National Spherical Torus eXperiment Upgrade

NSTX-U Personnel Safety System Development at PPPL - Community Interface

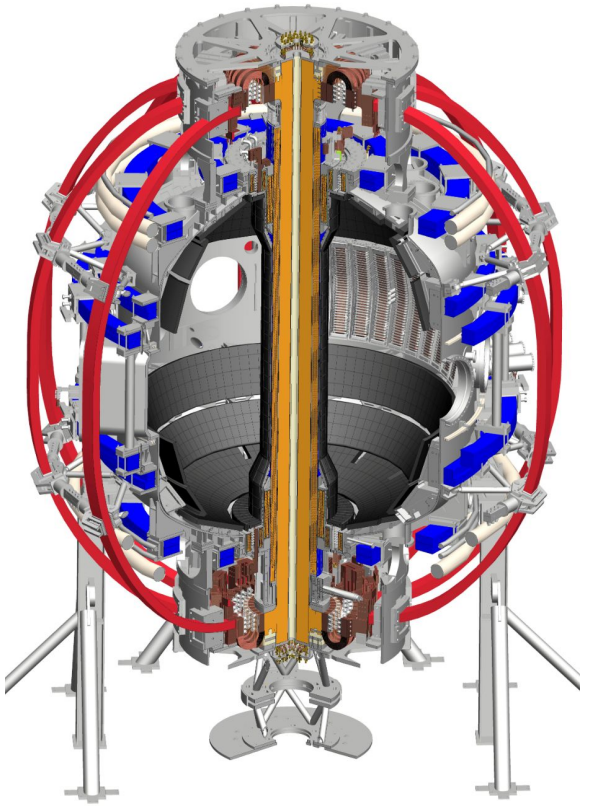
J. Petrella

PPPL PRINCETON PLASMA PHYSICS LABORATORY

PRINCETON UNIVERSITY

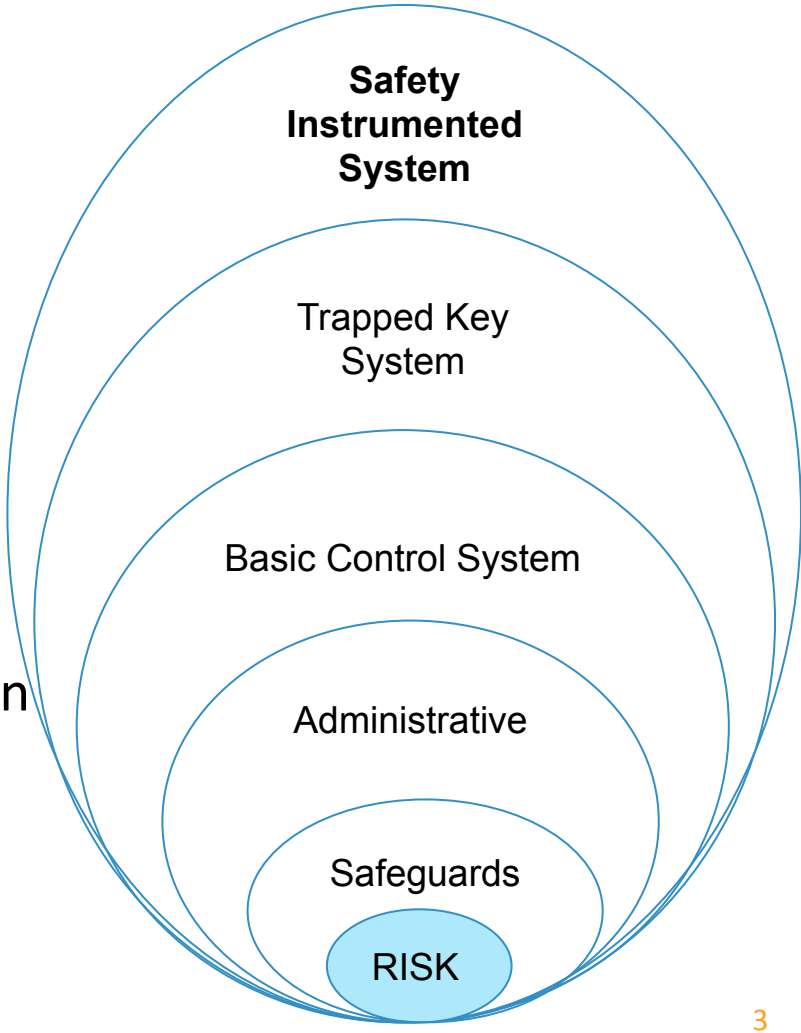
Introduction: Characteristics of NSTX-U

- Deuterium-Deuterium Pulsed Plasma Physics Fusion Experiment (Direct Ionizing Radiation only when pulsed)
- 5 second pulse; 20 minute cycle with upgrade to TF conductors
- Experimental campaigns typically 10-20 weeks per year on NSTX
- Typical 9 hour run day; 25 shots per day; 5 days/week
- Under vacuum and cryo on 6-7 months per research year
- Magnetic Confinement
  - Pulsed, water-cooled, copper-wound electromagnets
  - Toroidal Field, Poloidal Field, Ohmic Heating, RWM magnets
  - Up to 2 MA of electrical current flowing in the plasma itself
  - Background fields on order of 1 T
- 10-14 MW Neutral Beam heating depending on pulse length
  - Typically 90 kV accelerating voltage; 100 kV max on NSTX
- Up to 6 MW RF heating @ 30Mhz



Introduction: 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)
  - Configuration Managed Safeguards
  - Trapped Key System
- Direct Ionizing Radiation and Magnetic Hazards that require further risk reduction are mitigated through the PSS Safety Instrumented System (SIS)



Accelerator Community Supported our Search for references to Understand PSS Requirements (1)

Facility	Experiment	Contacts		Reviewed
ANL	60 MeV LINAC, ATLAS	John Quintana	DDO and Chief Operations Officer (COO)	SAD, ACIS Design Compliance with Principal Accelerator Safety Interlock Design Requirements, "Evolution of PSS"
		Greg Markovitch	Safety Interlocks Group Leader	
