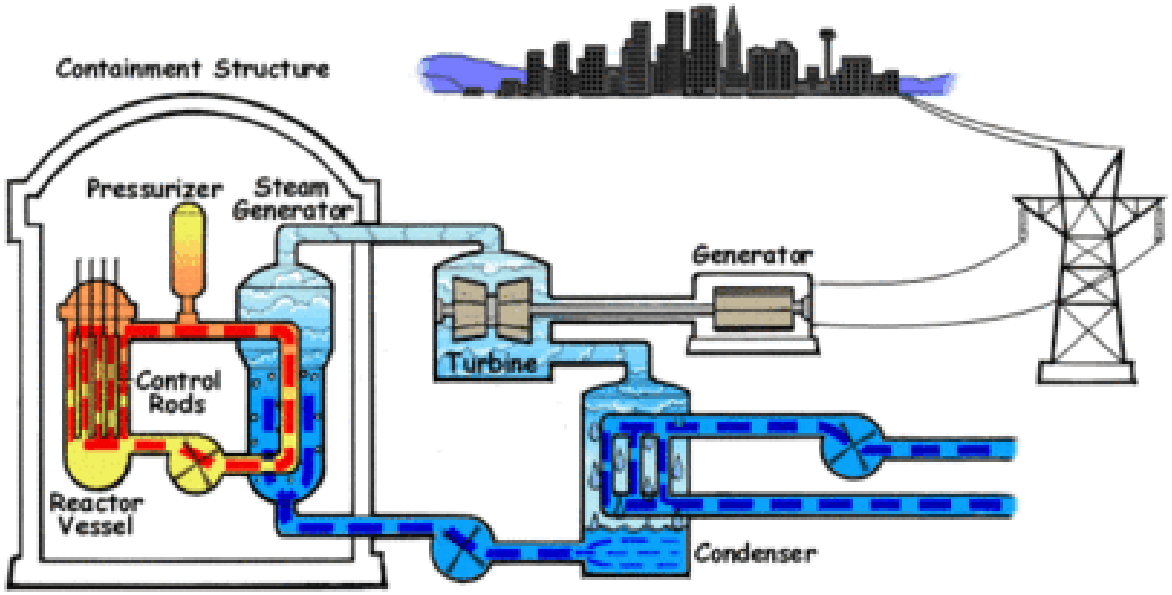
Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants

John Thomas

With many thanks to Francisco Lemos for the nuclear expertise provided!

System Studied: Generic Evolutionary Power Reactor

- Fully digital
  - All control systems including RPS are digital
- Case study focused on MSIV closure



* Image from Wikipedia

STPA Process

- Identify system-level accidents
- Identify system-level hazards
- Draw the control structure
- Identify Unsafe Control Actions (UCAs)
- Create corresponding safety constraints
- Identify causal factors
  - Process model flaws
  - Analyze controller, control path, feedback path, process

