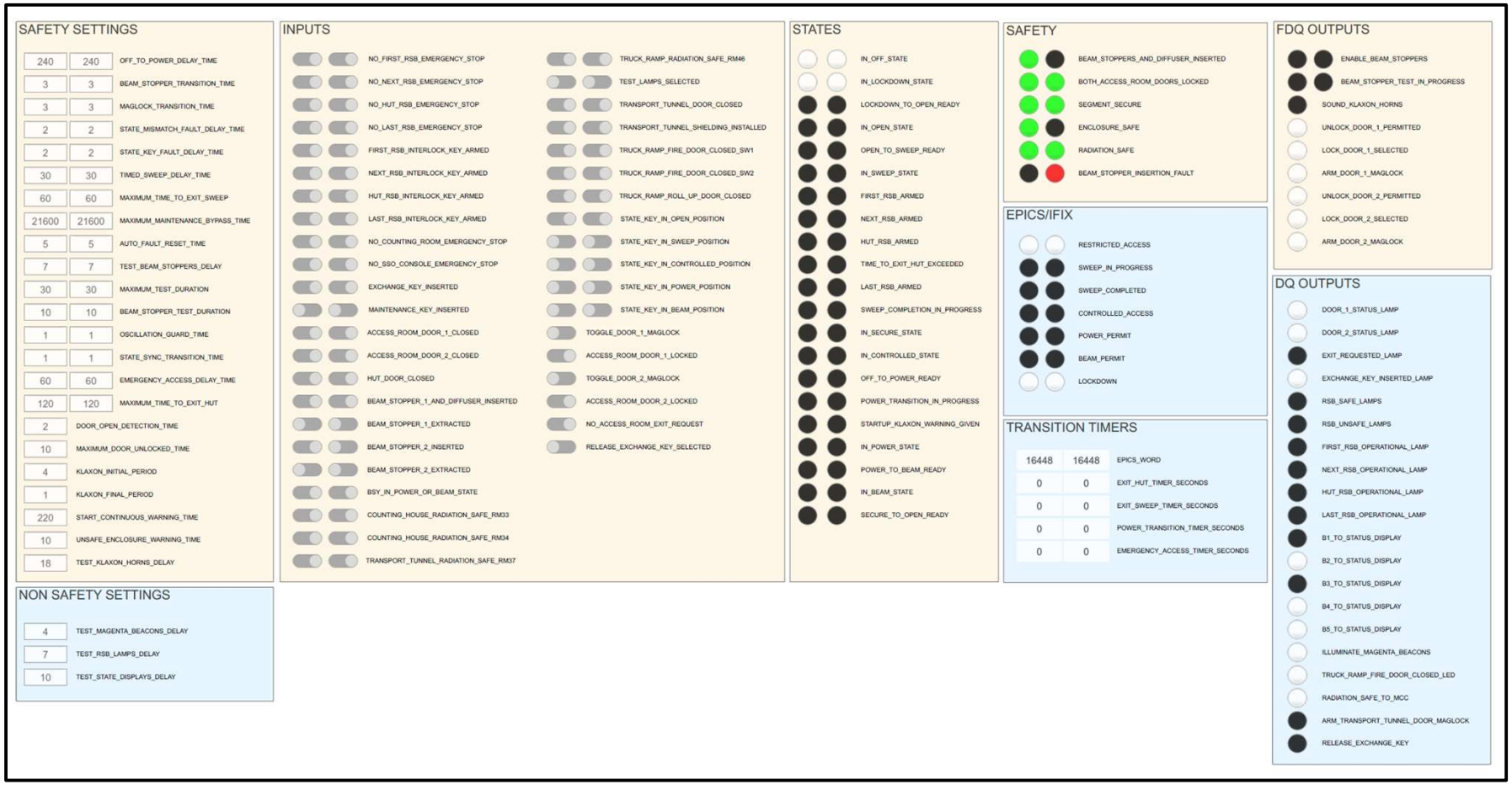
Unit Testing

- Unit testing is performed in Simulink using both semi-formal and formal methods
- Once modules are completed they are committed to a library of safety certified function blocks



