National Spherical Torus eXperiment Upgrade

Layer of Protection Analysis Overview

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

J. Petrella - Cognizant Engineer
T. Jernigan - APM

Last edit: 3/9/20

Motivation

- Director's Review in September 2018 revealed need to replace legacy Hardwired Interlock System
- PPPL has done extensive work on determining the correct path forward, and has arrived at a "Layer of Protection Analysis" (LOPA) to hazard mitigation.
- Three systems, all part of the Recovery Project, provide hazard mitigation

System	Hazards Mitigated	WBS	BAC
Personnel Safety System (PSS-SIS) (requirements)	Radiological, Magnetic	1.09.04.01	$11.5M
Trapped Key System (TKS) (requirements)	Radiological, Electrical, Thermal		
Configuration Managed Safeguards (CMS) (requirements)	Electrical, Thermal, Vacuum		
Centralized Control System (requirements)	N/A (not credited for personnel safety)	1.09.04.02	

Outline

1. LOPA Philosophy
2. Tolerable Risk
3. LOPA assumptions
4. System Performance Fault Tree
5. Summary

PLC-Based Personal Safety System (PSS) will be discussed in detail in the next talk.

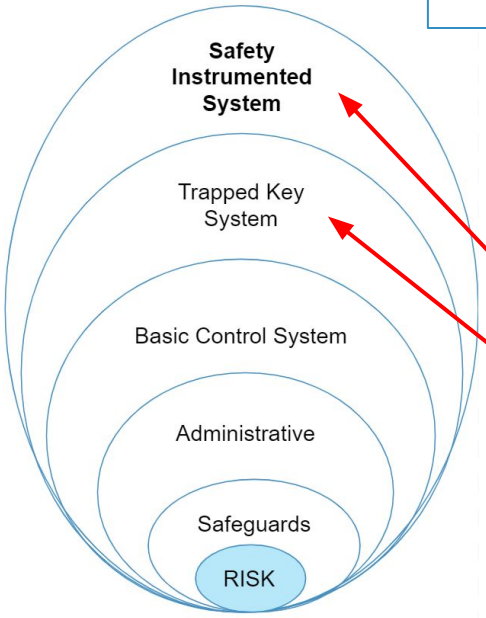
LOPA has been used to determine the PSS-SIS SIF risk reduction performance requirements.

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)

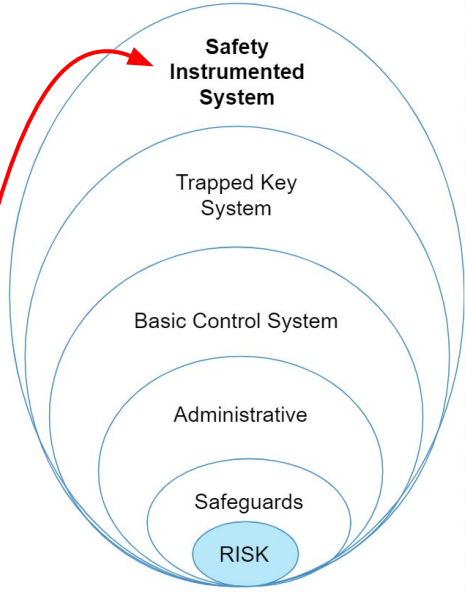


IPL

IPL

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)



Tolerable Risk Frequency Used in LOPA Established in FMECA and Hazard Analysis Plan

- Developed/documented in FMECA and Hazard Analysis Plan
- Thresholds for severity defined in FMECA Plan
- Consistent within the DOE/SC community
- Maximum frequency for each severity used as a maximum frequency target in the LOPA

	Maximum Allowable Frequency Per Year		
	1.00E-04	1.00E-02	1.00E+00
Low Severity			X
Medium Severity		X	
High Severity	X		

Similar Risks Condensed Into Impact Event Categories For LOPA

- Impact Event “A” → direct ionizing radiation exposure in unrestricted areas
- Impact Event “B” → Non-contact hazards in restricted areas
- Impact Event “C” → contact exposure to thermal or electrical hazards

Risk Initiating Cause Frequencies (what caused the hazard exposure) were conservatively derived from industrial conventions and national databases

- Failure of Search & Secure Process: $1x10^{-1}$/yr
  - Be missed by Engineered Search and Secure Process
  - Conservatively assume exclusion area is always occupied at the time of the search
  - Based upon industry convention for operator error (CCPS LOPA 'Purple Book' Table 5.1)
- Individual inappropriately in exclusion area *AND* removes Guards: $1x10^{-2}$/yr