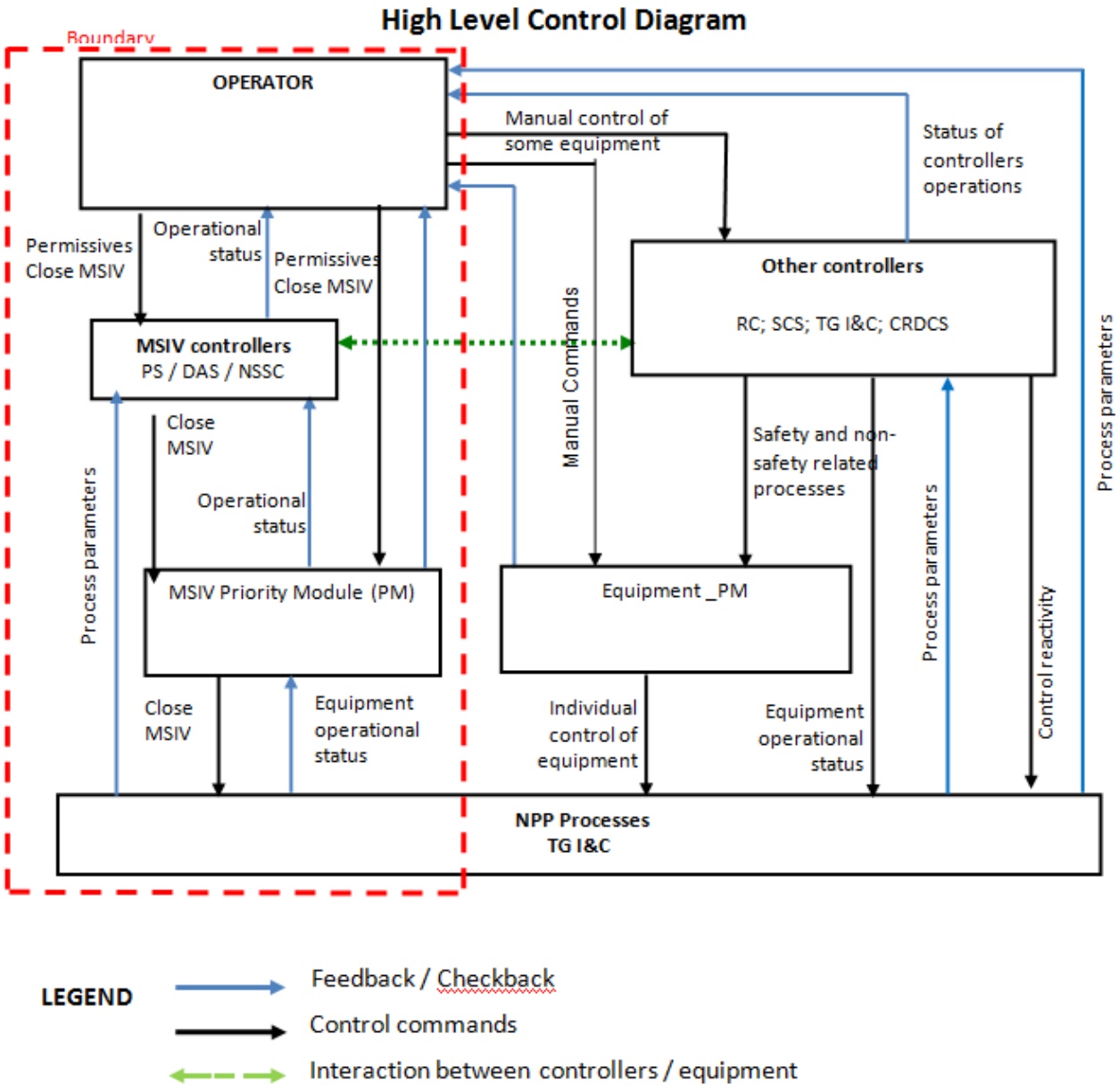
System-level Accidents

- A-1: People injured or killed
  - Includes employees and general population
  - May involve radiation exposure, explosion, etc.
- A-2: Environment contaminated
  - Includes radioactive material or other harmful release
  - Includes contamination to air, ground, groundwater, etc.
- A-3: Equipment damage (economic loss)
  - May occur with or without radiation release
- A-4: Loss of electrical power generation
  - Includes any unplanned plant shutdown

