National Spherical Torus eXperiment Upgrade

Centralized Control System
WBS 1.09.04.02

NSTX-U Recovery Project FDR – March 17-19, 2020

Ben Smith

Joe Petrella - Cognizant Engineer

Last edit: 3/9/20

Outline

1. Overview
2. Scope
3. Requirements and Interfaces
4. Analysis/Prototyping
5. Chit Closure
6. Procurement, Fabrication, Installation, and Test
7. Risk - Project Risks and Design FMECA
8. Quality, Environmental, Safety, and Health
9. Summary

Overview - WBS 1.09.04.02

WBS Title	Centralized Control System	WBS #	1.09.04.02
Project Cog.	Joe Petrella	Assoc. Proj. Man.	Tom Jernigan
Design Scope	Replace TFTR-era legacy relay logic with PLC system		
Technical Impact of Scope	CCS will be used to coordinate plant subsystems		
Design Status	FDR completed on 1/14/2020: review link All project chits are closed: link Calculations: N/A Drawings completed: link SoW/Tech Spec: N/A		
Fabrication Status	PLC logic under development at PPPL, COTS parts are selected		
Installation Status	Installation of panels & hardware will begin after CDE-3B approval		

Outline

1. Overview
2. Scope
3. Requirements and Interfaces
4. Analysis/Prototyping
5. Chit Closure
6. Procurement, Fabrication, Installation, and Test
7. Risk - Project Risks and Design FMECA
8. Quality, Environmental, Safety, and Health
9. Summary

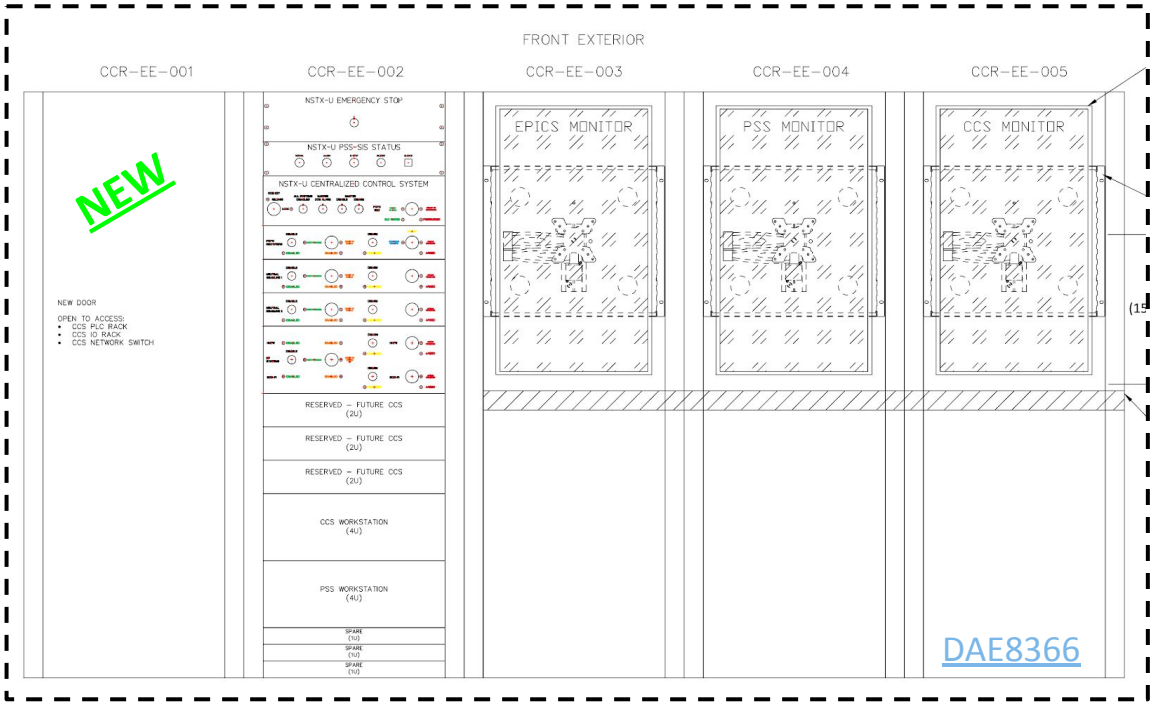
General Functions of the CCS

As defined in the RD's, the Centralized Control System shall:

- Receive signals from the PSS-SIS to shut down systems in the event of an E-Stop condition
- Receive feedback and provide enable / arm permissives to:
  - Neutral Beams
  - FCPC Rectifiers & SLD
  - HHFW
  - ECH-PI
- Provide the legacy No E-Stop and Loop Set functions
- Receive status signals from the Trapped Key blocks
- Provide the Chief Operating Engineer (COE) with an HMI to interface with plant systems