Risk Conditional Modifiers (conditions to develop the hazard to its maximum consequence) were conservatively reached through simplified conclusions

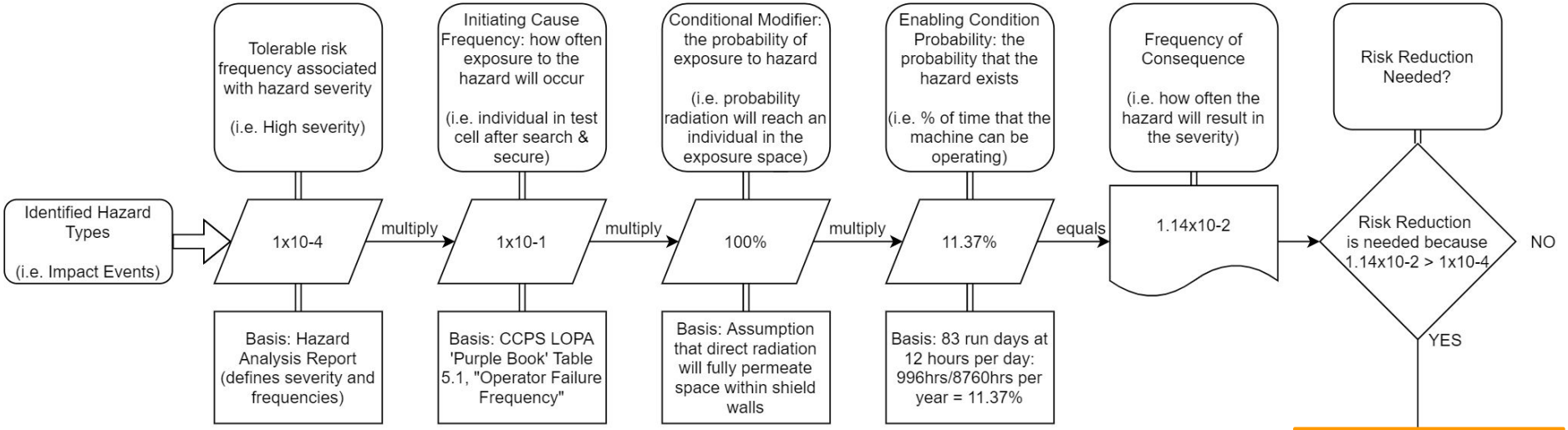
- Probability of Non-Contact Hazard Exposure within Exclusion Areas: 100%
  - There is no radiation/magnetic shielding once an individual is inside an Exclusion area
- Probability of Contact with Uninsulated electrical or thermal hazards: 50%
  - An individual must touch exposed hazardous surfaces inside an Exclusion area - the hazard does not extend beyond the surface

Risk Enabling Condition Probabilities (condition to have hazard) were based upon conservative estimations of time-at-risk and success of malicious acts

- Time-At-Risk for Non-Contact Hazards: 11.37%
  - Based upon 83 run days per year for operations assuming 12 hour days
- Time-At-Risk for Bakeout: 5.75%
  - Based upon 21 run days per year for bakeout (full 24 hour days)

The Initiating Causes, Conditional Modifiers, and Enabling Conditions were assembled into a spreadsheet to quantify required risk reduction. This process was reviewed with our Safety Instrumented System Expert consultant[1] as well as vetted during the PDR and FDR by accelerator community peers[2]

LOPA process of determining if Risk Reduction is needed by Independent Protection Layers