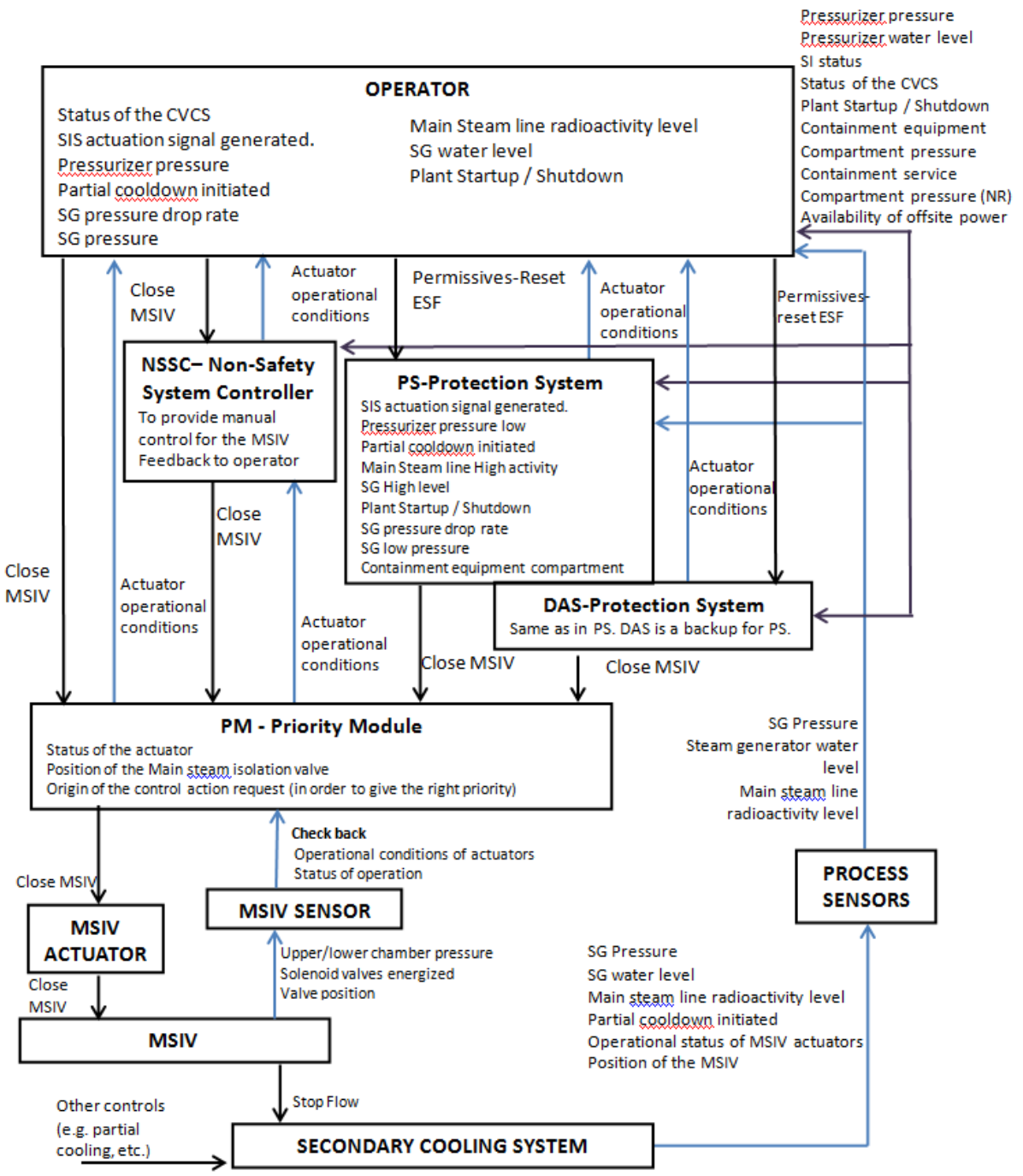
System-level Hazards

- H-1: Release of radioactive materials
  - Includes any release outside primary system (e.g. releases into secondary cooling system, groundwater, air inside or outside containment structures, etc.)
- H-2: Reactor temperature too high
  - Includes conditions that cause every accident (e.g. if fuel rods melt), or cause accidents without any radiation release (e.g. hydrogen production)
  - Makes no assumption about behavior of other protective systems (e.g. containment)
- H-3: Equipment operated beyond limits
  - Includes operation beyond safe limits that can cause reactor damage or operation beyond design limits that damages other equipment
- H-4: Reactor shut down
  - Includes any unplanned shutdown that may result in a loss of electrical power generation