SLAC	LCLS, LCLS-II	Ian Evans	Environment, Safety & Health Program Manager	SAD, HAR, Institutional Requirements Program, QA Program, ARR preparation Documentation, Readiness Review Process, Hazard Checklist, Credited Control Documentation
BNL	ATF	Ed Lessard	Associate Chair for ES&HQ	SAD
		Scott Buda	Electrical Engineer – Safety Systems Engineer	
LANSCE	3-GEV Upgrade	Mark Gulley	SME	Misc. Upgrade Documentation

Accelerator Community Supported our Search for references to Understand PSS Requirements (2)

Facility	Experiment	Contacts		Reviewed
ORNL	SNS Proton, SNS Neutron	Kelly Mahoney	Protection Systems Team Leader	SAD, Safety Upgrade Documentation
BNL	NSLS-II, C-AD	Dave Pasarello	Quality Assurance	SAD, PSS requirements documents
TJNAF	CEBAF (SAD covers entire site)	Bob May	Division Safety Officer	SAD, PSS Requirements Documents
		Jerry Kowal	Head of Safety Systems Group	
LBNL	ALS, 88-inch cyclotron	Susana Reyes	Project Manager for LCLS-II-HE	SAD, Interlock Failure Analysis, “Effectiveness of PPS”, Bella Interlock Software Spec
		Patrick Bong	Interlock SME	
MSU	FRIB LINAC	Peter Grivins	ESH&Q Manager	RSS SRD, RSS RD

Consensus Standards Survey of Community Documents pointed to IEC-61511

- Survey performed of 24 Access Control System documents from ANL, BNL, FRIB, LBNL, TJNAF, CCFE, ORNL, SLAC
- Documents principally reference IEC 61508/61511 and ANSI N43.1

	ANSI N43.1	ANSI 84	ANSI Z136.1	IEC 1508	IEC 61508	IEC 61508-1	IEC 61508-2	IEC 61508-3	IEC 61508-4	IEC 61508-5	IEC 61508-6	IEC 61508-7	IEC 61511	IEC 62061	ISO 13849	NFPA 70	NFPA 79
TOTAL	**3**	**1**	**1**	**1**	**5**	**2**	**2**	**2**	**1**	**1**	**1**	**1**	**3**	**2**	**1**	**1**	**1**

