SAND2022-8735C

Sandia National Laboratories

Exceptional service in the national interest

Technique for Managing STPA Results in Physical Security Applications

Using FT appearance frequency to improve VAI

Emily Sandt & Adam Williams

PSAM 16 Honolulu, HI

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Outline

- Security risk
- Overview of what STPA is and does
  - Advantages
  - Drawbacks
- Overview of physical security space where STPA is applied
- Case Study
  - Brief on Steps 0-3
  - Review of Step 3 results (UCAs)
  - Demonstration on subbing UCAs with fault trees of locations - using these area based UCAs as our countable items
  - Areas with most highest counts are deemed higher prioritization
- Future work

What is security risk?

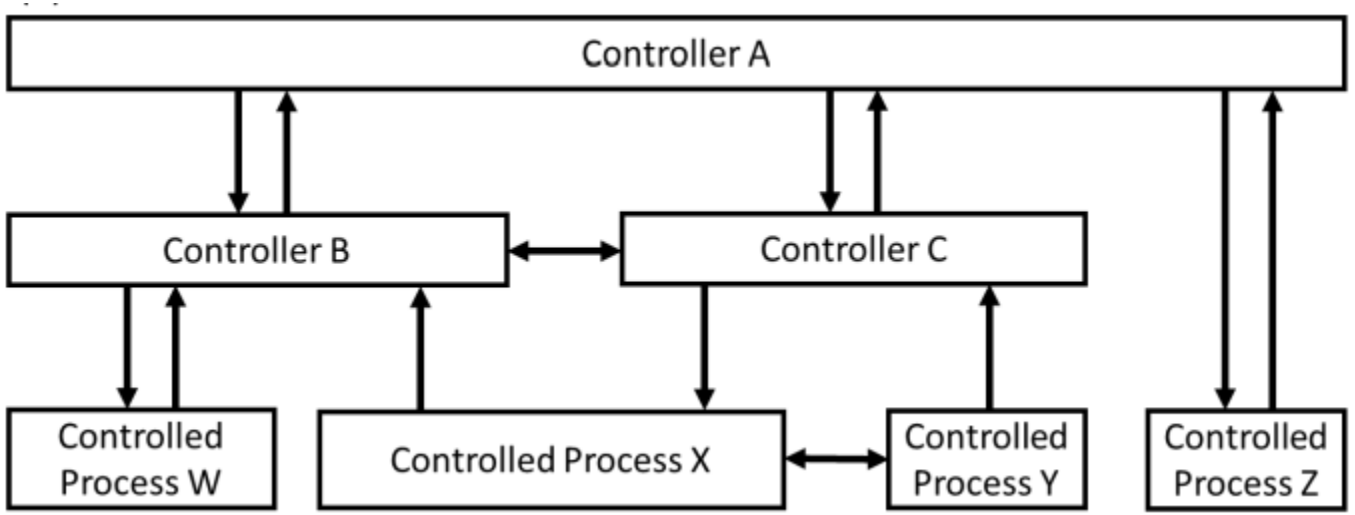
- Plowshares – Y-12 Incident – 2012
  - 3 members breached fence
  - Hung banners opposing nuclear weapons component production
  - Physically damaged structure
  - Protester/Civil disobedience act

- Surry Employees – 1979
  - 2 staff members spilled acid on new fuel rods
  - “Demonstrating” greater risk – 1hr20m timeframe
  - Sabotage
    - Protest – awareness to facility problems
  - BUT, on fresh fuel – not reactor core, SFP

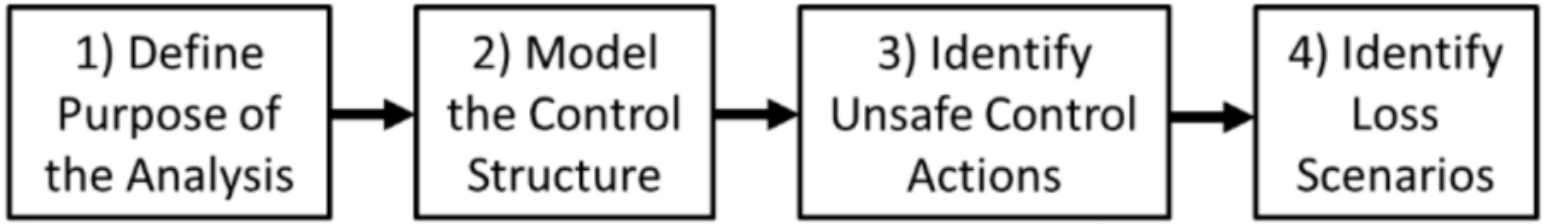
https://archive.knoxnews.com/news/local/plowshares-protesters-release-photos-of-y-12-break-in-ep-359812444-356536231.html/