Safety Control Structure



More Detailed Control Structure

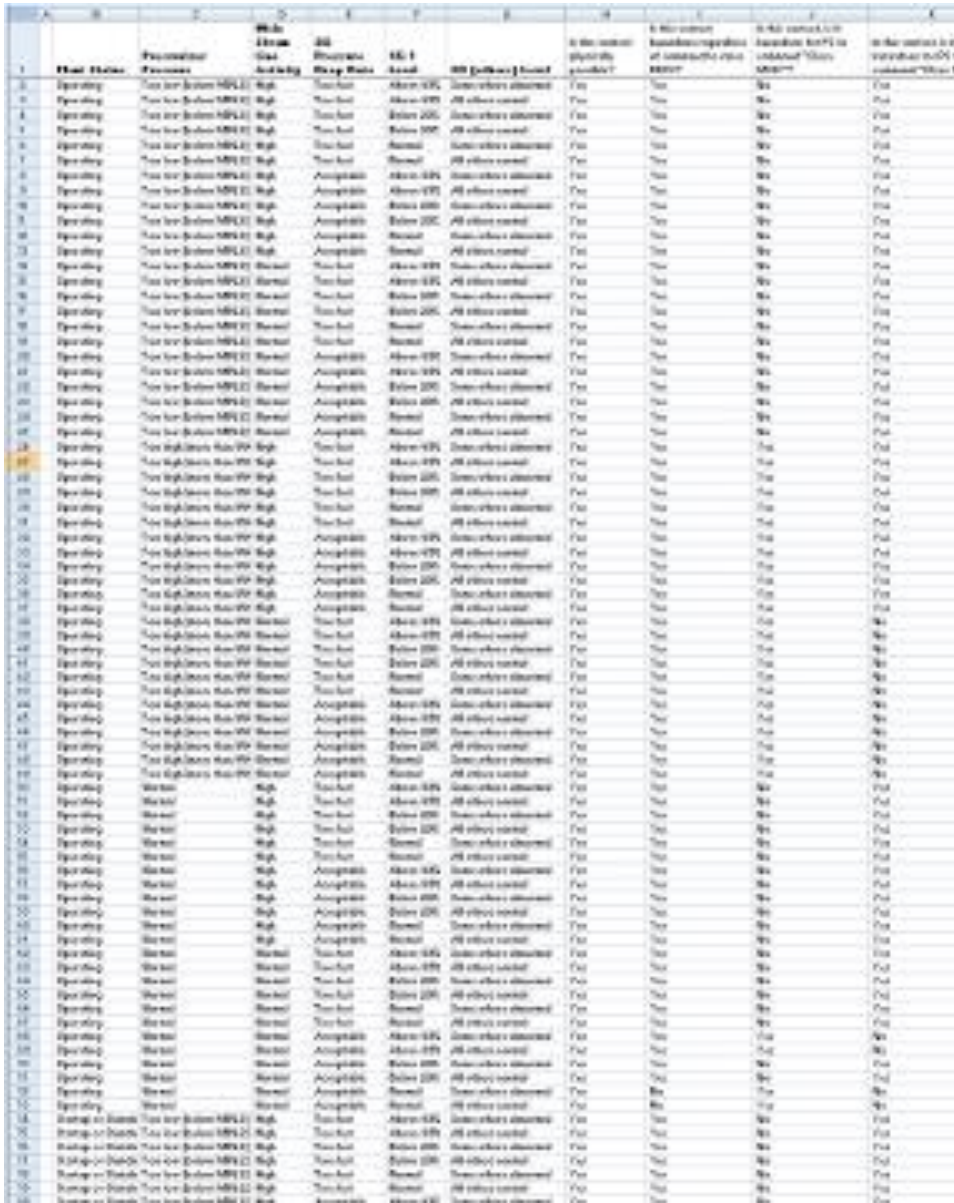


Brute-force approach

- Produced gigantic tables
- Embraced by some, but others found it hard to define, understand, and review