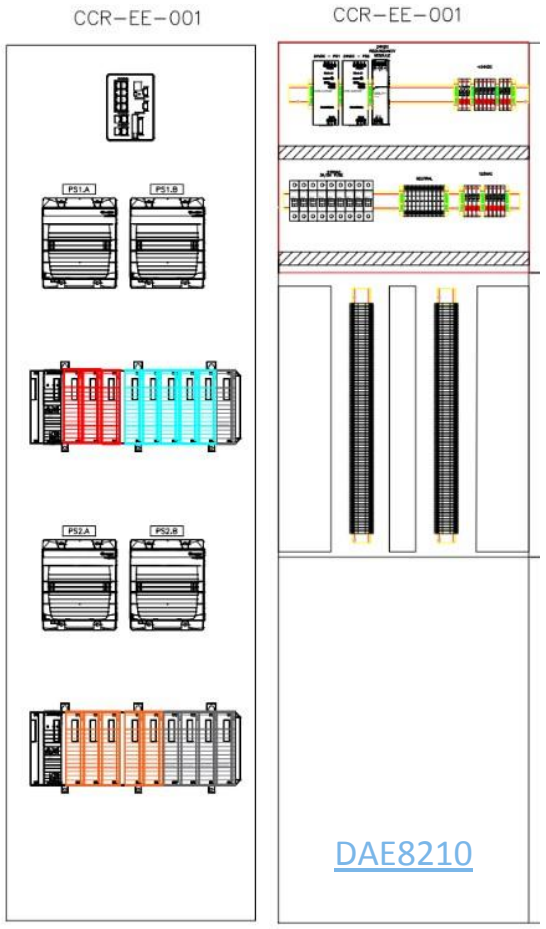
In Scope - Centralized Control System

- Modernize the existing Chief Operating Engineer station
  - Replace 200+ relays with a new PLC & HMI



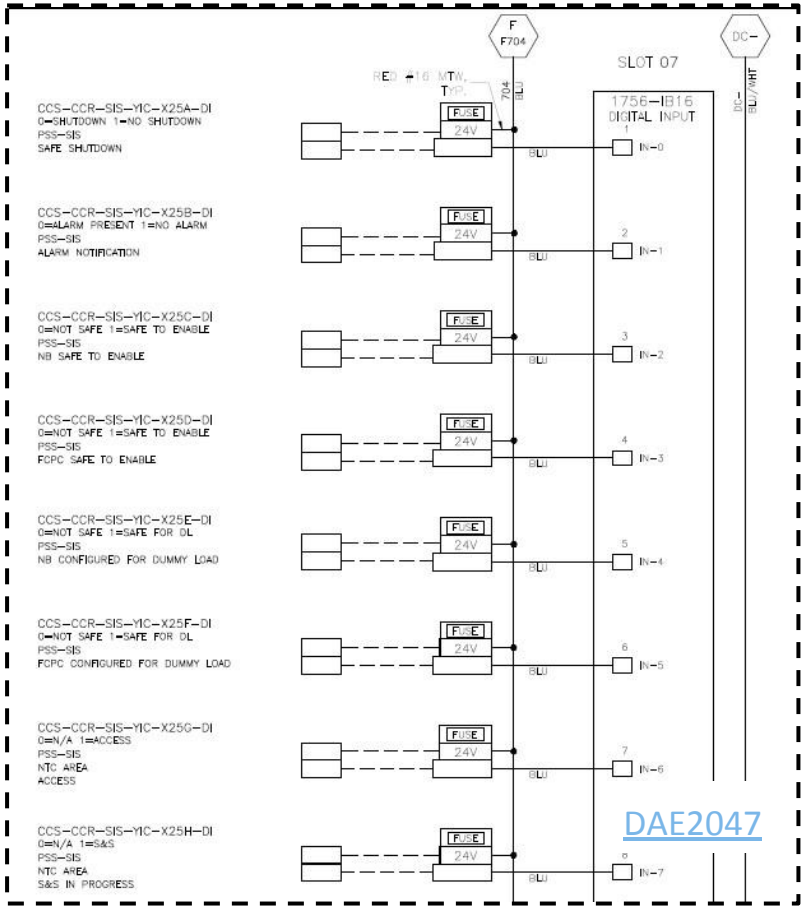
Rockwell PLC & HMI Software Solution

- Rockwell L84E PLC & Studio 5000 software
- FactoryTalk View HMI
  - Consistent with adjacent PSS-SIS screens
- Subsystem status feedback & control provided by physical front panel interface
- System provides capability to expand
  - Studio 5000 Logix Emulate creates virtual PLC testing environment
- Data sent via OPC DA to central EPICS NSTX-U archive server
  - Short-term local backup archive using FactoryTalk Data Logging feature



Scope Includes Panel & Wiring Alterations

- Field wiring changes utilize existing conduits between C-Site and D-Site
- 2 Legacy HIS panels will be replaced as junction boxes
- 1 panel will be modified
- Input signals from PSS-SIS and TKS are accommodated
  - PSS-SIS signals are air-gapped to protect safety system
  - Drive interlock logic for plant subsystems