- Current topics: Ukraine, Uvalde, etc. – All security risk events

Systems Theoretic Process Analysis Overview [1/2]



- What is it? → NOT RISK ANALYSIS, but safety and risk are related…
- Benefits?
  - Systematic approach
  - Combines concepts from systems and control theory (constraints, control, hierarchy)
  - Shifts thinking from "how X fails" to keeping system functionality in controlled space
  - Shown success in many domains – mainly in safety space



https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

- Utility for security
  - Using STPA to enhance previous security analysis techniques
  - For Vital Area Identification (VAI)
    - Can consider more than **radiological sabotage** as top event
    - Can consider things outside the DBT for future utility

STPA Overview [2/2]

- Limitations
  - Yields A LOT of output
  - Does not prioritize that output
  - Challenging to answer “what now?” question
- Implications for security applications
  - Security does not have 1E-6 threshold
  - All scenarios remain relevant
    - If within the Design Basis Threat (DBT)
  - $$$ limitations – infrastructure, personnel, supplies, etc.

Need for an opportunity for new thinking

- VAI: potential element of security to offer a chance to manage STPA results meaningfully

Vital Area Identification (VAI) Overview [1/2]

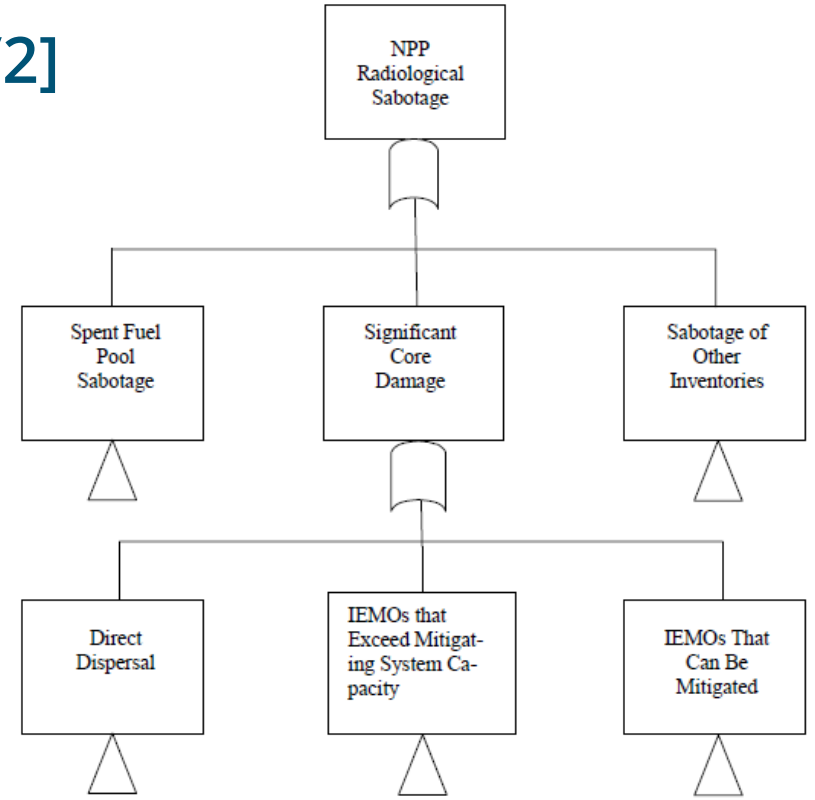
- *"Where do I need to keep the bad guys out of in order to prevent sabotage?"*
  - Minimize places, people (guards), infrastructure required to achieve objective
- A first attempt at bounding/identifying security risk
- Security risk thinking lags safety risk thinking
  - Efficiencies gained from "converting" safety analysis?
- Criticisms of traditional approaches to VAI…
  - Considers only **radiological** sabotage = only preventing release matters

