INL/MIS-19-56515-Revision-0

Demonstration of Integrated Hazard Analysis for Digital Reactor Trip Systems

November 2019

Tate Shorthill, Hongbin Zhang, Heng Ban, Han Bao

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-19-56515-Revision-0

Demonstration of Integrated Hazard Analysis for Digital Reactor Trip Systems

Tate Shorthill, Hongbin Zhang, Heng Ban, Han Bao

November 2019

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Demonstration of Integrated Hazard Analysis for Digital Reactor Trip Systems

Tate Shorthill*, Han Bao, Hongbin Zhang**, Heng Ban***

*University of Pittsburgh, 3700 O'Hara Street, Pittsburgh, PA 15261
**Idaho National Laboratory, 2525 Fremont Ave, Idaho Falls, ID 83402

Anecdote

Source: Unsplash

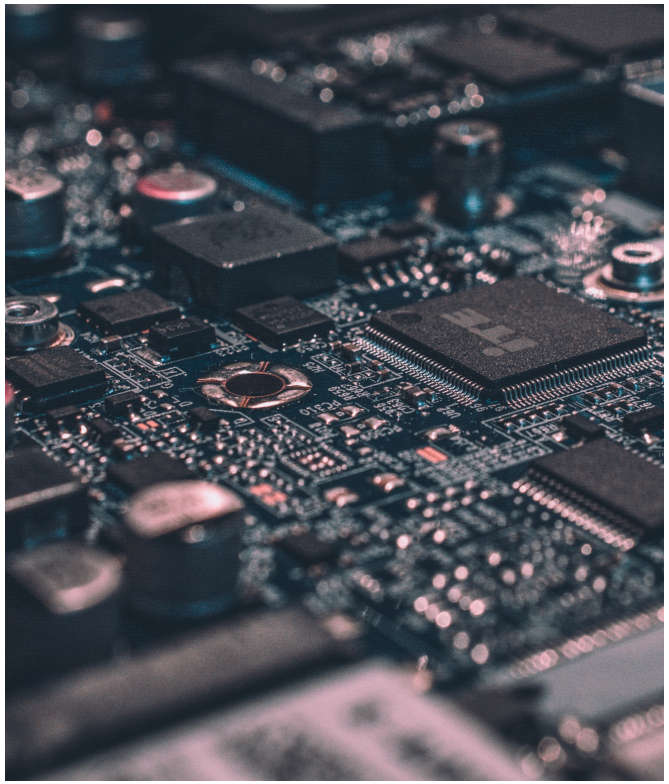
To support the transition to digital instrumentation and control (I&C)

Benefits of Digital I&C systems [1]

- Reduced signal noise
- Rapid data processing
- Automatic self-testing
- Remote Software modification

Technical Barriers for the implementation of digital I&C systems in Nuclear Power Plants [2]

- The unique characteristics of digital systems
- The potential for software based common cause failures (CCF)
- Need for an assessment method tailored to digital I&C



[1] H. Hashemian, "Nuclear Power Plant Instrumentation and Control," in Nuclear Power - Control, Reliability and Human Factors, P. Tsvetkov, Ed., Intech, 2011, pp. 49-66.
[2] National Research Council, Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues, Washington, DC: The National Academies Press, 1997.
Images: Unsplash

Status of Digital I&C Risk Assessment Research

NUREG/CR-5485: Modeling CCFs in risk assessments
NUREG/CR-6303: Application of diversity to minimize CCFs
NEI 16-16: Guidance on addressing CCFs [7]

EPRI: Hazard analysis compare/contrast FMEA, FTA, HAZOP, STPA, an PGA [4]
EPRI/Sandia: Hazard and consequence analysis (HAZCADS) [5]
NUREG 6430: mostly lists methods that might be used

NUREG/CR-6901: Reliability modeling
NUREG/CR-6942: Dynamic Reliability modeling
NUREG/CR-6985: Dynamic Reliability and Benchmark
IAEA Nuclear Energy Series: Dependability Assessment [6]

NUREG/CR-6303: Application of diversity to minimize CCFs
NUREG/KM-0009: Historical Review of Defense in Depth
NUREG/CR-7007: How much diversity is enough

EPRI/Sandia: Hazard and consequence analysis HAZCADS

[4] Electric Power Research Institute, "Hazard Analysis Methods for Digital Instrumentation and Control Systems," EPRI, Palo Alto, CA, 2013.
[5] A. J. Clark, et. al, "Hazard and Consequence Analysis for Digital Systems – A New Approach to Risk Analysis in the Digital Era for Nuclear Power Plants," in *Transactions of the American Nuclear Society*, Orlando, Florida, USA, 2018.
[6] International Atomic Energy Agency, "Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants," IAEA, Vienna, Austria, 2018.
[7] Nuclear Energy Institute, "Guidance for Addressing Digital Common Cause Failure," NEI, Washington D.C., 2017

Where our work fits

- We will provide a means to assess the risks of highly redundant digital systems by ensuring a systematic method of identifying hazards.

- **The objectives of this work (Hazards analysis) include:**
  1. Providing a technical basis for the implementation of a reliability analysis.
  2. Providing a technical basis to help utilities optimize the use of diversity attributes in a cost-effective manner.
  3. Helping engineers efficiently mitigate risk by allowing them to systematically identify the most critical hazards (including CCFs) of digital I&C systems.

- Hazard analysis comes in three bsic parts. Historically most of the interest has been in the reliability assessment and so there. But there generally has been work in all the areas. These nuregs are concerned with reliability.

- A risk assessment answers the tree main questions and for

Need a method for both digital I&C and CCF concerns

- The use of digital technologies may “increase the potential for CCF vulnerabilities because of the introduction of undetected systematic faults” [3].
- Redundancy breeds potential for CCFs
  - Need to capture redundant features in the method
- Vulnerabilities/systematic faults may result from [3]:
  - Errors in requirement specification
  - Inadequate provisions to account for design limits (environmental concerns etc.)
  - Technical faults in the system architecture or implementation of the design.