Outline

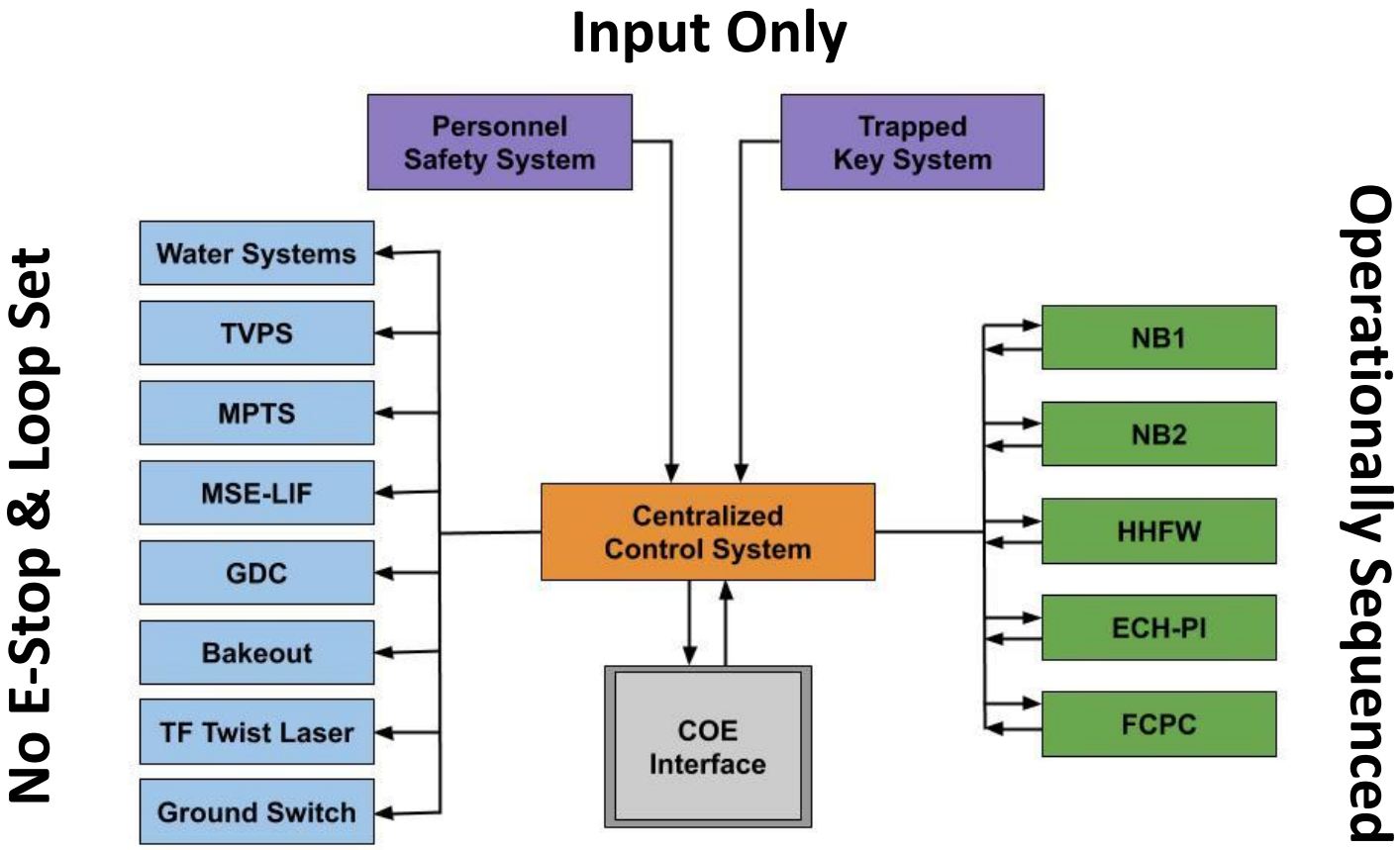
1. Overview
2. Scope
3. Requirements and Interfaces
4. Analysis/Prototyping
5. Chit Closure
6. Procurement, Fabrication, Installation, and Test
7. Risk - Project Risks and Design FMECA
8. Quality, Environmental, Safety, and Health
9. Summary

