National Spherical Torus eXperiment Upgrade

PSS-SIS

Part of WBS 1.09.04.01

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

J. Petrella - Cognizant Engineer

Last edit: 2/18/20

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

Note: The material presented in the PSS talks is an overview of material presented in a 2-day Final Design Review. Full material Final Design Review: LINK

Overview - WBS 1.09.04.01

WBS Title	Personnel Safety System	WBS #	1.09.04.01
Project Cog.	J. Petrella	Assoc. Proj. Man.	T. Jernigan
Design Scope	Upgrade Hardwired Interlock System		
Technical Impact of Scope	Protect Personnel from Experimental Hazards of NSTX-U		
Design Status	FDR completed on 1/29/20: review link chits: link calculations: link drawings: link		
Fabrication Status	Not Started - Part of 3B approval		
Installation Status	Not Started - Will be installed post 3B approval		

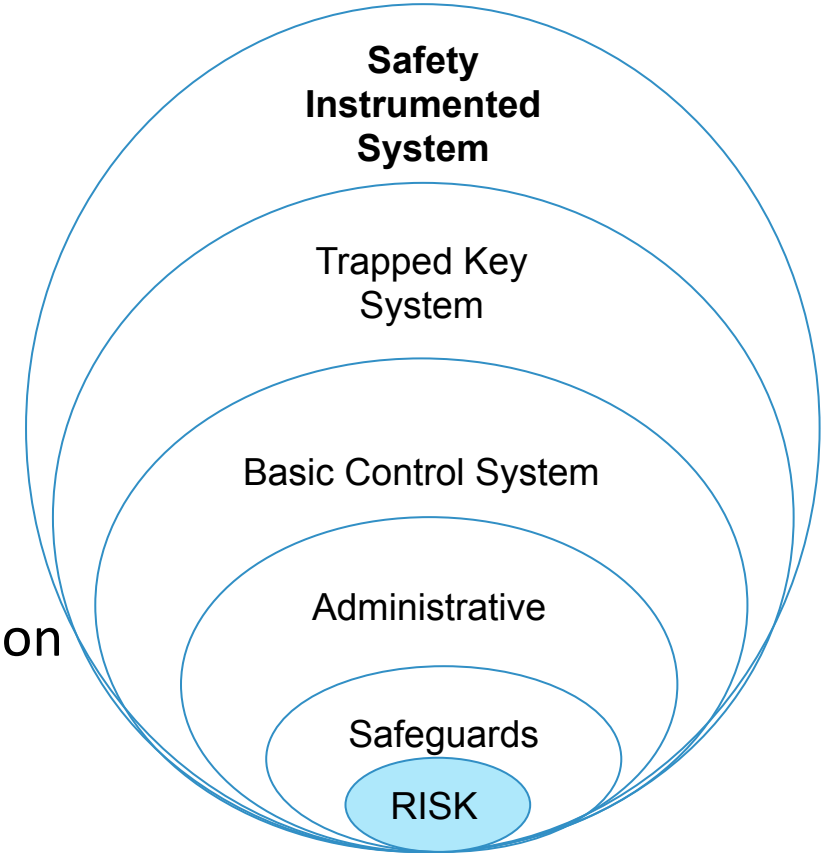
Configuration Managed Safeguards and the Trapped Key System will be covered in subsequent talks.

Outline

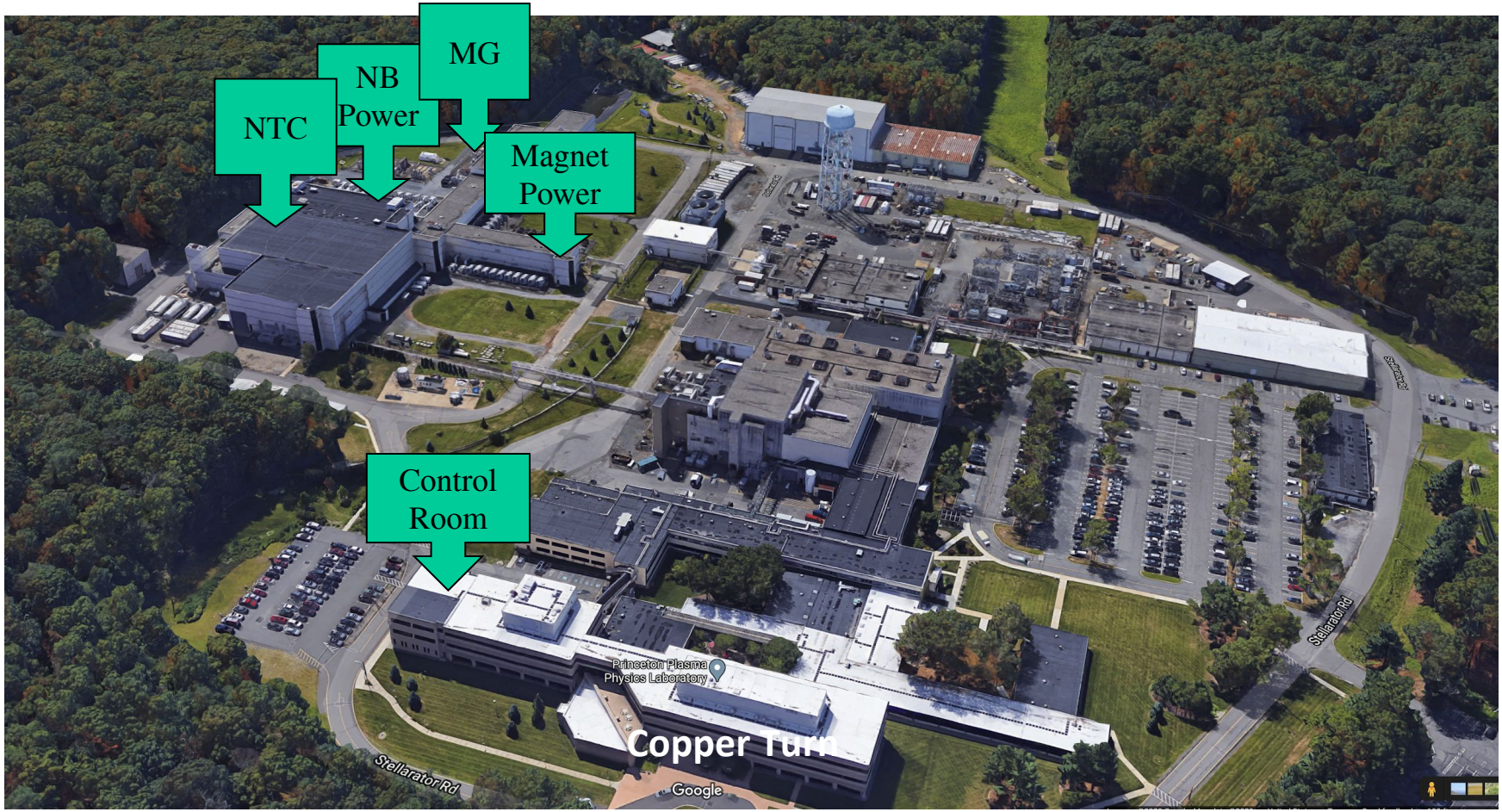
1. Overview
2. Scope
3. Requirements and Interfaces
4. Analysis/Prototyping
5. Chit Closure
6. Procurement, Fabrication, Installation, and Test
7. Risk - Project Risks and Design FMECA
8. Quality, Environmental, Safety, and Health
9. Summary

Personnel Safety System (PSS)

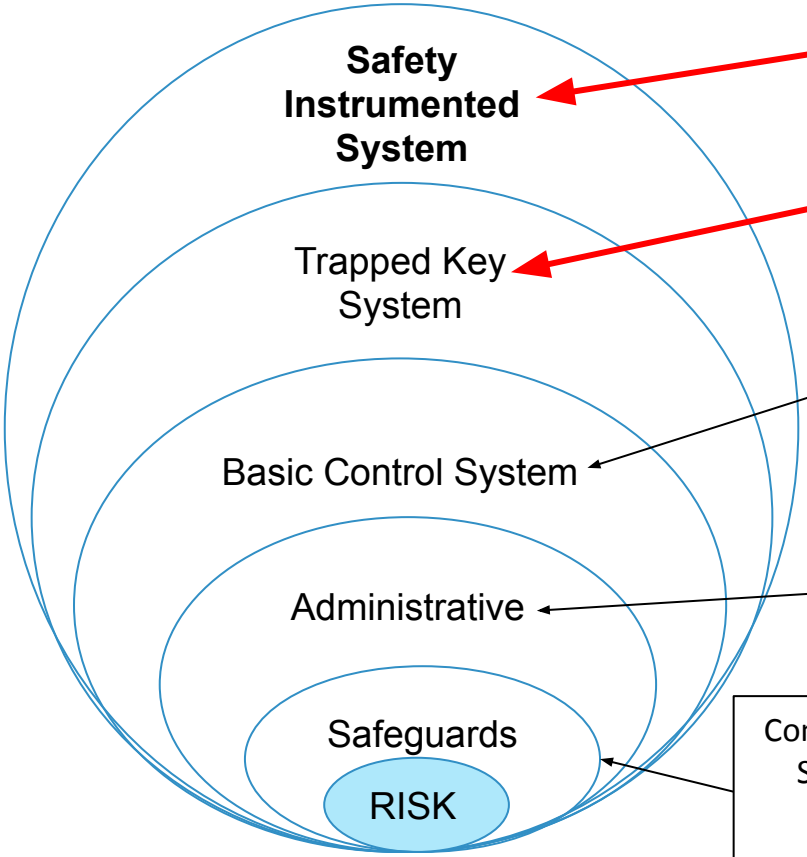
- **PSS is for personnel protection (not machine protection)**
  - **Keep the hazards from the people**
  - **Keep the people from the hazards**
- Hazards are mitigated through Independent Protection Layers (IPLs)
  - Safety Instrumented System (SIS)
  - Trapped Key System
- Direct Ionizing Radiation and Magnetic Hazards that require further risk reduction are mitigated through the PSS Safety Instrumented System (PSS-SIS)



PSS Interfaces with systems at both C and D Sites



Layers of protection reduce risk



Independent interdiction of Breakers upstream of BCS interdictions listed below
RRF of 12 needed, RRF[1] of 827 minimum achieved

Enforces Safeguards and Interlocks
Hazardous Energy Sources
RRF of 10

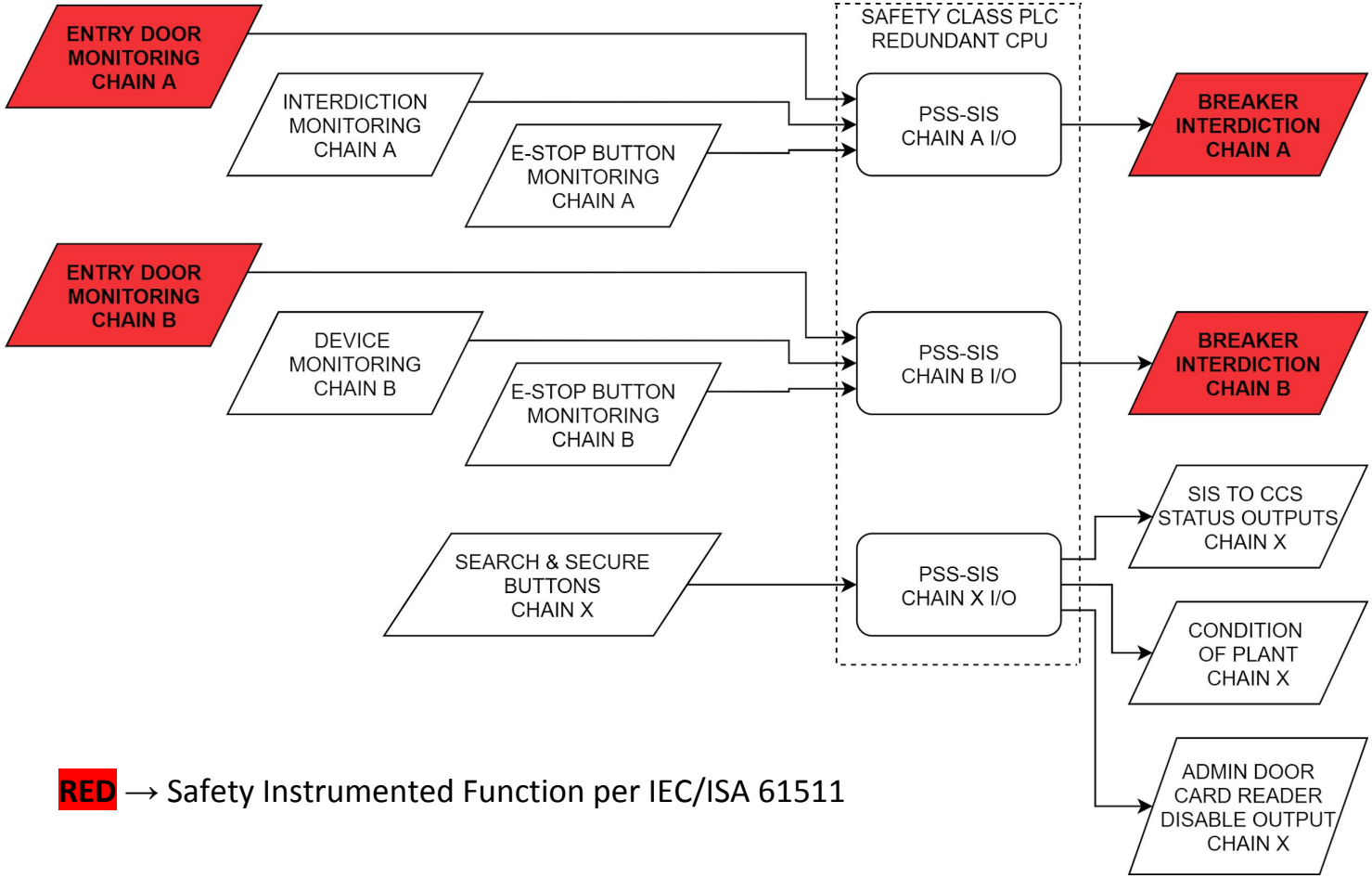
Local Control Systems that provide independent interdiction:
FCPC⟶ Rectifier Suppress/Bypass & Ground Switches
NB ⟶ Crowbar & Fast Vacuum Interrupters
RRF of 0 (IEC 61511 allows for up to 10)

Standardized Procedures, Lock out Tag out, Conduct of Operations, Operator Response
RRF of 0

Configuration Managed Safeguards, Shielding, Enclosures, Standard Industrial Covers
RRF of 0

[1]Risk Reduction Factor ⟶ Refer to LOPA talk.

PSS-SIS provides final risk reduction with a commercial safety-class redundant CPU Programmable Logic Controller (PLC) turning off primary power with breakers.



- AB Guardlogix PLC (Redundant w/safety partner)
- De-Energize-to-Trip interdiction
- Fiber-Optic backbone control system
- 25 interdicted breakers
- ~6,000 Feet of Conduit
- 9 Control Cabinets

RED → Safety Instrumented Function per IEC/ISA 61511

Hazardous energy sources are isolated (turned off) by SIS using interdiction devices installed on breakers in a Fail-Safe configuration

SIS uses a De-Energize-to-Trip (DET) configuration for breakers

- Medium Voltage Breakers (Upgrade part of breaker WBS and not in PSS scope)
  - Undervoltage Trip Device energized by N.O. safety relay
  - Breakers routinely maintained & tracked using Maximo under AC Power purview

SIS uses a De-Energize-to-Trip (DET) configuration for Distributed I/O

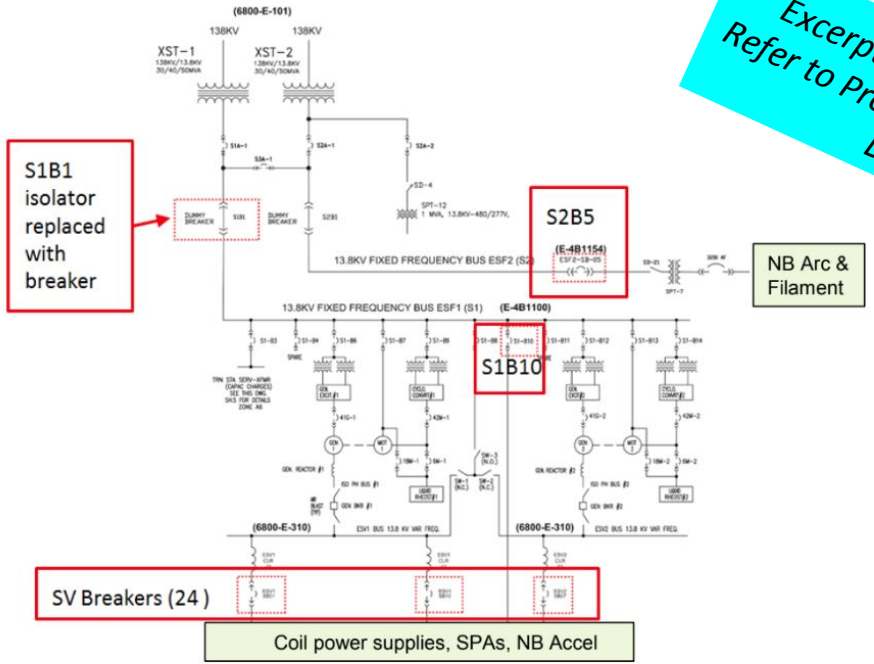
- Loss of network → de-energize outputs
- Broken Wire (BW) detection → de-energize outputs
- Shorted Wire (SW) detection → de-energize outputs

BW and SW detection are features of the Allen-Bradley POINT Guard I/O safety-rated modules

Interdicted Devices are breakers that are de-energized (safed) through fail-safe control circuits. Breaker Upgrades are Underway to Support PSS-SIS as part of a separate project. FDR Link

- Breakers have been identified for interdiction, requiring 52UVD.
- For refurb option, additional spares from in-house inventor to be included.
- Two 52S(MOC) contacts provided for state monitoring

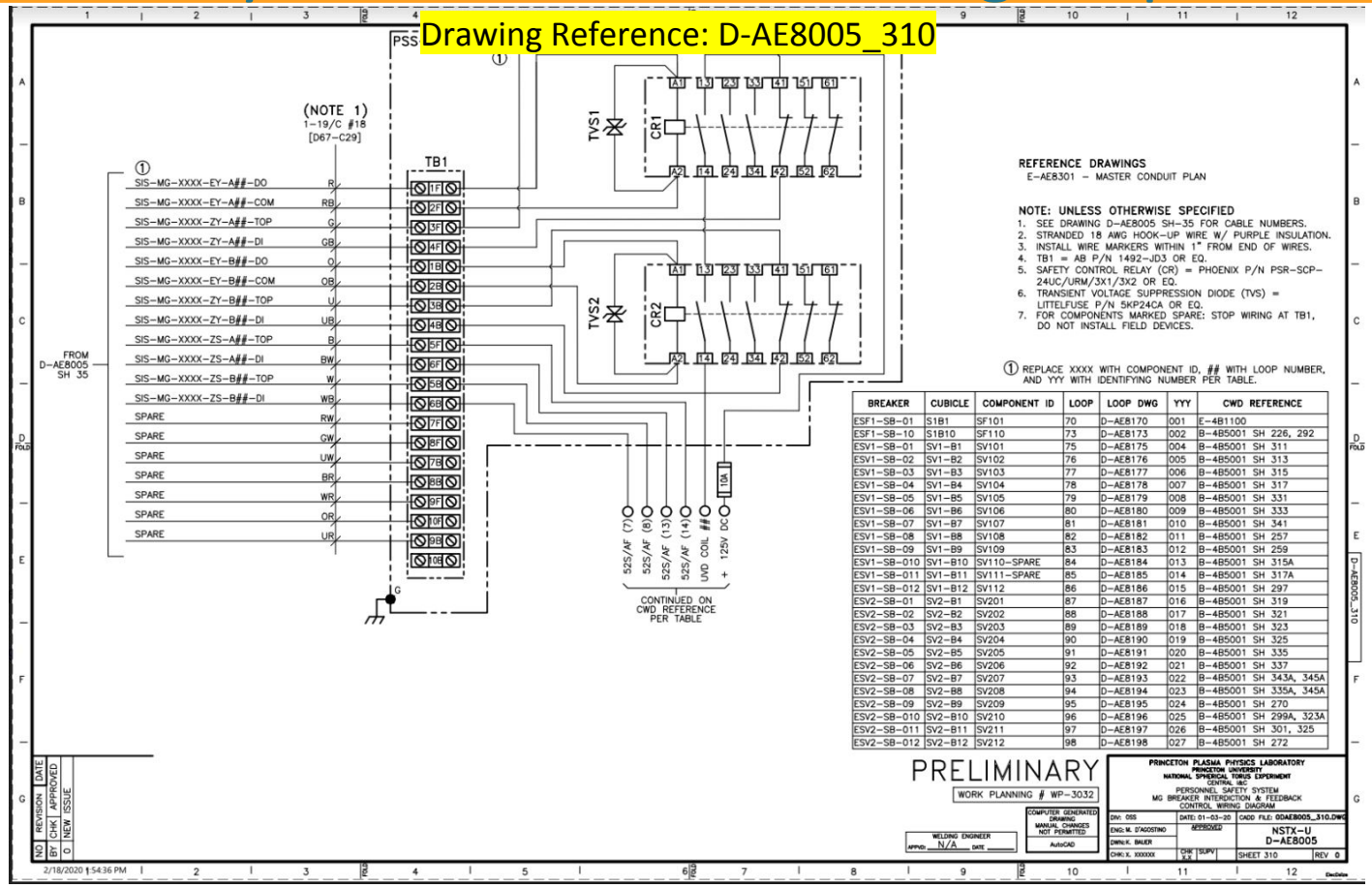
Breakers	1200A, 500MVA HK	1200A, 750MVA VHK	3000A, 1000MVA VHK(X)	Replace (Rep)/ Refurbish(Ref)
SV1	8	4		Ref
SV2	11	1		Ref
Spares	3	1		Ref
S1B1 (Dummy)			1	Rep
S1B1 Spare			1	Rep
S1B10	1			Ref
S2B5	1			Ref
Total	24	6	2	



Excerpt from FDR Slides Refer to Presentation by John Dellas

Note: breaker interdiction is indifferent to which MG is operating

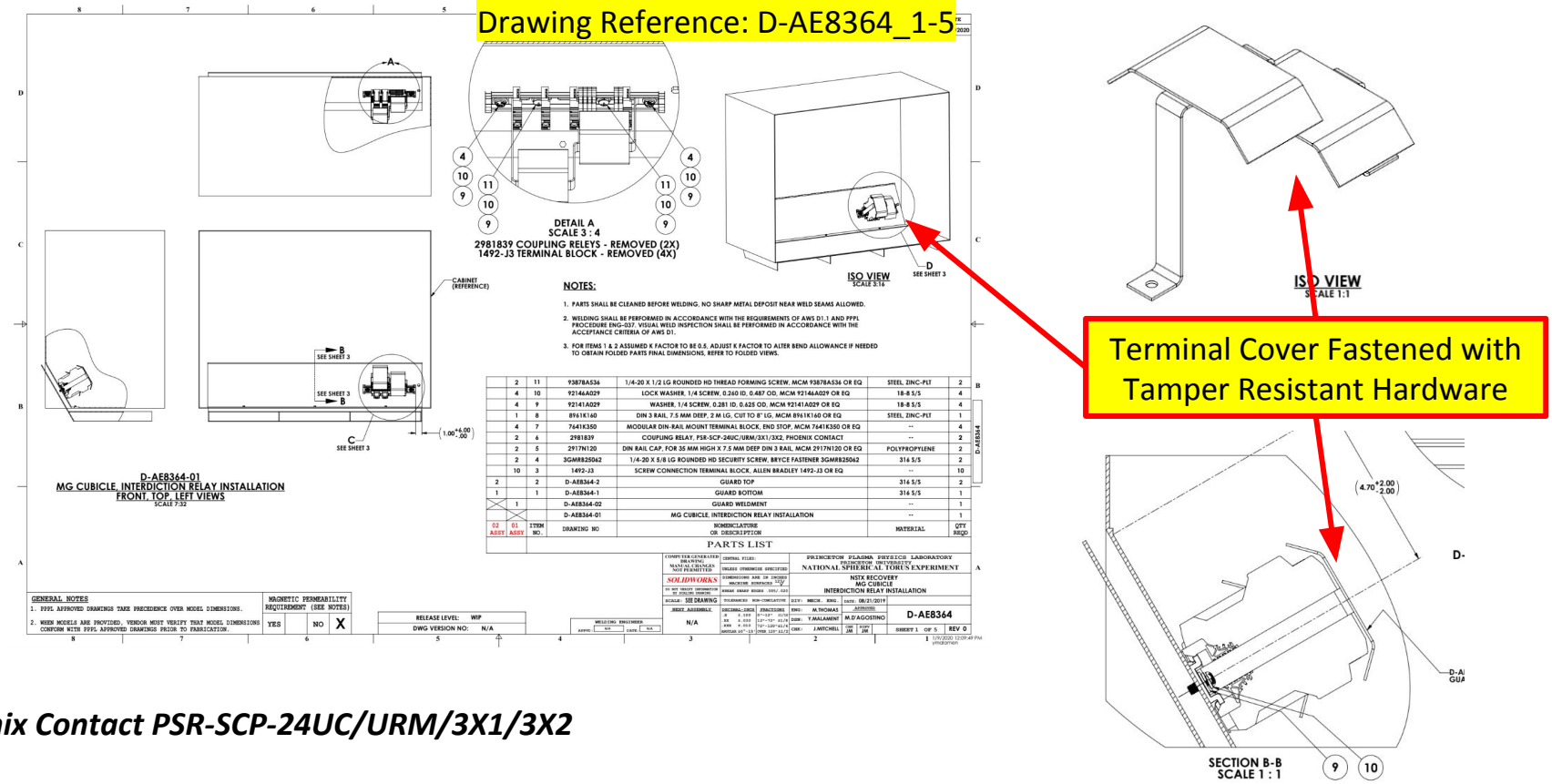
Breaker interdiction wiring (typical of all) with Chain A/B redundancy to breaker undervoltage trip solenoid



BREAKER	CUBICLE	COMPONENT ID	LOOP	LOOP DWG	YYY	CWD REFERENCE
ESF1-SB-01	S1B1	SF101	70	D-AE8170	001	E-4B1100
ESF1-SB-10	S1B10	SF110	73	D-AE8173	002	B-4B5001 SH 226, 292
ESV1-SB-01	SV1-B1	SV101	75	D-AE8175	004	B-4B5001 SH 311
ESV1-SB-02	SV1-B2	SV102	76	D-AE8176	005	B-4B5001 SH 313
ESV1-SB-03	SV1-B3	SV103	77	D-AE8177	006	B-4B5001 SH 315
ESV1-SB-04	SV1-B4	SV104	78	D-AE8178	007	B-4B5001 SH 317
ESV1-SB-05	SV1-B5	SV105	79	D-AE8179	008	B-4B5001 SH 331
ESV1-SB-06	SV1-B6	SV106	80	D-AE8180	009	B-4B5001 SH 333
ESV1-SB-07	SV1-B7	SV107	81	D-AE8181	010	B-4B5001 SH 341
ESV1-SB-08	SV1-B8	SV108	82	D-AE8182	011	B-4B5001 SH 257
ESV1-SB-09	SV1-B9	SV109	83	D-AE8183	012	B-4B5001 SH 259
ESV1-SB-010	SV1-B10	SV110-SPARE	84	D-AE8184	013	B-4B5001 SH 315A
ESV1-SB-011	SV1-B11	SV111-SPARE	85	D-AE8185	014	B-4B5001 SH 317A
ESV1-SB-012	SV1-B12	SV112	86	D-AE8186	015	B-4B5001 SH 297
ESV2-SB-01	SV2-B1	SV201	87	D-AE8187	016	B-4B5001 SH 319
ESV2-SB-02	SV2-B2	SV202	88	D-AE8188	017	B-4B5001 SH 321
ESV2-SB-03	SV2-B3	SV203	89	D-AE8189	018	B-4B5001 SH 323
ESV2-SB-04	SV2-B4	SV204	90	D-AE8190	019	B-4B5001 SH 325
ESV2-SB-05	SV2-B5	SV205	91	D-AE8191	020	B-4B5001 SH 335
ESV2-SB-06	SV2-B6	SV206	92	D-AE8192	021	B-4B5001 SH 337
ESV2-SB-07	SV2-B7	SV207	93	D-AE8193	022	B-4B5001 SH 343A, 345A
ESV2-SB-08	SV2-B8	SV208	94	D-AE8194	023	B-4B5001 SH 335A, 345A
ESV2-SB-09	SV2-B9	SV209	95	D-AE8195	024	B-4B5001 SH 270
ESV2-SB-010	SV2-B10	SV210	96	D-AE8196	025	B-4B5001 SH 299A, 323A
ESV2-SB-011	SV2-B11	SV211	97	D-AE8197	026	B-4B5001 SH 301, 325
ESV2-SB-012	SV2-B12	SV212	98	D-AE8198	027	B-4B5001 SH 272