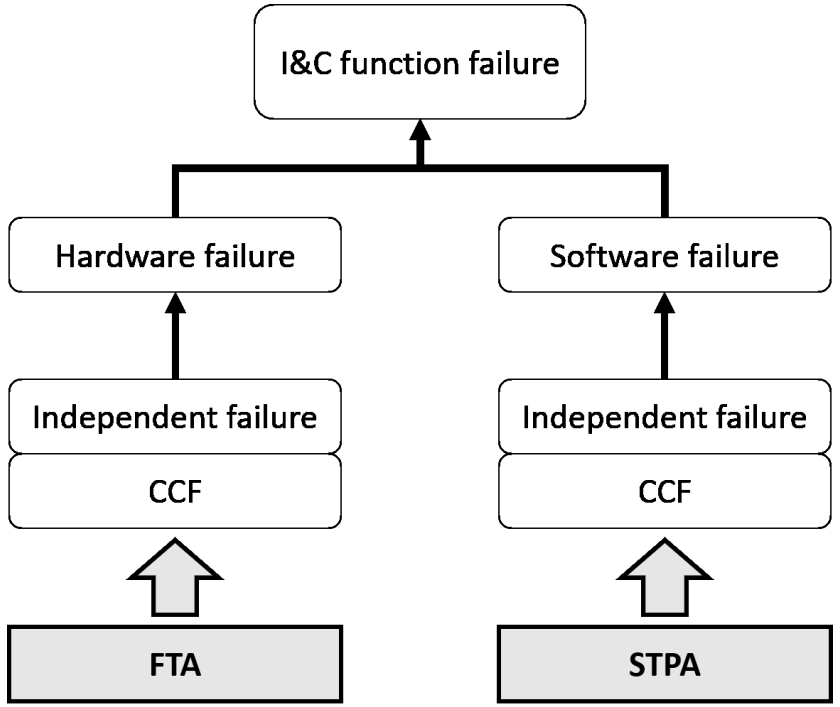
Combinations of analysis methods may be beneficial

- 2018 EPRI and Sandia National Laboratory created a hazard analysis method called HAZCADS which combines the benefits FTA and STPA for portion of their method [9].
- Our current work incorporates this concept of combining FTA and STPA as part of the approach for a redundancy guided hazard analysis.

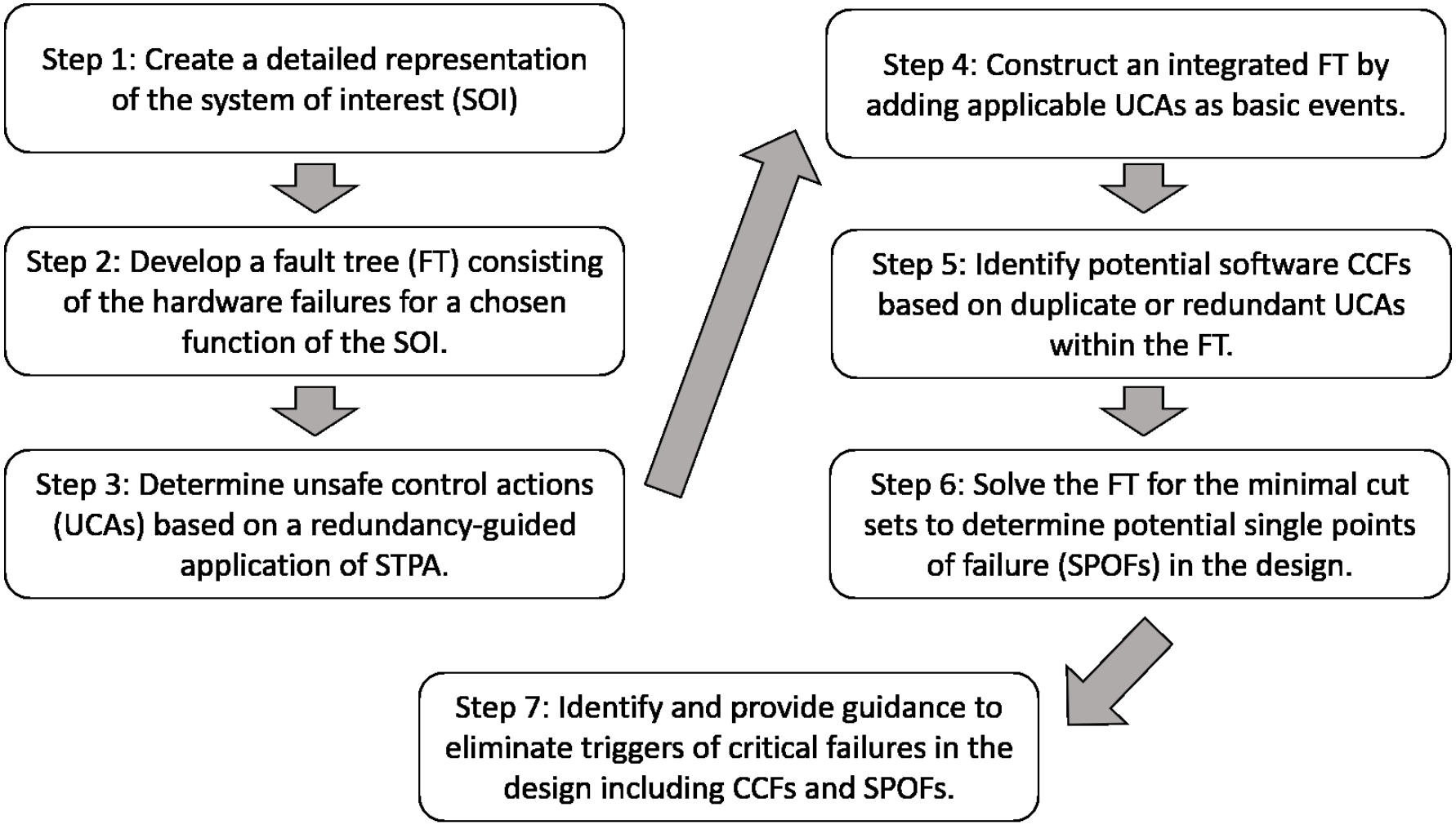
[3] M. Muhlheim and R. Wood, "Technical Basis for Evaluating Software-Related Common-Cause Failures," Oak Ridge National Laboratory, Oak Ridge, 2016.
[9] A. J. Clark, et. al, "Hazard and Consequence Analysis for Digital Systems – A New Approach to Risk Analysis in the Digital Era for Nuclear Power Plants,” in *Transactions of the American Nuclear Society*, Orlando, Florida, USA, 2018