Requirements Defined and Met

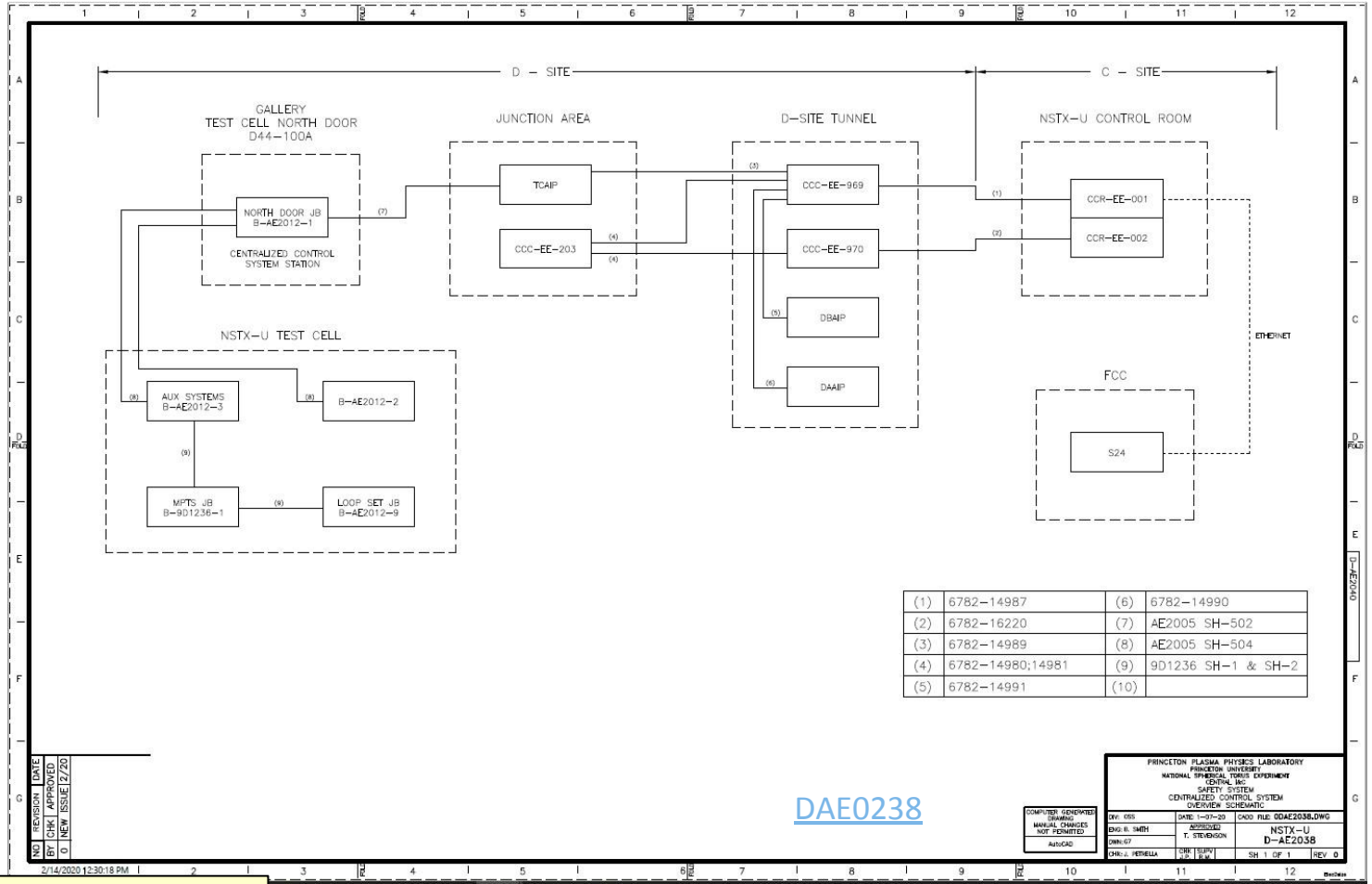
Source	Requirements	Comment	met
NSTX-U-RQMT-GRD-001	Permissives to Subsystems	Operationally sequenced and simple permissives, removed by PSS E-Stop	✓
NSTX-U-RQMT-SRD-012	Defines Interfaces	Specifies which subsystems receive enable/arm signals and which receive simple permissives	✓
NSTX-U-RQMT-SRD-012	Expansion Capacity	System must accommodate future expansion	✓
NSTX-U-RQMT-SRD-012	COE Control Station	HMI will be provided for COE to view & control plant subsystems	✓
NSTX-U-RQMT-RD-025	PSS-SIS and TKS Input Signals	Defines the signals CCS will receive from SIS PLC and TKS key blocks	✓
NSTX-U-RQMT-RD-025	Sequenced Subsystem Signals and Logic	Details the conditions necessary for permissives to be granted and revoked	✓
NSTX-U-RQMT-RD-025	Tag Archive	Data will be transmitted to NSTX EPICS network for central archive	✓
NSTXU_1-7-3-8_RD_101	Software Implementation	Details the features and methods to be implemented in the PLC and HMI programs	✓
NSTXU_1-7-3-8_RD_101	Security	Physical and cyber security defenses	✓

Complete RVTM maintained by Project Systems Engineering

Interfaces Defined & Accommodated



Connections Between C-Site & D-Site



DAE0238

Details of Interfaces Defined in Interface Control Documents

System 1	System 2	ICD Link	Exposition
Operations & Systems Safety	Heating Systems	link	Defines interface between Centralized Control System and the Heating Systems
Operations & Systems Safety	Power System	link	Defines interface between Centralized Control System and the Power System
Operations & Systems Safety	Vacuum Pumping System	link	Defines interface between Centralized Control System and the Vacuum Pumping System
Operations & Systems Safety	Bakeout System	link	Defines interface between Centralized Control System and the Bakeout System

Details of Interfaces Defined in Interface Control Documents

System 1	System 2	ICD Link	Exposition
Operations & Systems Safety	Diagnostics	link	Defines interface between Centralized Control System and Diagnostics
Operations & Systems Safety	Cooling System	link	Defines interface between Centralized Control System and the Cooling System

Drawings Created & Updated via ECN

- Overall 125 existing drawings were reviewed, of those:
  - Voided: 25
  - Redlined: 23
- 31 new drawings created
  - Overview schematic
  - Panel details
  - Control wiring drawings and loop diagrams

ECN/REQUEST#	Drawing	Sheet	Type	Existing / New	Action Required	Ready
ECN 8284	6782E14989	1	Wiring Diagram	Existing	Redline	Y
ECN 8284	6782D14985	1	Interconnection Diagram	Existing	Void	Y
ECN 8284	6782E16220	1	Wiring Diagram	Existing	Redline	Y
ECN 8284	6782D16349	1	Wiring Diagram	Existing	Void	Y
ECN 8284	B-EA3500	60	Wiring Diagram	Existing	Redline	Y
ECN 8284	B-9D1236	1	Wiring Diagram	Existing	Redline	Y
ECN 8284	B-9D1236	2	Wiring Diagram	Existing	Redline	Y
ECN 8284	B-4BA181	1	Wiring Diagram	Existing	Redline	Y