Note: "Preliminary" stamp present until drawing is signed/released for fabrication

Breaker interdiction relays* (IEC61508-2/3 rated) will be installed in breaker cubicles with terminals protected by tamper-resistant features



Terminal Cover Fastened with Tamper Resistant Hardware

Phoenix Contact PSR-SCP-24UC/URM/3X1/3X2

Feedback hardware was selected and fitted to existing and new infrastructure

Feedback sensors are installed on the following components:

SIF input (Chain A & Chain B inputs)

- NSTX-U Test Cell Entries
- Mechanical Equipment Room Entry

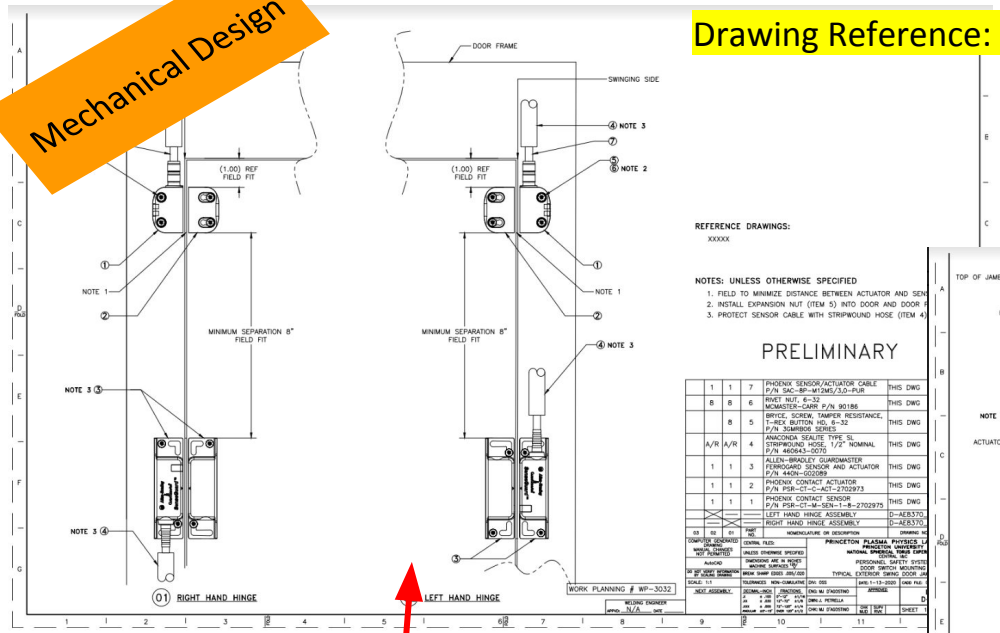
Additional engineering action input (Chain A & Chain B inputs)

- Neutral Beam Ross Ground Switches (configuration monitoring)
- Neutral Beam Pringle Ground Switches (configuration monitoring)
- FCPC Ground Switches (configuration monitoring)
- FCPC Line Switches (configuration monitoring)
- PCTS Bus Links (dummy load testing configuration monitoring)
- Select Trapped Key Blocks (dummy load testing & configuration monitoring)
- Cage egress buttons (configuration monitoring)
- Cable Spread Room & Test Cell Basement Electrical Enclosure Doors (configuration monitoring)

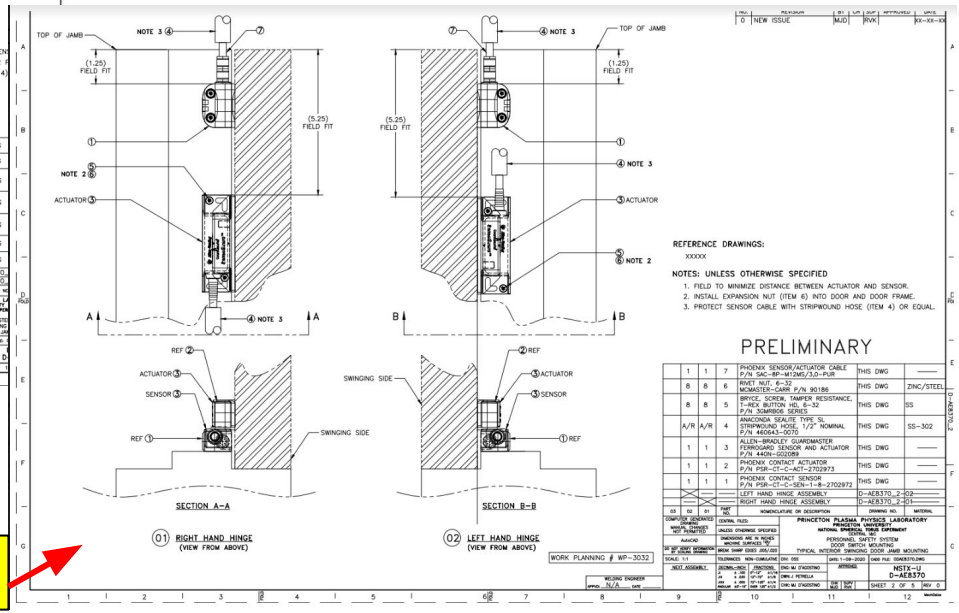
Personnel Doors monitored with (1) AB RFID Sensor (440N-G02089) & (1) Phoenix Contact RFID Sensor (PSR-CT-C-ACT-2702973) → SIF input

Mechanical Design

Drawing Reference: D-AE8370_1-2



Typical Mount to Exterior Door Frame

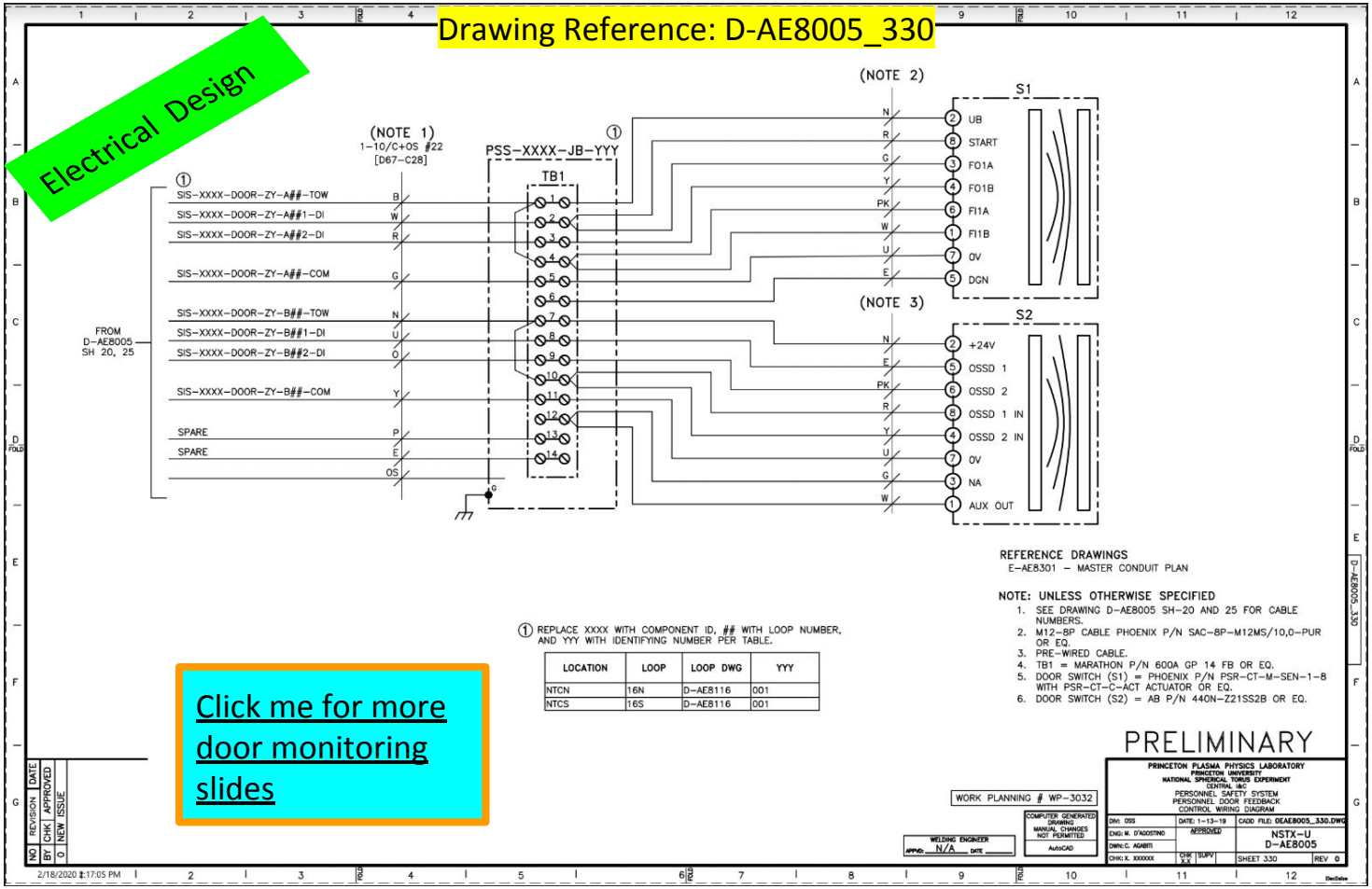


Typical Mount to Interior Door Frame

Personnel Doors monitored with (1) AB RFID Sensor (440N-G02089) & (1) Phoenix Contact RFID Sensor (PSR-CT-C-ACT-2702973) → SIF input

Drawing Reference: D-AE8005_330

Electrical Design

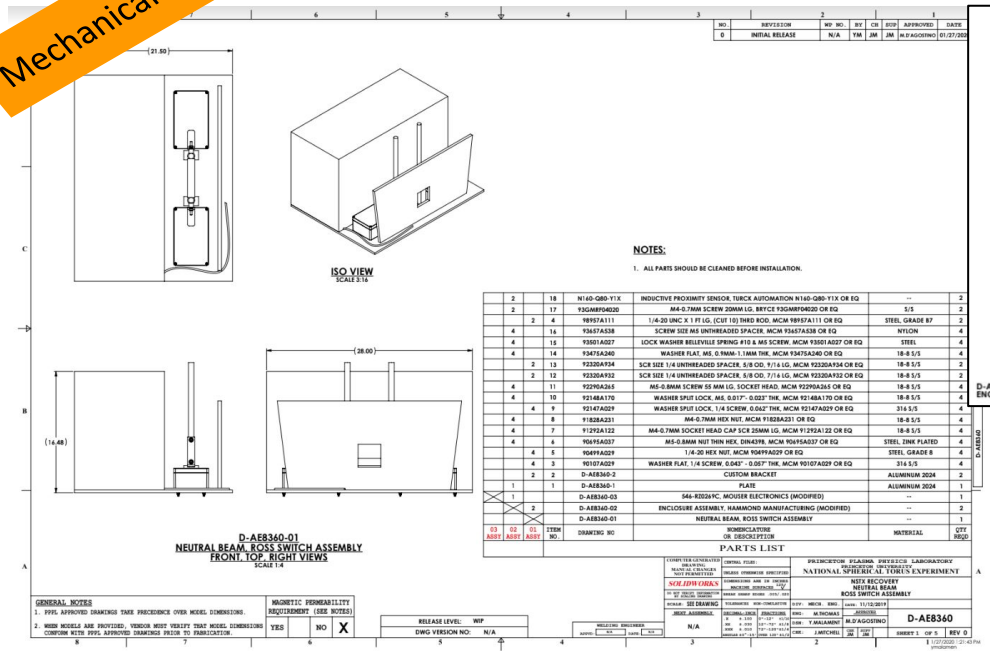


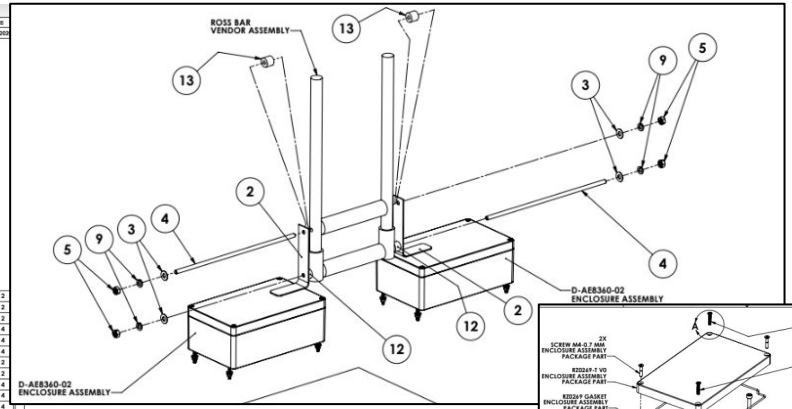
Click me for more door monitoring slides

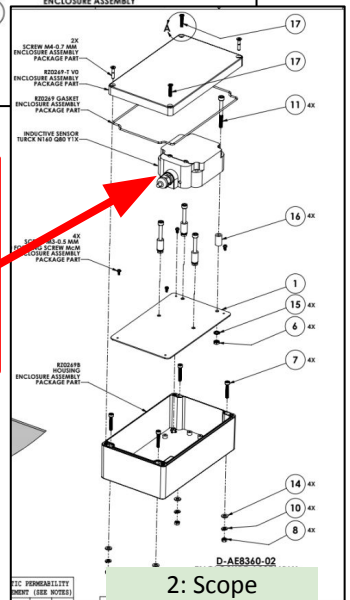
NB Ground Ross Switch Position Monitored with Turck Inductive Sensors(N160-Q80-Y1X) for additional engineering actions (not a SIF)

Mechanical Design

Drawing Reference: D-AE8360_1-5







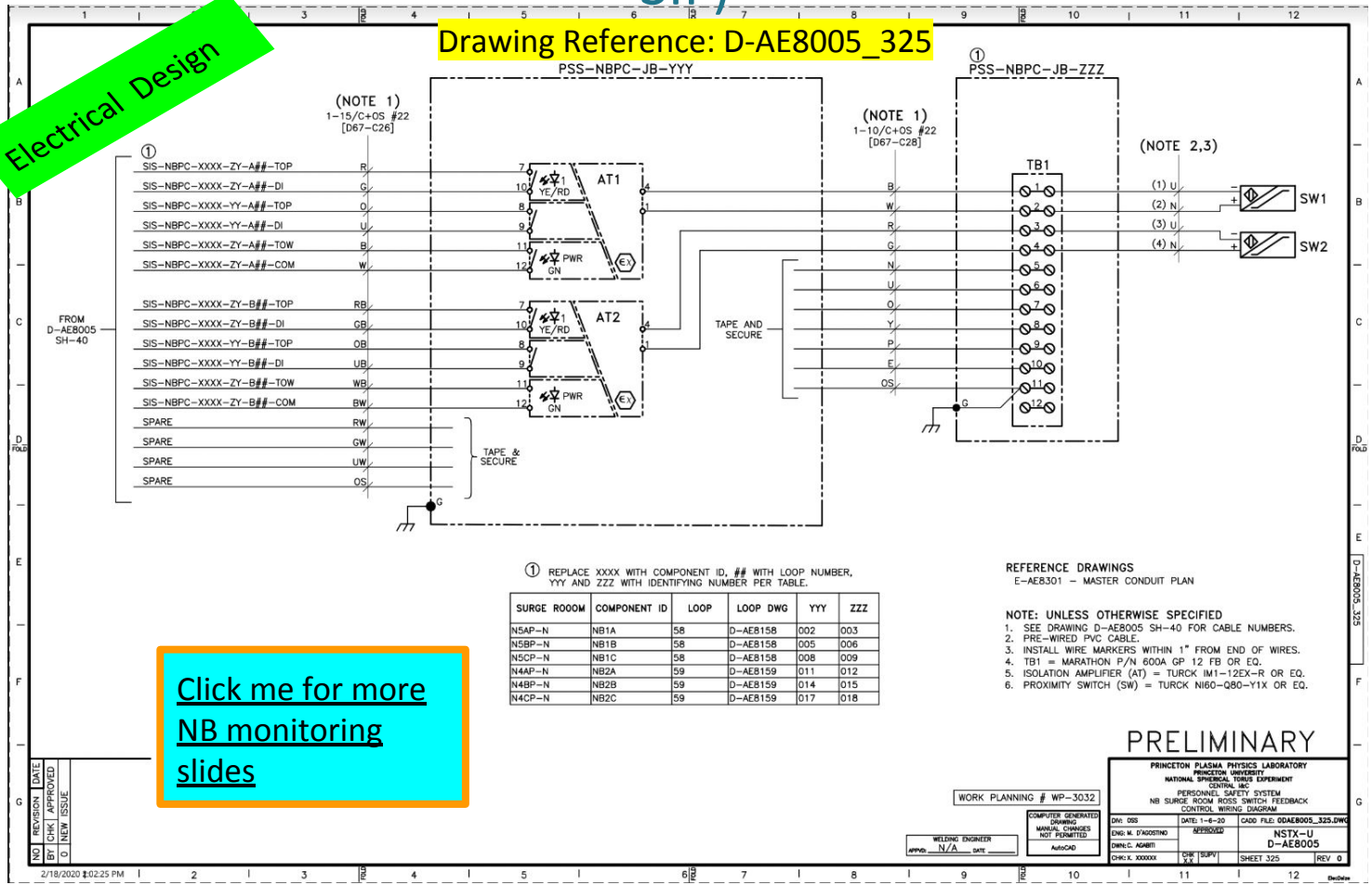
Turck Inductive Sensor: N160-Q80-Y1X

2: Scope

NB Ground Ross Switch Position Monitored with Turck Inductive Sensors(N160-Q80-Y1X) for additional engineering actions (not a SIF)

Electrical Design

Drawing Reference: D-AE8005_325



① REPLACE XXXX WITH COMPONENT ID, ## WITH LOOP NUMBER, YYY AND ZZZ WITH IDENTIFYING NUMBER PER TABLE.

SURGE ROOOM	COMPONENT ID	LOOP	LOOP DWG	YYY	ZZZ
N5AP-N	NB1A	58	D-AE8158	002	003
N5BP-N	NB1B	58	D-AE8158	005	006
N5CP-N	NB1C	58	D-AE8158	008	009
N4AP-N	NB2A	59	D-AE8159	011	012
N4BP-N	NB2B	59	D-AE8159	014	015
N4CP-N	NB2C	59	D-AE8159	017	018

REFERENCE DRAWINGS
E-AE8301 – MASTER CONDUIT PLAN

NOTE: UNLESS OTHERWISE SPECIFIED
1. SEE DRAWING D-AE8005 SH-40 FOR CABLE NUMBERS.
2. PRE-WIRED PVC CABLE.
3. INSTALL WIRE MARKERS WITHIN 1" FROM END OF WIRES.
4. TB1 = MARATHON P/N 600A GP 12 FB OR EQ.
5. ISOLATION AMPLIFIER (AT) = TURCK IM1-12EX-R OR EQ.
6. PROXIMITY SWITCH (SW) = TURCK NI60-Q80-Y1X OR EQ.

PRELIMINARY

PRINCETON PLASMA PHYSICS LABORATORY
PRINCETON UNIVERSITY
NATIONAL SPHERICAL TORUS EXPERIMENT
CENTRAL I&C
PERSONNEL SAFETY SYSTEM
NB SURGE ROOM ROSS SWITCH FEEDBACK
CONTROL WIRING DIAGRAM

NSTX-U
D-AE8005

WORK PLANNING # WP-3032

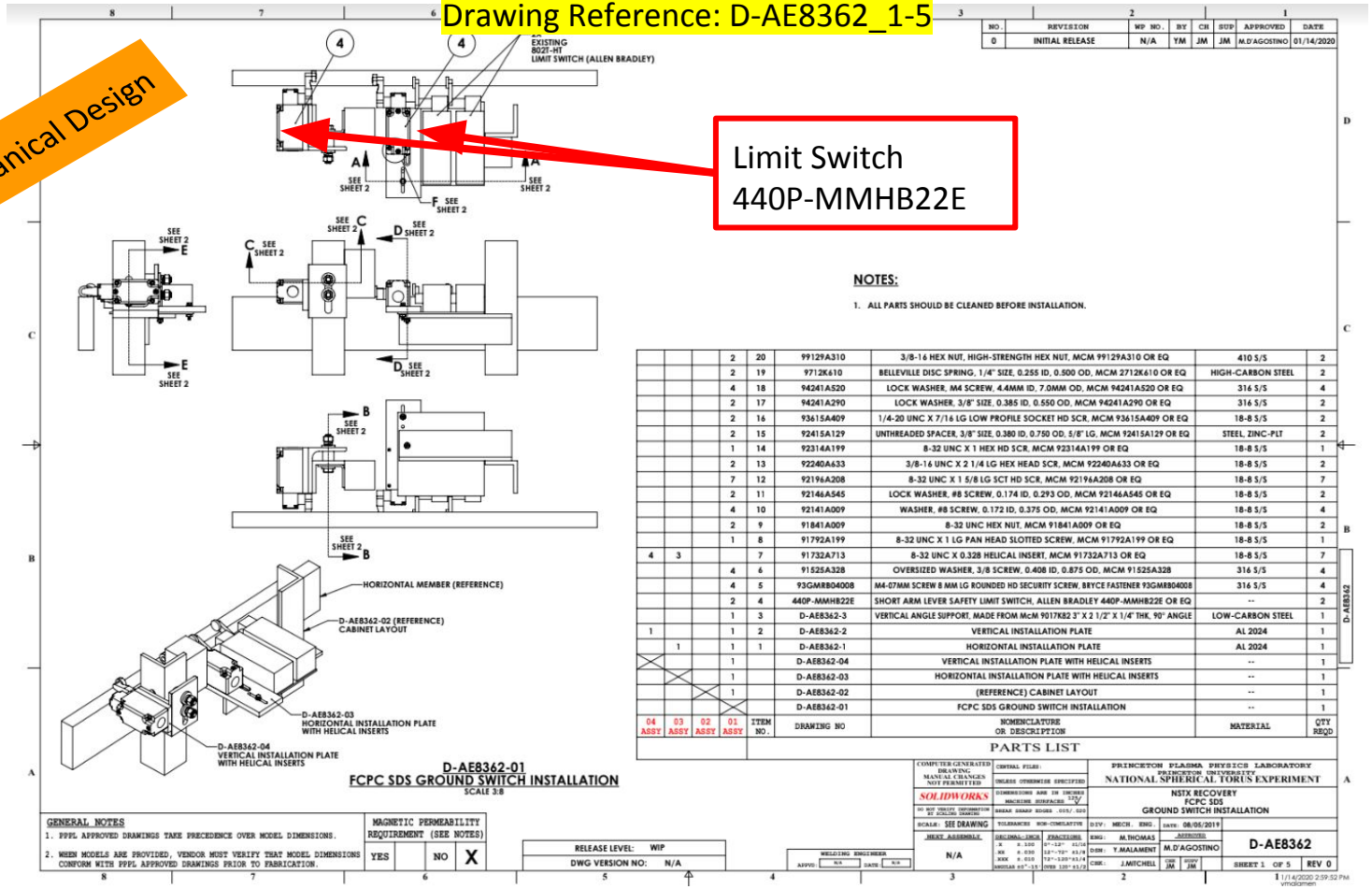
Click me for more NB monitoring slides

FCPC Ground Switch Monitored with AB Limit Switches (440P-MMHB22E) for additional engineering actions (not a SIF)