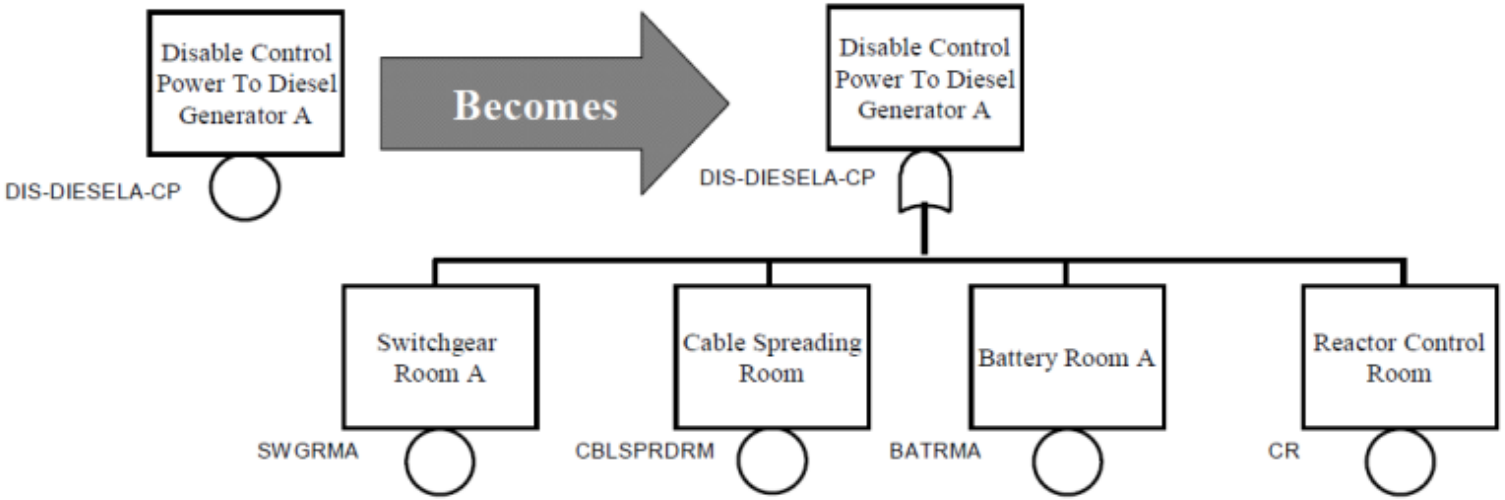
NO! Want to keep equipment working, keep making money, keep our reputation, etc.

- Y-12 – didn't reach the vital areas. Still had consequences.
- Surry attack on fresh fuel – not mandated vital area. Still had consequences.

Vital Area Identification (VAI) Overview [2/2]

- Methodology in practice is modified Fault Tree Analysis (FTA)
- Logic of Fault Trees (FTs) → top-down identification of all possible combinations leading to top event
- Even without including probabilities into the FTs, quantitative analysis an be used to categorize and prioritize results/solutions





Proposed Approach

VAI "converts" FT from basic component-level events to areas

STPA good at identifying areas/items of concern missed by traditional approaches

...so

Integrating STPA into VAI methods could be beneficial.

HAZCADS has shown STPA is compatible with FTA in meaningful ways in safety/DI&C space.

How would it work?

0) Define Adversary Types & Motivations

1) Define Purpose of the Analysis → 2) Model the Control Structure → 3) Identify Unsafe Control Actions → 4) ~~[illegible]~~

Build FT for each UCA. UCA serves as top event.

Basic events ➔ basic areas

Rank "basic areas" based on frequency of appearance

Most frequently appearing basic areas suggest higher priority of protection as vital area

How would it work?

End of STPA Step 3 yields Undesired Control Action (UCA) list

Example is from HARI (Hypothetical pool-type research reactor):

CA	Needed, not provided	Provided, not needed	Taken too early/late / wrong order	Given too long/Stopped too soon
CA1: water injected into pool	UCA1A: Operator did not inject water into pool when water was needed [H#]			