Outline

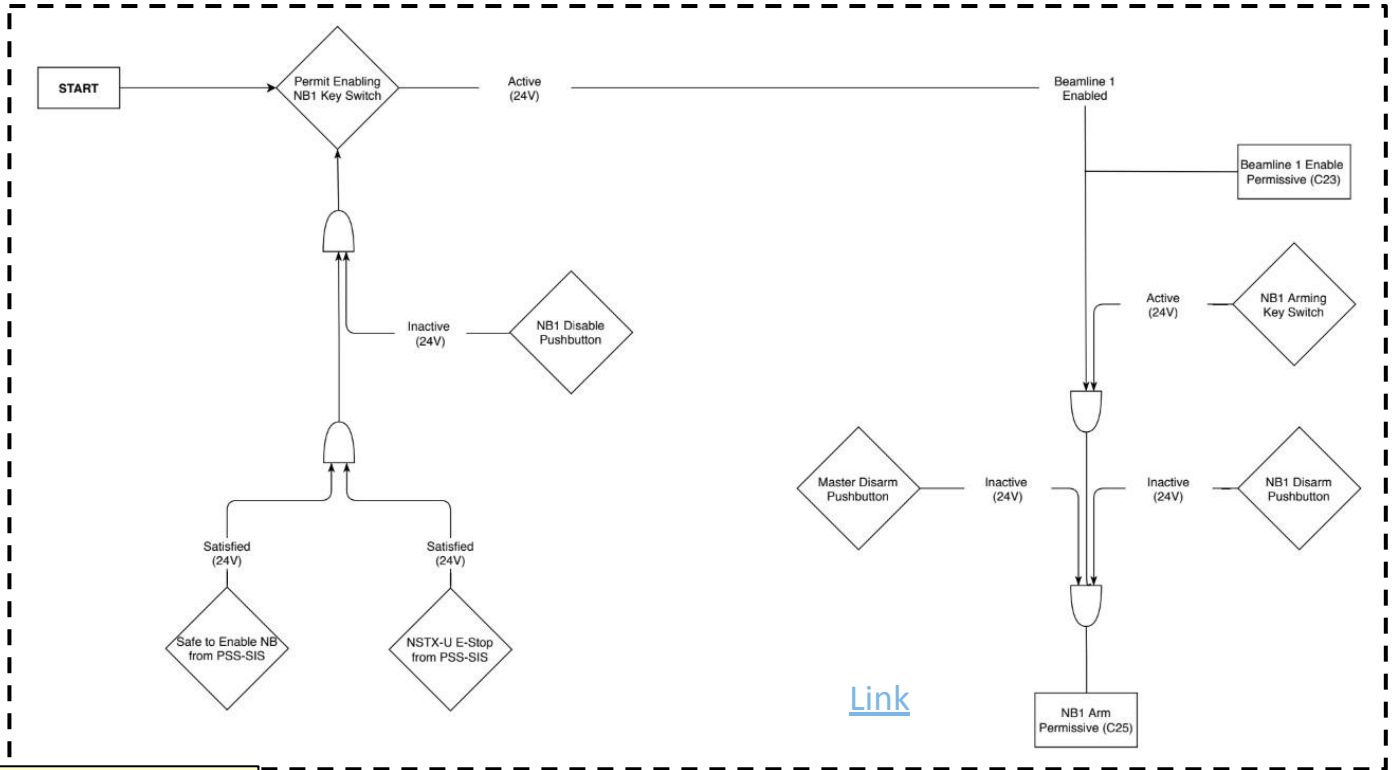
1. Overview
2. Scope
3. Requirements and Interfaces
4. Analysis/Prototyping
5. Chit Closure
6. Procurement, Fabrication, Installation, and Test
7. Risk - Project Risks and Design FMECA
8. Quality, Environmental, Safety, and Health
9. Summary

All COTS Items - No Prototyping

- All hardware for the project is COTS
  - No custom engineering solutions are employed
- Software components are COTS (Rockwell Automation)
  - In-house expertise with software platform
  - Manufacturer led training at PPPL took place in July 2019
- Soft “prototyping” of the new COE interface
  - Scale printout of the front panel was made
  - Performed test-run of the sequence of plant operations
  - Multiple iterations with COE’s led to current agreed-upon design
- All COE’s are satisfied with the operational control and improved visibility on the status of plant

Legacy Relay Logic Captured in Diagrams

Logic diagrams created for each plant subsystem, confirmed through discussion with COE's and subsystem supervisors



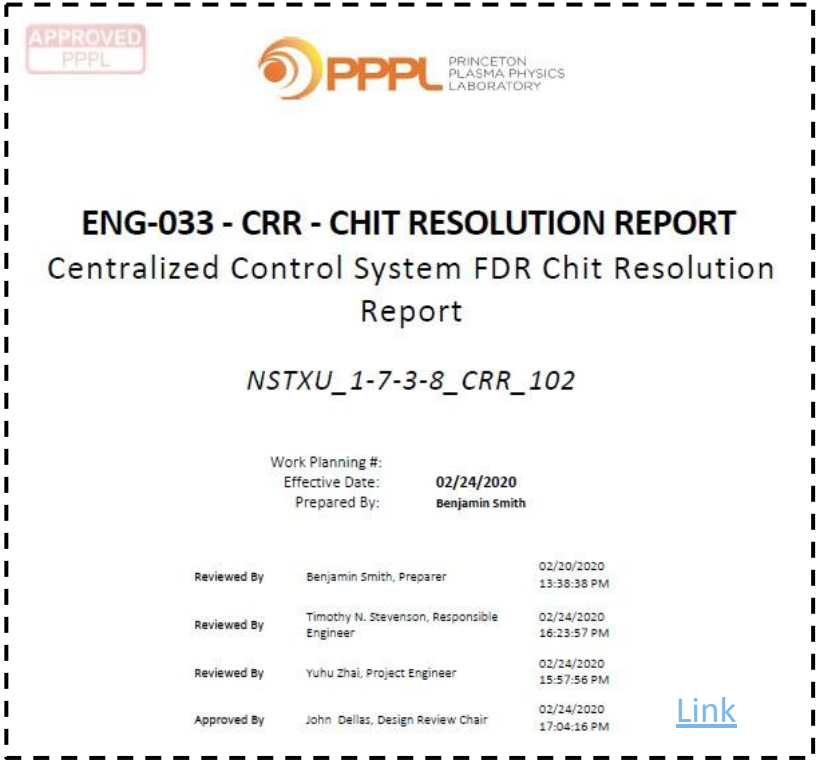
Outline

1. Overview
2. Scope
3. Requirements and Interfaces
4. Analysis/Prototyping
5. Chit Closure
6. Procurement, Fabrication, Installation, and Test
7. Risk - Project Risks and Design FMECA
8. Quality, Environmental, Safety, and Health
9. Summary