Drawing Reference: D-AE8362_1-5

Mechanical Design

Limit Switch
440P-MMHB22E



NO.	REVISION	WP NO.	BY	CH	SUP	APPROVED	DATE
0	INITIAL RELEASE	N/A	YM	JM	JM	M.D'AGOSTINO	01/14/2020

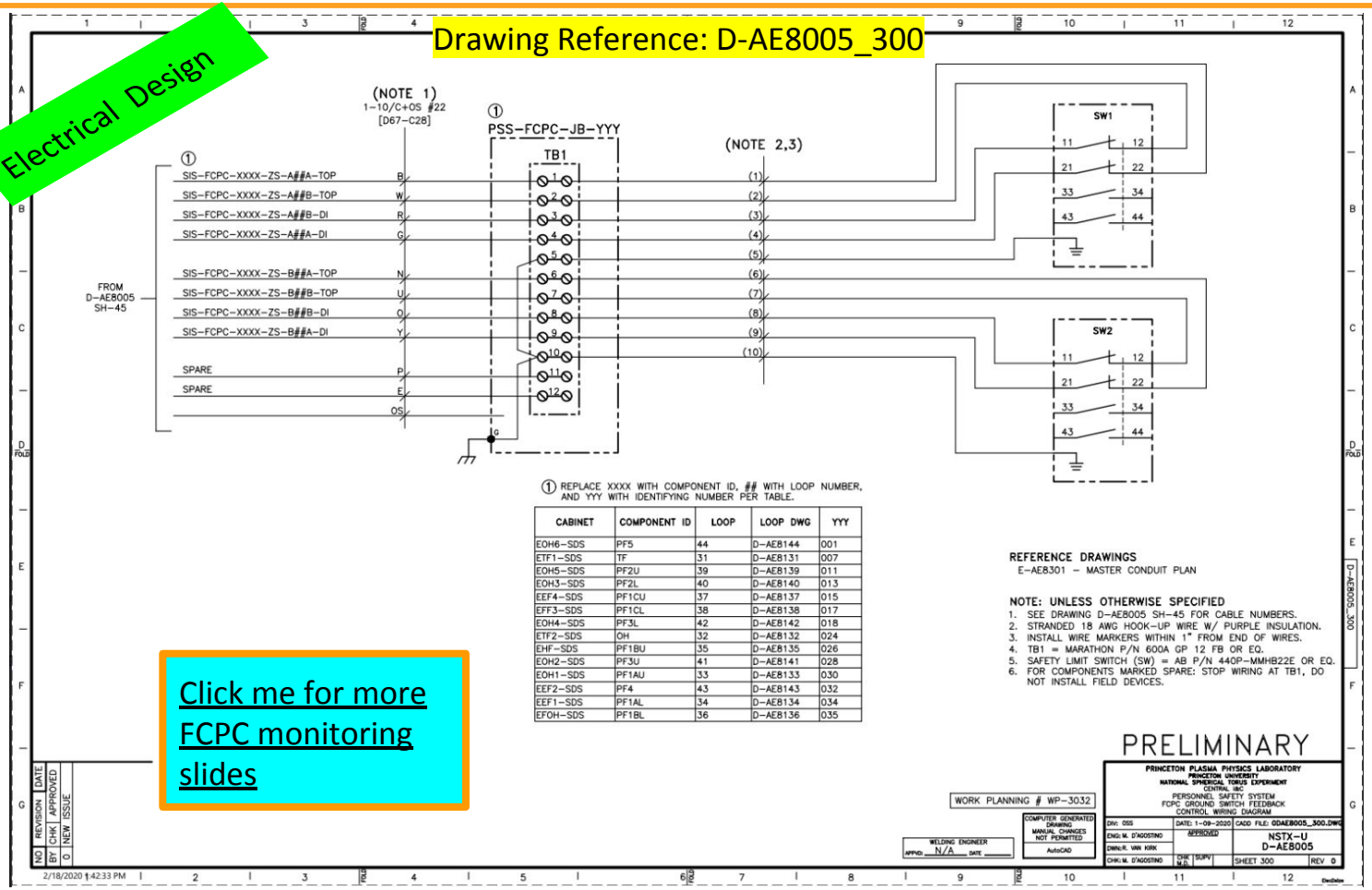
04 ASSY	03 ASSY	02 ASSY	01 ASSY	ITEM NO.	DRAWING NO	NOMENCLATURE OR DESCRIPTION	MATERIAL	QTY REQD
			2	20	99129A310	3/8-16 HEX NUT, HIGH-STRENGTH HEX NUT, MCM 99129A310 OR EQ	410 S/S	2
			2	19	9712K610	BELLEVILLE DISC SPRING, 1/4" SIZE, 0.255 ID, 0.500 OD, MCM 2712K610 OR EQ	HIGH-CARBON STEEL	2
			4	18	94241A520	LOCK WASHER, M4 SCREW, 4.4MM ID, 7.0MM OD, MCM 94241A520 OR EQ	316 S/S	4
			2	17	94241A290	LOCK WASHER, 3/8" SIZE, 0.385 ID, 0.550 OD, MCM 94241A290 OR EQ	316 S/S	2
			2	16	93615A409	1/4-20 UNC X 7/16 LG LOW PROFILE SOCKET HD SCR, MCM 93615A409 OR EQ	18-8 S/S	2
			2	15	92415A129	UNTHREADED SPACER, 3/8" SIZE, 0.380 ID, 0.750 OD, 5/8" LG, MCM 92415A129 OR EQ	STEEL, ZINC-PLT	2
			1	14	92314A199	8-32 UNC X 1 HEX HD SCR, MCM 92314A199 OR EQ	18-8 S/S	1
			2	13	92240A633	3/8-16 UNC X 2 1/4 LG HEX HEAD SCR, MCM 92240A633 OR EQ	18-8 S/S	2
			7	12	92196A208	8-32 UNC X 1 5/8 LG SCT HD SCR, MCM 92196A208 OR EQ	18-8 S/S	7
			2	11	92146A545	LOCK WASHER, #8 SCREW, 0.174 ID, 0.293 OD, MCM 92146A545 OR EQ	18-8 S/S	2
			4	10	92141A009	WASHER, #8 SCREW, 0.172 ID, 0.375 OD, MCM 92141A009 OR EQ	18-8 S/S	4
			2	9	91841A009	8-32 UNC HEX NUT, MCM 91841A009 OR EQ	18-8 S/S	2
			1	8	91792A199	8-32 UNC X 1 LG PAN HEAD SLOTTED SCREW, MCM 91792A199 OR EQ	18-8 S/S	1
4	3			7	91732A713	8-32 UNC X 0.328 HELICAL INSERT, MCM 91732A713 OR EQ	18-8 S/S	7
			4	6	91525A328	OVERSIZED WASHER, 3/8 SCREW, 0.408 ID, 0.875 OD, MCM 91525A328	316 S/S	4
			4	5	93GMR804008	M4-07MM SCREW 8 MM LG ROUNDED HD SECURITY SCREW, BRYCE FASTENER 93GMR804008	316 S/S	4
			2	4	440P-MMHB22E	SHORT ARM LEVER SAFETY LIMIT SWITCH, ALLEN BRADLEY 440P-MMHB22E OR EQ	--	2
			1	3	D-AE8362-3	VERTICAL ANGLE SUPPORT, MADE FROM McM 9017K82 3" X 2 1/2" X 1/4" THK, 90° ANGLE	LOW-CARBON STEEL	1
1			1	2	D-AE8362-2	VERTICAL INSTALLATION PLATE	AL 2024	1
	1		1	1	D-AE8362-1	HORIZONTAL INSTALLATION PLATE	AL 2024	1
X	X	X	1		D-AE8362-04	VERTICAL INSTALLATION PLATE WITH HELICAL INSERTS	--	1
X	X	X	1		D-AE8362-03	HORIZONTAL INSTALLATION PLATE WITH HELICAL INSERTS	--	1
X	X	X	1		D-AE8362-02	(REFERENCE) CABINET LAYOUT	--	1
X	X	X	X		D-AE8362-01	FCPC SDS GROUND SWITCH INSTALLATION	--	1

PARTS LIST

FCPC Ground Switch Monitored with AB Limit Switches (440P-MMHB22E) for additional engineering actions (not a SIF)

Electrical Design

Drawing Reference: D-AE8005_300



CABINET	COMPONENT ID	LOOP	LOOP DWG	YYY
EOH6-SDS	PF5	44	D-AE8144	001
ETF1-SDS	TF	31	D-AE8131	007
EOH5-SDS	PF2U	39	D-AE8139	011
EOH3-SDS	PF2L	40	D-AE8140	013
EEF4-SDS	PF1CU	37	D-AE8137	015
EFF3-SDS	PF1CL	38	D-AE8138	017
EOH4-SDS	PF3L	42	D-AE8142	018
ETF2-SDS	OH	32	D-AE8132	024
EHF-SDS	PF1BU	35	D-AE8135	026
EOH2-SDS	PF3U	41	D-AE8141	028
EOH1-SDS	PF1AU	33	D-AE8133	030
EEF2-SDS	PF4	43	D-AE8143	032
EEF1-SDS	PF1AL	34	D-AE8134	034
EFOH-SDS	PF1BL	36	D-AE8136	035

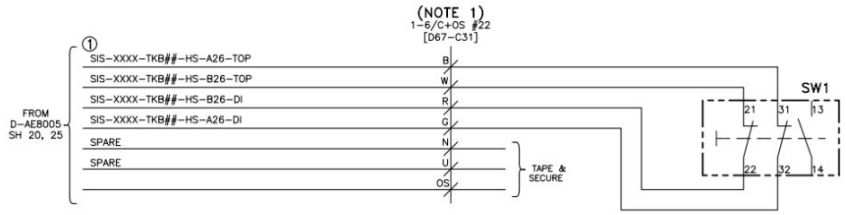
Click me for more FCPC monitoring slides

Select Trapped Key Blocks Monitored with integrated position switch for additional engineering actions (not a SIF)

Electrical Design

Mechanical Design
Refer to TKS
Presentation

Drawing Reference: D-AE8005_350



REFERENCE DRAWINGS
E-AE8301 – MASTER CONDUIT PLAN

NOTE: UNLESS OTHERWISE SPECIFIED
1. SEE DRAWING D-AE8005 SH-20 AND 25 FOR CABLE NUMBERS.
2. BELDEN P/N 9942, 1-6/C+OS 22 AWG, PPL B/M D67-C31.
3. LIMIT SWITCH (SW1) = FORTRESS mGARD LIMIT SWITCH MODULE.

① REPLACE XXXX WITH LOCATION, AND ## WITH TRAPPED KEY BLOCK NUMBER PER TABLE.

LOCATION	TKB	LOOP DWG
NTCN	01	D-AE8126
NTCS	01	D-AE8126
MERM	01	D-AE8126
CSR	01	D-AE8126
TCB	01	D-AE8126

PRELIMINARY

PRINCETON PLASMA PHYSICS LABORATORY
PRINCETON UNIVERSITY
NATIONAL SPHERICAL TORUS EXPERIMENT
CENTRAL, NJ
PERSONNEL SAFETY SYSTEM
TRAPPED KEY LIMIT SWITCH FEEDBACK
CONTROL WIRING DIAGRAM

WORK PLANNING # WP-3032

COMPUTER GENERATED DRAWING. MANUAL CHANGES NOT PERMITTED
AutoCAD

WELDING ENGINEER APPRD: N/A DATE

DWN: OSS | DATE: 1-21-19 | CADD FILE: ODAE8005_350.DWG
ENG: M. D'AGOSTINO | APPROVED | NSTX-U D-AE8005
DWN: C. AGABITI
CHK: X. XXXXXX | CHK X.X | SUPV | SHEET 350 | REV 0

NO | REVISION | DATE
BY | CHK | APPROVED
O | NEW ISSUE

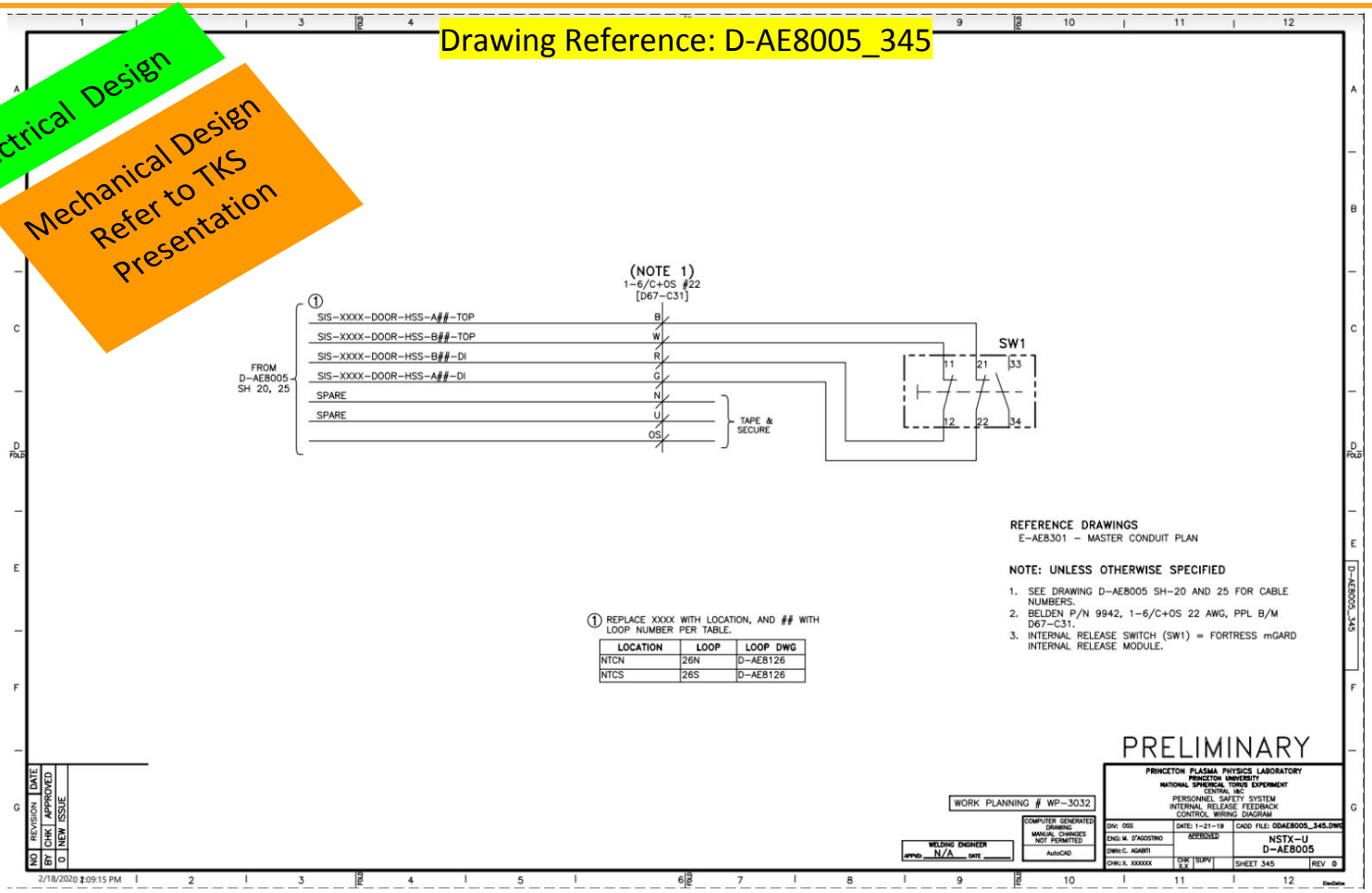
2/18/2020 1:06:39 PM

Cage egress buttons monitored with integrated position switch for additional engineering actions (not a SIF)

Electrical Design

Mechanical Design Refer to TKS Presentation

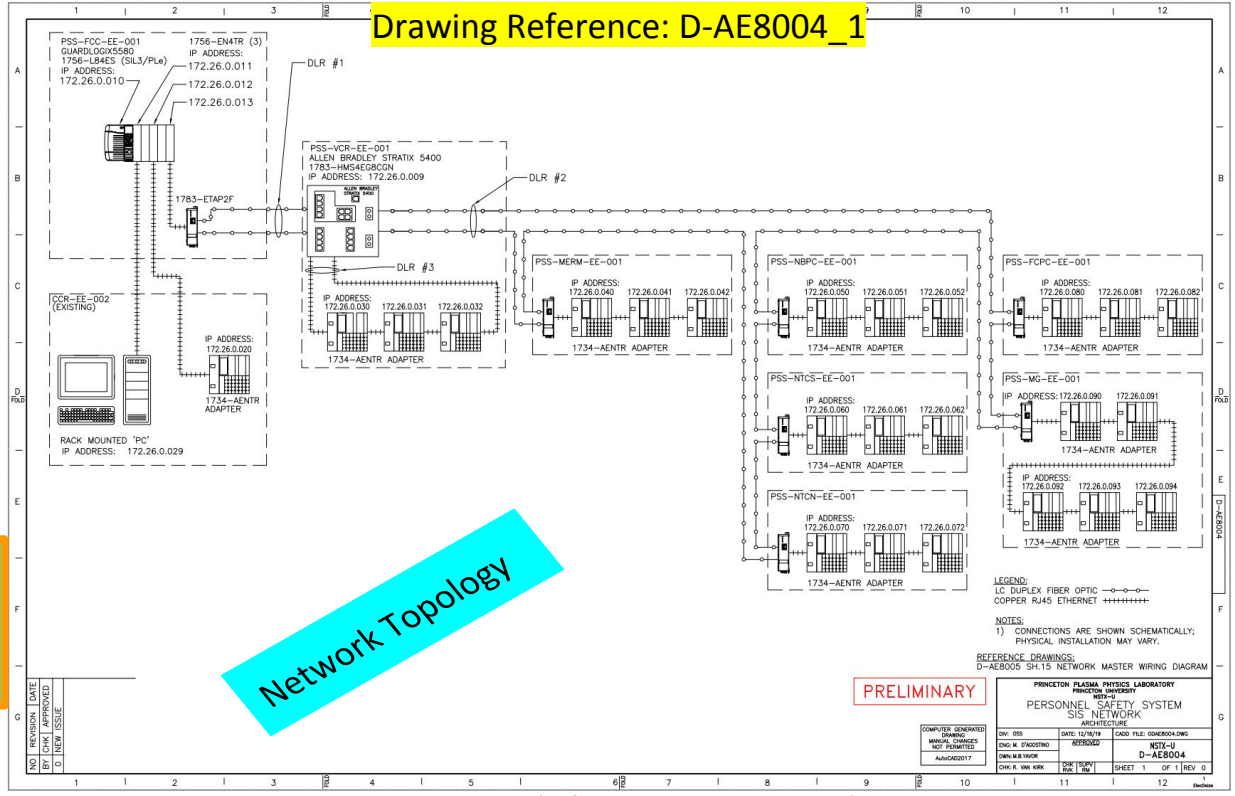
Drawing Reference: D-AE8005_345



The SIS Architecture uses one managed switch, the robust Device Level Ring (DLR) protocol, distributed I/O “drops”, and an IEC-61508-2/3 Logic Solver with its Safety Partner (Guardlogix). The network is air-gapped from all other networks.

- There are redundant I/O chains: *Chain A* and *Chain B*.
- The components have been designed for *safety applications* and are configured to provide De-Energize-to-Trip, fail-safe operation.

Drawing Reference: D-AE8004_1



Network Topology

Click me for HMI & Control Panel Drawings

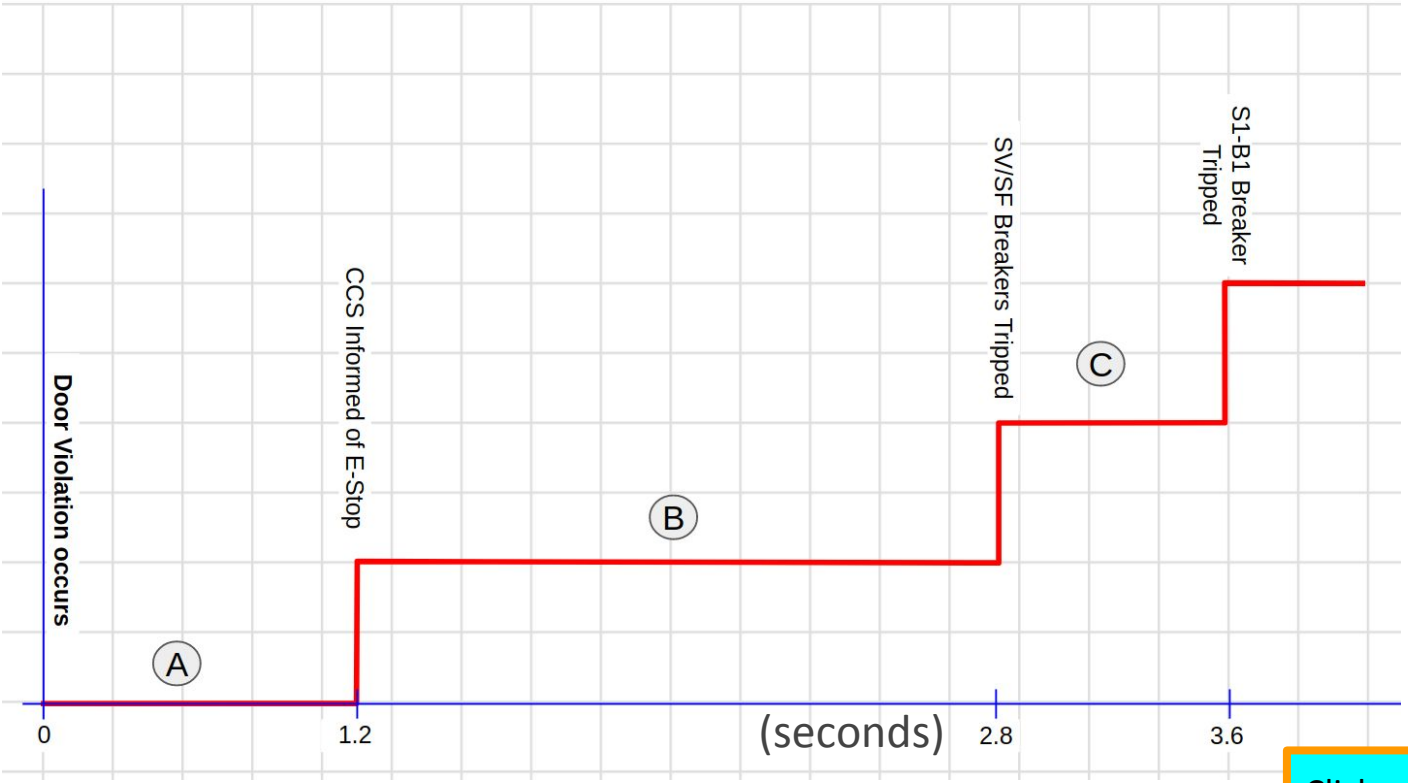
The PLC program uses software modules to facilitate a programming *team* and testability

Outline of NSTXU_1-7-3-1_RD_100
(Software Specification Requirements):

1. Introduction
2. Overall Description
3. External Interface Specifications
4. **Software Modules**
   - **12 Modules**
   - **65 Functions**
5. Non-Functional Requirements

Modular programming is a software design technique that emphasizes separating the functionality into independent modules, such that each contains everything necessary to execute **only one aspect** of the desired functionality.

A conservatively-derived timing diagram illustrates the actions and elapsed time for interdiction following a *door violation.* Requirement is 4.0 seconds.

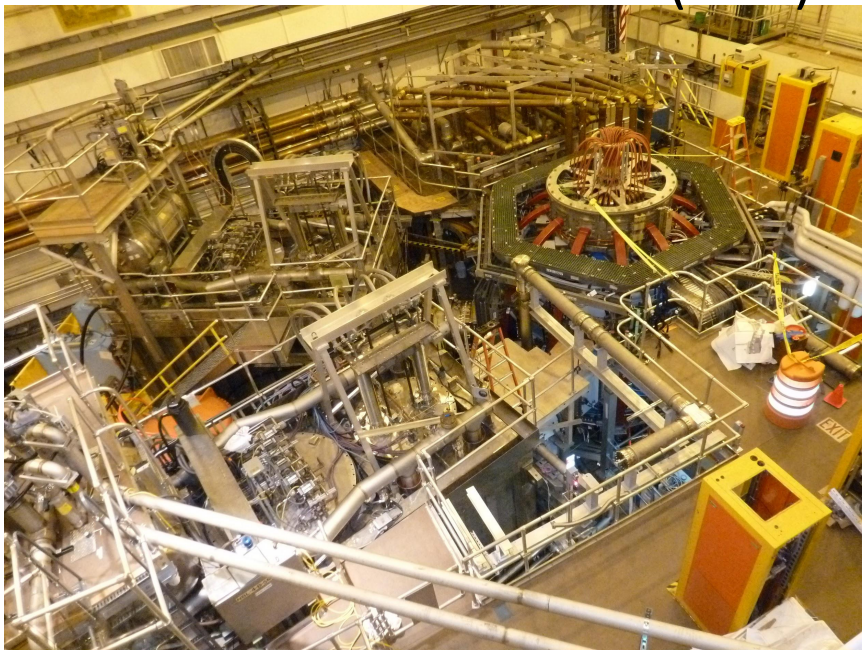


Click me for more overview slides

Assumptions and timing breakdown in *NSTXU_1-7-3-1_RD_100*

There are two SIS-monitored Exclusion Areas that are protected by SIF 1: The NTC and the MER Mezzanine.

NSTX-U Test Cell (NTC)



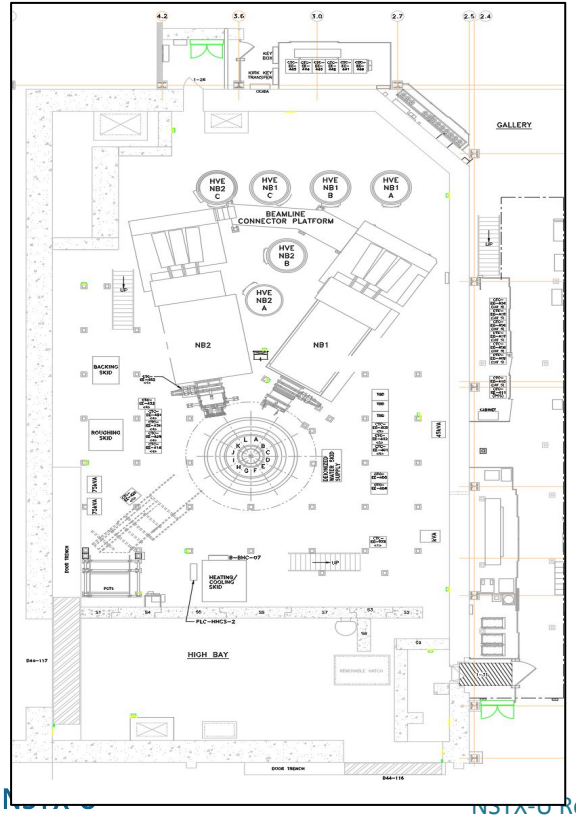
Note: Card Readers Not Used for SIFs

Hazard producing device interdictions will be performed following an Access Violation of these areas (SIF ID S-1)

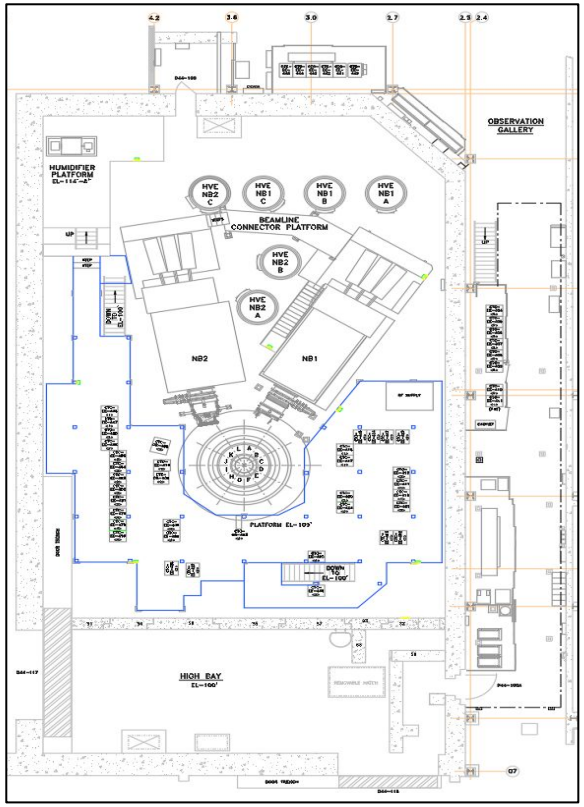
Mechanical Equipment Room (MER) Mezzanine (below the NTC → potential for dose)

The NTC is a complex space with three levels.

