



**NUSCALE**™  
Power for all humankind

# Use of STPA in the Development of a Reactor Protection System at NuScale Power

July 29, 2020

Paul G. Butchart  
Instrumentation and Controls Engineer

**NuScale Nonproprietary**

Copyright © 2020 by NuScale Power, LLC.

Template #: 0000-20955-F01 R11

# Acknowledgement & Disclaimer

This material is based upon work supported by the Department of Energy under Award Number(s) DE-NE0008928.

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

## About Me and NuScale Power

- Instrumentation and Controls Engineer
  - 7 years at NuScale
  - 30+ Years Experience in I&C
  - 6 Years Experience in STPA
- Performed Hazard Analysis on the NuScale MPS
  - 3 Revisions
  - ~1000 Pages of Documentation
- Performed HA on the NuScale safety display and instrumentation system
- Trained analysts for additional systems
- NuScale Power – Power for all Humankind

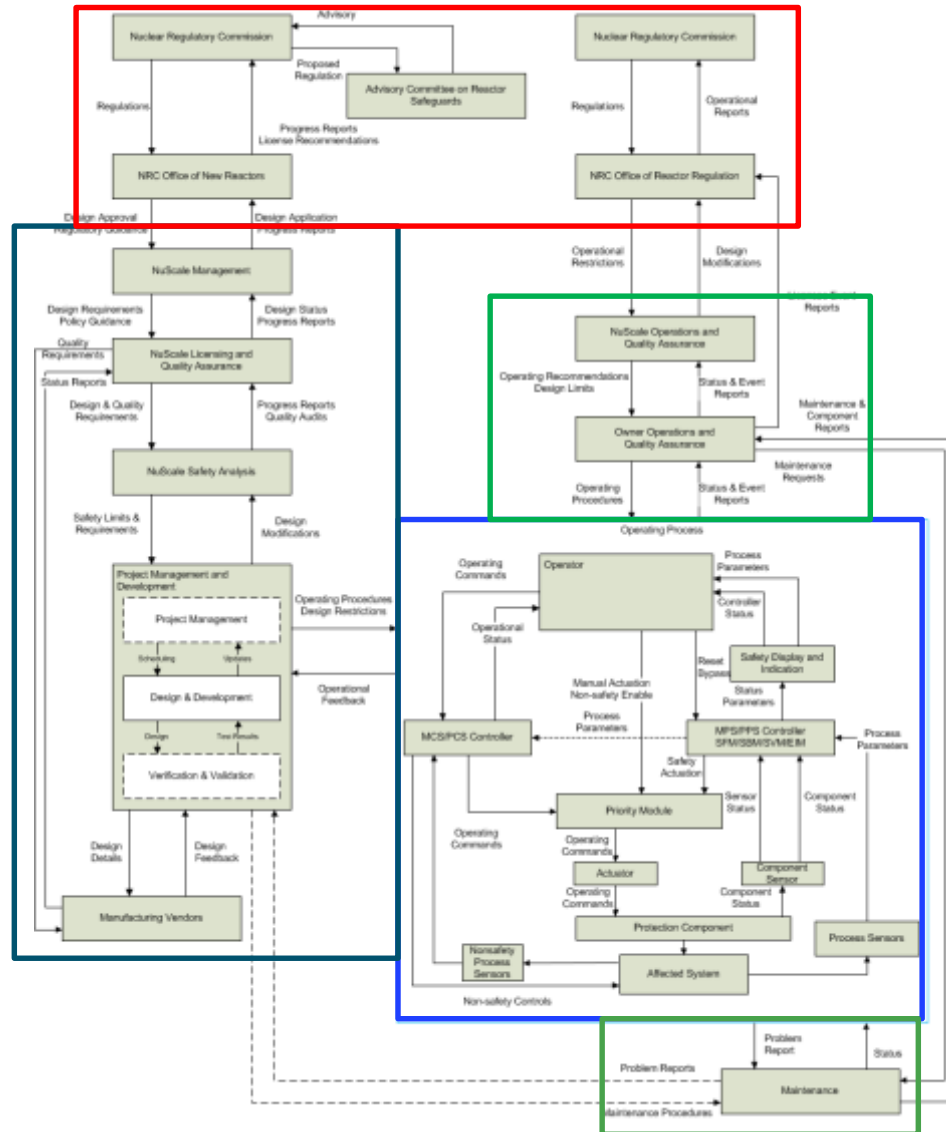
# Normal Nuclear Processes

- High degree of safety is key in any nuclear project
- Typical analysis methodology
  - Preliminary Hazard Analysis (PHA)
  - Failure Modes and Effects Analysis (FMEA)
  - Fault Tree Analysis (FTA)
- Failure Modes and Effects and Fault Tree Analyses have commonly been used to evaluate system failure modes.
  - These methods have limitations when applied to modern digital control systems