Lessons Learned from Examination of the Accelerator Community Requirements and Designs

- IEC 61511/08 are commonly used safety system standards
- The concept of “SIL” is central to design throughout the accelerator community
- The design of the ACS/PSS flows from a detailed hazard and risk analysis
- With rare exceptions, relay based systems are no longer used.
  - Modern expectations tends towards PLC based systems.
- Facilities without (any noted) exception utilize a redundant chain-A/chain-B approach.
- Search and secure stations are used to reinforce routes
- Tamper resistance is a expectation

SAD/ASE Impacts Are Addressed Through Corresponding ASO Implementation

- Hazards were analyzed during NSTX-U HAR development and hazards requiring mitigation by PSS were identified
- HAR serves as a direct input to the development of the new SAD (in progress)
- PSS-SIS has been identified as a potential credited control for mitigation of the following hazards in exclusion areas:
  - Direct Ionizing Radiation hazards
  - Magnetic Field hazards
- SAD and ASE will include PSS
  - Maintained using the USI process
  - Any proposed changes to the PSS-SIS will require a USID
  - PSS-SIS will be managed as a credited control

SAD → Safety Assessment Document

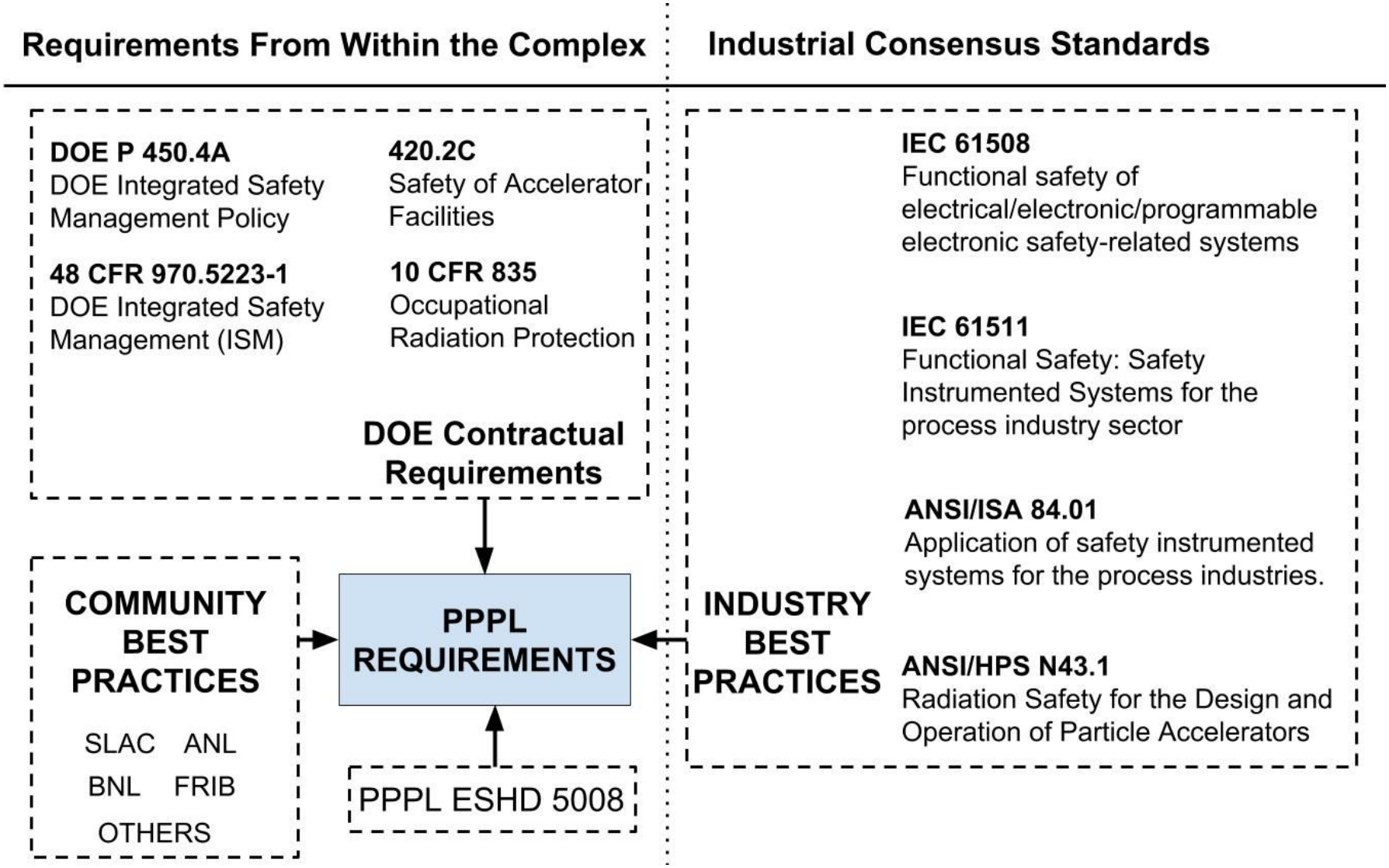
ASE → Accelerator Safety Envelope

HAR → Hazard Analysis Report

USI → Unreviewed Safety Issue

USID → USI Determination

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



LOPA has been used to determine the PSS-SIS SIF risk reduction performance requirements.

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

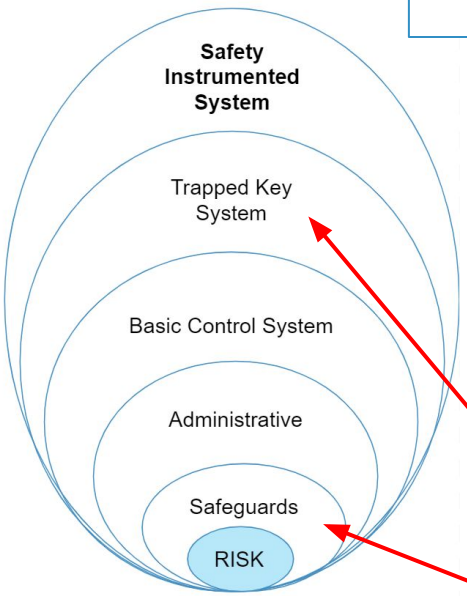
1: Identify Risks, Probabilities & Severities (HAR)

2: Define Tolerable Risk

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

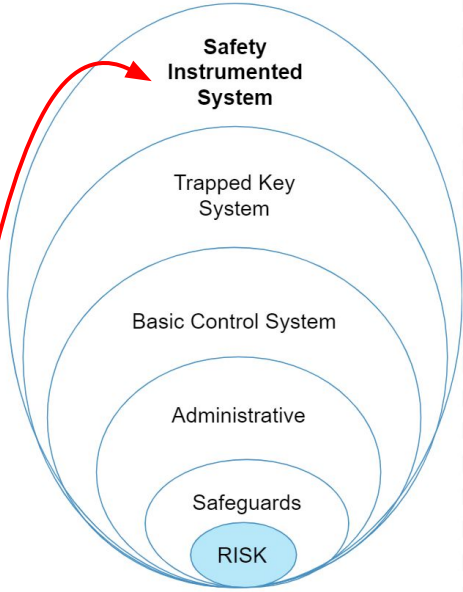
4: Identify Mitigating Independent Protection Layers and risk reduction factors (LOPA)

5: Identify residual risk requiring additional mitigation (i.e. by a Safety Instrumented System). Identify SIFs & Performance Requirements (LOPA)