Continued On Next Slide

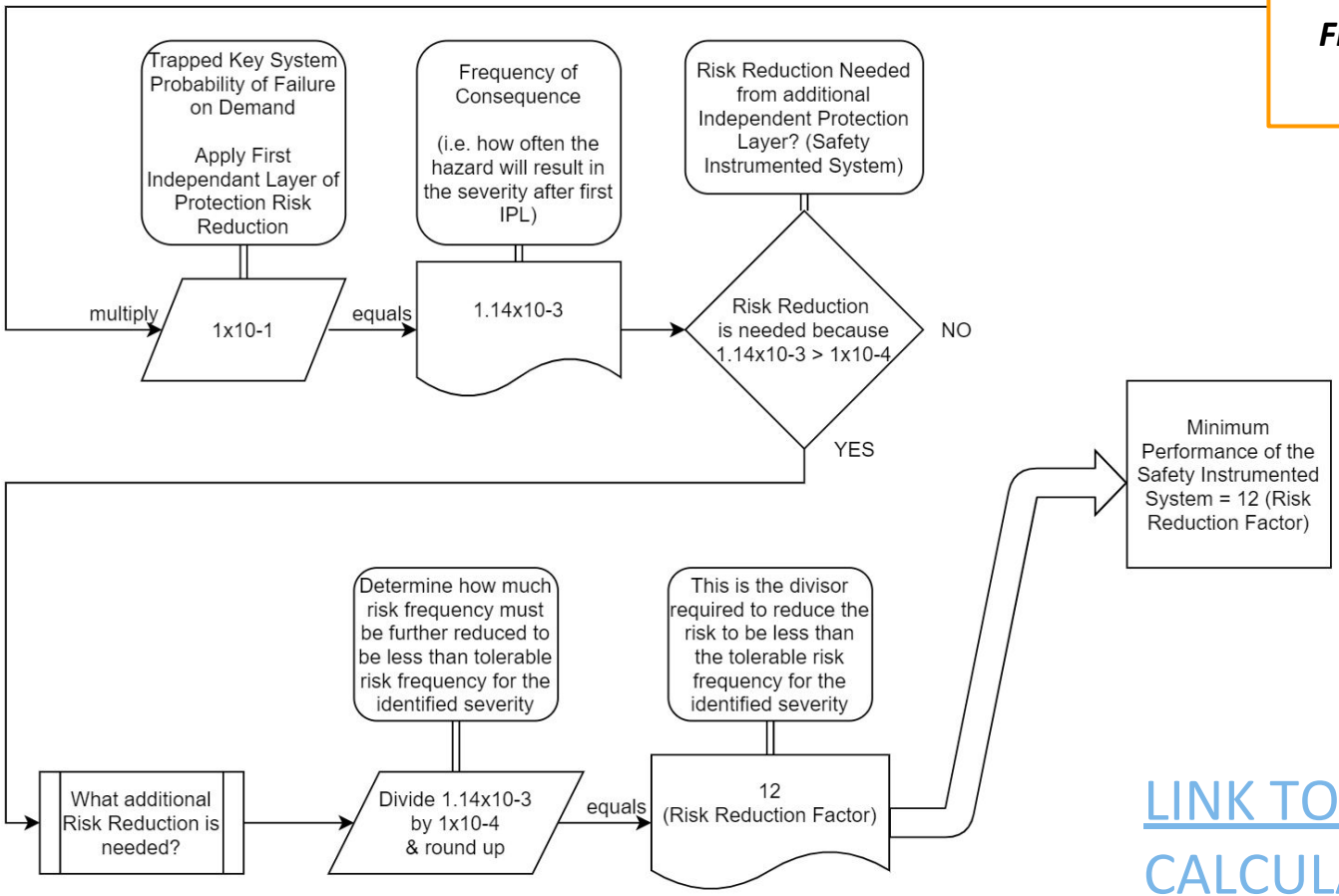
LINK TO FULL LOPA CALCULATION

[1]Joe Veasey AE Solutions contractor, IEC 61511 Expert

[2](PDR) S. Buda, K. Mahoney (FDR) J. Kowal, P. Bong, D. Freeman, S. Davis

The resulting event frequency is mitigated, as necessary, by Independent Protection Layers (IPLs)

From Previous Slide



[LINK TO FULL LOPA CALCULATION]

Hazards are mitigated by three independent systems*

Safety Instrumented System (SIS):

- Ionizing Radiation Hazards - Direct (Within the NTC)
- Ionizing Radiation Hazards - Direct (Outside the NTC)
- Magnetic Field Hazards

Trapped Key System (TKS):

- Electrical Hazards - Experimental Power
- Hot Gas & Fluid Hazards
- Ionizing Radiation Hazards - Direct (Within the NTC)
- Ionizing Radiation Hazards - Direct (Outside the NTC)
- Magnetic Field Hazards

Configuration Managed Safeguards (CMS):

- Vacuum Hazards
- Radio Frequency Hazards
- Hot Gas & Fluid Hazards
- Laser Hazards
- Electrical Hazards -Experimental Power

*Hazard Analysis Report (HAR): located here

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

The Safety Instrumented Function requires 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