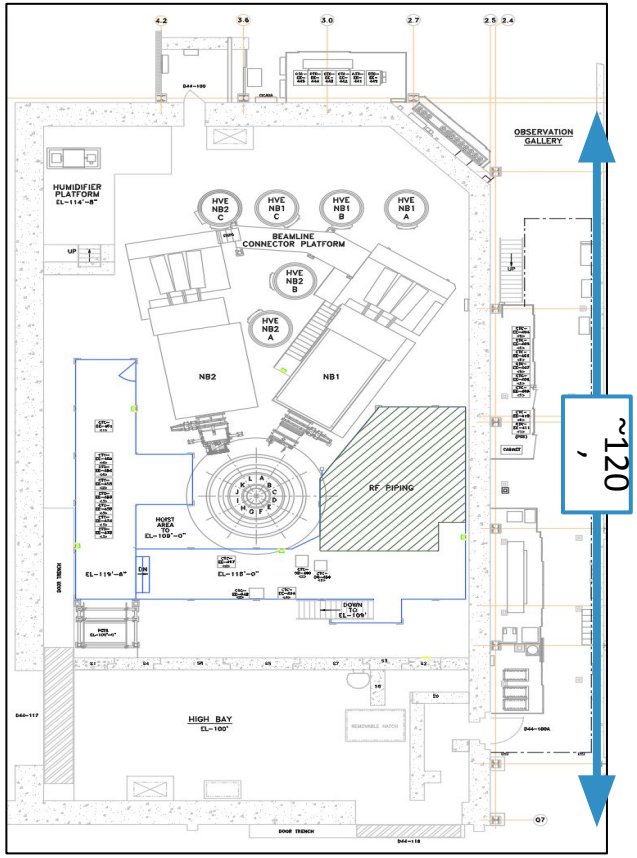
100’ EL



109’ EL



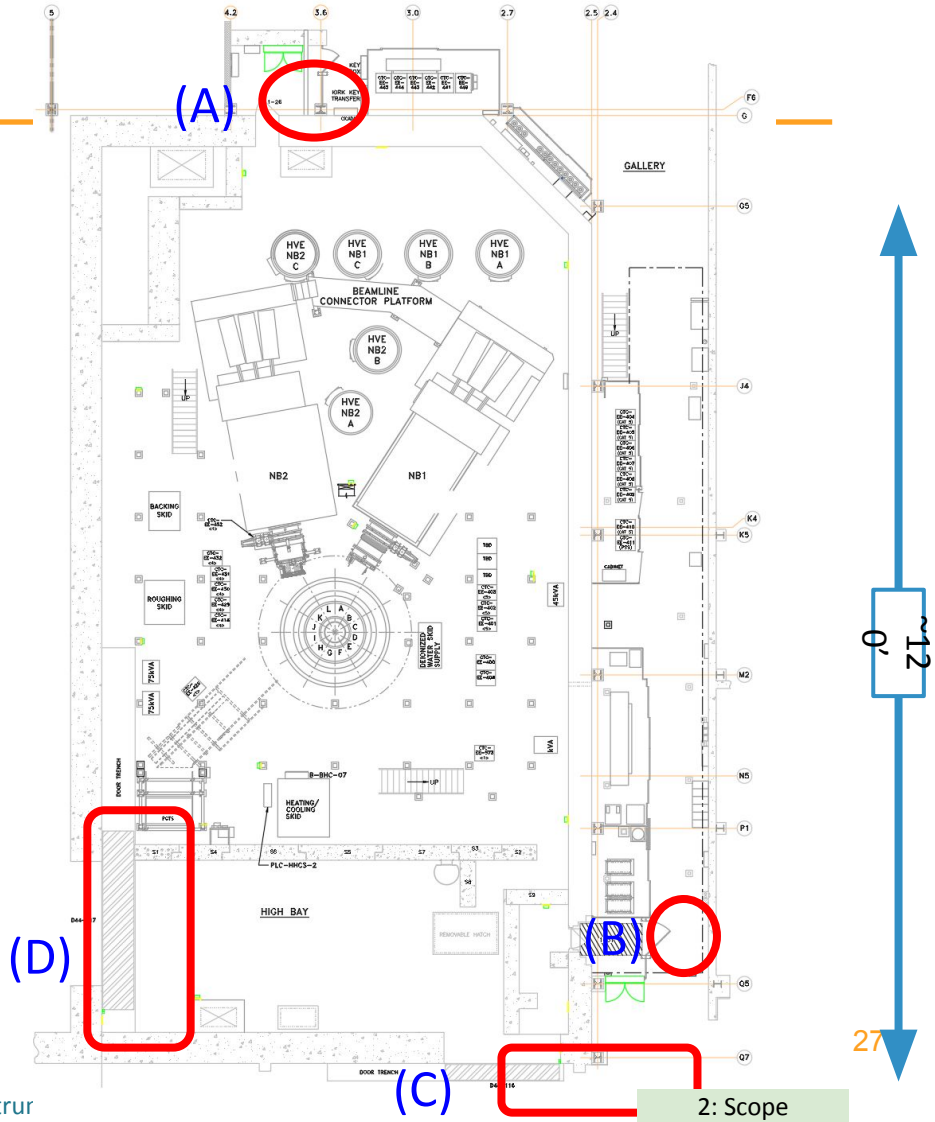
118’ EL



~120’

There are four access points to the NTC:

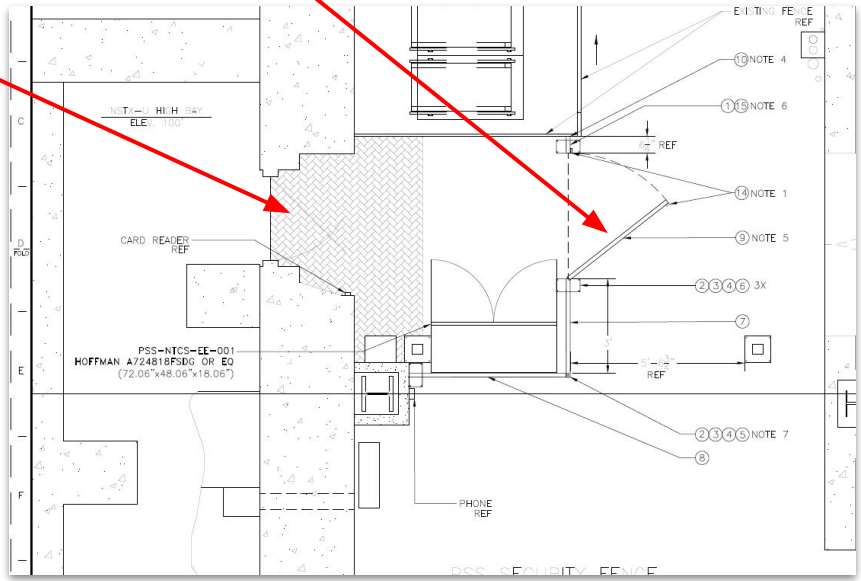
- Two personnel entryways
  - (A) NTC North Door
  - (B) NTC South Door
- Two movable shield doors
  - (C) South Shield Door
  - (D) West Shield Door
- Note: There is a hinged movable shield door at the North Door that will be closed during operations



Personnel Doors will be monitored for Access Violations by the SIS as described previously. Additional protections are described below:

- Personnel entryways to Exclusion Areas will have two independent protection layers:
  - Trapped key locks the outer vestibule door
  - SIS monitors inner door with safety rated components
    - NTC North: movable shield door
    - NTC South: personnel door
    - MER Mezzanine: personnel door
- Violation of inner door during Search & Secure will terminate the S&S
- Violation of inner door during "No Access" state will trigger a PSS-SIS Emergency Stop

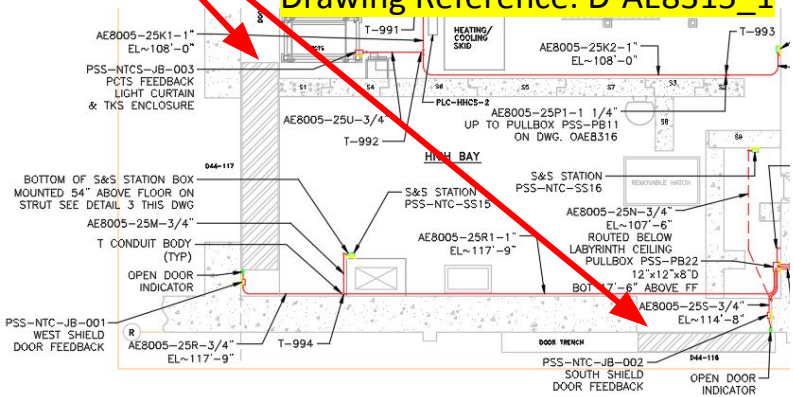
Drawing Reference: D-AE8352_2



Movable Shield Walls will be monitored for Access Violations by SIS as described previously on slides 9-12. Additional protections are described below:

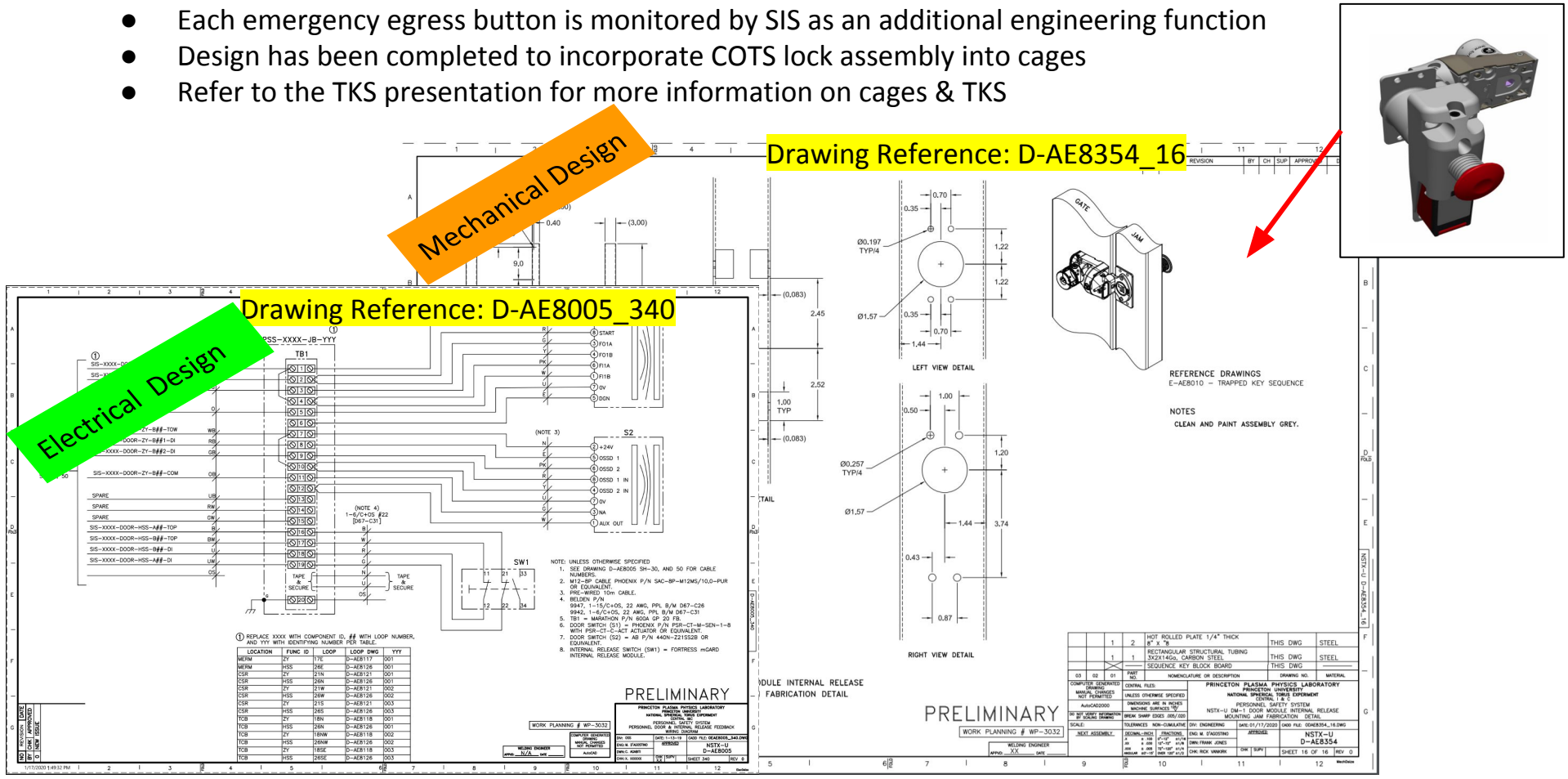
- NTC South and West movable Shield Doors will have two independent layers of protection:
  - Trapped key locks controls in closed position
  - SIS monitors shield door position with safety rated components
- Opening of shield door during Search & Secure will terminate the S&S
- Opening of shield door during “No Access” state will trigger a PSS-SIS Emergency Stop

Drawing Reference: D-AE8315_1



Vestibule door locks feature monitored internal releases for emergency egress.

- Each emergency egress button is monitored by SIS as an additional engineering function
- Design has been completed to incorporate COTS lock assembly into cages
- Refer to the TKS presentation for more information on cages & TKS

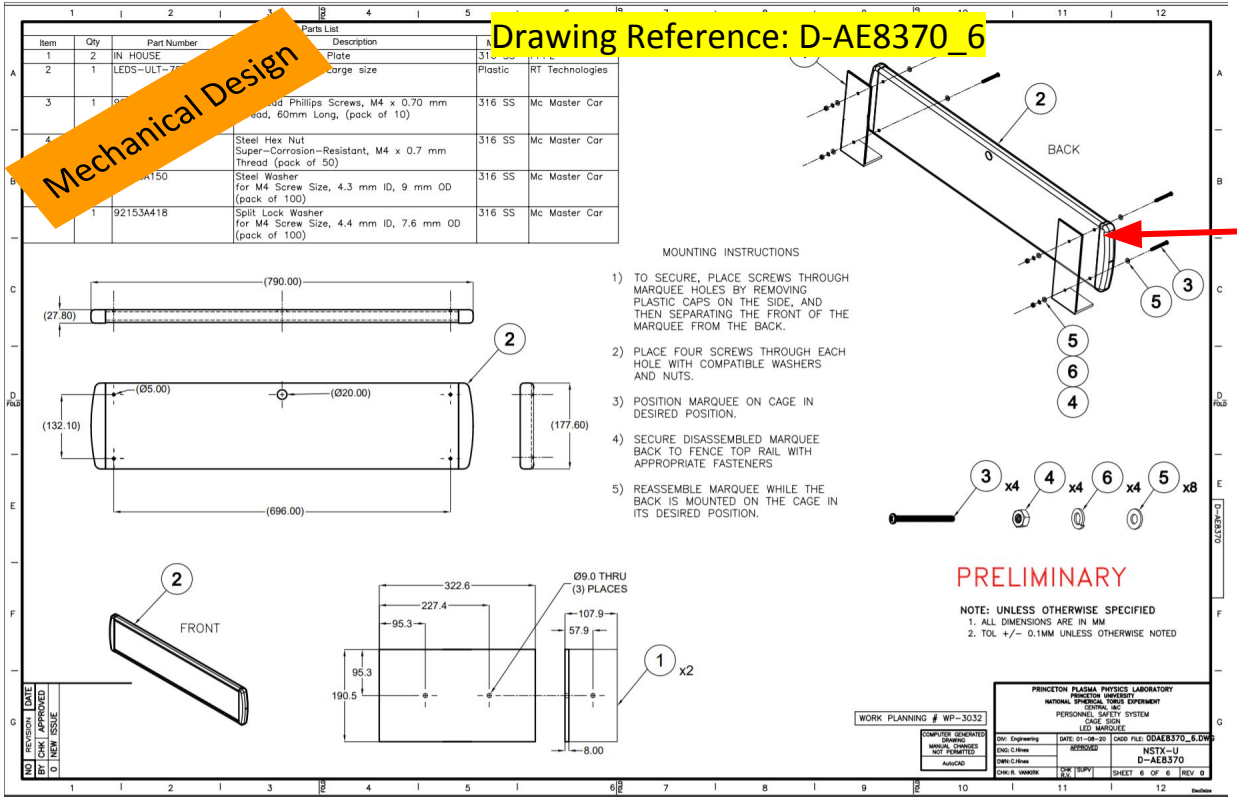


Access State & Area Status is visually displayed for Exclusion Areas, includes fail-safe design.

- Area Status lamp on all Search & Secure stations inside and directly outside Exclusion Areas
  - **GREEN** - SAFE for personnel access
  - **YELLOW** - S&S in progress
  - **RED** - UNSAFE for personnel access (DEFAULT)

- Access State marquee display outside of personnel entryway vestibules
  - Default is **Access Prohibited** unless SIS actively commands **Access Allowed** state
  - Local and remote (COE) administrative control is provided

Marquee to be mounted on top of vestibule doors to display access state.



LEDS-ULT-790-AP-2W

The Search & Secure (S&S) stations provide area status, S&S feedback, and E-Stop functionality

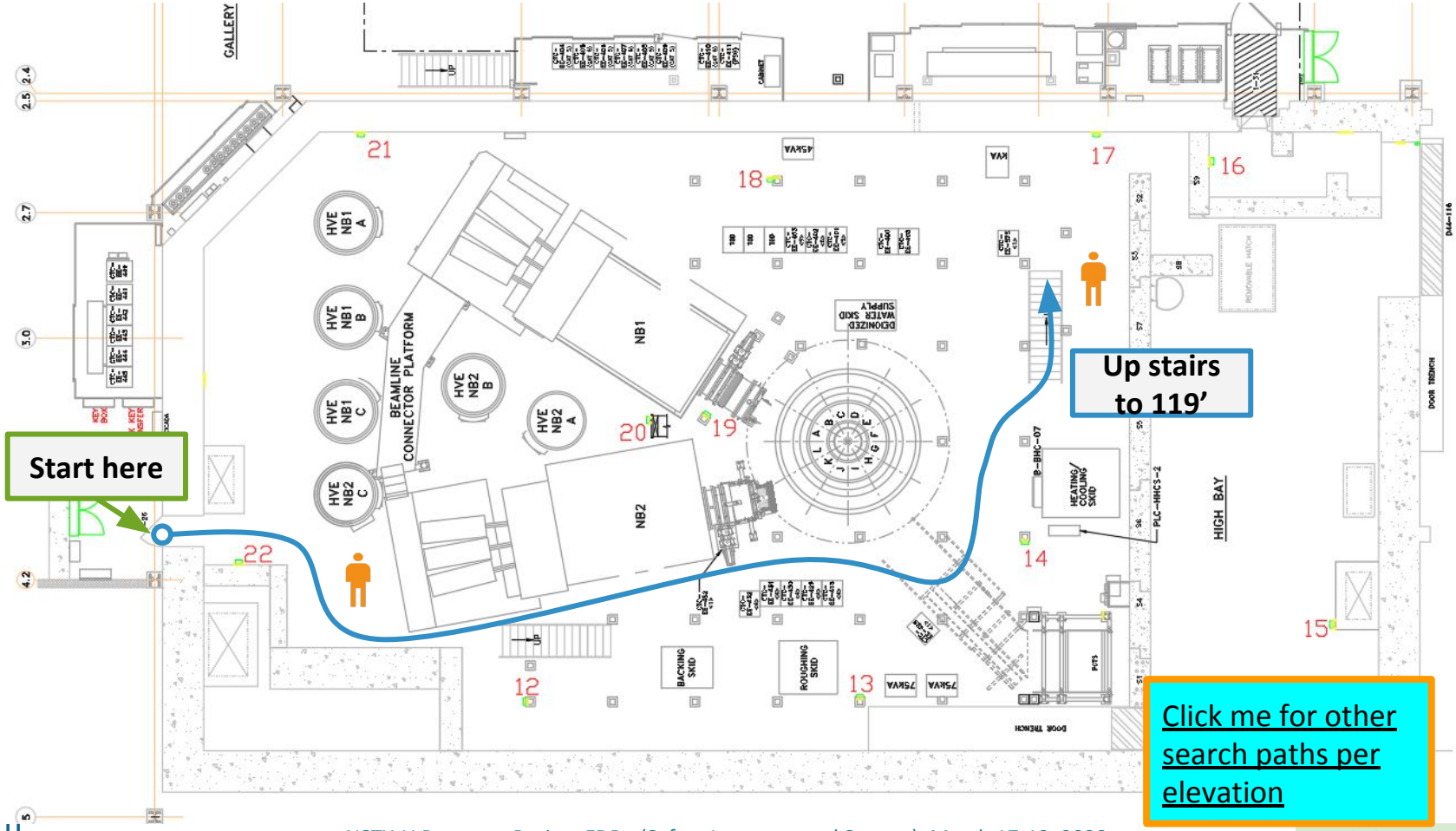
- S&S will be performed in SIS protected Exclusion Areas prior to NSTX-U operations
  - NSTX-U Test Cell (NTC)
    - 22 Stations plus 1 for Control and 1 for Status
  - MER Mezzanine
    - 3 Stations plus 1 for Control
- Simple user interface
- Integrated E-Stop button
  - ESHD 5008 requires: “Personnel within an interlocked area shall not have to travel more than 50 feet to reach an ESTOP”
- Search & Secure will be performed by **trained** and **qualified** personnel

Click me for S&S Drawing slide

The Search & Secure process has been defined and verified with the Machine Technicians.

- Machine techs perform initial sweep to warn personnel to leave
- NSTX-U Test Cell (shown in following slides):
  - South vestibule door, South and West Shield doors are locked and secured via TKS. This releases a trapped key used to initiate S&S (see presentation on TKS for details)
  - Three people are required to complete
  - S&S is initiated at the North door, card readers are disabled after the search team enters
  - Each search team member takes a trapped key with them for personnel accountability
- MER Mezzanine:
  - Similar process to NTC, much smaller and less complex
  - Two people required

S&S is initiated at the North Door, two guards stand within view of the stairs to upper levels (100’ elevation).



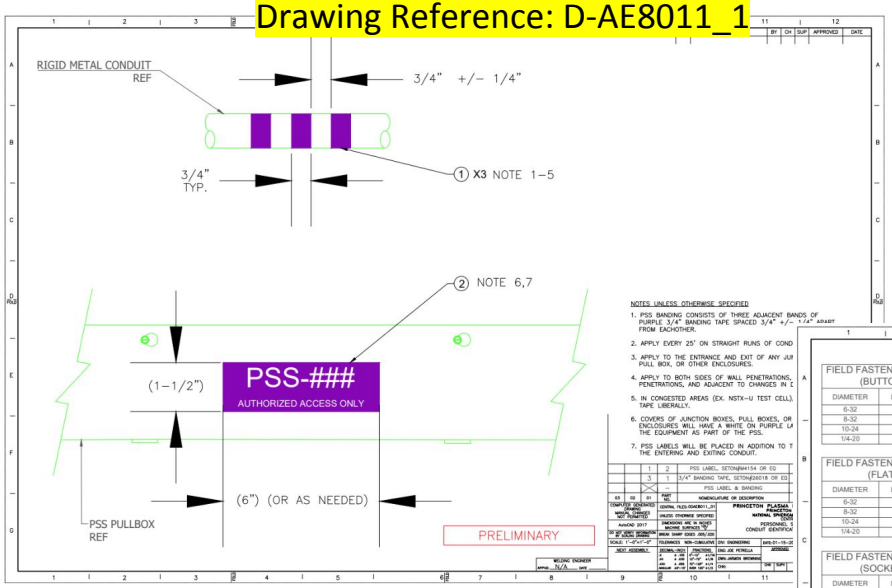
Final steps of the NTC S&S are completed.

- Search team exits
- Hinged movable shield door at the North Door is closed
- Trapped key is removed from S&S Control Station; this key plus the search team keys release a key used to lock and secure the North vestibule door

Search & Secure Complete!

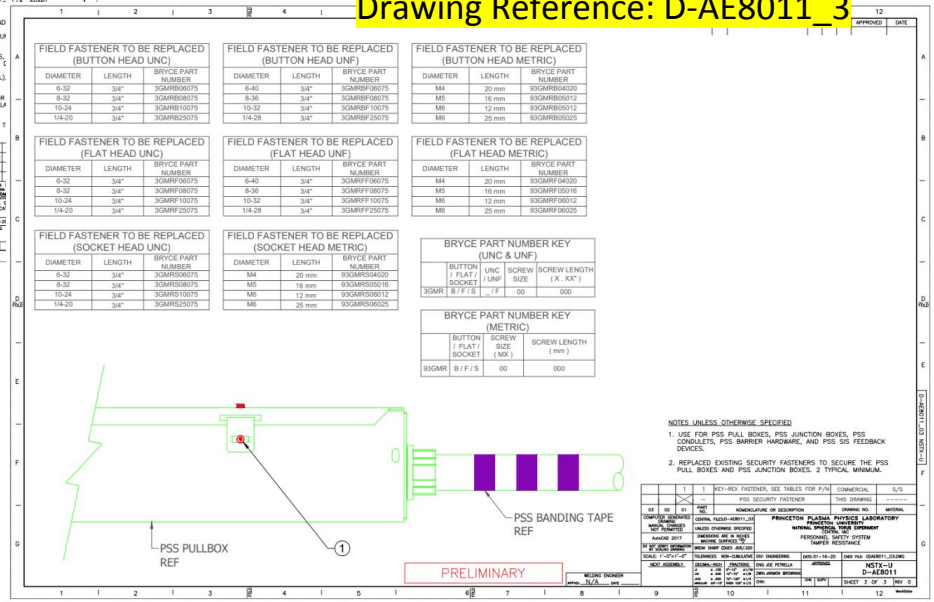
Conduit and enclosures will be uniquely marked/labeled and secured with Bryce Fasteners when installed

Drawing Reference: D-AE8011_1



Bryce Fastener
→

Drawing Reference: D-AE8011_3



FIELD FASTENER TO BE REPLACED (BUTTON HEAD UNC)

DIAMETER	LENGTH	BRYCE PART NUMBER
6-32	3/4"	3GMRB06075
8-32	3/4"	3GMRB08075
10-24	3/4"	3GMRB10075
1/4-20	3/4"	3GMRB25075

FIELD FASTENER TO BE REPLACED (BUTTON HEAD UNF)

DIAMETER	LENGTH	BRYCE PART NUMBER
6-40	3/4"	3GMRBF06075
8-36	3/4"	3GMRBF08075
10-32	3/4"	3GMRBF10075
1/4-28	3/4"	3GMRBF25075

FIELD FASTENER TO BE REPLACED (BUTTON HEAD METRIC)

DIAMETER	LENGTH	BRYCE PART NUMBER
M4	20 mm	93GMRB04020
M5	16 mm	93GMRB05012
M6	12 mm	93GMRB05012
M6	25 mm	93GMRB05025

FIELD FASTENER TO BE REPLACED (FLAT HEAD UNC)

DIAMETER	LENGTH	BRYCE PART NUMBER
6-32	3/4"	3GMRF06075
8-32	3/4"	3GMRF08075
10-24	3/4"	3GMRF10075
1/4-20	3/4"	3GMRF25075

FIELD FASTENER TO BE REPLACED (FLAT HEAD UNF)

DIAMETER	LENGTH	BRYCE PART NUMBER
6-40	3/4"	3GMRFF06075
8-36	3/4"	3GMRFF08075
10-32	3/4"	3GMRFF10075
1/4-28	3/4"	3GMRFF25075

FIELD FASTENER TO BE REPLACED (FLAT HEAD METRIC)

DIAMETER	LENGTH	BRYCE PART NUMBER
M4	20 mm	93GMRF04020
M5	16 mm	93GMRF05016
M6	12 mm	93GMRF06012
M6	25 mm	93GMRF06025

FIELD FASTENER TO BE REPLACED (SOCKET HEAD UNC)

DIAMETER	LENGTH	BRYCE PART NUMBER
6-32	3/4"	3GMRS06075
8-32	3/4"	3GMRS08075
10-24	3/4"	3GMRS10075
1/4-20	3/4"	3GMRS25075

FIELD FASTENER TO BE REPLACED (SOCKET HEAD METRIC)

DIAMETER	LENGTH	BRYCE PART NUMBER
M4	20 mm	93GMRS04020
M5	16 mm	93GMRS05016
M6	12 mm	93GMRS06012
M6	25 mm	93GMRS06025

BRYCE PART NUMBER KEY (UNC & UNF)

	BUTTON / FLAT / SOCKET	UNC /UNF	SCREW SIZE	SCREW LENGTH (X.XX")
3GMR	B / F / S	_ / F	00	000

BRYCE PART NUMBER KEY (METRIC)

	BUTTON / FLAT / SOCKET	SCREW SIZE (MX)	SCREW LENGTH (mm)
93GMR	B / F / S	00	000

Click me for more tamper resistance & labeling slides

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

Critical Design and Requirements Guided by the Accelerator Community - People

Institution	Individual	Consultation, Director's Reviews & Independent Project Reviews	CDR	PDR	Site Visit (11/5/19)	FDR
TJNAF	J. Kowal	X	X			X
LBNL	P. Bong	X			X	X
BNL	S. Buda	X	X	X		
ORNL	K. Mahoney	X	X	X	X	
ORNL	D. Freeman	X				X
Ret.	S. Davis	X	X			X

Industrial Consensus Standards served as **guidelines** to the development of PPPL requirements

Requirements From Within the Complex

DOE P 450.4A
DOE Integrated Safety Management Policy

48 CFR 970.5223-1
DOE Integrated Safety Management (ISM)

10 CFR 835
Occupational Radiation Protection

PPPL Safety Manual (ESHD 5008), other ES&H Programs

COMMUNITY BEST PRACTICES

SLAC ANL
BNL FRIB
OTHERS

PPPL REQUIREMENTS

420.2C
Safety of Accelerator Facilities

Industrial Consensus Standards

INDUSTRY BEST PRACTICES

IEC 61508
Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61511
Functional Safety: Safety Instrumented Systems for the process industry sector

ANSI/ISA 84.01
Application of safety instrumented systems for the process industries.