FTA and STPA

- FTA Provides fast qualitative indicators of most significant failures.(objective 3)
- Redundant features with FTA is straightforward (chief motivation)
- STPA has been demonstrated to address digital systems
- STPA does not center the analysis on redundancy
  - STPA is ideally applied early[10] in design before the addition of safety features (e.g. diversity, redundancy)
- An analysis focused on identifying CCFs should include all the redundant features and components of the system.
  - **STPA should be reframed in a redundancy-guided way** to accomplish this purpose

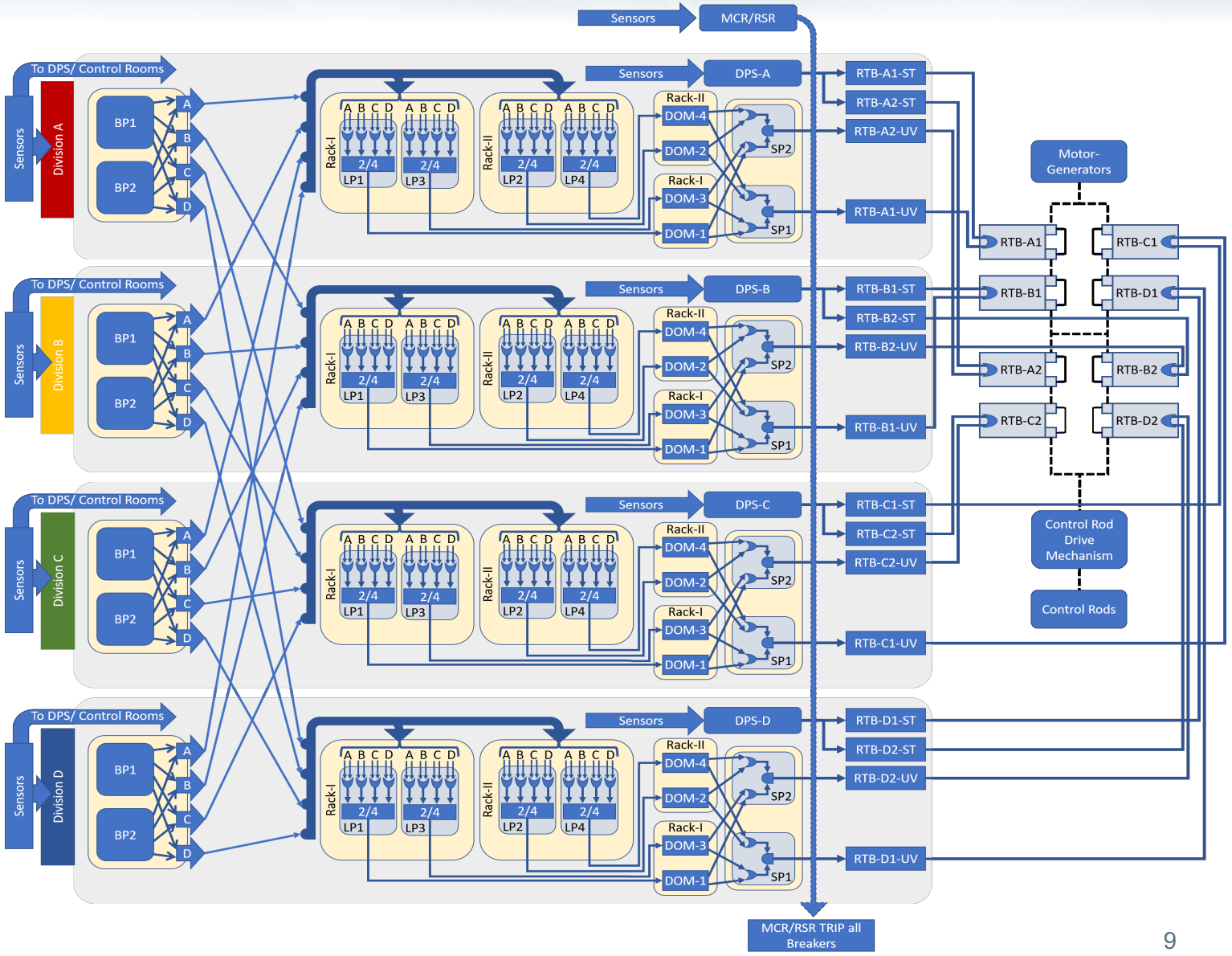


Process for a redundancy-guided systems-theoretic hazard analysis



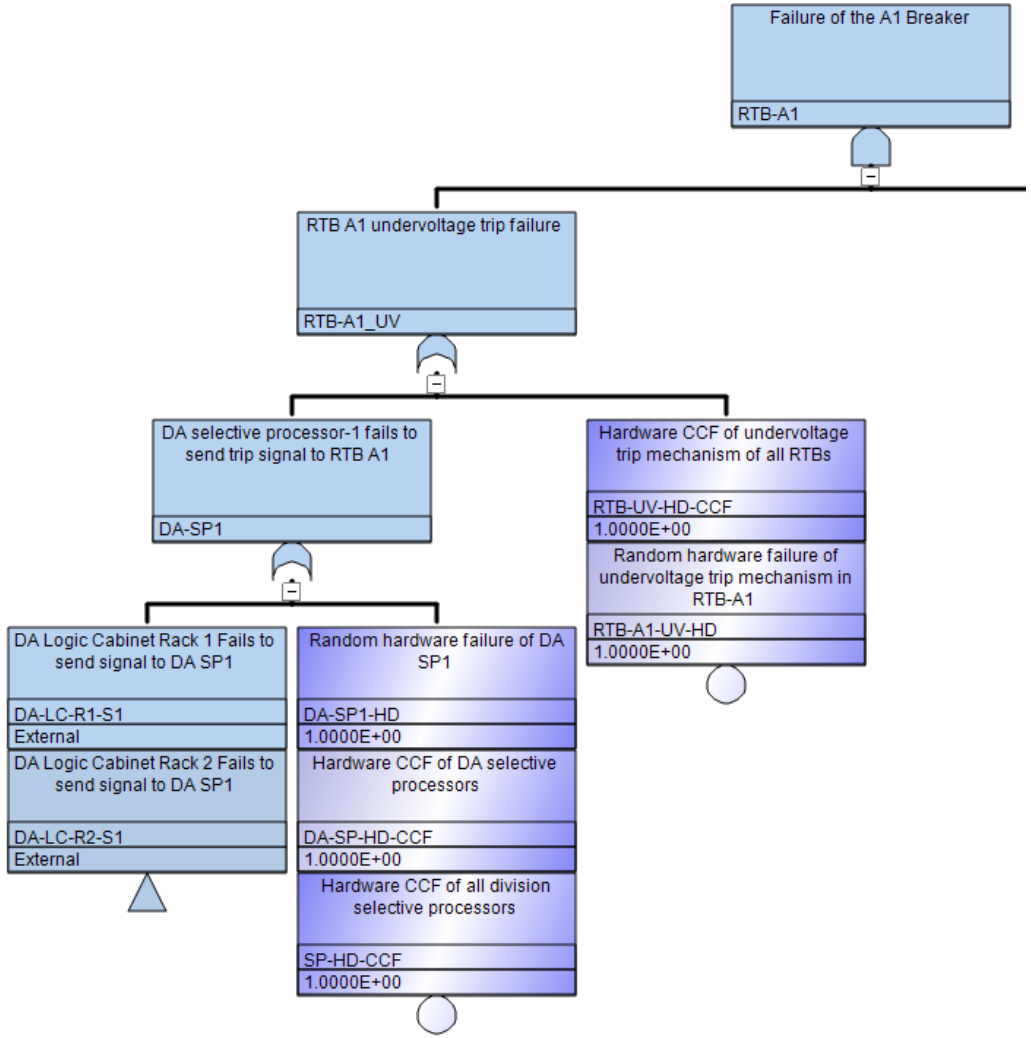
Step 1: System Sketch

- Boundary and scope
- Detail the hardware and software
- Map out the system



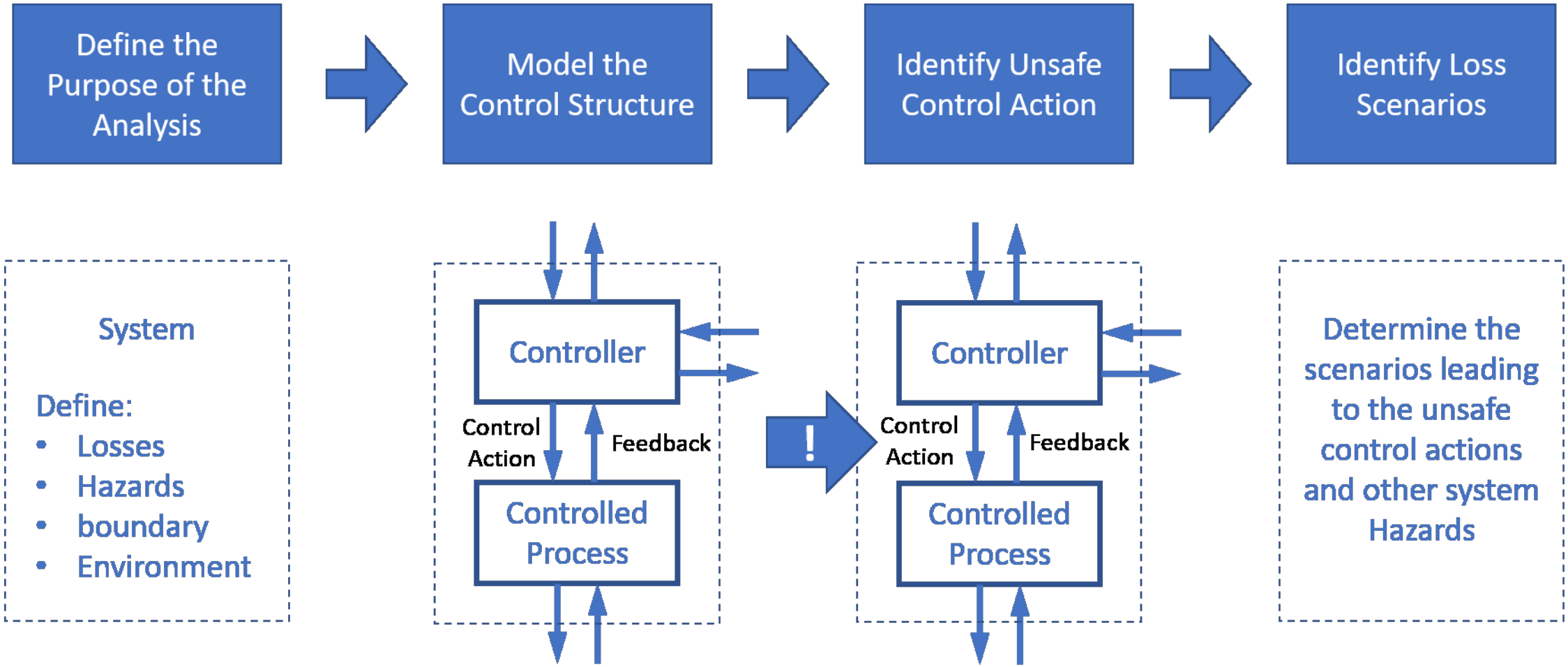
STEP-2: Develop a fault tree (FT) consisting of the hardware failures for a chosen function of the SOI.