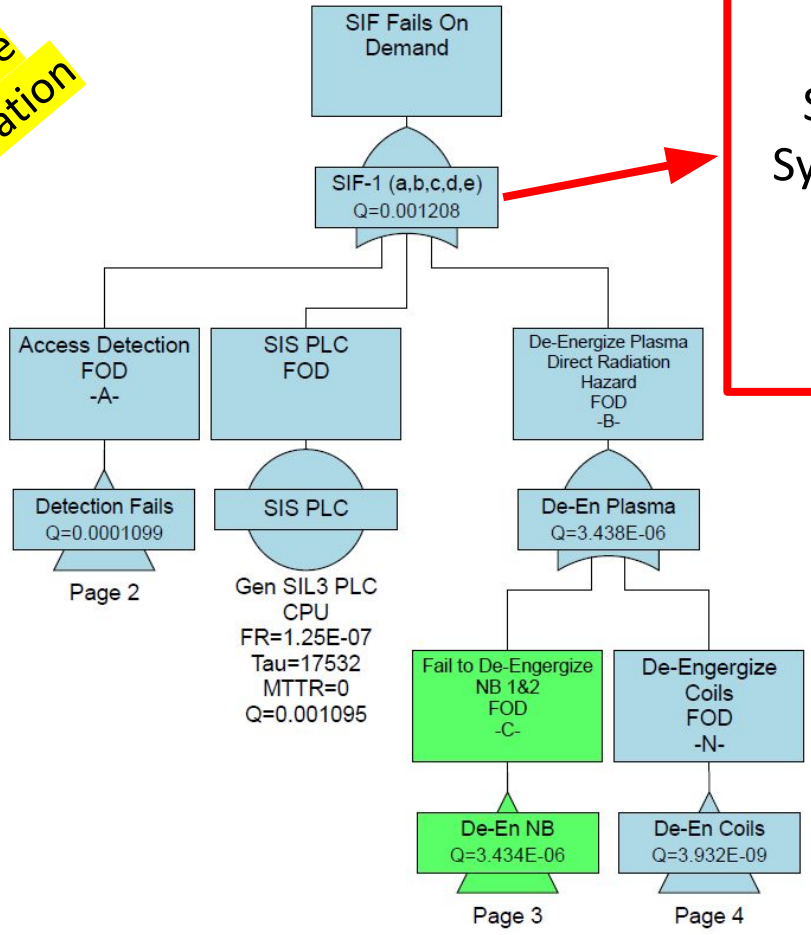
The Safety Instrumented System Design was input into a Fault Tree to Determine Performance. Calculation Approach & Input Parameter Overview Below:

The Fault Tree & Probability of Failure on Demand (PFD) calculation was constructed in ***Isograph's Reliability Workbench incorporating FaultTree+.***

- Switchgear dataset → Journal of Loss Prevention white paper: "Integrating switchgear breakers and contactors into a safety instrumented function"
- All other hardware → generic datasets from Exida's Safety Equipment Reliability Handbook (SERH)
  - **Generic data** allows for alternative components in the SIF without prompting any need to adjust the SIL calculations.
  - The Logic Solver, Door Switches, and Interdiction Relays qualify for selection because they were manufactured in accordance with IEC 61508-2 and IEC 61508-3

PSS-SIS achieves a minimum Risk Reduction Factor (RRF) of 827 with a two year test interval > the RRF requirement of 12 & one year test interval

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

Third-Party Stage 1 Functional Safety Assessment Completed With No Deficiencies Found

- A stage 1 FSA is an independent review of the requirements and specifications driving the design of the SIS
- The assessment was conducted by Greg Hardin (TUV FSEng) of aeSolutions who served as an independent reviewer
- No deficiencies were identified

Link

Summary

- Layer of Protection Analysis was used to quantifiably define the risk mitigation requirements for independent protection layers
- The Trapped Key System and a Safety Instrumented System (SIS) are used to reduce risks to a defined tolerable likelihood
- A minimum Risk Reduction Factor (RRF) for the SIS of 12 was determined for Safety Instrumented Functions (SIF)-1a/b/c/d/e
- SIS configurations of Neutral Beam only and Neutral Beam and coil operation achieve a risk reduction factor of 827
- Achieved SIS RRF exceeds requirements as established in the LOPA (827>12)

Final Design components and configuration exceeds the minimum RRF