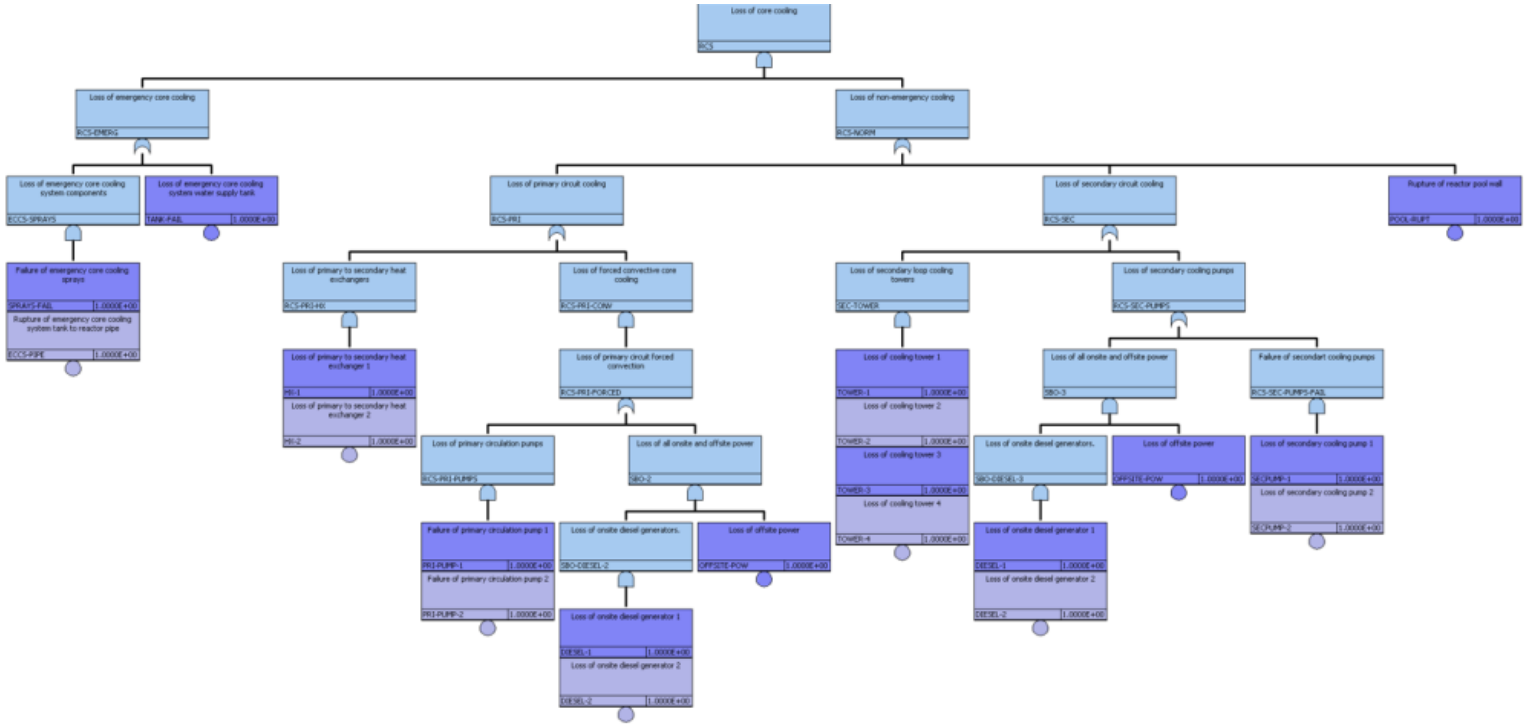
Note: only a sample UCA is included and carried forward from this table.