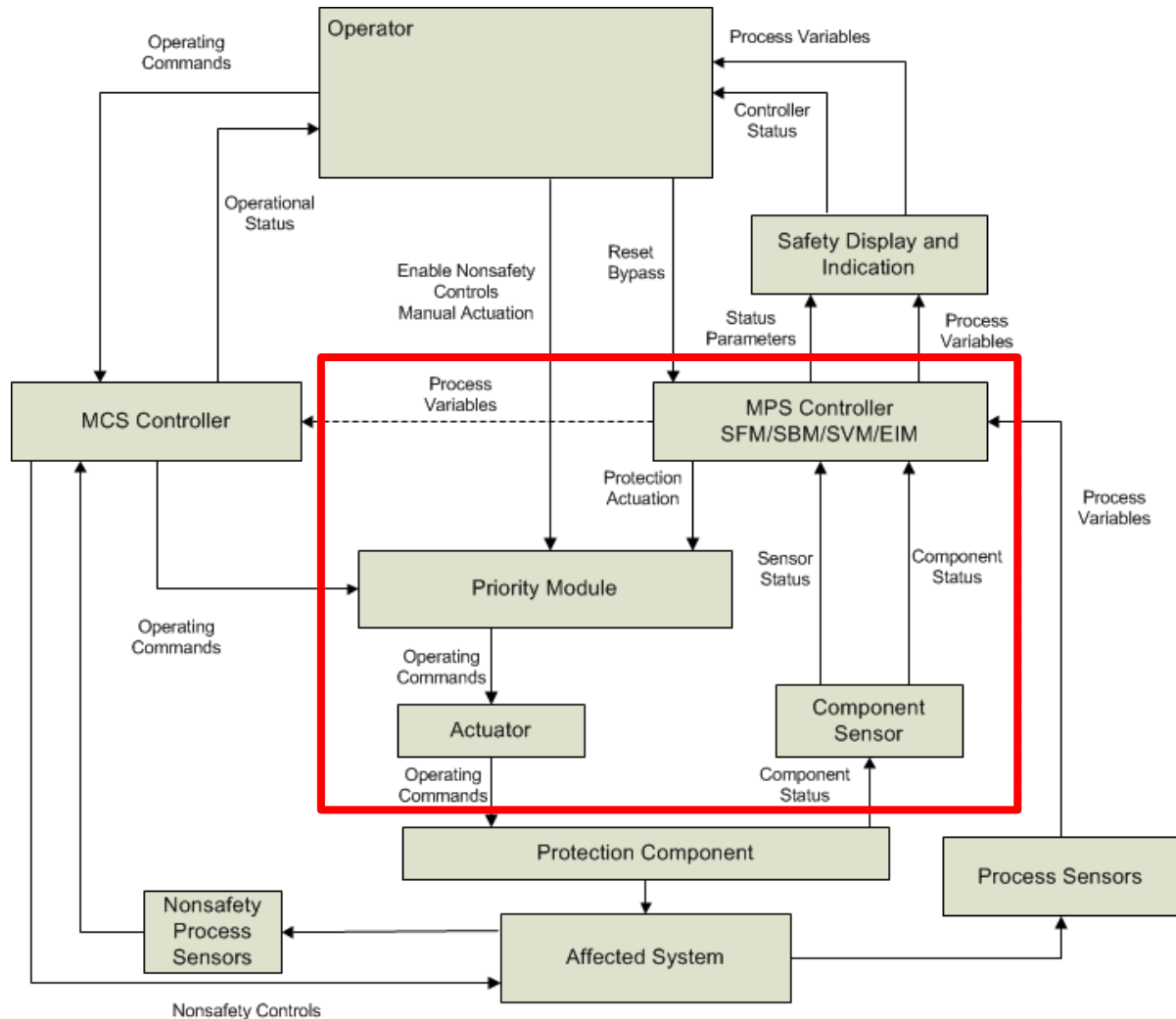
## Defining the Scope

- Limited resources
  - New method in an industry where change is slow
  - Instrumentation and control priorities
  - Regulatory requirements
- Scope defined as
  - Module protection system
  - Plant protection system
  - Neutron monitoring
  - Safety display and indication
- However, we decided to show the potential scope

# Processes Affecting Design



# Limited Scope



# Analysis Workflow

- Broke down the system into primary functions
  - Signal acquisition and processing
  - Trip analysis functions
  - Voting
  - Trip actuation
- Built the control diagrams
- Performed the analysis
- Incorporated safety constraints in system design - Note
- Performed a cross-reference to Preliminary Hazard List
- Performed a cross-reference of safety constraints to system requirements
  - Analyzed relationships through various design phases



# Cross-Reference Example

Safety Constraint ID	Constraint		Comments
	Requirement ID	Contributing	Evaluation
SC-1.1.	Inputs to the signal conditioner should be reliable and continuous.		
	E011-MPS-FR-7123	Yes	The requirement imposes the need to sense accident conditions.
	E011-MPS-FR-7135	Yes	
	E011-MPS-FR-7143	Yes	

# Relationship Statistics

	Functional Requirement Relationships	System Design Requirement Relationships	Design Solution Relationships
Total Relationships	942	2237	5525
Safety Constraints (SC) with 10 or more relationships	8	75	236
SC with no relationships	82	20	15
SC with less than 5 relationships	208	75	34

## Acceptance

- NuScale and the NRC engaged for several years in development of Hazards Analysis framework
- The NuScale Design Certification Application was the first implementation of an HA for a digital I&C system design.
  - Overall positive results from NRC safety reviews
- Electric Power Research Institute (EPRI) – very interested
- Overall the response and acceptance was very positive

Thank you for your time!



**Paul Butchart**  
Instrumentation and Controls Engineer  
[pbutchart@nucscalepower.com](mailto:pbutchart@nucscalepower.com)