All Chits have been Closed

8 PDR chits closed by FDR

7 FDR chits closed post-FDR, Design Approval Form completed



APPROVED PPPL

PPPL PRINCETON PLASMA PHYSICS LABORATORY

ENG-033 - CRR - CHIT RESOLUTION REPORT

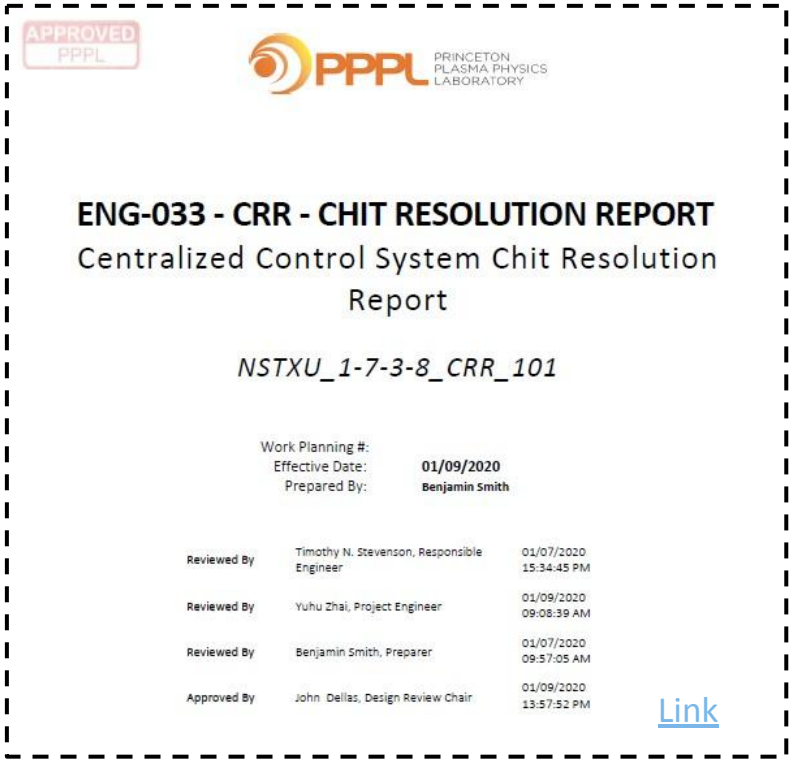
Centralized Control System FDR Chit Resolution Report

NSTXU_1-7-3-8_CRR_102

Work Planning #:
Effective Date: **02/24/2020**
Prepared By: **Benjamin Smith**

Reviewed By	Benjamin Smith, Preparer	02/20/2020 13:38:38 PM
Reviewed By	Timothy N. Stevenson, Responsible Engineer	02/24/2020 16:23:57 PM
Reviewed By	Yuhu Zhai, Project Engineer	02/24/2020 15:57:56 PM
Approved By	John Dellas, Design Review Chair	02/24/2020 17:04:16 PM

Link



APPROVED PPPL

PPPL PRINCETON PLASMA PHYSICS LABORATORY

ENG-033 - CRR - CHIT RESOLUTION REPORT

Centralized Control System Chit Resolution Report

NSTXU_1-7-3-8_CRR_101

Work Planning #:
Effective Date: **01/09/2020**
Prepared By: **Benjamin Smith**

Reviewed By	Timothy N. Stevenson, Responsible Engineer	01/07/2020 15:34:45 PM
Reviewed By	Yuhu Zhai, Project Engineer	01/09/2020 09:08:39 AM
Reviewed By	Benjamin Smith, Preparer	01/07/2020 09:57:05 AM
Approved By	John Dellas, Design Review Chair	01/09/2020 13:57:52 PM

Link

Outline

1. Overview
2. Scope
3. Requirements and Interfaces
4. Analysis/Prototyping
5. Chit Closure
6. Procurement, Fabrication, Installation, and Test
7. Risk - Project Risks and Design FMECA
8. Quality, Environmental, Safety, and Health
9. Summary

Procurement & Installation

- Components are all COTS, A-3 - detailed in BOM
- Vendors are identified and pre-qualified
  - Turtle & Hughes 1 Req executed to date, A-1 Qualified
  - Wolock & Lott A-1 Qualified
  - Rumsey A-1 Qualified
- Design support services are integrated into PPPL design team
  - G7 Automation (PLC) BOA in place, 3 req's executed to date
- Construction services are pre-qualified
  - Powers Electric (Conduit & Wiring) BOA in place
  - Maul Electric (Conduit & Wiring) BOA in place
- Installation Procedures per ENG-030 for:
  - Control room cabinet modifications
  - Test cell updates - junction boxes, wiring & conduit

Testing

- Software acceptance testing to validate logical configuration
  - Supported by Studio 5000 Logix Emulate
- Pre-Operational Test Procedures for subsystems
  - Step 1: I/O verification (point-to-point checkout)
  - Step 2: logic testing using override of inputs & outputs
- Cyber security testing to confirm implementation
- Integrated System Test Procedure
  - Full end-to-end system checkout
- Tests will be performed in accordance with ENG-062