ANSI/HPS N43.1
Radiation Safety for the Design and Operation of Particle Accelerators

Charge questions: 1

A Hierarchical Set of Requirements Were Developed for Personnel Safety

GENERAL REQUIREMENTS DOCUMENT
NSTX-U-RQMT-GRD-001

OPERATIONS & SAFETY SYSTEMS SYSTEM REQUIREMENTS DOCUMENT
NSTX-U-RQMT-SRD-012

PERSONNEL SAFETY SYSTEM SAFETY INSTRUMENTED SYSTEM REQUIREMENTS DOCUMENT
NSTX-U-RQMT-RD-024

TRAPPED KEY SYSTEM REQUIREMENTS DOCUMENT
NSTX-U-RQMT-RD-026

CONFIGURATION CONTROLLED SAFEGUARDS REQUIREMENTS DOCUMENT
NSTX-U-RQMT-RD-027

SAFETY INSTRUMENTED SYSTEM SOFTWARE SPECIFICATIONS REQUIREMENTS DOCUMENT
NSTX-U-RQMT-RD-100

In total these documents form the basis of the IEC-61511 §10 Safety Requirements Specification

Click me for more overview of each document

SRD - Key Requirements for PSS-SIS
Additional Actions and Additional Functions

3.1.1.2 PSS-SIS Additional Actions

b. Prevent operation of interlocked devices when personnel have access to exclusion area.

c. Prevent personnel from accessing areas where interlocked devices may be capable of creating a hazard.

d. Provide E-STOP button functionality for interlocked devices.

e. Monitor personnel door status and interdict interlocked devices upon a door violation and/or emergency exit from the doors in Table 3.1.1.2-1

***Table 3.1.1.2-1**: Additional action areas*

1	Personnel doors on the cable spread room
2	Personnel doors on the TFTR test cell basement caged area

3.1.1.3 PSS-SIS Additional Functions

a. Provide engineered support for search and secure functions for exclusion areas.

b. Provide audible and visual warnings of unsafe status for each securable area.

i. Provide audible and visual warnings within each securable area when transition from safe to unsafe status of the securable area is underway.

ii. Provide a display near primary personnel entryways to securable areas showing the securable area status, the ACCESS system state, etc.

f. Provide centralized display of the NSTX-U Safety System (PSS) status and its associated equipment.

✔ Refer to Slides in the Scope section of this talk and the TKS Talk

✔ Refer to Scope

✔ Refer to Scope

✔ Refer to TKS Talk

✔ Refer to Scope

✔ Refer to Scope

SRD - Key Requirements for PSS-SIS
Key Design Requirements (Highlights,Paraphrasing)

- Fail-safe design (3.2.2 c & d)

  ✔ See Scope & refer to presentation by John Dellas: Project is replacing all 13.8kV breakers with a fail-safe trip mechanism

- Tamper resistance and labelling (3.2.2 e)

  ✔ See Scope

- Testability of features supporting safety functions (3.2.2 f)

  ✔ See Scope

- Monitor interlocked devices for inconsistent state (3.2.2 h)

  ✔ See Scope

- Cybersecurity (3.2.2 i-k)

  ✔ See Scope

SRD - Key Requirements for PSS-SIS
Key Configuration Requirements (Highlights,Paraphrasing)

- No use of card readers for safety functions (3.3 a)
  - ✓ See Scope
- Monitoring of interlocked equipment (3.3 c)
  - ✓ See Scope
- Control room status display (3.3d)
  - ✓ See Scope
- Annunciation outside of exclusion areas (3.3e)
  - ✓ See Scope
- List of interlocked devices - SV breakers and select SF breakers (3.3i)
  - ✓ See Scope

SRD - Key Requirements for PSS-SIS
Key Configuration Requirements (Highlights,Paraphrasing)

***Table 3.3-2**. Conditions for declaring a PSS-SIS Emergency Stop*

	Condition
1	Activation of an E-STOP button
2	Opening of a monitored door to a secured area when PSS-SIS interlocked equipment is in an unsafe state
3	Inconsistent status between the allowed and present state of Interlocked equipment if interlocked equipment is in an unsafe state
4	Internal or timing error in digital processing elements (if applicable)
5	Actuation of the (TKS) Emergency Egress push-button when PSS-SIS interlocked equipment is in an unsafe state

✔ See Scope Slides

k. Upon the occurrence of a PSS-SIS Emergency Stop, the steps in Table 3.3-3 shall be taken.

***Table 3.3-3**. Actions to take upon the declaration of a PSS-SIS Emergency Stop*

1	Transmission of shutdown signal to the CCS
2	Shutdown of all PSS-SIS interlocked systems after an allowed delay
3	Place all securable areas in a LOCKDOWN state

✔ See Scope Slides & CCS Talk

SRD - Key Requirements for PSS-SIS
Key Performance Requirements (Highlights, Paraphrasing)

- Transition to a safe state shall occur in < 4 seconds after Emergency Stop (3.4a)

✔ See Scope

- 300 second gap between transition to NO ACCESS and the transition to an unsafe state (3.4b)

✔ Refer to FUNC-ASTAT-07 in Software Specifications RD NSTXU_1-7-3-1-1_RD_100

Details of Interfaces Defined in Interface Control Documents

System 1	System 2	ICD Link	Exposition
Operations & Systems Safety	Power Systems	link	Defines interface between the PSS-SIS and the Power Systems
Operations & Systems Safety	Heating Systems	link	Defines interface between the PSS-SIS and the Heating Systems
Operations & Systems Safety	Test Cell	link	Defines interface between the PSS-SIS and the Test Cell

Outline

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

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

Chit Resolution Report for Personnel Safety System

Chit resolution report: NSTXU_1-7-3-1_CRR_chit_100

REVISION 0

July 12, 2019

PREPARED BY:	**Kathleen Lukazik**	6/20/2019 4:31:46 PM
	Kathleen Lukazik,	
REVIEWED BY:	**Joseph Petrella**	6/24/2019 7:20:18 AM
	Joseph Petrella,	
REVIEWED BY:	**Peter Dugan**	7/2/2019 11:17:26 AM
	Peter Dugan,	
REVIEWED BY:	**Timothy N. Stevenson**	7/2/2019 12:10:08 PM
	Timothy N. Stevenson,	
APPROVED BY:	**Stefan Gerhardt**	7/12/2019 1:36:55 PM
	Stefan Gerhardt,	

PRINCETON PLASMA PHYSICS LABORATORY
P.O. BOX 451
PRINCETON, N.J. 08543

CDR Chit Resolution Report R0: link

APPROVED PPPL

PPPL PRINCETON PLASMA PHYSICS LABORATORY

CRR_CHITID - CHIT RESOLUTION REPORT
CHIT RESOLUTION REPORT FOR PERSONNEL SAFETY SYSTEM

NSTXU_1-7-3-1_CRR_100
Rev. 1

Work Planning #:
Effective Date: **01/21/2020**
Prepared By: **Joseph Petrella**

Approved By Kathleen Lukazik, Preparer 01/21/2020 13:21:37 PM

PRINCETON PLASMA PHYSICS LABORATORY
P.O. BOX 451 PRINCETON, N.J. 08543

PDR Chit Resolution Report R1: link

APPROVED PPPL

PPPL PRINCETON PLASMA PHYSICS LABORATORY

ENG-033 - CRR - CHIT RESOLUTION REPORT
CHIT RESOLUTION REPORT FOR PERSONNEL SAFETY SYSTEM

NSTXU_1-7-3-1_CRR_100
Rev. 2

Work Planning #:
Effective Date: **02/20/2020**

FDR Chit Resolution Report R2: link

Chit Resolution Report for *Personnel Safety System*

March 2, 2020

NSTXU_1-7-3-1_CRR_chit_100 Rev 3

Prepared By: Joseph R. Petrella Jr. — Digitally signed by Joseph R. Petrella Jr. Date: 2020.03.02 11:34:58 -05'00'
J. Petrella, PSS Cognizant Engineer

Reviewed By: Timothy N. Stevenson — Digitally signed by Timothy N. Stevenson Date: 2020.03.03 13:13:51 -05'00'

FDR Chit Resolution Report R3: link

Outline

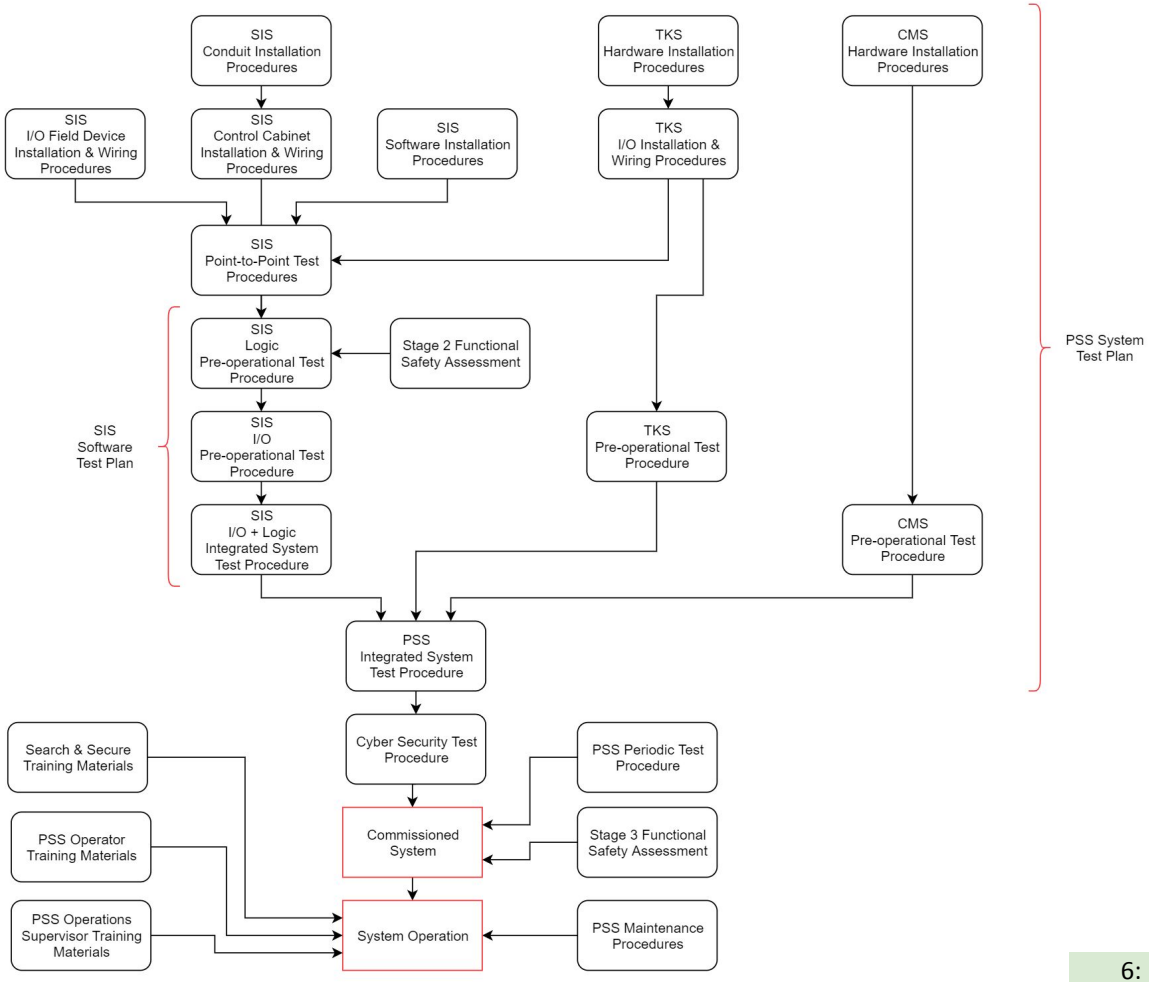
1. Overview
2. Scope
3. Requirements and Interfaces
4. Analysis/Prototyping
5. Chit Closure
6. Procurement, Fabrication, Installation, and Test
7. Risk - Project Risks and Design FMECA
8. Quality, Environmental, Safety, and Health
9. Summary

COTS, Labor, and Panel Assembly planned to be procured through pre-qualified vendors.

Vendors have been identified and pre-qualified for A-1 Components and/or critical services

- Logic Solver & Feedback Components (A-1 components):
  - Five (5) A-1 vendors qualified
  - Purchase requisitions will be ready to issue upon CDE-3B authorization
- Design Support Services (A-1 services)
  - Two (2) Basic Ordering Agreements in place for PLC and SIS design support and have already been extensively utilized
  - Additional tasks can easily be assigned via Job Orders
- Construction Services (A-3 installations)
  - Conduit system installation
    - Expected >$1M Subcontract based on vendor budgetary estimate
    - PSO approval ("Red Book") required prior to issuance of RFP
    - Red Book with RFP will be ready at CDE-3B authorization
  - Control Panel Assembly
    - Vendors identified
    - SOW & purchase requisitions will be ready for issuance upon CDE-3B authorization

Overview of Installation and Commissioning Procedures



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

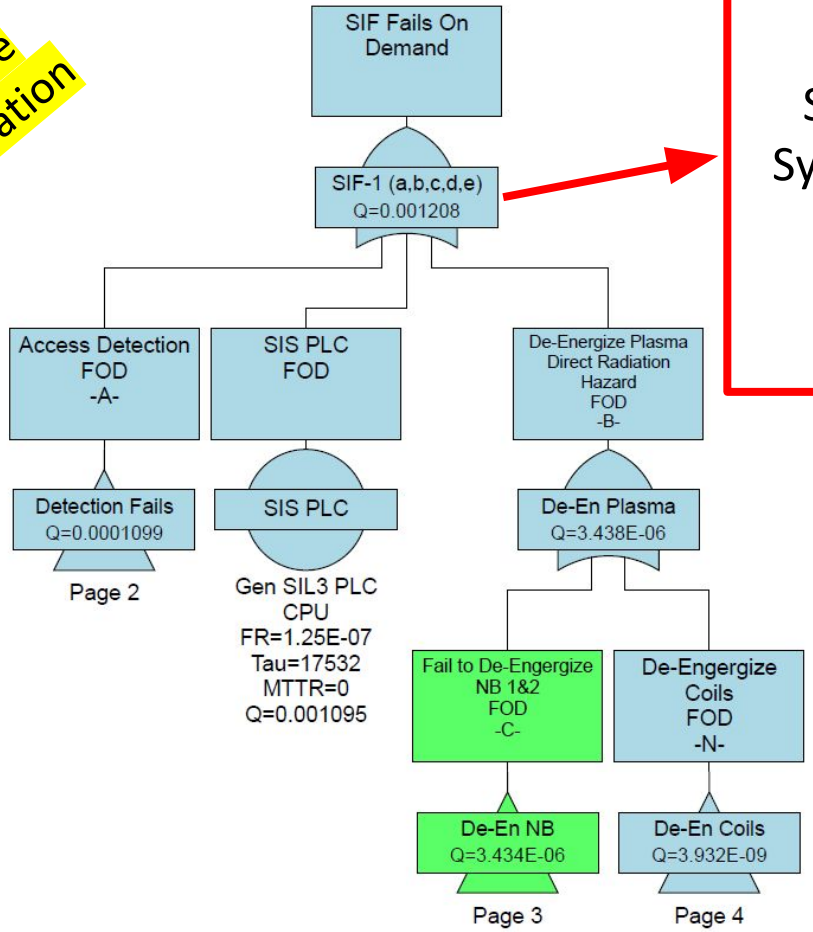
Project Risks are Actively Being Managed

Risk	Score (1-81)	Open/Closed	Risk Retirement Event
If Interlocked Energy Control Devices do not meet minimum performance requirements	49	RETIRED	PDR of PSS
If independent architectures are required for each SIS chain	28	RETIRED	PDR of PSS
Proposed Independent Protection Layers (IPLs) do not meet minimum performance requirements	20	RETIRED	FDR of PSS
If the PSS Qualitative Risk Assessment reduces required Risk Reduction components	0	RETIRED	FDR of PSS
If value engineering reduces the number of interdictive devices in PSS by 50% .	0	RETIRED	FDR of PSS
Install finger-safe guarding around Gaseous helium and exposed electrical to remove/reduce an interlock requirement	0	RETIRED	PDR of PSS

Follow-on risks associated with fitup and installation held at the Project level in the Risk Register

PSS-SIS FMECA encompassed by IEC-61511 Fault Tree Analysis → Refer to LOPA talk at this review

Summation Fault Tree (Top Level) NB Operation & Coils



Performance of the Safety Instrumented System is calculated as:

1/Q=RRF

1/0.001208 = 827

For balance of Fault Trees, refer to:

CALCULATION LINK

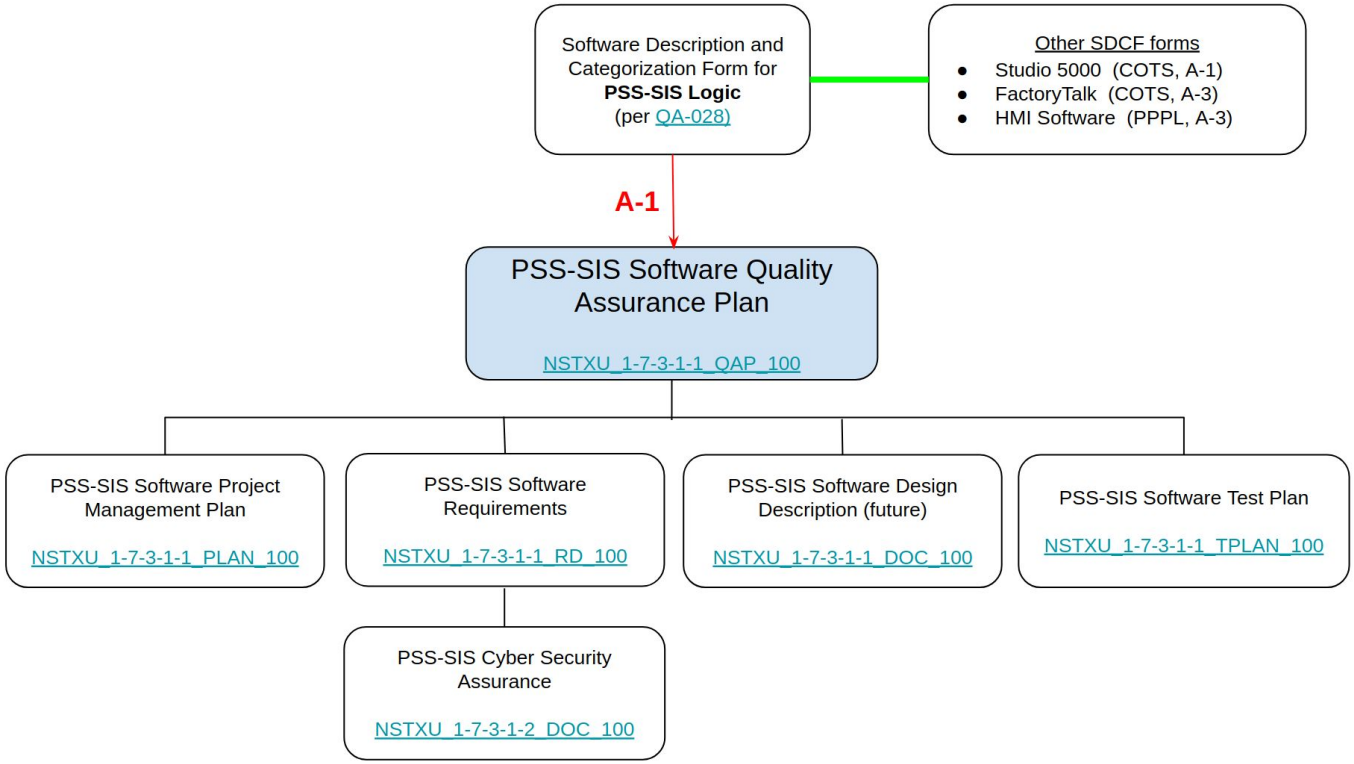
Outline

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

QA/QC, Validation & Oversight

- PPPL QA supplier qualifications for all A-1 components
- Majority of components are COTS - no fabrication oversight needed
- PPPL QA & PPPL Engineering will be used for on-site work and contracted labor oversight
- All PSS-SIS equipment shall be installed by personnel approved by the NSTX-U Head of Operations
- The PSS-SIS validation procedure shall follow a written Integrated System Test Procedure.
- PSS-SIS validation shall include static and functional tests of all PSS inputs, outputs, and operational modes
- Software developed for the PSS shall implement the PPPL Software QA procedures, as appropriate

Quality: Overview of SQA Documents & Plans



Environmental, Safety, & Health

- Work hazards during installation are standard industrial hazards:
  - Hand tools, LOTO, etc.
- Hazards mitigated through PPPL ISM and ES&H internal procedures:
  - Job Hazard Analysis completed prior to the start of planned work.
    - (Cutting, using power tools, eye protection, etc.)
  - Silica Hazard - conduit & hardware component installation
    - Air monitoring - as required
    - Respiratory protection - as required
    - Dust minimization controls - vacuum & water
  - Work scheduled via the rollover and work control center to avoid work area conflicts.
  - All Lockout/Tagout preformed per PPPL procedure ESH-016

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

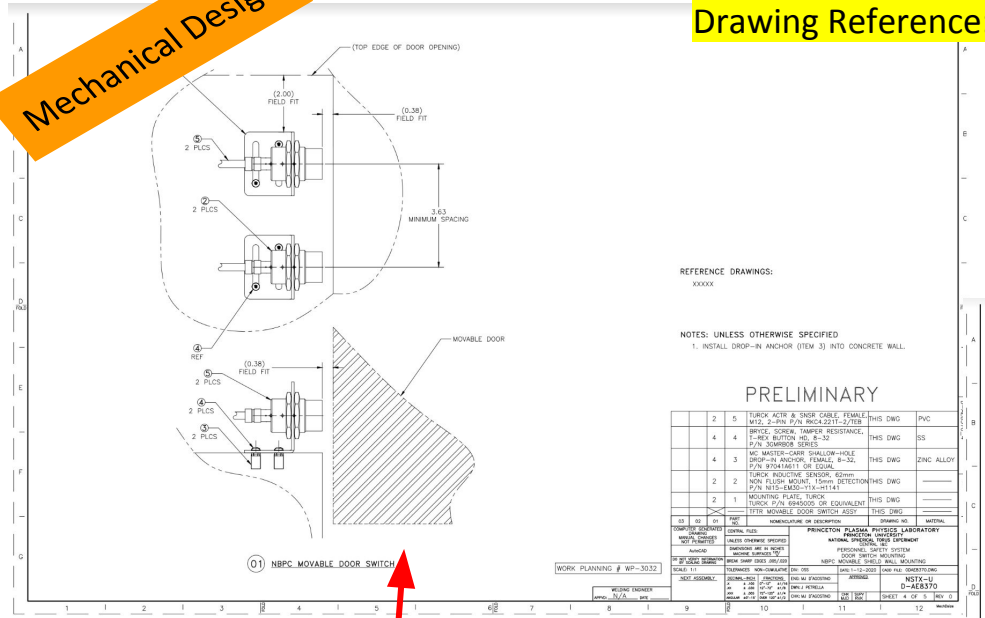
- PSS-SIS Requirements have been met by the design as supported by analysis and an extensive drawing set.
- Interfaces are considered in the design and documented in the ICDs
- All chits are closed
- All Design Risks have been mitigated through the design
- Procurement strategy established
- Majority of vendors already QA qualified
- BOAs used for labor augmentation & construction
- PSS Configuration Managed Credited Controls identified for ASE
- Environmental, Safety, & Health considerations are standard practices for the laboratory

Backup Slides

Movable Shield Walls monitored with (2) Turck Sensors (NI15-EM30-Y1X-H1141) → SIF input

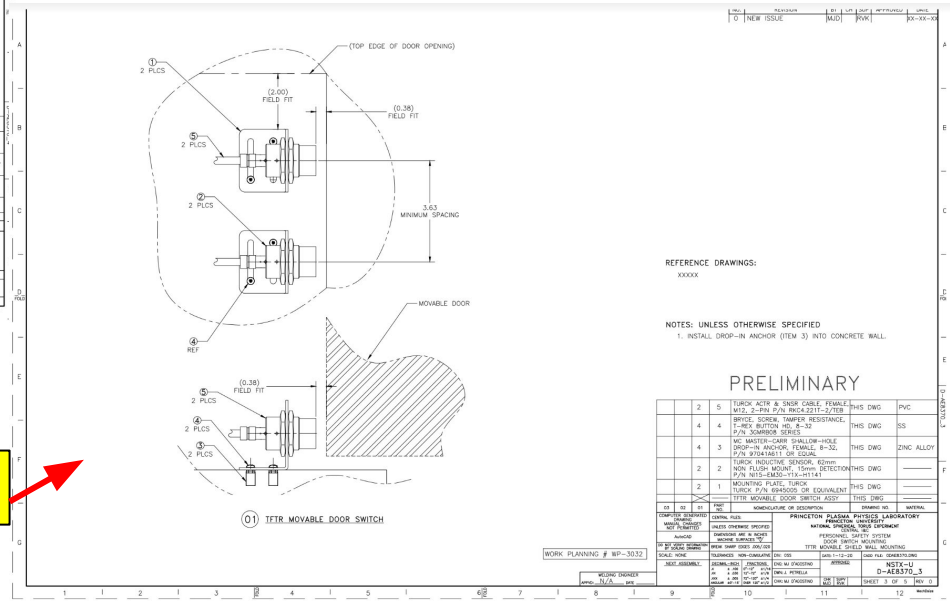
Mechanical Design

Drawing Reference: D-AE8370_3-4



South Shield Wall to adjacent NBPC Building

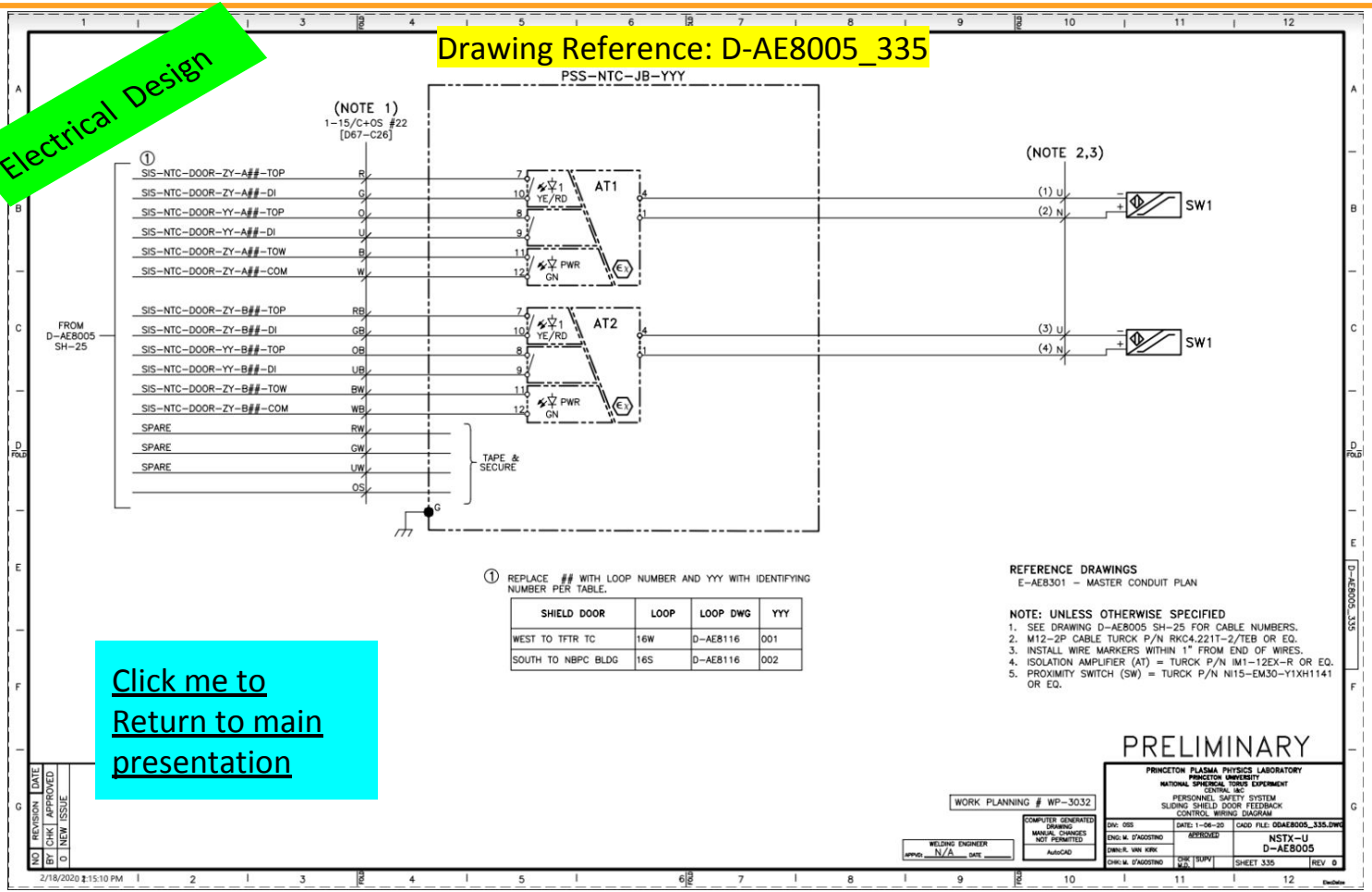
West Shield Wall to adjacent TFTR Test Cell