- Select a top event and resolution for the analysis
- Include basic events for hardware
- Include any CCFs for hardware components
- The main assumption for this step is that all software failures will be captured using STPA in STEP-3



FT models were made with SAPHIRE program [11].

STEP-3: Determine unsafe control actions (UCAs) based on a redundancy-guided application of STPA.



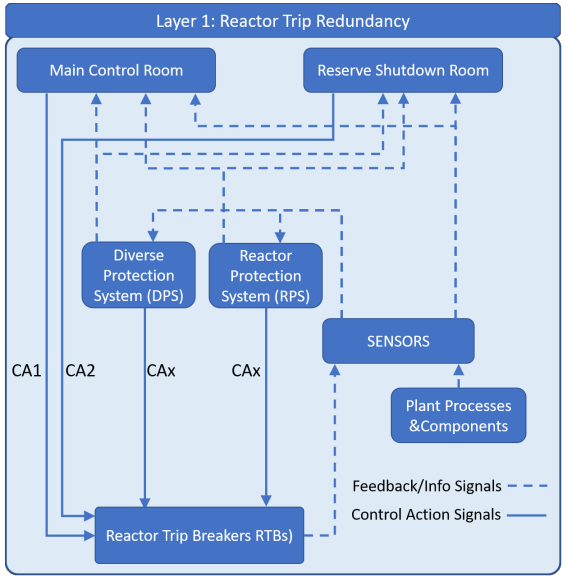
The details shown have been adapted from the STPA Handbook [10]

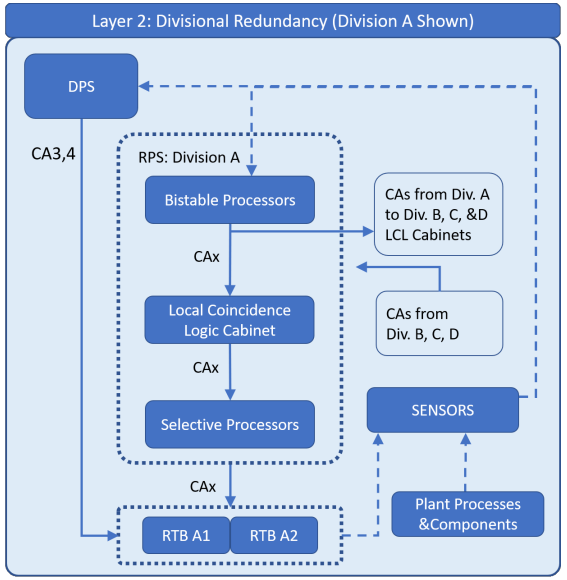
STEP-3: Determine unsafe control actions (UCAs) based on a redundancy-guided application of STPA.

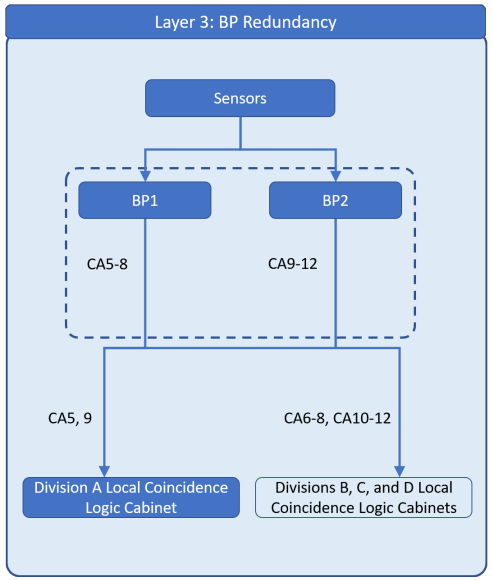
- STEP 3A: defining the system
- STEP 3B: create a model of the c…cu…

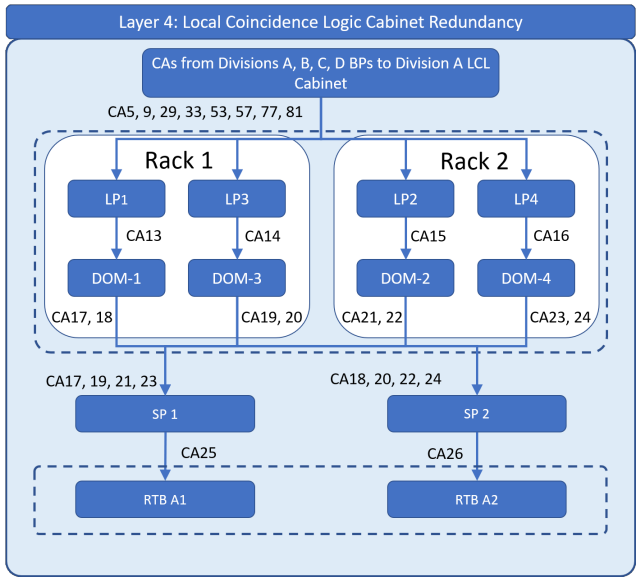
Table 1: Major losses to be prevented [6]	
L1	Human injury or loss of life
L2	Environmental contamination
L3	Equipment damage
L4	Power generation
L5	Public perception

Table 2. Hazards which may lead to Losses [6]	
H1	Reactor temperature too high (L1, L2, L3, L4, L5)
H2	Equipment beyond limits (L1, L2, L3, L4, L5)
H3	Release of radioactive materials (L1, L2, L5)
H4	Reactor shutdown (L4, L5)









STEP 3C: Create a table of UCAs

- A UCA is control action that, in a particular context and environmental conditions, will lead to a hazard.
- Categories[10]:
  - Control action is not provided when it is needed.
  - Control action is provided when it is not needed.
  - Control action is provided when it is needed, but too early, too late, or in a wrong order.
  - Control action lasts too long or stops too soon (only applicable to continuous control actions).

Table 3. Examples of UCAs.