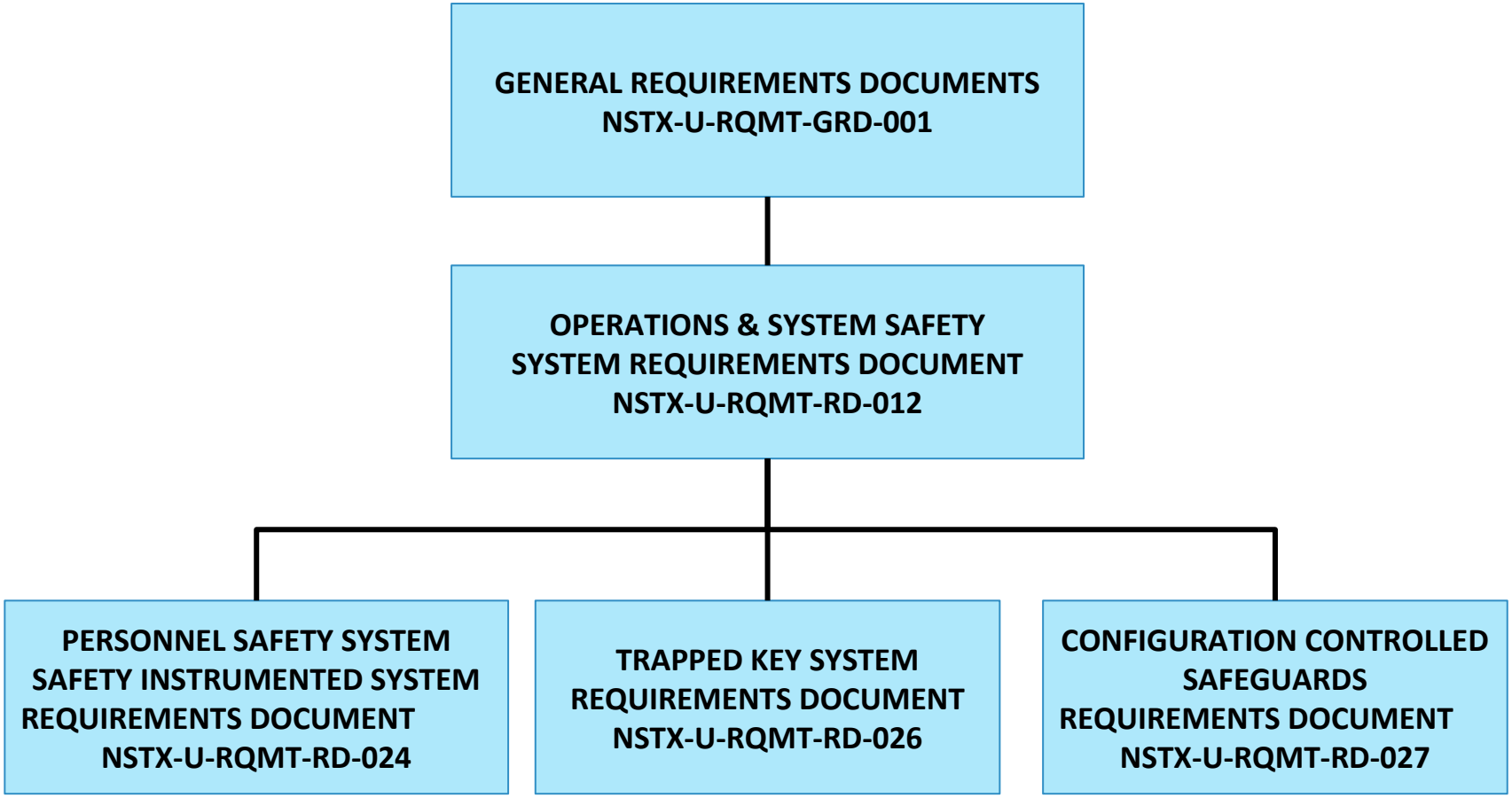


IPL

IPL



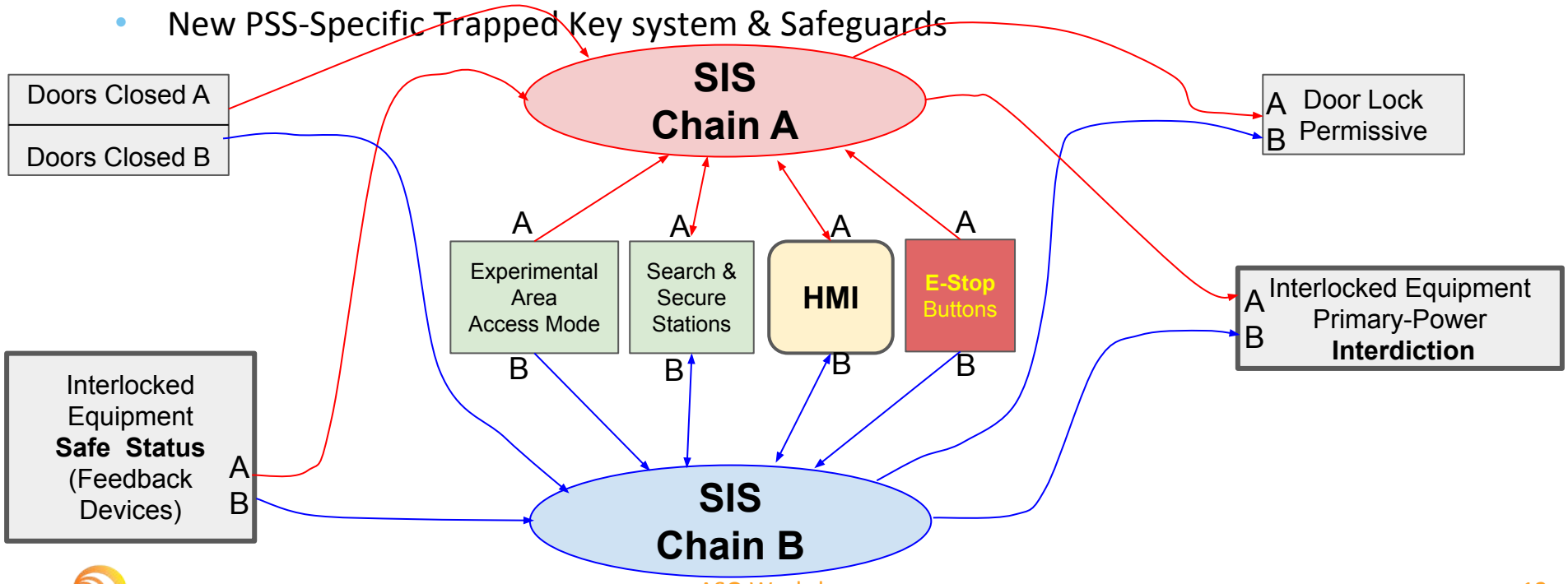
A Hierarchical Set of Requirements Were Developed for Personnel Safety



The PSS design concept meets high level requirements and community expectations

Install Dual Chain “shell” over updated Centralized Control System

- New Dual Chain SIL-capable Logic Solvers
- New SIL-capable Instruments
- New SIL-capable Output Hazard Control Devices (interrupt existing control wiring)
- New PSS-Specific Trapped Key system & Safeguards