UCA1A: water not injected when needed

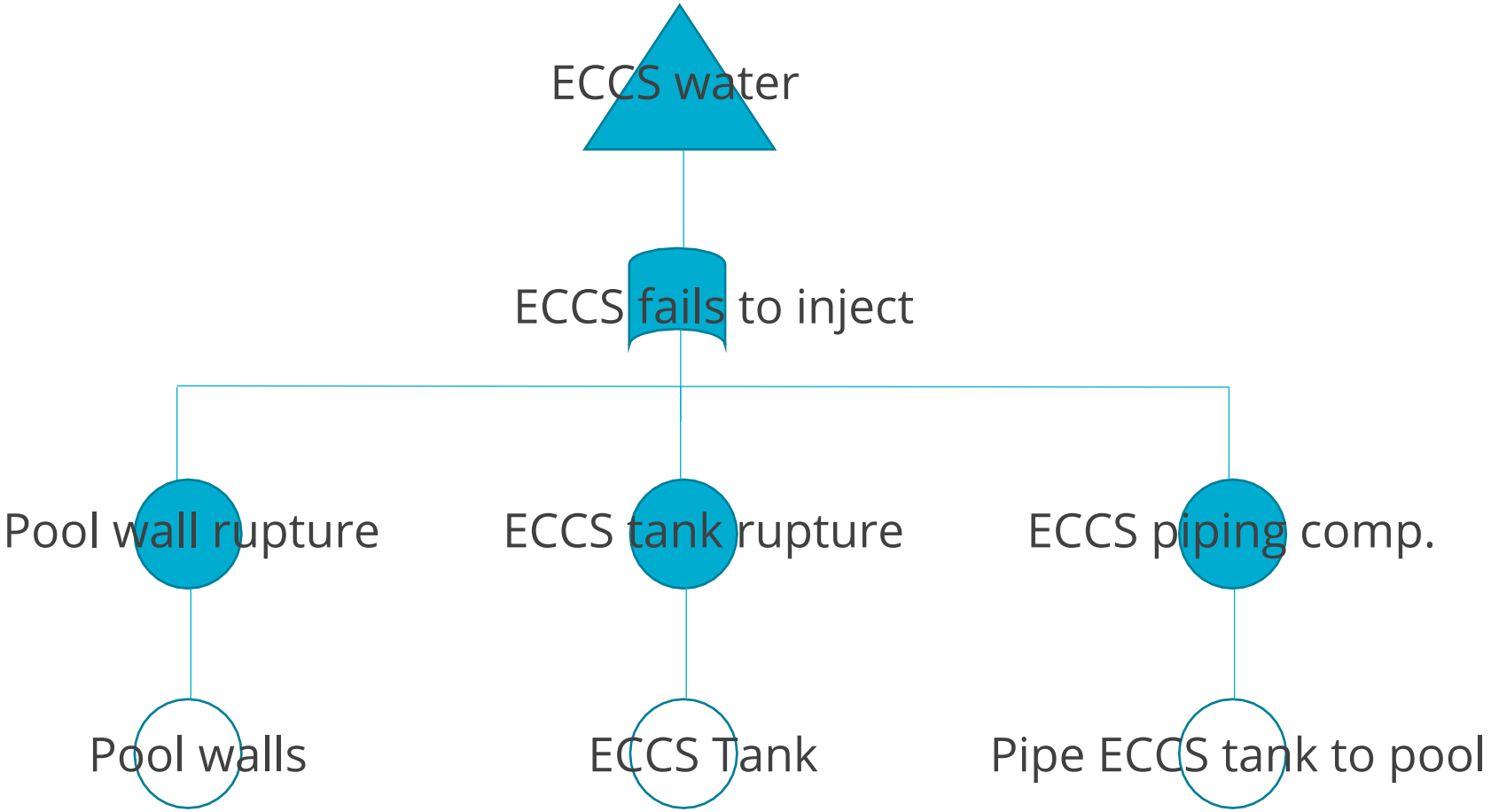
Consider:

- Lack of water
  - Various sources
- Piping compromised
  - Various systems
- Pumps non-functional
  - Various systems/trains
- Signal to inject compromised
- Operator error

Etc.



Sample FT Leg Conversion



Outcomes

Generate a frequency table:

(demonstrative table)

Area	Frequency
Pool wall (rupture)	5
ECCS piping	1
Primary pumps (co-located)	2
Cooling towers/heat sink	3
Secondary pumps (co-located)	2
Cabling from CR to pumps (co-located)	3

Based on this modified, hypothetical example:

Suggested VAs may be:

- Pool wall
- Cooling towers
- Cabling from CR

Next steps,

Implement these as VA and re-analyze.

Does having these as VAs reduce # of UCAs?

What can I take away from this method?

	Analytical	Practical
Insights	• Can get VA candidates without using safety PRAs (A/SMR friendly) • Continued practicality of STPA in security AND STPA used in conjunction with other methods (FTA)	• Lends itself to planning (think A/SMRs) situations • Demonstrates prioritization without probabilities
Implications	• Using frequency of appearance as criterion for prioritization implies other characteristics not relevant	• May require iterations on front end • Need analysts who understand traditional VAI and STPA methods
Potential Benefits	• Appearance frequency as a proxy for importance, a quantitative measure of priority WITHOUT having to use probabilities • Overcome barrier of NOT having a complete safety PRA	• Can inform security (and facility) design in near real time • Risk-informing without challenges of uncertainty quantification and matriculation • Opportunity for physical security system design that moves away from costly retrofitting and prioritizing critical components for this protection

Conclusions

Conclusions

- Probability free, yet provides prioritization
- Does not rely on PRA assumptions
- Does not rely directly on DBT
- Great for next generation of nuclear still in planning process

Potential Next Steps

- Potential for a hybrid method of this with *x* being frequency and *y* being consequence measure to determine importance.