Control Action (CA)	UCAa: CA is needed, but not given	UCAb: CA is Given, but not needed	UCAc: CA is given too early, too late, wrong order	UCAd: CA is applied too long or stopped too soon
CA18: DOM-1 demands SP1 to trip the reactor	UCA18a: DOM-1 does not provide trip command to SP1 during AOO [H1, H2, H3].	UCA18b: DOM-1 provides trip command to SP1 when there is NO AOO [H4].	UCA18c: DOM-1 provides trip command to SP1 after AOO has existed for some time [H1, H2, H3].	UCA18d: Not applicable.
CA20: DOM-3 demands SP1 to trip the reactor	UCA20a: DOM-3 does not provide trip command to SP1 during AOO [H1, H2, H3].	UCA20b: DOM-3 provides trip command to SP1 when there is NO AOO [H4].	UCA20c: DOM-3 provides trip command to SP1 after AOO has existed for some time [H1, H2, H3].	UCA20d: Not applicable.

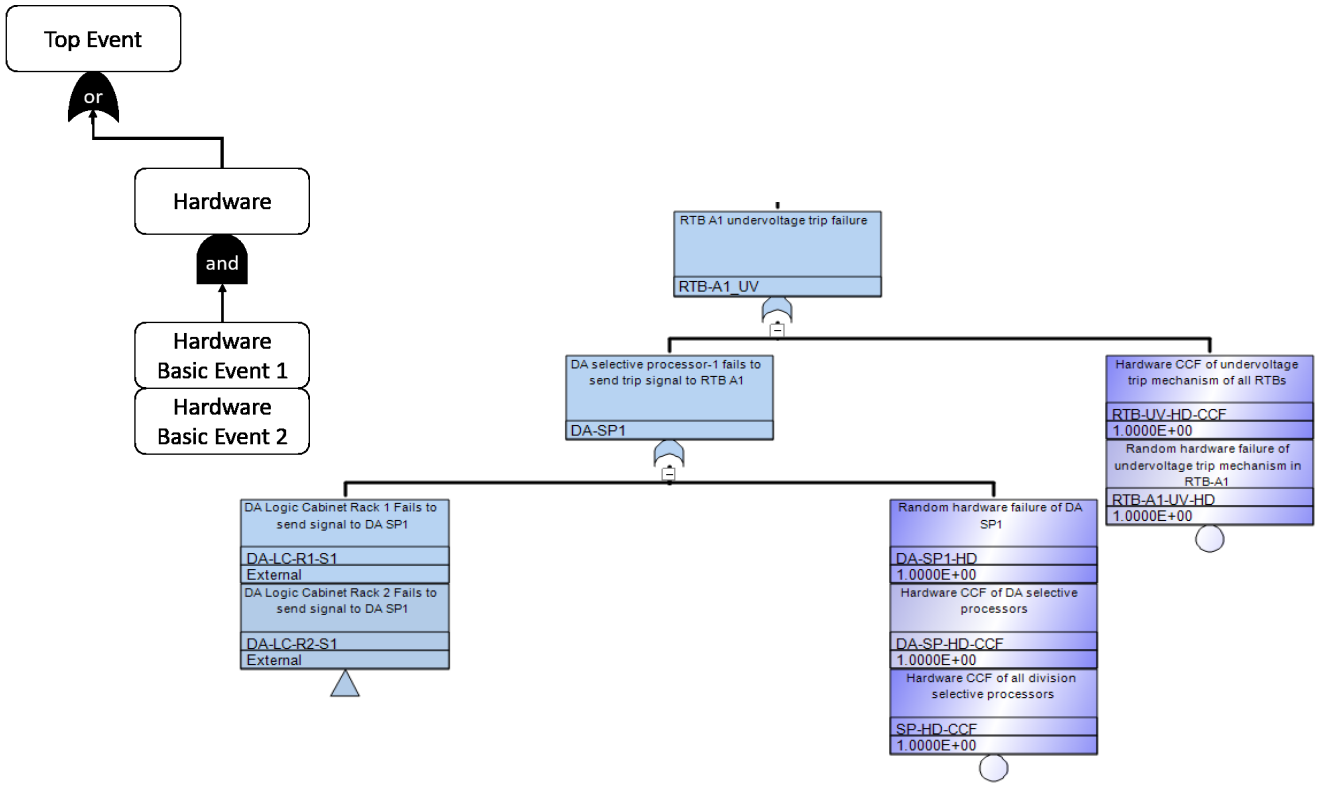
Note: AOO: Anticipated Operational Occurrence; DOM: Digital Output Module; SP: Selective Processor.

STEP-4: Construct an integrated FT by adding applicable UCAs as basic events.

Table 3. Examples of UCAs.

Control Action (CA)	UCAa: CA is needed, but not given	UCAb: CA is Given, but not needed	UCAc: CA is given too early, too late, wrong order	UCAd: CA is applied too long or stopped too soon
CA18: DOM-1 demands SP1 to trip the reactor	UCA18a: DOM-1 does not provide trip command to SP1 during AOO [H1, H2, H3].	UCA18b: DOM-1 provides trip command to SP1 when there is NO AOO [H4].	UCA18c: DOM-1 provides trip command to SP1 after AOO has existed for some time [H1, H2, H3].	UCA18d: Not applicable.
CA20: DOM-3 demands SP1 to trip the reactor	UCA20a: DOM-3 does not provide trip command to SP1 during AOO [H1, H2, H3].	UCA20b: DOM-3 provides trip command to SP1 when there is NO AOO [H4].	UCA20c: DOM-3 provides trip command to SP1 after AOO has existed for some time [H1, H2, H3].	UCA20d: Not applicable.

Note: AOO: Anticipated Operational Occurrence; DOM: Digital Output Module; SP: Selective Processor.