Movable Shield Walls monitored with (2) Turck Sensors (NI15-EM30-Y1X-H1141) → SIF input

Electrical Design

Drawing Reference: D-AE8005_335



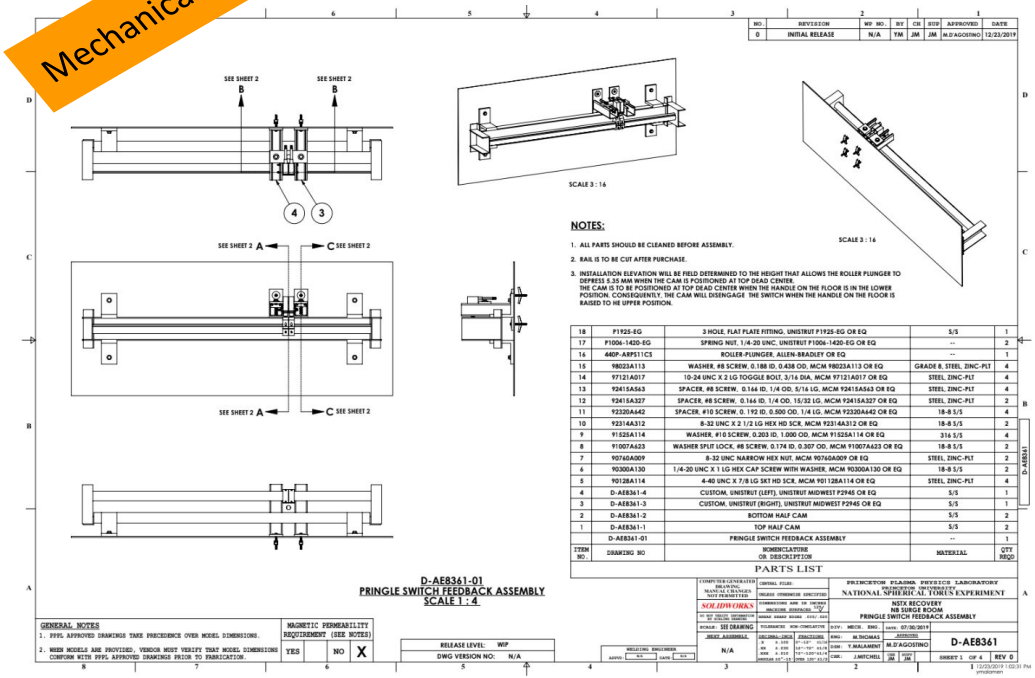
SHIELD DOOR	LOOP	LOOP DWG	YYY
WEST TO TFTR TC	16W	D-AE8116	001
SOUTH TO NBPC BLDG	16S	D-AE8116	002

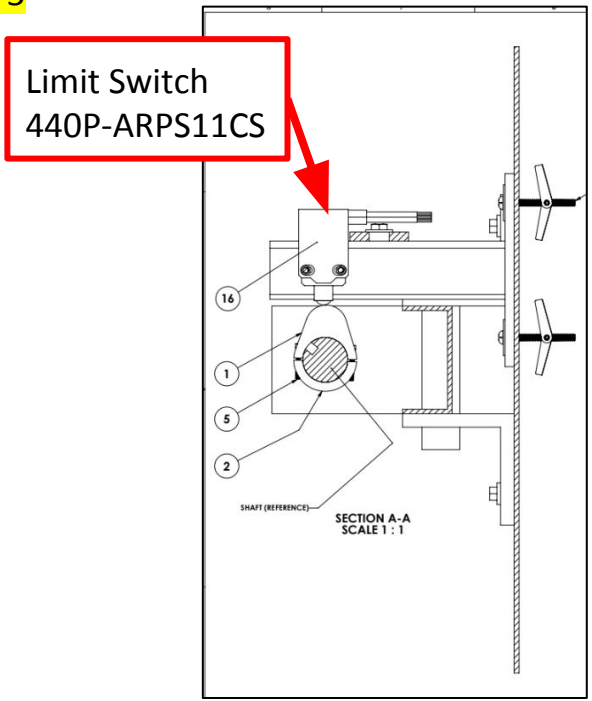
Click me to Return to main presentation

NB Pringle Switch Position Monitored with AB Limit Switches (440P-ARPS11CS) for additional engineering actions (not a SIF)

Mechanical Design

Drawing Reference: D-AE8361_1-5

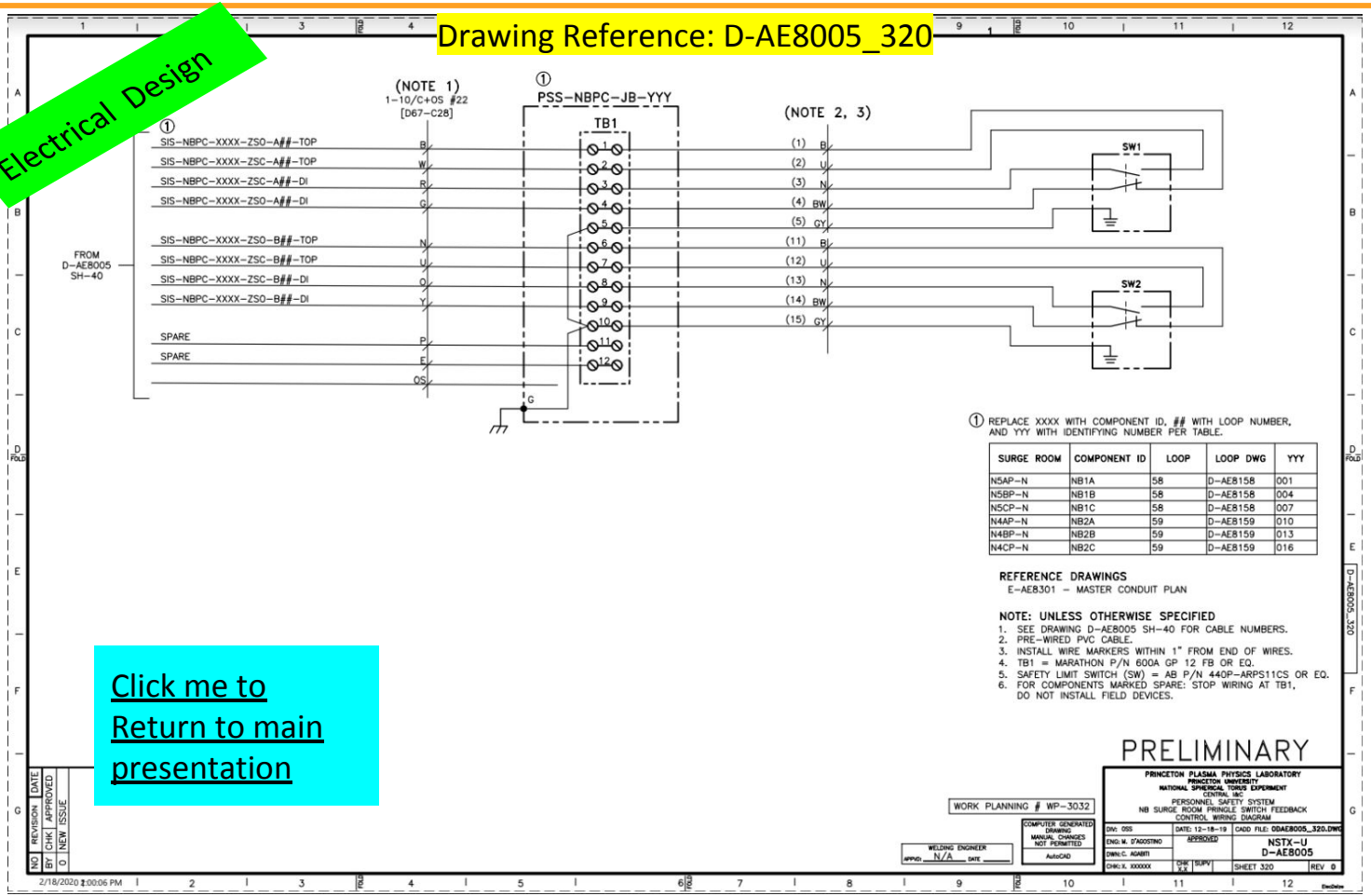




NB Pringle Switch Position Monitored with AB Limit Switches (440P-ARPS11CS) for additional engineering actions (not a SIF)

Drawing Reference: D-AE8005_320

Electrical Design



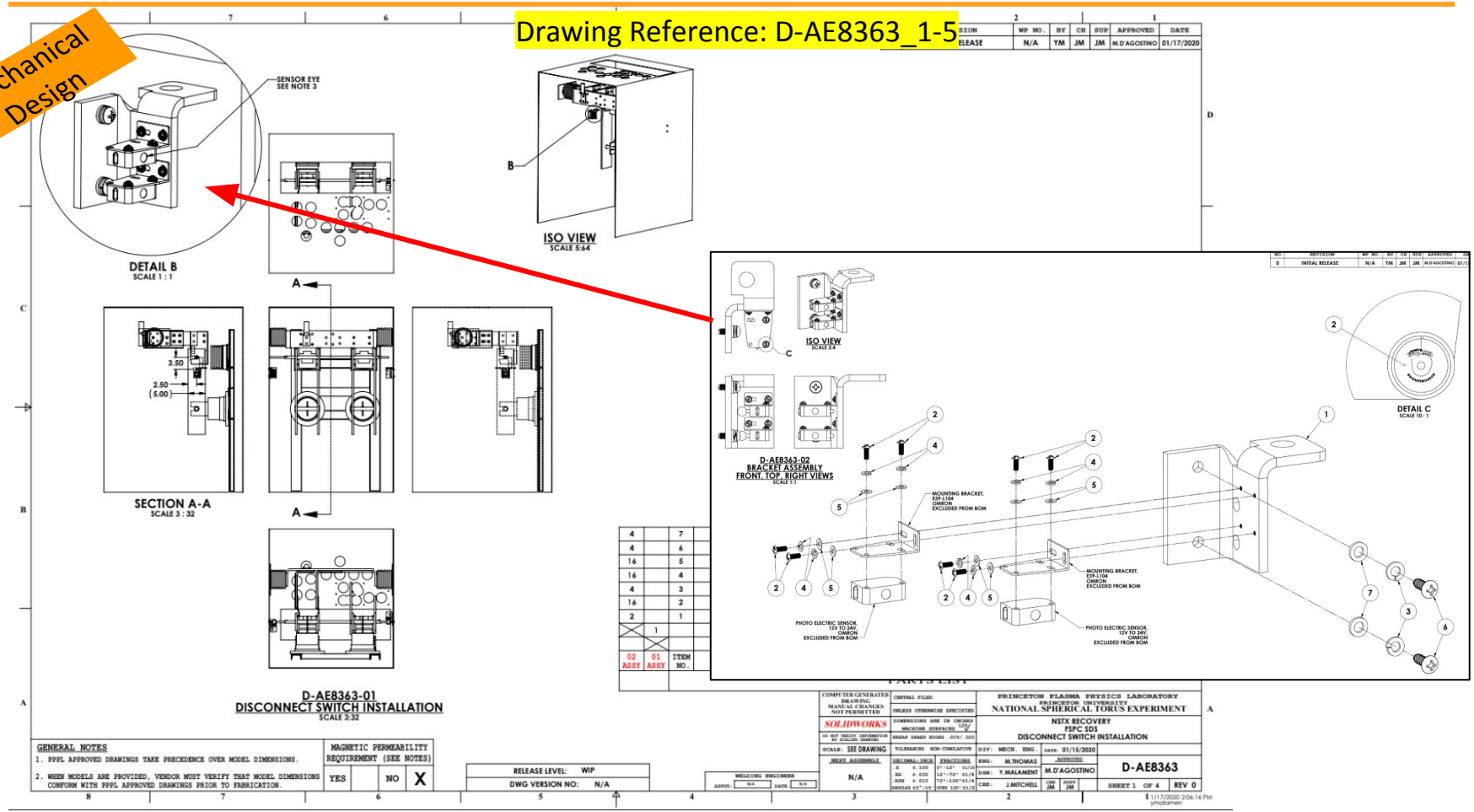
SURGE ROOM	COMPONENT ID	LOOP	LOOP DWG	YYY
N5AP-N	NB1A	58	D-AE8158	001
N5BP-N	NB1B	58	D-AE8158	004
N5CP-N	NB1C	58	D-AE8158	007
N4AP-N	NB2A	59	D-AE8159	010
N4BP-N	NB2B	59	D-AE8159	013
N4CP-N	NB2C	59	D-AE8159	016

Click me to Return to main presentation

FCPC Line Switch Monitored with Omron Optical Switches (E3ZA-T81A) for additional engineering actions (not a SIF)

Mechanical Design

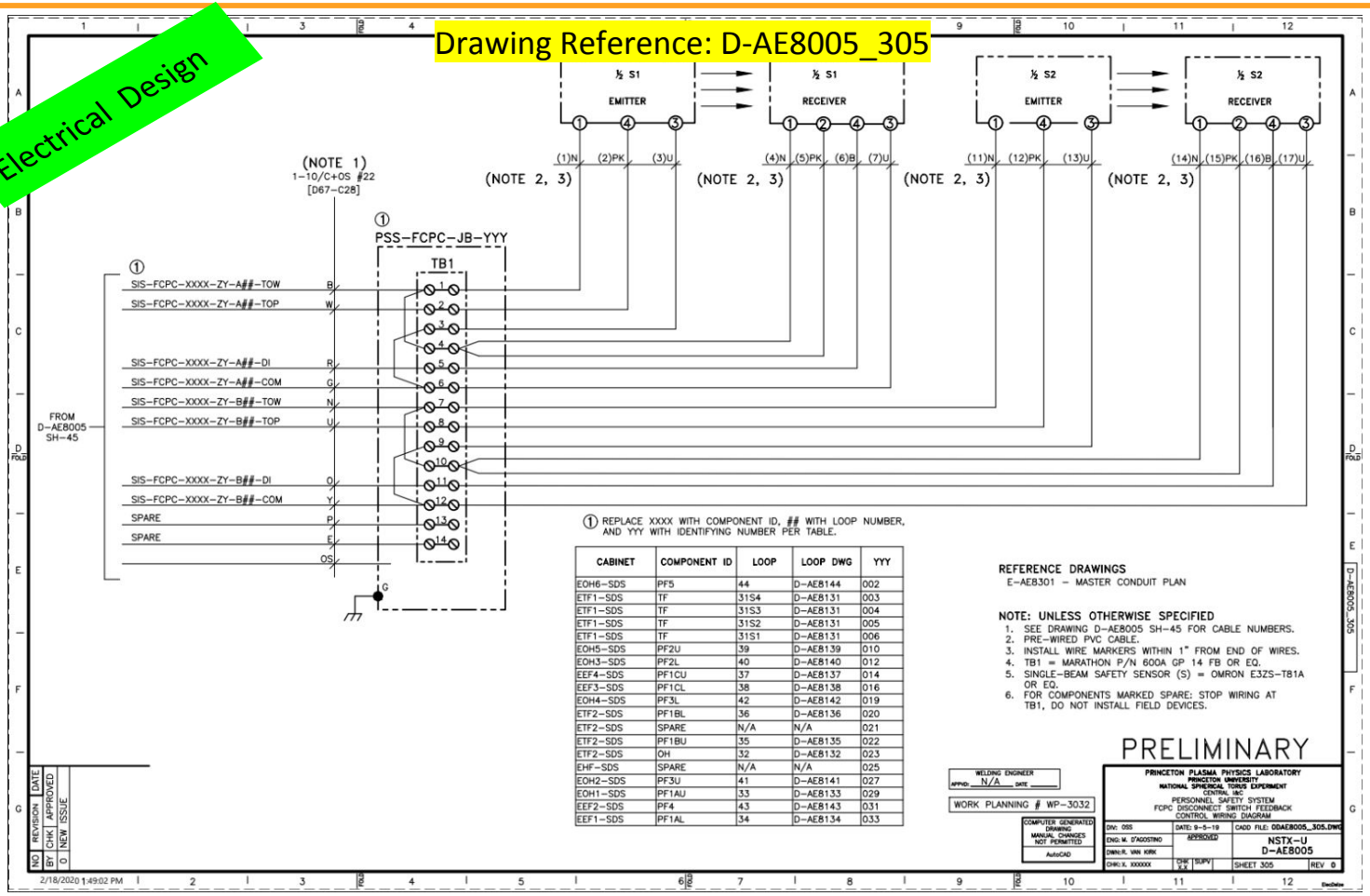
Drawing Reference: D-AE8363_1-5



FCPC Line Switch Monitored with Omron Optical Switches (E3ZA-T81A) for additional engineering actions (not a SIF)

Electrical Design

Drawing Reference: D-AE8005_305

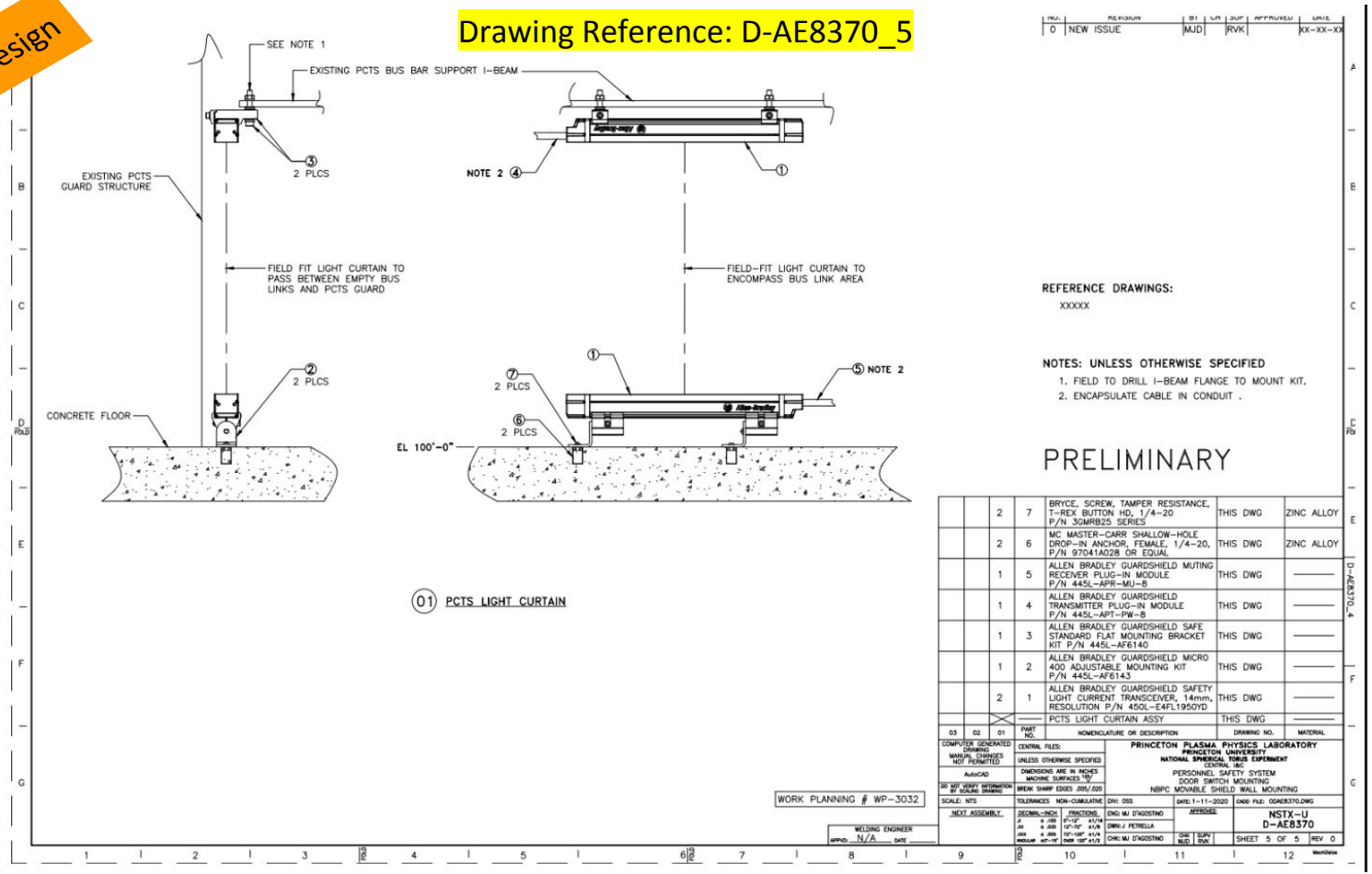


CABINET	COMPONENT ID	LOOP	LOOP DWG	YYY
EOH6-SDS	PF5	44	D-AE8144	002
ETF1-SDS	TF	31S4	D-AE8131	003
ETF1-SDS	TF	31S3	D-AE8131	004
ETF1-SDS	TF	31S2	D-AE8131	005
ETF1-SDS	TF	31S1	D-AE8131	006
EOH5-SDS	PF2U	39	D-AE8139	010
EOH3-SDS	PF2L	40	D-AE8140	012
EEF4-SDS	PF1CU	37	D-AE8137	014
EEF3-SDS	PF1CL	38	D-AE8138	016
EOH4-SDS	PF3L	42	D-AE8142	019
ETF2-SDS	PF1BL	36	D-AE8136	020
ETF2-SDS	SPARE	N/A	N/A	021
ETF2-SDS	PF1BU	35	D-AE8135	022
ETF2-SDS	OH	32	D-AE8132	023
EHF-SDS	SPARE	N/A	N/A	025
EOH2-SDS	PF3U	41	D-AE8141	027
EOH1-SDS	PF1AU	33	D-AE8133	029
EEF2-SDS	PF4	43	D-AE8143	031
EEF1-SDS	PF1AL	34	D-AE8134	033

PCTS Bus Links Monitored with AB Light Curtain (450L-E4FL1950YD) for additional engineering actions (not a SIF)

Mechanical Design

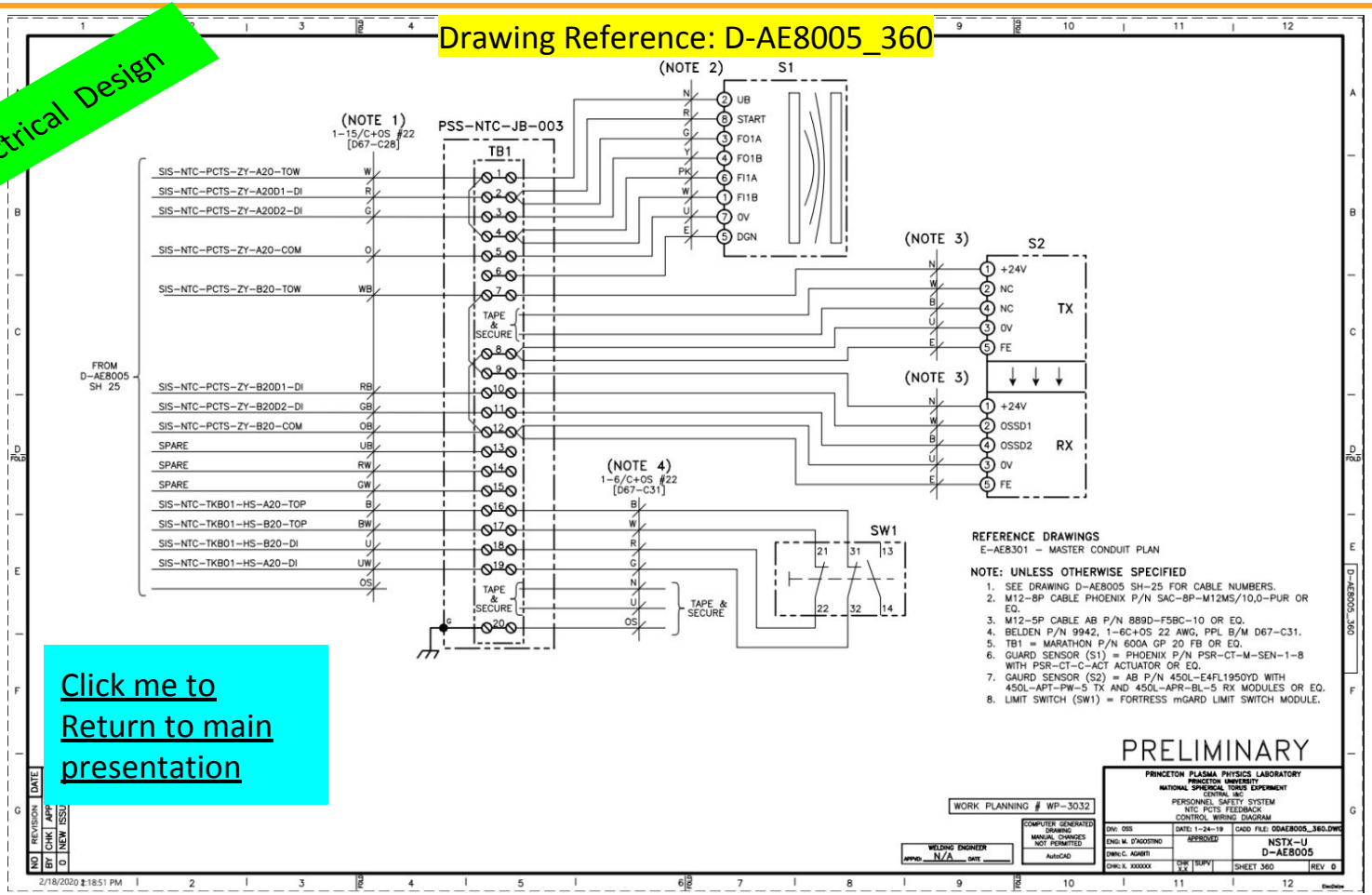
Drawing Reference: D-AE8370_5



PCTS Bus Links Monitored with AB Light Curtain (450L-E4FL1950YD) for additional engineering actions (not a SIF)