Outline

1. Overview
2. Scope
3. Requirements and Interfaces
4. Analysis/Prototyping
5. Chit Closure
6. Procurement, Fabrication, Installation, and Test
7. Risk - Project Risks and Design FMECA
8. Quality, Environmental, Safety, and Health
9. Summary

Project Risks are Actively Managed

Risk	Score (1-81)	Open/Retired	Risk Retirement Event
No WBS-specific risks for the CCS WBS element			

Generic risks such as component delivery delays are held at the project level in the Risk Registry

CCS FMECA (I)

System	Failure Mode	Failure Cause	Failure Effect	R	Detection/ Mitigation System (1)	Detection/ Mitigation System (2)	Detection/ Mitigation System (3)	R_R
Central Control System (CCS)	Individual output signal lost	blown fuse	permissive revoke for individual signal, must open cabinet and replace fuse	4	Central Control System (CCS)	None	None	4
Central Control System (CCS)	Individual input signal lost	loose wire or disconnection	loss of status on specific signal, must open cabinet and investigate	4	Central Control System (CCS)	None	None	4
Central Control System (CCS)	HMI loses connection to PLC	HDMI failure	COE loses visibility on one screen, still has front panel and other screens	3	None	None	None	3
Central Control System (CCS)	PLC Input module failure	defective input card	loss of status signals on card	3	Central Control System (CCS)	None	None	3
Central Control System (CCS)	PLC Output module failure	defective output card	permissives get revoked from devices on card	3	Central Control System (CCS)	None	None	3
Central Control System (CCS)	Controller power supply fails	defective power supply	enter cabinet and replace	3	Central Control System (CCS)	None	None	3
Central Control System (CCS)	Fail to enable subsystem	logic error	operations delayed, must connect to PLC and troubleshoot	3	None	None	None	3

CCS FMECA (II)

System	Failure Mode	Failure Cause	Failure Effect	R	Detection/ Mitigation System (1)	Detection/ Mitigation System (2)	Detection/ Mitigation System (3)	R_R
Central Control System (CCS)	Fail to enable subsystem	I/O wiring error	operations delayed, must investigate cabinet wiring	3	Central Control System (CCS)	None	None	3
Central Control System (CCS)	Fail to disable subsystem	logic error	operations delayed, potential to operate subsystem when in unsafe state, must connect to PLC and troubleshoot	3	None	None	None	3
Central Control System (CCS)	Fail to disable subsystem	I/O wiring error	operations delayed, potential to operate subsystem when in unsafe state, must investigate cabinet wiring	3	Central Control System (CCS)	None	None	3
Central Control System (CCS)	Fail to disarm subsystem	logic error	potential to operate subsystem in unsafe state, must connect to PLC and troubleshoot	3	None	None	None	3
Central Control System (CCS)	Ethernet connection to network fails	cord failure or disconnected	loss of data archive to EPICS, enable and arm permissives to ECH-PI are revoked	3	Central Control System (CCS)	None	None	3

CCS FMECA (III)

System	Failure Mode	Failure Cause	Failure Effect	R	Detection/ Mitigation System (1)	Detection/ Mitigation System (2)	Detection/ Mitigation System (3)	R_R
Central Control System (CCS)	Key switch input fails	defective key switch module	loss of ability for COE to provide permissive to subsystem, must troubleshoot and replace	3	Central Control System (CCS)	None	None	3
Central Control System (CCS)	PSS - CCS input failure	defective input module	loss of signals from PSS, permissives are revoked, must troubleshoot	3	Central Control System (CCS)	None	None	3
Central Control System (CCS)	PSS - CCS input failure	loose wire or disconnection	loss of signal from PSS, revoke permissives, must troubleshoot	3	Central Control System (CCS)	None	None	3
Central Control System (CCS)	Key switch stuck in active position	defective key switch module	signal remains active until disarm or disable initiated from HMI	3	Central Control System (CCS)	None	None	3
Central Control System (CCS)	HMI fault	Defective module	COE cannot control system from HMI, could only be operated through front panel. Subsystems can still be disabled	3	None	None	None	3
Central Control System (CCS)	24V DC power supply failure	Defective module	Must enter cabinet and replace	3	Central Control System (CCS)	None	None	3

CCS FMECA (IV)

System	Failure Mode	Failure Cause	Failure Effect	R	Detection/ Mitigation System (1)	Detection/ Mitigation System (2)	Detection/ Mitigation System (3)	R_R
Central Control System (CCS)	Network switch failure	Defective module	loss of data archive to EPICS, enable and arm permissives to ECH-PI are revoked	3	Central Control System (CCS)	None	None	3
Central Control System (CCS)	PLC network card failure	Defective module	loss of control and loss of EPICS data and/or loss of system control. troubleshoot and replace	3	Central Control System (CCS)	None	None	3
Central Control System (CCS)	loss of power to PLC in control room	breaker trip	permissives and no e-stop signal go to 0V state, subsystems shutdown	2	Central Control System (CCS)	None	None	2
Central Control System (CCS)	Controller stops execution	major fault	loss of control of CCS signals	2	Central Control System (CCS)	None	None	2
Central Control System (CCS)	Fail to disarm subsystem	I/O wiring error	potential to operate subsystem in unsafe state, must investigate cabinet wiring	2	Central Control System (CCS)	None	None	2

CCS FMECA (IV)