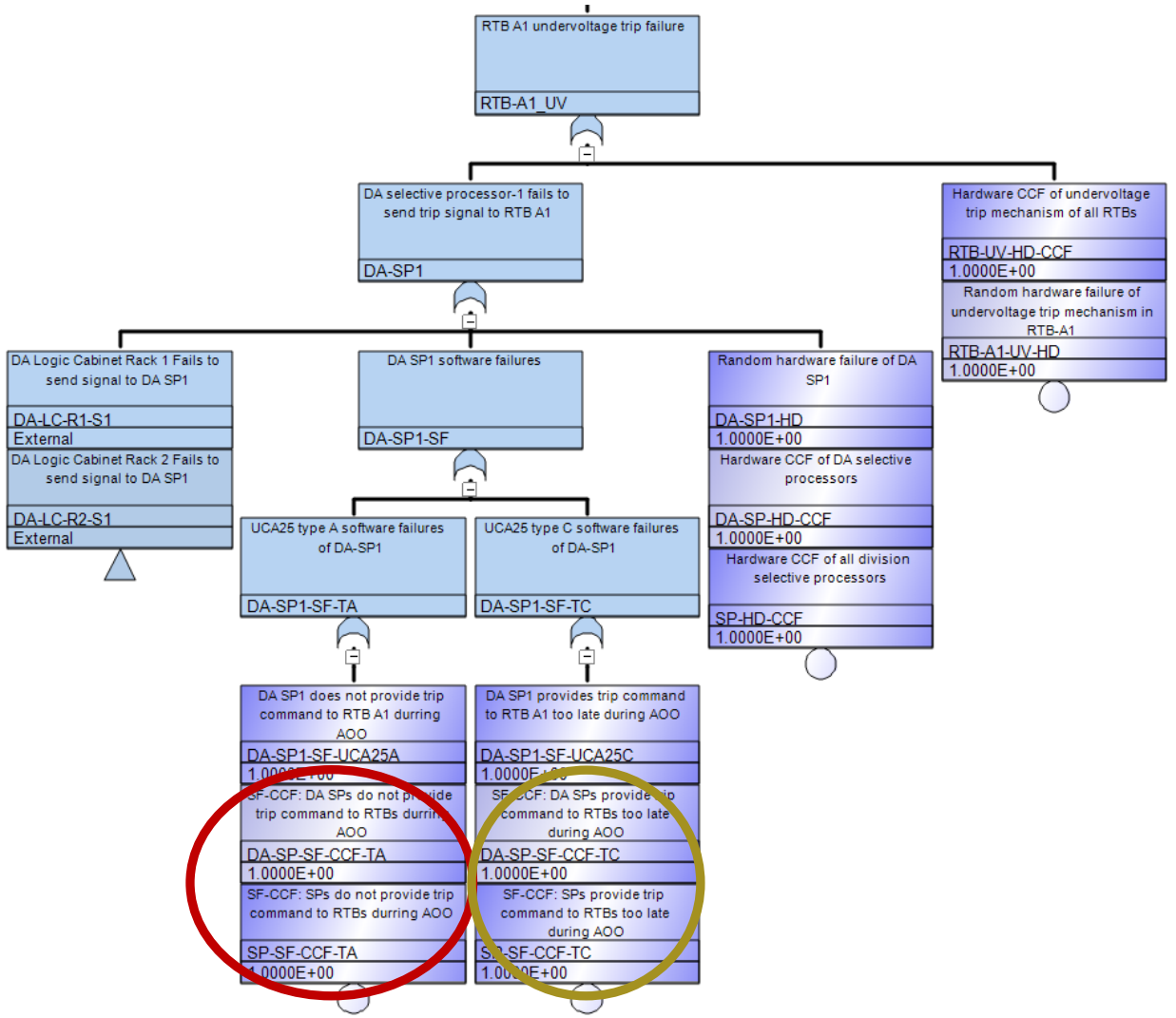


STEP-5 Identify potential software CCFs based on duplicate or redundant UCAs within the FT.

Table 3. Examples of UCAs.

Control Action (CA)	UCAa: CA is needed, but not given	UCAb: CA is given, but not needed	UCAc: CA is given too early, too late, wrong order	UCAd: CA is applied too long or stopped too soon
CA18: DOM-1 demands SP1 to trip the reactor	UCA18a: DOM-1 does not provide trip command to SP1 during AOO [H1, H2, H3].	UCA18b: DOM-1 provides trip command to SP1 when there is NO AOO [H4].	UCA18c: DOM-1 provides trip command to SP1 after AOO has existed for some time [H1, H2, H3].	UCA18d: Not applicable.
CA20: DOM-3 demands SP1 to trip the reactor	UCA20a: DOM-3 does not provide trip command to SP1 during AOO [H1, H2, H3].	UCA20b: DOM-3 provides trip command to SP1 when there is NO AOO [H4].	UCA20c: DOM-3 provides trip command to SP1 after AOO has existed for some time [H1, H2, H3].	UCA20d: Not applicable.

Note: AOO: Anticipated Operational Occurrence; DOM: Digital Output Module; SP: Selective Processor.



STEP-6: Solve the FT for the minimal cut sets to determine potential single points of failure (SPOFs) in the design.

Table 4. Cut set results.

Truncation (order)	Full RTS model	RTS hardware only	Automatic trip only	RPS only
None	N/A	15234	N/A	N/A
6	1,184,652	-	4,583,568	N/A
5	85788	-	1,038,956	328,355
4	468	-	13,1628	54,899
3	0	-	9,532	15,283
2	0	-	**52**	1,203
1	0	-	0	**13**

Table 5: First order cut sets or single points of failure for the RPS system, UV trip only.

Number	Cut set	Description
1	SP-HD-CCF	Selective processor hardware CCF.
3	LC-DOM-HD-CCF	Logic cabinet digital output module hardware CCF.
4	RTB-UV-HD-CCF	Reactor trip breaker undervoltage hardware CCF.
5	LC-BP-HD-CCF	Logic bistable processor hardware CCF.
6	LC-LP-SF-CCF-TA	Logic cabinet logic processor software CCF type A.
7	LC-LP-SF-CCF-TC	Logic cabinet logic processor software CCF type C.
8	LC-DOM-SF-CCF-TA	Logic cabinet digital output module software CCF type A.
9	LC-DOM-SF-CCF-TC	Logic cabinet digital output module software CCF type C.
10	SP-SF-CCF-TC	Selective processor software CCF type C.
11	SP-SF-CCF-TA	Selective processor software CCF type A.
12	LC-BP-SF-CCF-TA	Logic cabinet bistable processor software CCF type A.
13	LC-BP-SF-CCF-TC	Logic cabinet bistable processor software CCF type C.