Electrical Design

Drawing Reference: D-AE8005_360

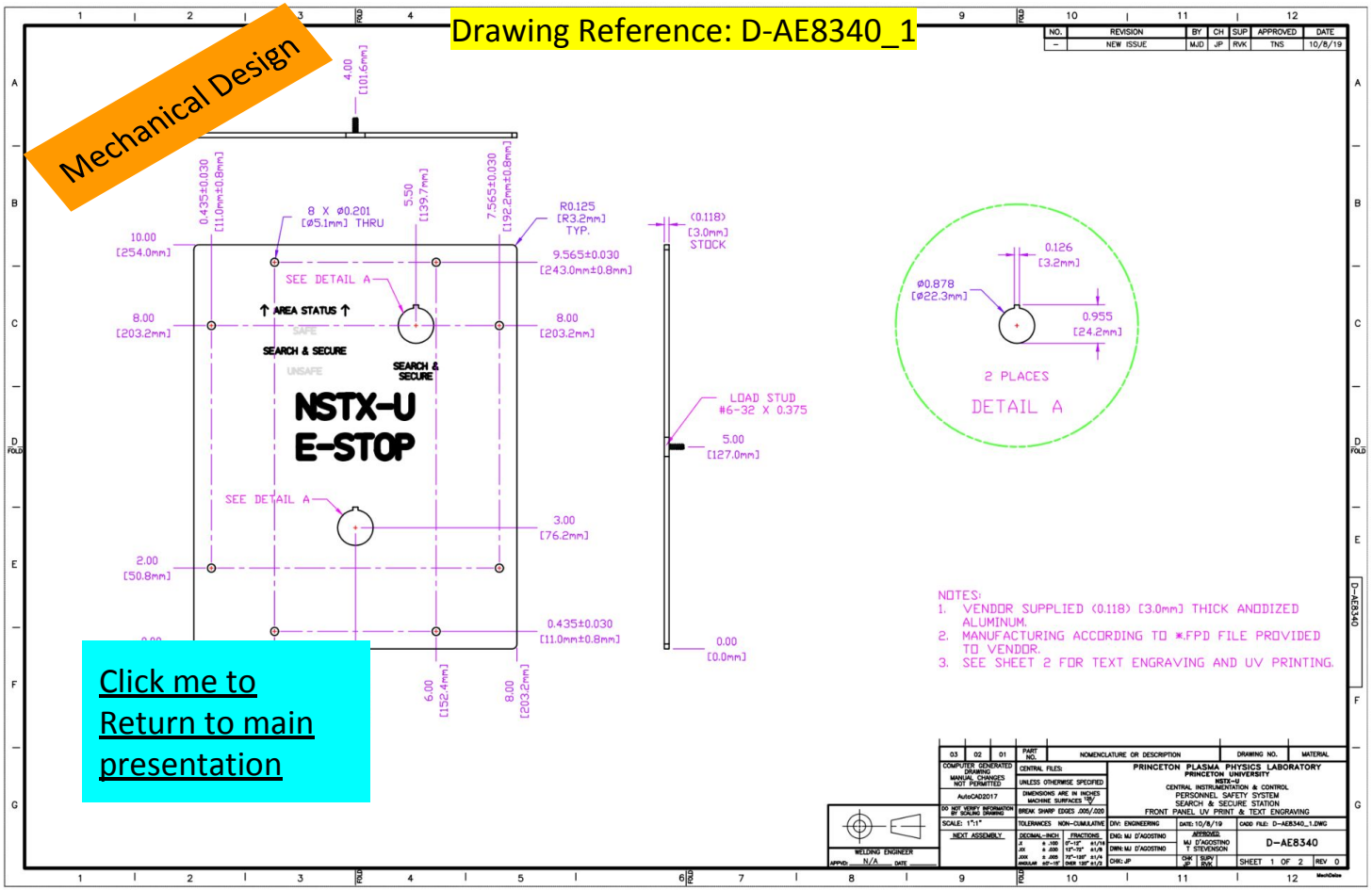


Click me to Return to main presentation

Search & Secure stations have been designed

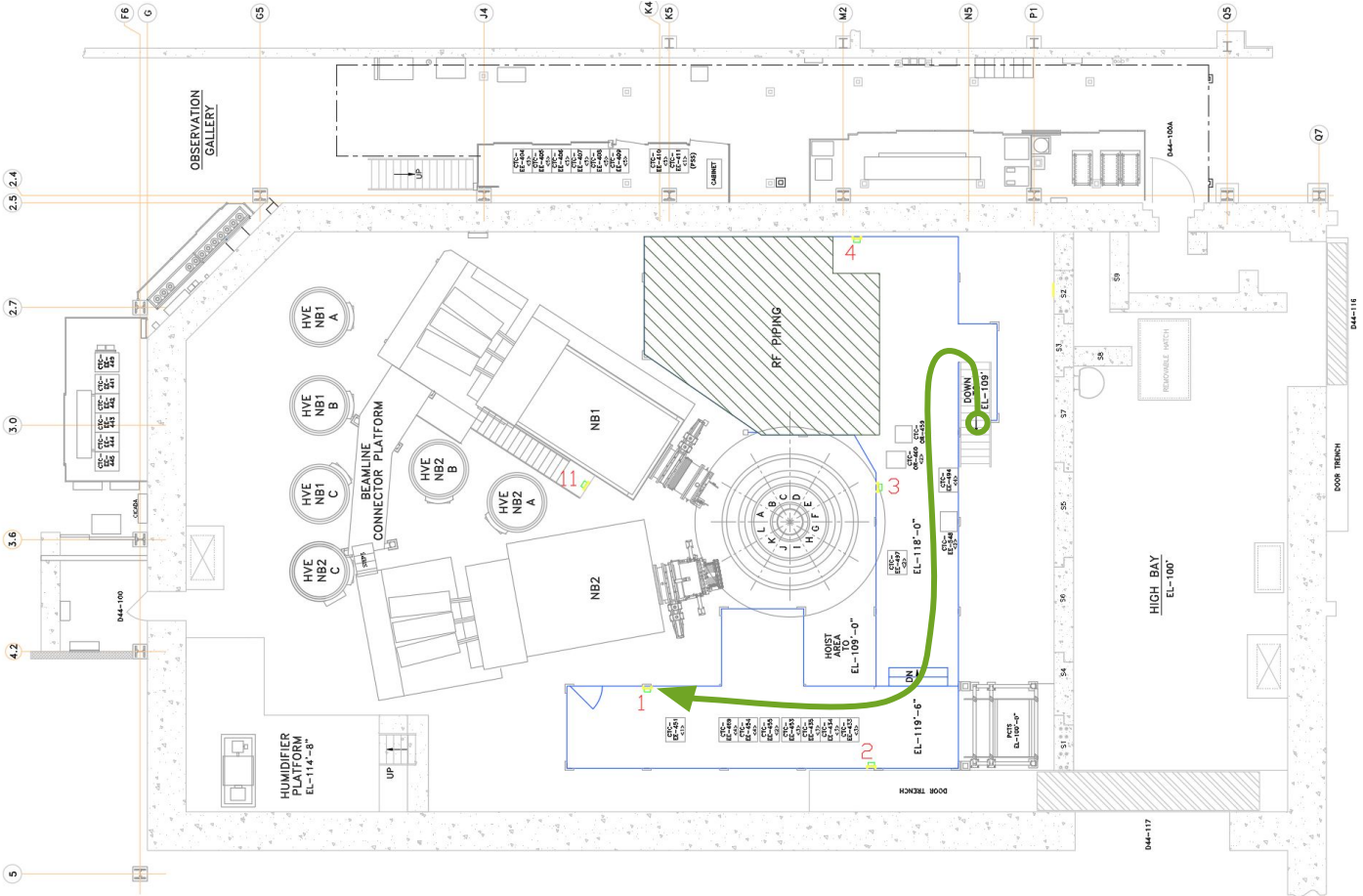
Mechanical Design

Drawing Reference: D-AE8340_1

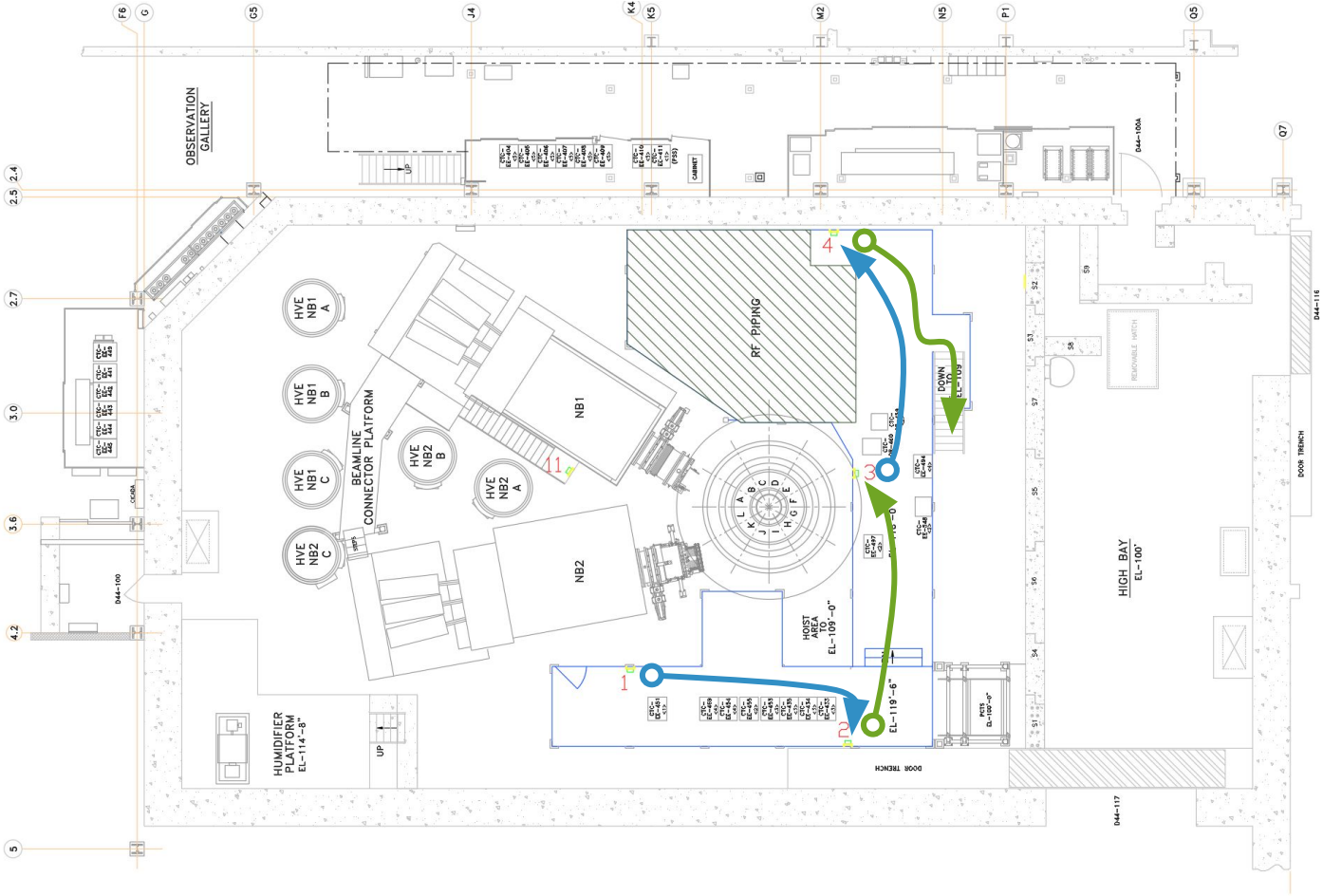


Click me to Return to main presentation

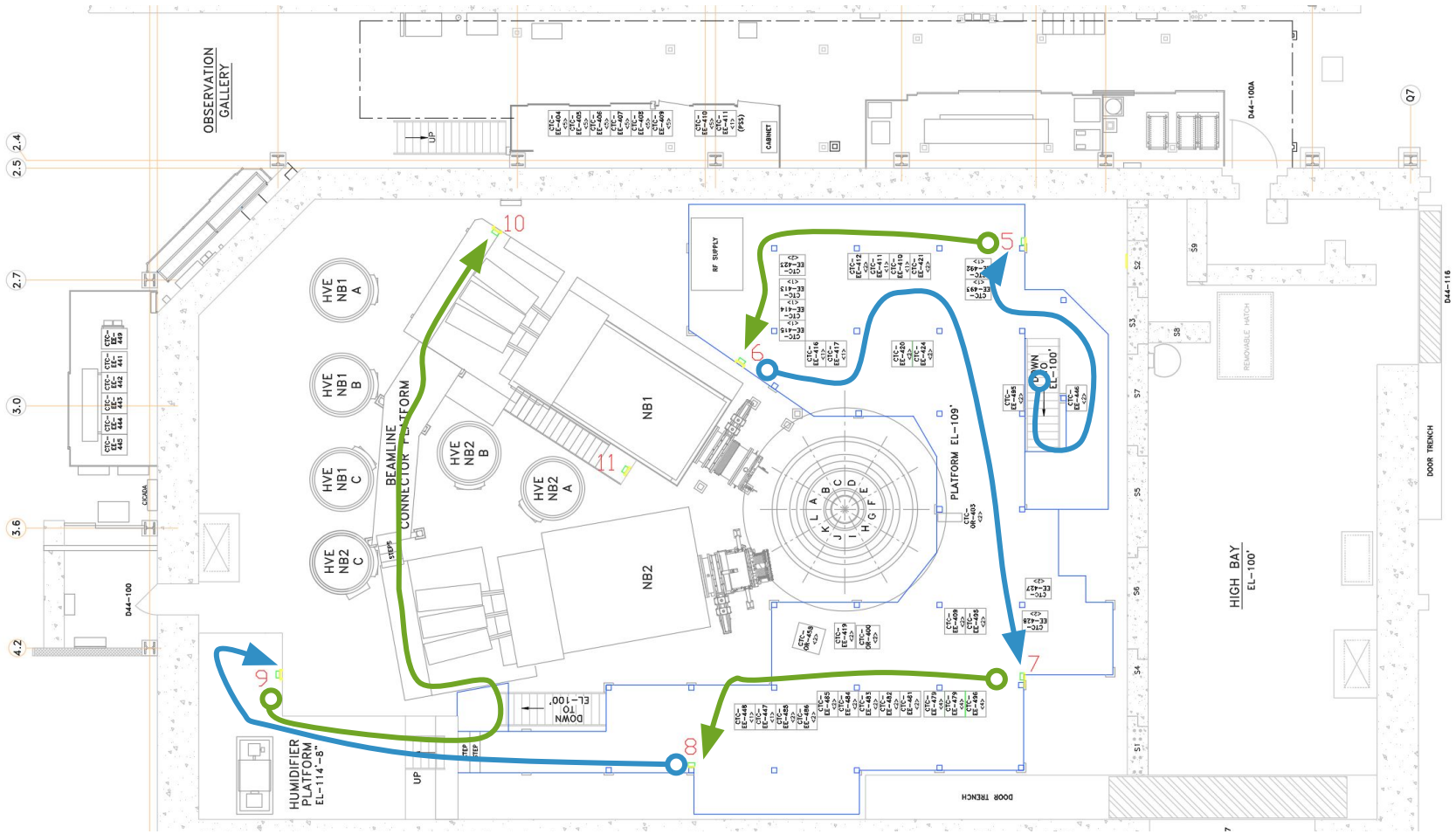
Primary searcher goes to first S&S station on uppermost level (118/119’ elevation).



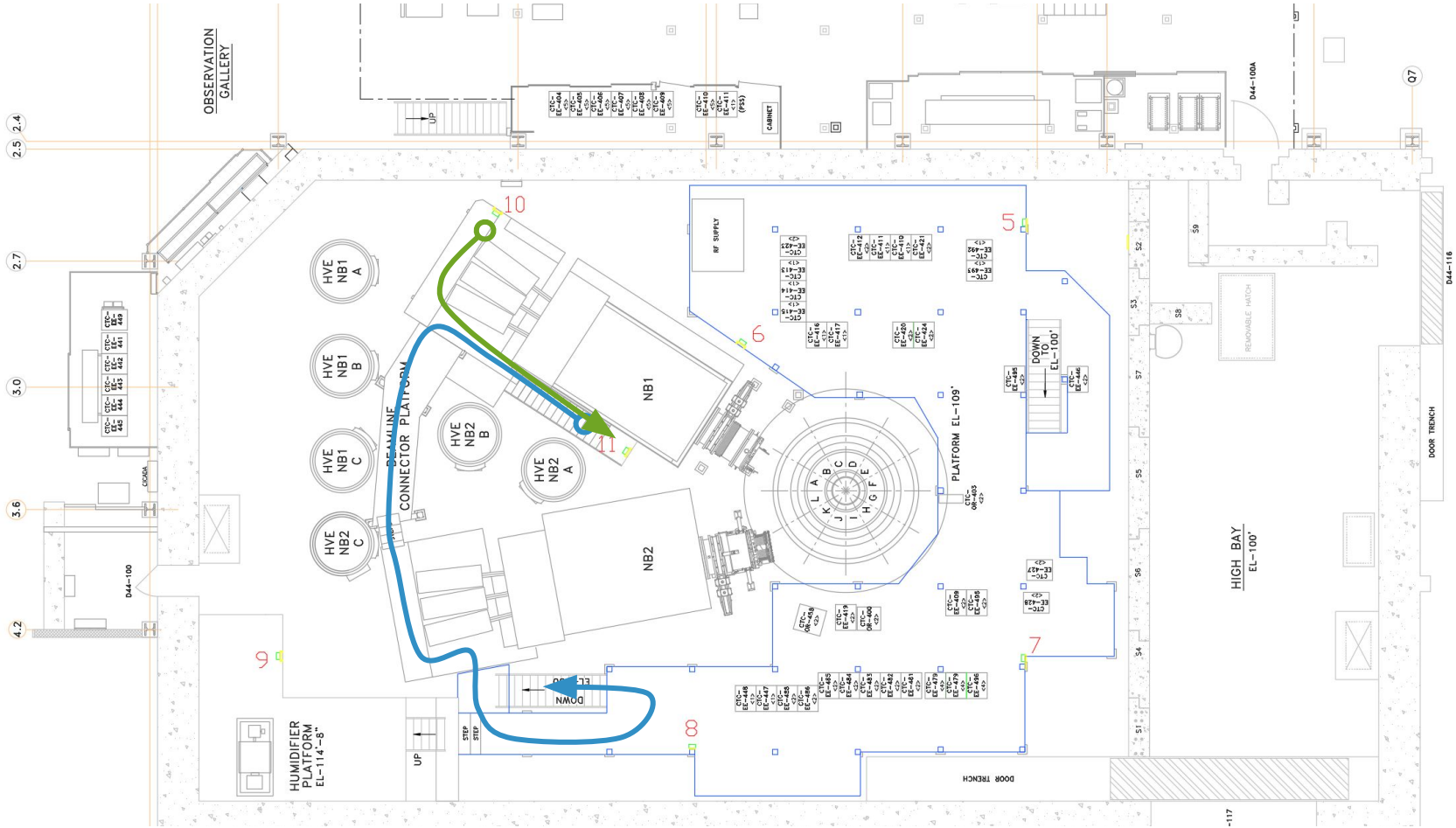
Searcher completes prescribed route as shown (118/119’ elevation).



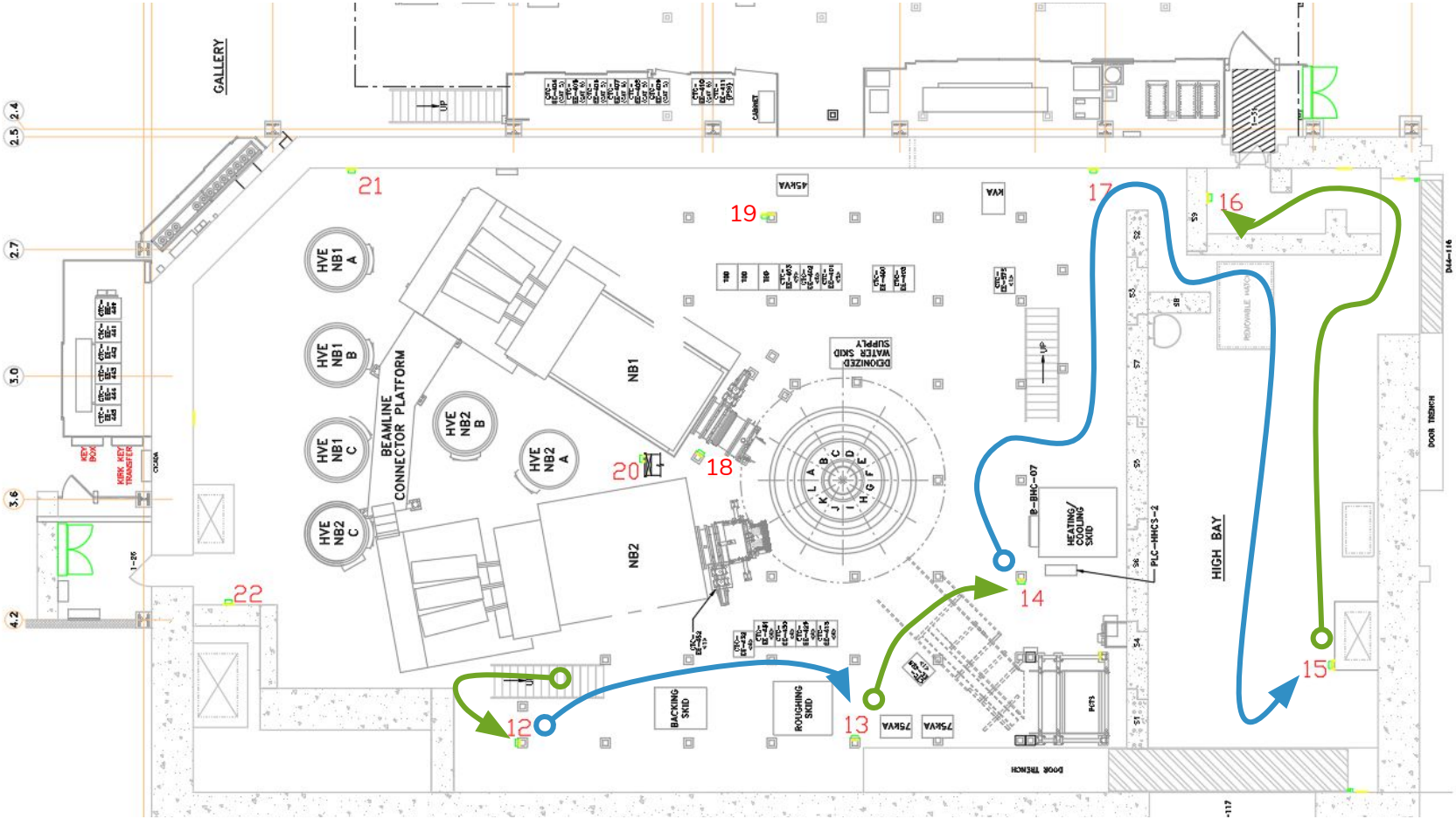
Searcher takes stairs down to middle level, continues on path as shown (109’ elevation).



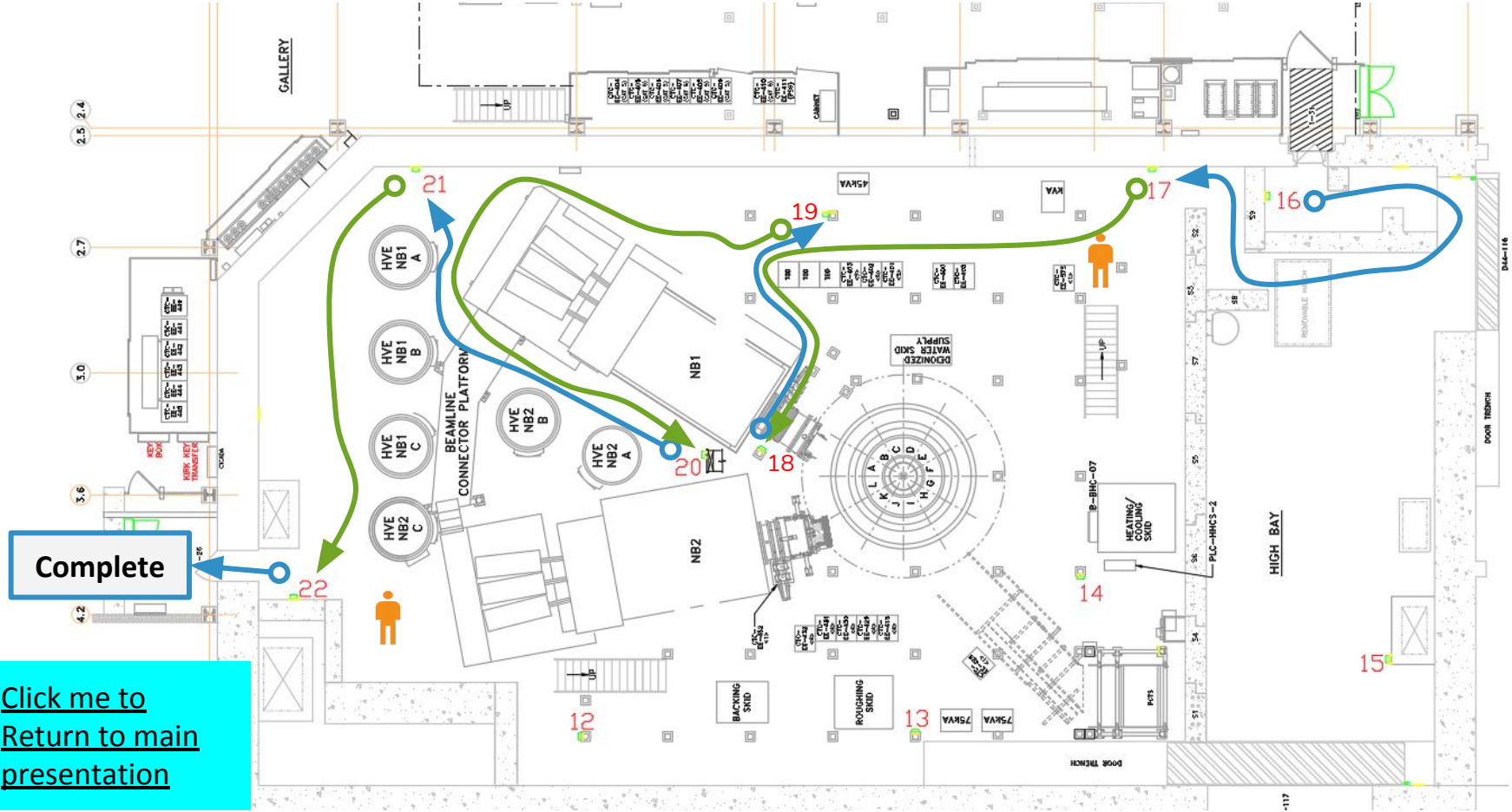
Searcher completes path on middle level (109’ elevation), follows path downstairs to ground level (100’ elevation).



Searcher continues on path shown, including South bay (100’ elevation).



Searcher follows path back from South bay, guards join as they are passed (100’ elevation).



Click me to Return to main presentation

LOPA was been used to determine the PSS-SIS SIF risk reduction performance requirements (refer to LOPA talk given previously)

Layer of Protection Analysis (LOPA) is one method described within IEC 61511 for the determination of Safety Instrumented Function risk reduction requirements.