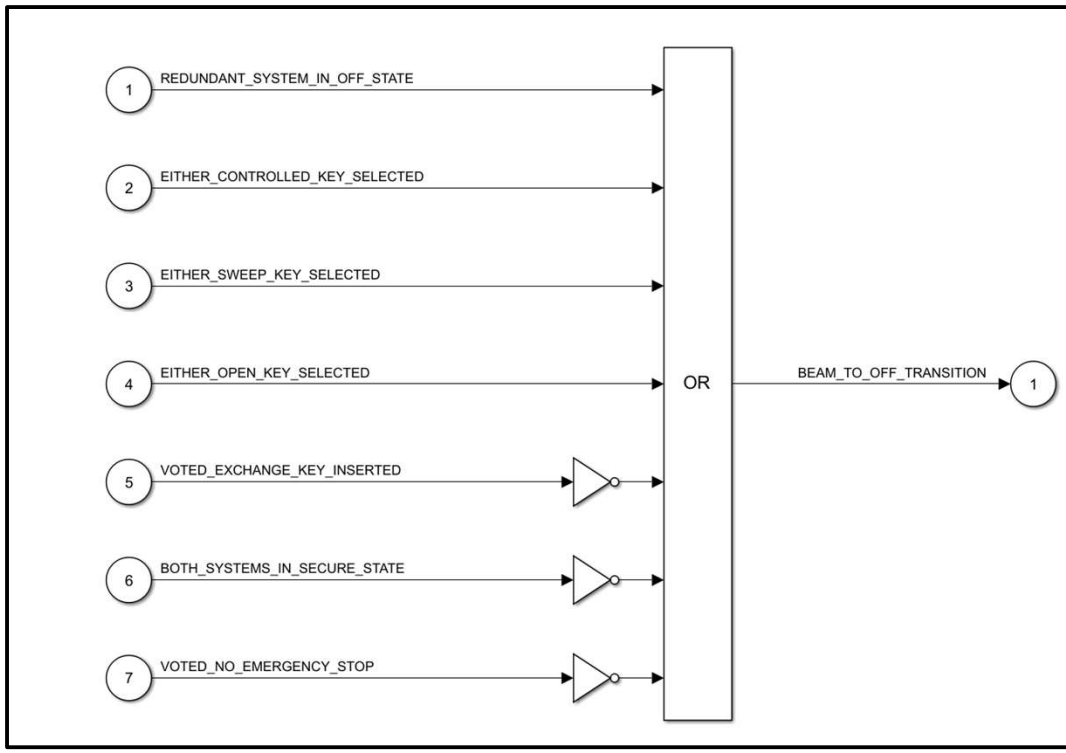


Integration Testing

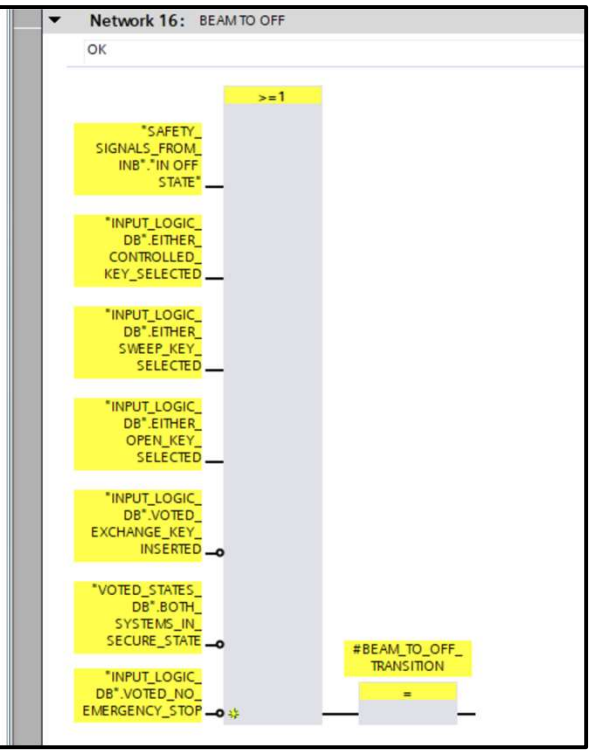


Implementation – Model to Code

Simulink

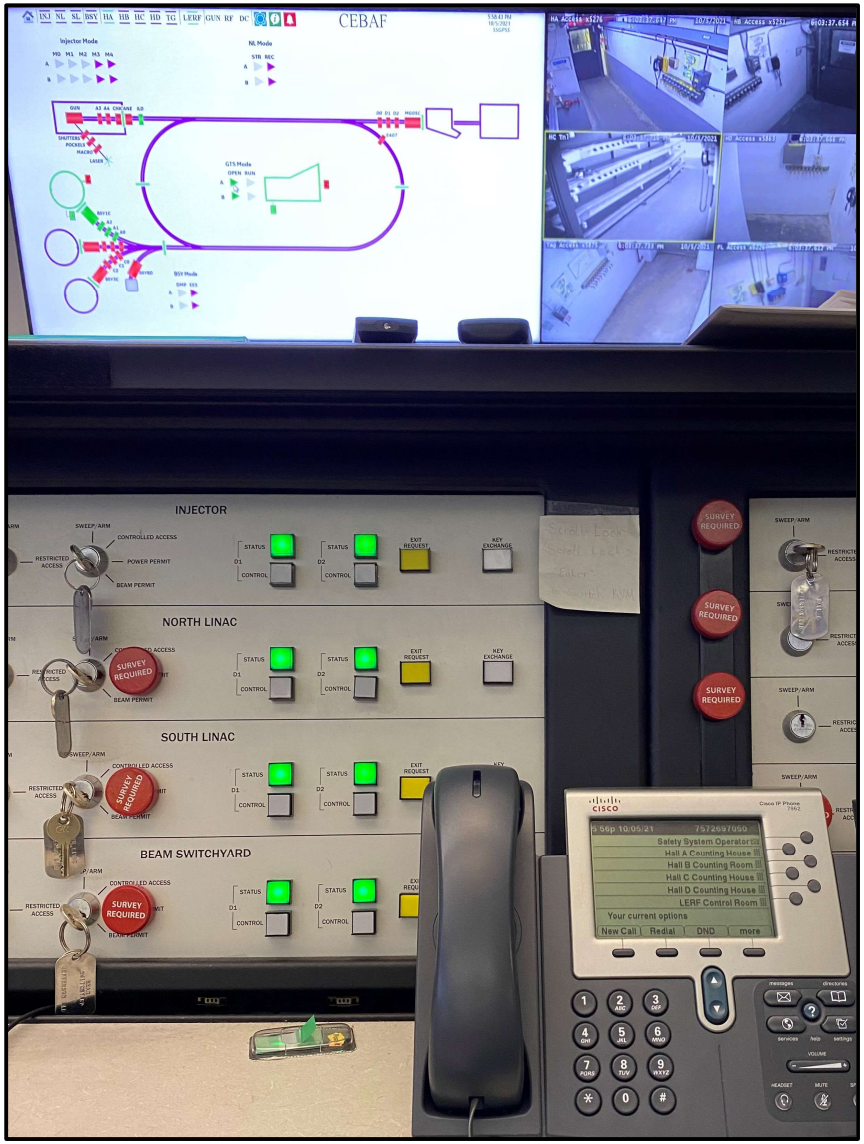


TIA Portal



Security

- Firewalls were introduced to separate the safety system process network from the accelerator network
- Note that the accelerator network is also secured by IT using multi-factor authentication
- External hosts includes JLab atomic clock time servers
  - Accurate time stamping of alarms is essential to permit detailed sequence of events analysis



Progress

Segment	Status	I/O (A)	I/O (B)	Diag. (A)	Diag. (B)
Injector	Completed	119	95	243	127
North Linac	Completed	360	286	666	281
South Linac	In Progress	312	252	TBD	TBD
Beam Switchyard	Not Started	205	150	TBD	TBD
Hall A	Completed	102	59	167	55
Hall B	Completed	93	56	153	51
Hall C	Partial	131	76	TBD	TBD
Hall D / Tagger	Partial	155	79	TBD	TBD

Paul Metcalf

metcalf@jlab.org

- Upgrades to the CEBAF Personnel Safety System are ~50% completed
  - Updated architecture
  - Inter-PLC communication
  - Online diagnostics
- These changes will increase the level of risk reduction (safety) provided by the PSS by up to 10X
  - Equivalent to a whole SIL level
- The increased safety margin will be used to justify extension of the PTI to 12 months or longer