These tables inform engineers of system vulnerabilities, allowing them to make defensive strategies incorporate safety measures to ensure that the system is successful (goal 3).

STEP-7: Identity and provide guidance to eliminate triggers of critical failures in the design including CCFs and SPOFs.

Table 5: First order cut sets or single points of failure for the RPS system, UV trip only.

Number	Cut set	Description
1	SP-HD-CCF	Selective processor hardware CCF.
3	LC-DOM-HD-CCF	Logic cabinet digital output module hardware CCF.
4	RTB-UV-HD-CCF	Reactor trip breaker undervoltage hardware CCF.
5	LC-BP-HD-CCF	Logic bistable processor hardware CCF.
6	LC-LP-SF-CCF-TA	Logic cabinet logic processor software CCF type A.
7	LC-LP-SF-CCF-TC	Logic cabinet logic processor software CCF type C.
8	LC-DOM-SF-CCF-TA	Logic cabinet digital output module software CCF type A.
9	LC-DOM-SF-CCF-TC	Logic cabinet digital output module software CCF type C.
10	SP-SF-CCF-TC	Selective processor software CCF type C.
11	SP-SF-CCF-TA	Selective processor software CCF type A.
12	LC-BP-SF-CCF-TA	Logic cabinet bistable processor software CCF type A.
13	**LC-BP-SF-CCF-TC**	**Logic cabinet bistable processor software CCF type C.**

- Causal factors due to category 1 (**unsafe controller behavior**): Processing delay in the BPs
- Casual factor due to category 2 (**wrong or incorrect feedback from critical systems**): e.g. Pressure sensor may be incorrectly programed leading to BP failing to receive adequate information.

Conclusions

- This work defines a step-by-step approach for the hazard analysis of digital systems, that can help engineers efficiently make design and risk mitigation decisions by providing them a means to **systematically identify the most critical CCFs** and hazards of digital I&C systems(objective 3);
- This method identifies the critical hazards of a system, allowing utilities to effectively reduce the cost of safety-rated digital I&C by strategically **eliminating unnecessary design features** (objective 2);
- This method provides **a technical basis for reliability analysis** by identifying crucial failure modes and qualitatively determining their effects on system vulnerability (objective 1).
- Ultimately, this method helps improve the design of highly redundant digital I&C through a detailed qualitative hazard analysis.

Acknowledgements

- This submitted manuscript was authored by a contractor of the U.S. Government under DOE Contract No. DE-AC07-05ID14517. Accordingly, the U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for U.S. Government purposes.

- This work was also supported by consultations and contributions from Ken Thomas, and James Knudsen from INL, Andrew Clark and Adam Williams from Sandia National Laboratory, and Edward (Ted) Quinn from Technology Resources.

References

- [1] H. Hashemian, "Nuclear Power Plant Instrumentation and Control," in Nuclear Power - Control, Reliability and Human Factors, P. Tsvetkov, Ed., Intech, 2011, pp. 49-66.
- [2] National Research Council, Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues, Washington, DC: The National Academies Press, 1997.
- [3] T. Aldemir, D. Miller, M. Stovsky, J. Kirschenbaum, P. Bucci, A. Fentiman and L. Mangan, "NUREG/CR-6901 Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments," U.S. Nuclear Regulatory Commission, Washington, DC, 2006.
- [4] J. Kirschenbaum, P. Bucci, M. Stovsky, D. Mandelli, T. Aldemir, M. Yau, S. Guarro, E. Ekici and S. A. Arndt, "A Benchmark System for Comparing Reliability Modeling Approaches for Digital Instrumentation and Control Systems," *Nuclear Technology,* vol. 165, no. 1, pp. 53-95, 2009.
- [5] T. E. Wierman, D. M. Rasmuson and A. Mosleh, "NUREG/CR-6268, Rev. 1 Common-Cause Failure Databased and Analysis System: Event Data Collection, Classification, and Coding," Idaho National Laboratory, Idaho Falls, ID, 2007.
- [6] M. Muhlheim and R. Wood, "Technical Basis for Evaluating Software-Related Common-Cause Failures," Oak Ridge National Laboratory, Oak Ridge, 2016.
- [7] NRC, "Risk Assessment in Regulation," January 2018. [Online]. Available: https://www.nrc.gov/about-nrc/regulatory/risk-informed.html. [Accessed 2019].
- [8] Electric Power Research Institute, "Hazard Analysis Methods for Digital Instrumentation and Control Systems," EPRI, Palo Alto, CA, 2013.
- [9] A. J. Clark, A. D. Williams, A. Muna and M. Gibson, "Hazard and Consequence Analysis for Digital Systems – A New Approach to Risk Analysis in the Digital Era for Nuclear Power Plants," in *Transactions of the American Nuclear Society*, Orlando, Florida, USA, 2018.
- [10] N. G. Leveson and J. P. Thomas, STPA Handbook, March 2018.
- [11] ""Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8.0".

Digital systems exhibit unique failure modes [3,4] extra slide

- Errors in design and software implementation relating to system inputs (Type2)
- Resource allocation can lead to deadlock and starvation (Type 2)
- Communication protocols may introduce dependencies between different systems (Type 2)
  - improper protocols could cause a program to hang or get stuck.
- Digital systems depend on many common (commination, processors, equipment etc.) (Type1/Type2)
  - may be more vulnerable to CCF
- Environmental conditions may effect the performance (Type1)
  - Electromagnetic/radio-frequency interference
  - Temperature
  - Pressure
  - Radiation, etc. (Type 1)
- **Type 1: Interactions between the components of the system and the process physics or environments**.
- **Type 2: Interactions between the components themselves.**