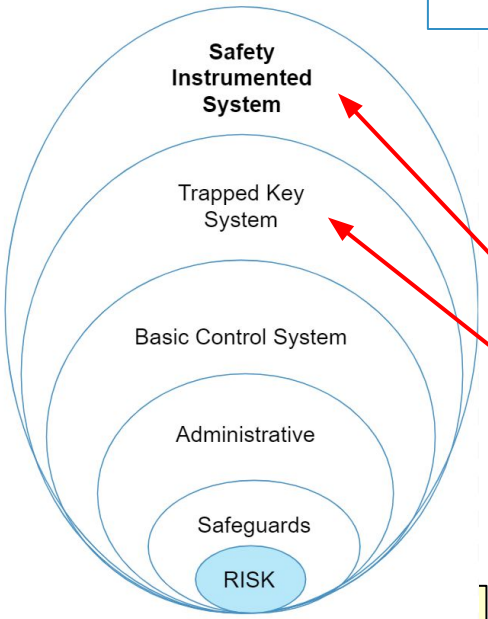
1: Identify Risks, Probabilities & Severities (HAR)

2: Define Tolerable Risk

3: Identify Impact Events, Initiating Causes, Conditional Modifiers, Enabling Conditions (LOPA)

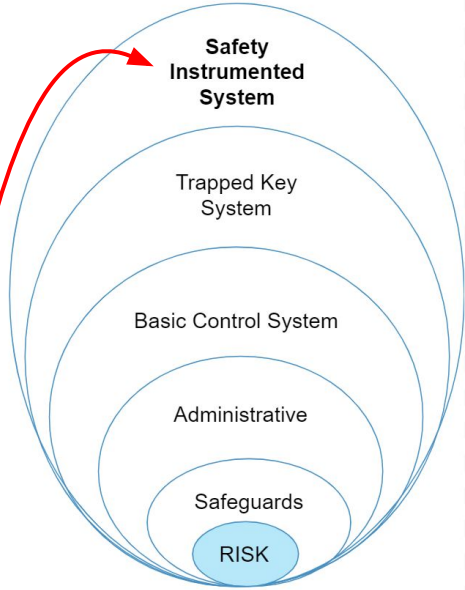
4: Identify Mitigating **I**ndependent **P**rotection **L**ayers (IPLs) and risk reduction factors (LOPA)

5: Identify residual risk requiring additional mitigation (i.e. by a **S**afety **I**nstrumented **S**ystem [SIS]). Identify **S**afety **I**nstrumented **F**unctions (SIFs) & Performance Requirements (LOPA)



IPL

IPL



SIS mitigation and minimum performance requirements have been defined for (5) Safety Instrumented Functions (Ref: SRD-012)

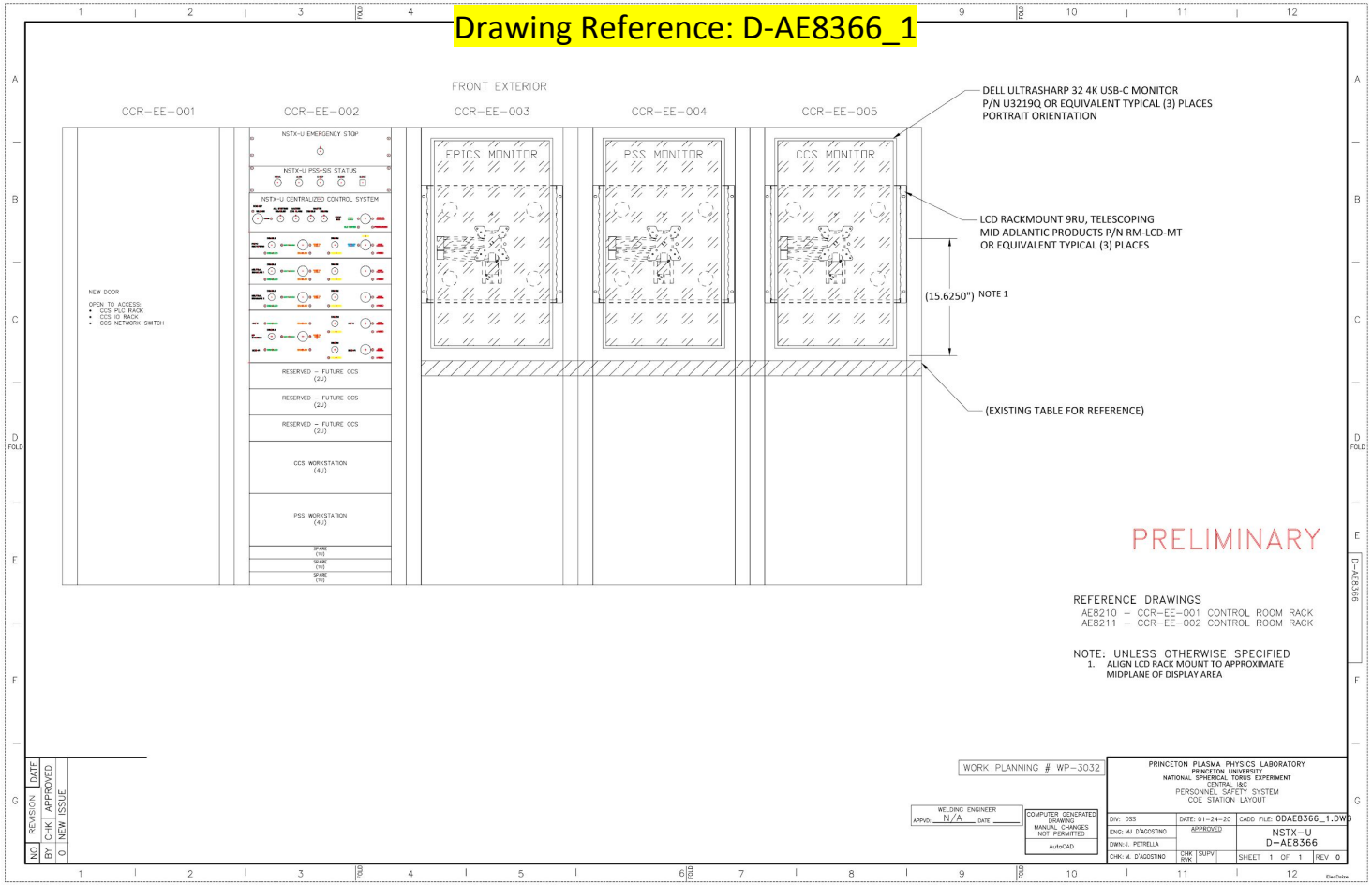
The Safety Instrumented Functions (Defined by LOPA/SRD-012) require the interdiction of PSS-SIS interlocked devices (final elements) when an access door to an exclusion area is violated (opened during No-Access) for mitigating Direct Ionizing Radiation and Magnetic Hazards

SIF Identifier	Action	Monitored Process Variable(s)	Risk Reduction Factor Target	SIL Target	Minimum Hardware Fault Tolerance
S-1	**Interdict Final Element Devices on Access Violation**	**Exclusion Area Access Doors**	**12**	**1**	**0**
S-1.a	Interdict Final Element Devices on Access Violation	NTC North Tritium Door	12	1	0
S-1.b	Interdict Final Element Devices on Access Violation	NTC South Entryway Door	12	1	0
S-1.c	Interdict Final Element Devices on Access Violation	NTC TFTR Tritium Door	12	1	0
S-1.d	Interdict Final Element Devices on Access Violation	NTC NB Tritium Door	12	1	0
S-1.e	Interdict Final Element Devices on Access Violation	MER Mezzanine Door	12	1	0

Click me to Return to main presentation

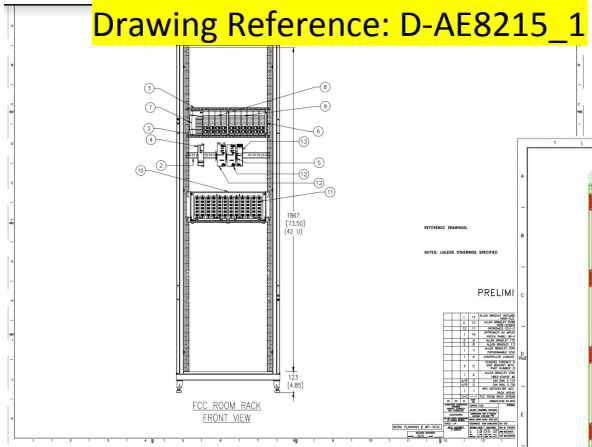
COTS computer monitor / keyboard / mouse interface will be used for PSS, CCS, and EPICs COE work stations

Drawing Reference: D-AE8366_1

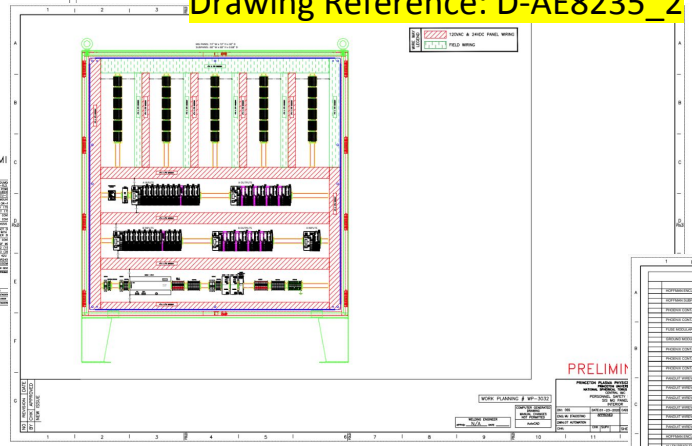


The SIS I/O locations and their signals have been determined. Control panel layouts/BOMs have been completed (examples below).

Drawing Reference: D-AE8215_1



Drawing Reference: D-AE8235_2



Drawing Reference: D-AE8235_1

Click me to Return to main presentation

Note: Control Panel Interior panel wiring documentation will be completed as part of control panel requisition

Timing & Sequencing Detail of PSS-SIS Emergency Stop

Table 5.4-1 Detail of the timing and sequencing in support of figure 5.4-1.

Action Phase	Phase Time (sec)	Actions (using 0.2 s logic scan)
A	1.2	• During NO ACCESS, a **door opens at T=0**. Digital input sees input change at T+0.2 s. • FUNC-COND-01 Input signal conditioning take 0.2 s. • FUNC-SS-01 then FUNC-SACT-05 then FUNC-SACT-01 uses 0.6 s. • FUNC-CCS-01 asserts digital output. no output signal conditioning. 0.2 s • **E-Stop is asserted, safe-to-enable revoked, to CCS at T+1.2 s.**
B	1.6	• FUNC-SACT-02 allows CCS/BCS 1.0 s to trip breakers and then evaluates need to interdict . • FUNC-SACT-03 asserts interdiction process variables (0.2 s). • FUNC-COND-02 use 0.3 s for signal conditioning, asserts digital outputs. • assume 0.1 s for safety relay and SV/SF breaker trip. • **SV/SF breakers open at T+2.8 s.**
C	0.8	• digital inputs read for SV/SF breaker positions. • FUNC-COND-01 Input signal conditioning take 0.2 s. • FUNC-SACT-04 decides whether S1-B1 interdiction is necessary, and asserts interdiction process variables (0.2 s). • FUNC-COND-02 use 0.3 s for signal conditioning, asserts digital outputs. • assume 0.1 s for safety relay and S1-B1 breaker trip. • **S1-B1 breaker open at T+3.6 s.**

Ref: *NSTXU_1-7-3-1_RD_100*

Twelve *software modules* detail the structure, purpose, dependency, and result of each module

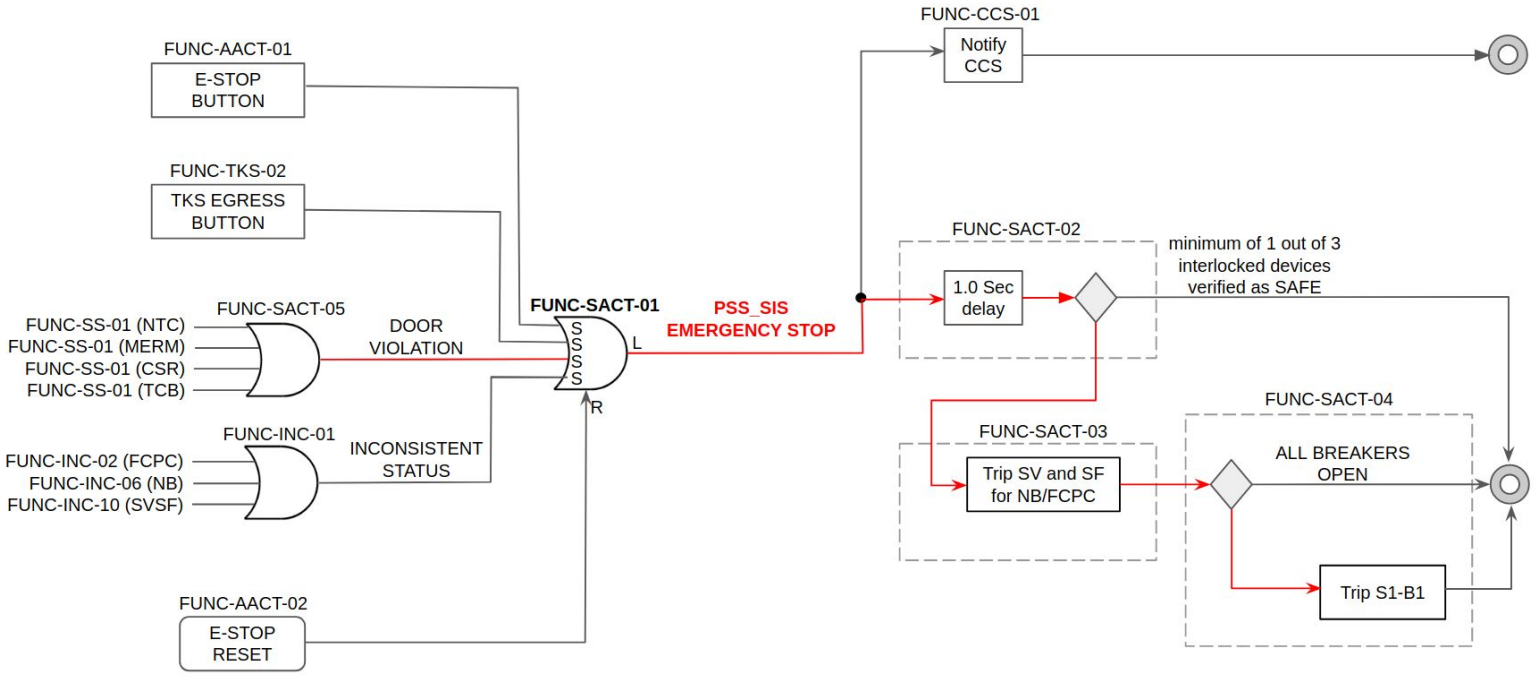
4. Software Modules	13
4.1 Actions Module	13
4.2 I/O Conditioning Module	17
4.3 Operating Mode Module	20
4.4 Exclusion Areas State Module	21
4.5 Inconsistency Module	26
4.6 TKS Module	30
4.7 Search and Secure Module	31
4.8 CCS Interface Module	36
4.9 Centralized HMI Module	44
4.10 Alarm Module	50
5.5 System Monitoring Module	57
5.7 Data Export (USB)	59

Each module includes associated functions that are defined in tabular form (example below).

Table 4.1.1-1 PSS-SIS Emergency Stop

FUNCTION ID	FUNC-SACT-01
Title	PSS-SIS Emergency Stop Condition
Description	Per Table 3.3-2 in reference [2], declare and latch a PSS-SIS Emergency Stop condition, which will initiate the Interdiction action.
Dependency	• FUNC-AACT-01 (E-Stop buttons) • FUNC-TKS-02 (TKS Egress buttons) • FUNC-SACT-05 (door violation) • FUNC-INC-01 (inconsistent status) • FUNC-AACT-02 (E-Stop Reset)
Result	A *process variable* for a PSS-SIS Emergency Stop Condition will be set. This variable is latched and will require field device reset and operator intervention to reset the condition (FUNC-AACT-02).

Some functions are chained to provide the Safety Instrumented Function (example below)

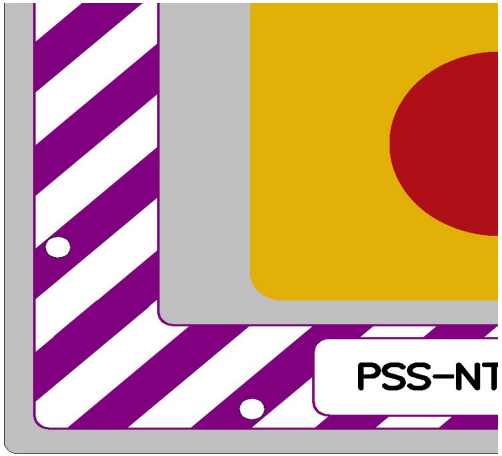


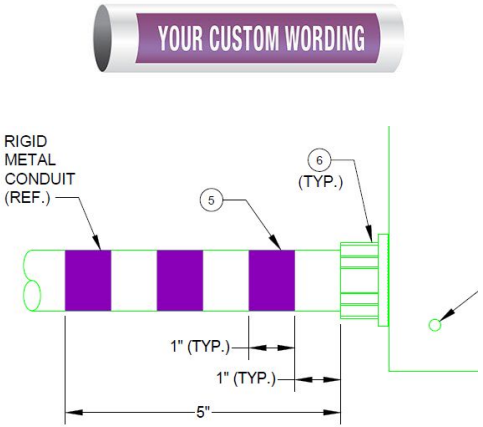
Click me to Return to main presentation

* The red line is the SIF. Everything else is considered “additional actions”.

The PSS-SIS uses a unique and easily identifiable scheme for labeling and identification of conduit and components.

- The “defined by user” ANSI/ASME A13.1 color combination White on Purple has been selected
  - Pipe banding tape
  - Pipe markers
  - Labels





Fire quenching fluids	White on Red
Toxic & corrosive fluids	Black on Orange
Flammable & oxidizing fluids	Black on Yellow
Combustible fluids	White on Brown
Potable, cooling, boiler feed, & other water	White on Green
Compressed Air	White on Blue
Defined by user	White on Purple
	Black on White
	White on Grey
	White on Black

ANSI/ASME A13.1 Guidelines

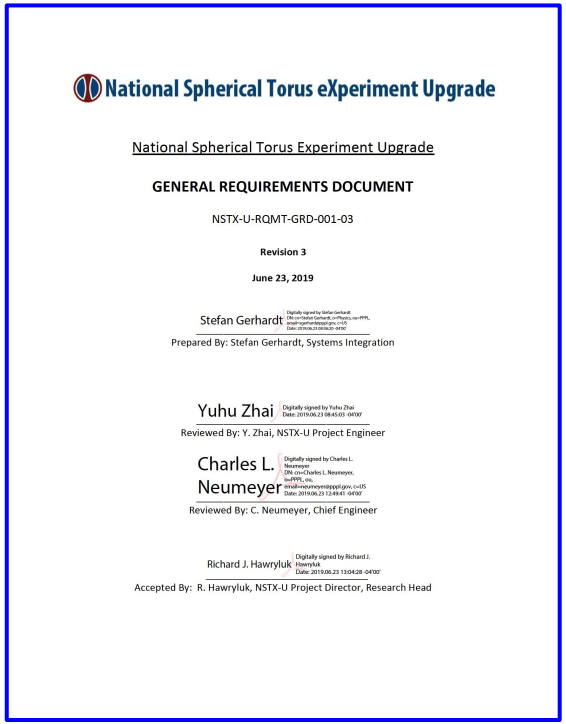
Hardware has been chosen that replaces COTs fasteners for tamper resistance and access control

- Permanent installations
  - Pull boxes, junction boxes, condulets, etc. will be fastened with unique hardware
  - These locations will either contain no reconfigurable components or not be expected to be modified
  - Bryce Fasteners Key-Rex fasteners have been chosen
    - Keyway is unique to the NSTX-U PSS-SIS
- Locked enclosures
  - Locked enclosures, such as for reconfigurable network equipment, are instrumented to the SIS with a switch to detect a door opening

Click me to Return to main presentation

General Requirements Document Requirements Summary (paraphrasing) → **Requirements Met By Design**

- Comply with the Accelerator Safety Order (DoE Order 420.2c) (6.7.1a)
- Prevent access to the NSTX-U test cell and related areas when they are in an unsafe condition (6.7.3.1a)
- Prevent sources of energy such as neutral beams from turning on when areas allow access (6.7.3.2b)
- Support search and secure, provide emergency stop capability, sense door violations (6.7.3.1c).
- Permit multiple layers of protection to achieve the desired risk reduction level (6.7.3.1d)
- ES&H: Complete the project in a way "...protect personnel, visitors, the public, property and the environment from injury."(7)



National Spherical Torus eXperiment Upgrade

National Spherical Torus Experiment Upgrade

GENERAL REQUIREMENTS DOCUMENT

NSTX-U-RQMT-GRD-001-03

Revision 3

June 23, 2019

Stefan Gerhardt Digitally signed by Stefan Gerhardt DN: cn=Stefan Gerhardt, o=Physics, ou=PPPL, email=sgerhardt@pppl.gov, c=US Date: 2019.06.20 08:06:20 -04'00'

Prepared By: Stefan Gerhardt, Systems Integration

Yuhu Zhai Digitally signed by Yuhu Zhai Date: 2019.06.23 08:45:03 -04'00'

Reviewed By: Y. Zhai, NSTX-U Project Engineer

Charles L. Neumeyer Digitally signed by Charles L. Neumeyer DN: cn=Charles L. Neumeyer, ou=PPPL, o=, email=neumeyer@pppl.gov, c=US Date: 2019.06.23 12:49:41 -04'00'

Reviewed By: C. Neumeyer, Chief Engineer

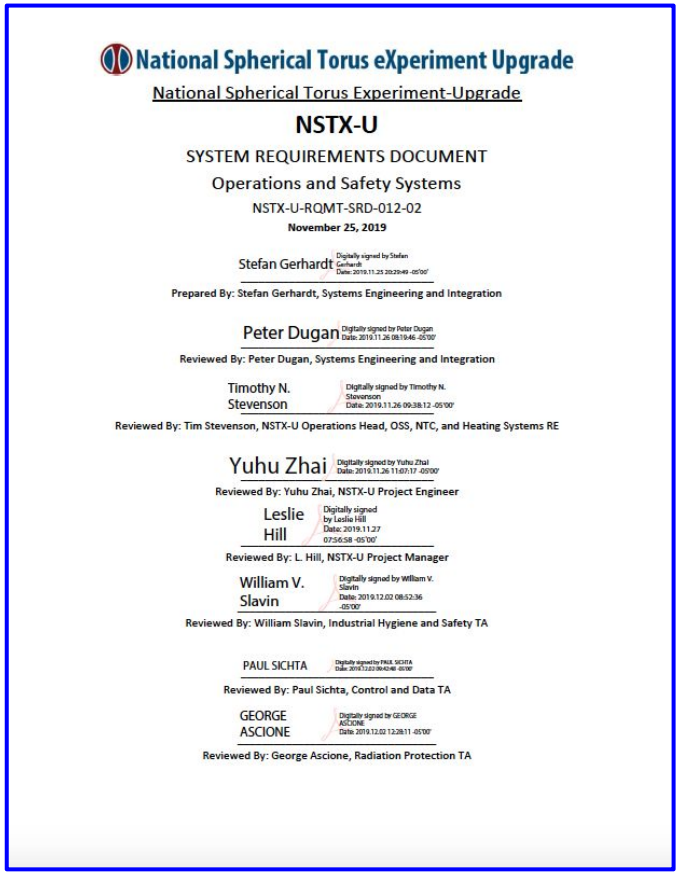
Richard J. Hawryluk Digitally signed by Richard J. Hawryluk Date: 2019.06.23 13:04:28 -04'00'

Accepted By: R. Hawryluk, NSTX-U Project Director, Research Head

Click document or follow link

Operations and Safety Systems SRD Overview → **Requirements Met By Design**

- Covers numerous systems:
  - PSS-SIS
  - Trapped Key System
  - Configuration Managed Safeguards
  - Centralized Control System
  - Grounding
  - Radiation Monitoring and Annunciation
  - Test Cell Oxygen Monitors
- Also contains a listing of definitions supporting the PSS-SIS deployment
- Flow requirements down one level of granularity from the GRD
- On Rev. 2 of the document.
- Follows Project standard for SRDs regarding format



National Spherical Torus eXperiment Upgrade

National Spherical Torus Experiment-Upgrade

NSTX-U

SYSTEM REQUIREMENTS DOCUMENT

Operations and Safety Systems

NSTX-U-RQMT-SRD-012-02

November 25, 2019

Stefan Gerhardt Digitally signed by Stefan Gerhardt Date: 2019.11.25 20:29:49 -05'00'

Prepared By: Stefan Gerhardt, Systems Engineering and Integration

Peter Dugan Digitally signed by Peter Dugan Date: 2019.11.26 08:19:46 -05'00'

Reviewed By: Peter Dugan, Systems Engineering and Integration

Timothy N. Stevenson Digitally signed by Timothy N. Stevenson Date: 2019.11.26 09:38:12 -05'00'

Reviewed By: Tim Stevenson, NSTX-U Operations Head, OSS, NTC, and Heating Systems RE

Yuhu Zhai Digitally signed by Yuhu Zhai Date: 2019.11.26 11:07:17 -05'00'

Reviewed By: Yuhu Zhai, NSTX-U Project Engineer

Leslie Hill Digitally signed by Leslie Hill Date: 2019.11.27 07:56:58 -05'00'

Reviewed By: L. Hill, NSTX-U Project Manager

William V. Slavin Digitally signed by William V. Slavin Date: 2019.12.02 08:52:36 -05'00'

Reviewed By: William Slavin, Industrial Hygiene and Safety TA

PAUL SICHTA Digitally signed by PAUL SICHTA Date: 2019.12.02 09:42:40 -05'00'

Reviewed By: Paul Sichta, Control and Data TA

GEORGE ASCIONE Digitally signed by GEORGE ASCIONE Date: 2019.12.02 12:28:11 -05'00'

Reviewed By: George Ascione, Radiation Protection TA

Click document or follow link

RD-24 Flows Down Requirements for the Safety Instrumented System → **Requirements Met By Design**

Comprehensive Requirements for the PSS-SIS
(only show ToC in this talk)

3.1: Hazard Analysis and SIS SIFs	6
3.2 PSS-SIS Interlocked systems	6
3.3 Access Control	8
3.3.1 Exclusion Areas	8
3.3.2 Access Control Requirements	8
3.3.3 Search and Secure	9
3.4 PSS E-STOP Buttons	9
3.5 Interlock Requirements	9
3.6 States of Operation and Inconsistent Configurations	10
3.7 Design Features for Testing	11
3.7.1 Interlocked Equipment Testing	11
3.7.2 PSS-SIS Testing	11
3.8 Human Machine Interface	11
3.8.1 Centralized HMI	11
3.8.2 HMI At and Within Exclusion Areas	12
3.9 Tamper Resistance and Labeling	12
3.10 Logging	13
3.11 Cyber Security	13
3.12 Modifications	14
3.13 Expansion	14
3.14 Design, Installation, & Commissioning	15
3.15 Certification & Maintenance	16
3.16 Interfaces	16
3.17 Codes and Standards	16
3.18 Interactions with the Trapped Key System	16
3.19: Interactions with the Centralized Control System (CCS)	17

National Spherical Torus eXperiment Upgrade

NSTX-U Personnel Safety System-Safety Instrumented Systems Requirements

NSTX-U-RQMT-RD-024-02

November 25, 2019

Stefan Gerhardt — Digitally signed by Stefan Gerhardt Date: 2019.11.25 20:31:16 -05'00'

Prepared by: Stefan Gerhardt , Systems Engineering and Integration

Peter Dugan — Digitally signed by Peter Dugan Date: 2019.11.26 08:20:41 -05'00'

Reviewed by: Peter Dugan, Systems Engineering and Integration

Timothy N. Stevenson — Digitally signed by Timothy N. Stevenson Date: 2019.11.26 09:39:31 -05'00'

Reviewed By: Tim Stevenson, NSTX-U Operations Head, OSS RE

Joseph R_ Petrella Jr_ — Digitally signed by Joseph R_ Petrella Jr_ DN: C=US, O=PPPL, CN=Joseph R_ Petrella Jr_, E=jpetrel@pppl.gov Reason: I have reviewed this document Location: Date: 2019-11-26 10:20:05

Reviewed by: Joseph Petrella, Project Cognizant Engineer

PAUL SICHTA — Digitally signed by PAUL SICHTA Date: 2019.11.26 14:39:26 -05'00'

Reviewed by: Paul Sichta, Control and Data TA

Yuhu Zhai — Digitally signed by Yuhu Zhai Date: 2019.11.27 13:42:59 -05'00'

Approved By: Y. Zhai, NSTX-U Project Engineer

1

Click document or follow link

SRD - Key Requirements for PSS-SIS *SIFs*

***Table 3.1.1.1-1**: PSS-SIS safety instrumented functions*

SIF	Description	Minimum Safety Integrity Level*
S-1.a	Interdict Interlocked Devices on Access Violation of the NTC North Shield Door[1]	SIL 1
S-1.b	Interdict Interlocked Devices on Access Violation of the NTC South Entryway Door	SIL 1
S-1.c	Interdict Interlocked Devices on Access Violation of the NTC West Shield Door	SIL 1
S-1.d	Interdict Interlocked Devices on Access Violation of the NTC South Shield Door	SIL 1
S-1.e	Interdict Interlocked Devices on Access Violation of the MER Mezzanine Entryway Door	SIL 1

Click me to Return to main presentation

✔ Refer to LOPA talk and this presentation for the scope/design that implements them