System	Failure Mode	Failure Cause	Failure Effect	R	Detection/ Mitigation System (1)	Detection/ Mitigation System (2)	Detection/ Mitigation System (3)	R_R
Central Control System (CCS)	Individual defeats panel door with uniquely keyed fasteners, touches 120V AC in cabinet		reported incident >50V, low to negligible injury risk	2	None	None	None	2
Central Control System (CCS)	Individual touches 24V DC in cabinet		negligible, <50V	0	None	None	None	0
Central Control System (CCS)	Ethernet port on front panel fails	Disconnected cable	programmer / engineer cannot access PLC without opening panel	0	None	None	None	0
Central Control System (CCS)	USB port on front panel fails	Disconnected cable	programmer / engineer cannot access data archive without opening panel	0	None	None	None	0

27 FMs, all of acceptable risk

CCS provides only permissives, and so does not cause or prevent equipment damage; Can quickly repair COTS components

Outline

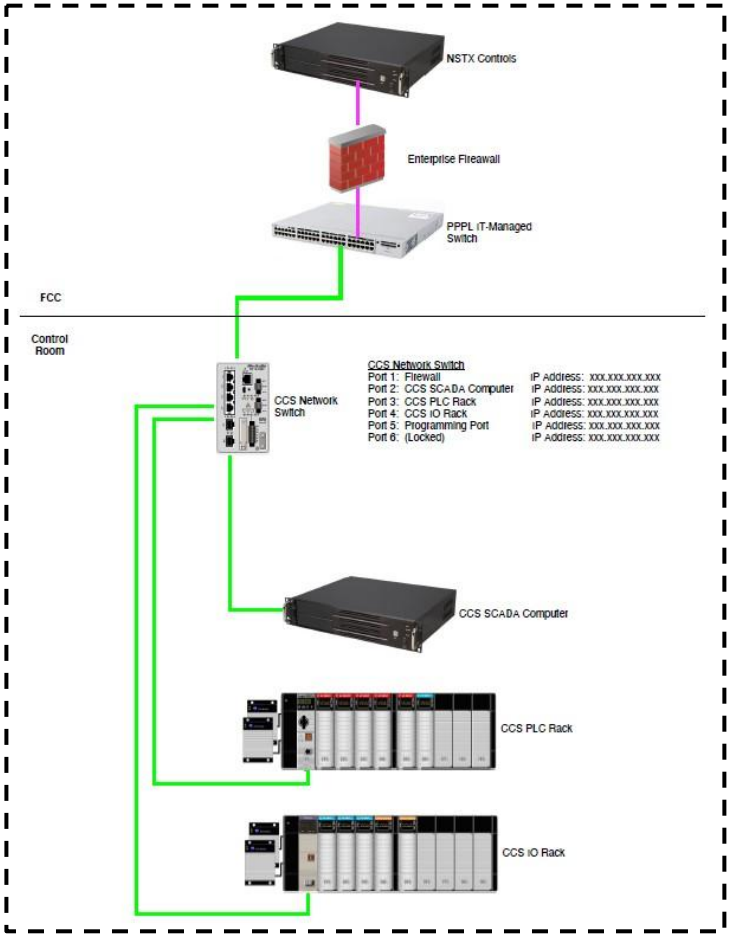
1. Overview
2. Scope
3. Requirements and Interfaces
4. Analysis/Prototyping
5. Chit Closure
6. Procurement, Fabrication, Installation, and Test
7. Risk - Project Risks and Design FMECA
8. Quality, Environmental, Safety, and Health
9. Summary

Software Quality Assurance Addressed

- CCS is not responsible for personnel safety: A-3 system
- A-3 systems require no SQA documentation
  - Electing to follow guidelines as best practice
- Software Requirements Document complete
  - Defines system capabilities & implementation constraints
- Software Design Description will be written post-installation
  - Verify implementation of required features from software RD
  - Document control logic & user interface
  - Define how cyber security controls are configured
- Sufficient detail to re-build system
- User documentation - COE operating manual

Cyber Security Risks Controlled

- Cyber security risks evaluated and classified as moderate risk level system
  - Appropriate controls identified, test document drafted
- Connection to NSTX-U Controls Network protected by enterprise firewall rules
- Physical panel protected by:
  - Tamper-resistant hardware
  - Door switches
  - COE key locking mechanism



Safety Concerns Identified

- CCS receives air-gapped communication from PSS-SIS
  - No ability to affect the safety-rated system
- Installation will be performed by qualified PPPL staff
  - Appropriate ESHD 5008 (safety manual) sections identified
- Section 2.0: Electrical Safety defines necessary precautions for proposed work & installations (up to 110VAC circuits)
  - Section 2.3: General Requirements
  - Section 2.4: Isolation of Hazards
  - Section 2.7: Electrical Conductors and Connectors
  - Section 2.8: Enclosures for Electrical Equipment
  - Section 2.10: Instrumentation & Control Systems

Outline

1. Overview
2. Scope
3. Requirements and Interfaces
4. Analysis/Prototyping
5. Chit Closure
6. Procurement, Fabrication, Installation, and Test
7. Risk - Project Risks and Design FMECA
8. Quality, Environmental, Safety, and Health
9. Summary

Summary

- CCS meets all defined requirements:
  - Replace existing relay logic with PLC
  - Modernize COE plant interface
  - Provide all existing subsystem signals
- Interfaces are considered in the design and documented in the ICDs and updated drawings
- All chits from design reviews are closed
- No WBS specific risks
- CCS interacts with, but does not compromise the safety functions of, the PSS-SIS