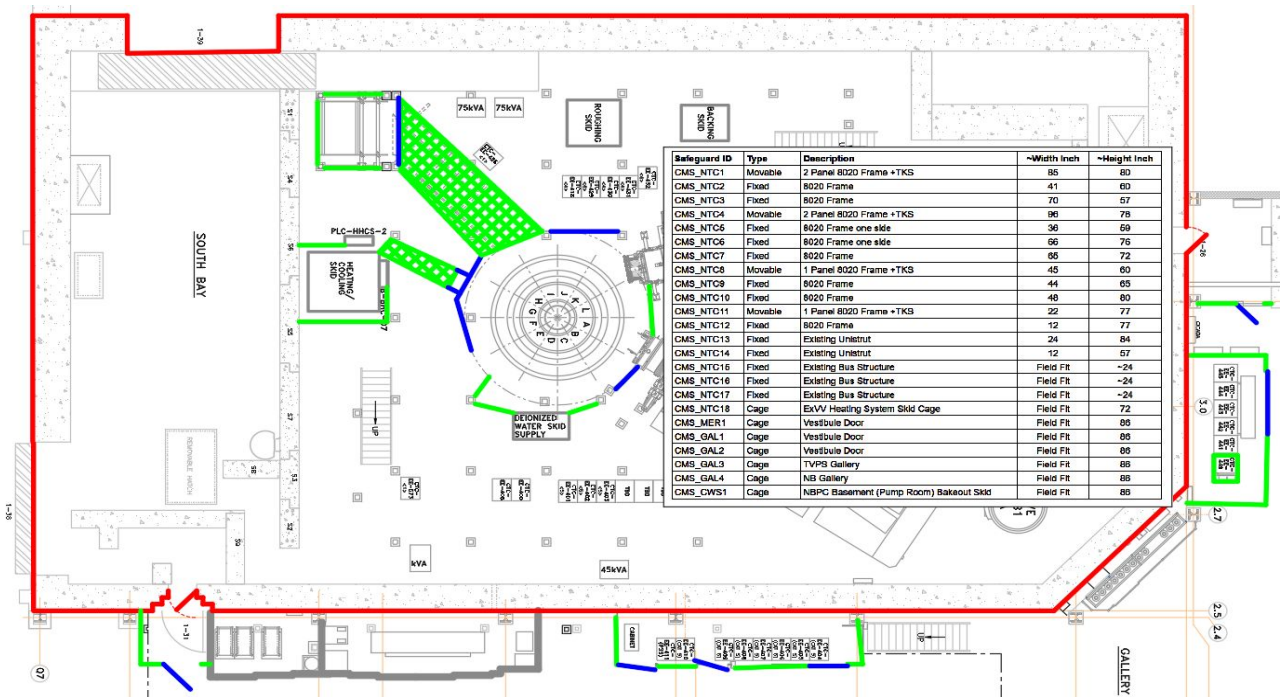


Configuration Managed Safeguards *eliminate* industrial contact hazards (non-radiation) so that experimental areas are General Access Areas* in regards to contact hazards

Direct Ionizing Radiation Hazard Exists Only When Pulsing

Bolted safeguards (Green)
Hatched Area = Elevated enclosure

Movable safeguard (Blue)



Safeguard ID	Type	Description	~Width inch	~Height inch
CMS_NTC1	Movable	2 Panel 8020 Frame +TKS	85	80
CMS_NTC2	Fixed	8020 Frame	41	60
CMS_NTC3	Fixed	8020 Frame	70	57
CMS_NTC4	Movable	2 Panel 8020 Frame +TKS	96	78
CMS_NTC5	Fixed	8020 Frame one side	36	69
CMS_NTC6	Fixed	8020 Frame one side	66	75
CMS_NTC7	Fixed	8020 Frame	66	72
CMS_NTC8	Movable	1 Panel 8020 Frame +TKS	45	60
CMS_NTC9	Fixed	8020 Frame	44	65
CMS_NTC10	Fixed	8020 Frame	48	80
CMS_NTC11	Movable	1 Panel 8020 Frame +TKS	22	77
CMS_NTC12	Fixed	8020 Frame	12	77
CMS_NTC13	Fixed	Existing Unistrut	24	84
CMS_NTC14	Fixed	Existing Unistrut	12	57
CMS_NTC15	Fixed	Existing Bus Structure	Field Fit	~24
CMS_NTC16	Fixed	Existing Bus Structure	Field Fit	~24
CMS_NTC17	Fixed	Existing Bus Structure	Field Fit	~24
CMS_NTC18	Cage	ExVV Heating System Skid Cage	Field Fit	72
CMS_MER1	Cage	Vestbule Door	Field Fit	88
CMS_GAL1	Cage	Vestbule Door	Field Fit	88
CMS_GAL2	Cage	Vestbule Door	Field Fit	88
CMS_GAL3	Cage	TVPS Gallery	Field Fit	88
CMS_GAL4	Cage	NB Gallery	Field Fit	88
CMS_CWS1	Cage	NBPC Basement (Pump Room) Bakeout Skid	Field Fit	88

Prototype Movable CMS

*in compliance with ESHD-5008 (PPPL Safety Manual)

Community Members Generously Participated in Design Reviews

PSS Conceptual Design Review

PSS Preliminary Design Review

Patrick Bong of Lawrence Berkeley Laboratory

Jerry Kowal of Jefferson National Laboratory

David Freeman of Oak Ridge National Laboratory

Kelly Mahoney of Oak Ridge National Laboratory

Scott Buda of Brookhaven National Laboratory

Summary

- Accelerator community documents surveyed for community and Industrial Consensus Standards references
- IEC 61511 was selected to guide the NSTX-U PSS development phase
  - Design process
  - Hazards Analysis
  - Risk Assessment
  - Requirements, SIFs & Required Risk Reduction Factor(s)
  - System Performance
- ANSI N43.1 was referenced for exclusion area assessment
- IEC 61508 applicable for component qualification of COTS
- Community members generously participated in Design Reviews

Backup Slides