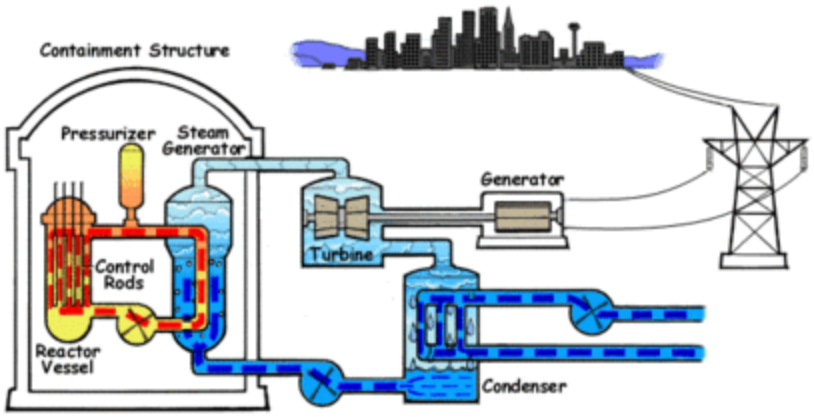
- Went back to basics
  - STPA is a top-down method
  - Really need to start at high level, add detail through refinement

- How can we start with simpler analysis, then add more detail in a way that is easy to define, understand, and review?



Identify Unsafe Control Actions

- What are the high-level process model variables?
- MSIV remains open during normal plant operation
- MSIV only used to control a few specific abnormal conditions:
  - **Steam generator tube rupture**
    - Can cause uncontrolled SG level increase, release contaminated fluid into secondary system
  - **Steam system piping failure**
    - Can depressurize SG, cause overcooling transient and energy release into containment
  - **Feedwater system piping failure**
    - Can depressurize SG, cause overcooling transient and energy release into containment
- MSIV also controls heat exchange within SG
  - **Other support systems** must be engaged to provide additional cooling if closed



Context table for *Close MSIV* control action not provided

- Template automatically generated from control structure and process model
- To identify the UCAs, engineers fill in the last column

	1	2	3	4	5	6
	Control Action	**Condition of Steam Generator Tube**	**Condition of Main Feedwater Pipe**	**Condition of Main Steamline**	**Operation of other support systems**	**Not Providing Control Action is Hazardous?**
1	*Close MSIV*	Not Ruptured	Not Ruptured	Not Ruptured	Adequate	
2		Ruptured	Not Ruptured	Not Ruptured	Adequate	
3		Not Ruptured	Ruptured	Not Ruptured	Adequate	
4		Not Ruptured	Not Ruptured	Ruptured	Adequate	
5		Ruptured	Ruptured	Not Ruptured	Adequate	
6		Not Ruptured	Ruptured	Ruptured	Adequate	
7		Ruptured	Not Ruptured	Ruptured	Adequate	
8		Ruptured	Ruptured	Ruptured	Adequate	
9		Not Ruptured	Not Ruptured	Not Ruptured	Adequate	
10		Ruptured	Not Ruptured	Not Ruptured	Inadequate	
11		Not Ruptured	Ruptured	Not Ruptured	Inadequate	
12		Not Ruptured	Not Ruptured	Ruptured	Inadequate	
13		Ruptured	Ruptured	Not Ruptured	Inadequate	
14		Not Ruptured	Ruptured	Ruptured	Inadequate	
15		Ruptured	Not Ruptured	Ruptured	Inadequate	
16		Ruptured	Ruptured	Ruptured	Inadequate	

Context table for *Close MSIV* control action not provided

- Keeping MSIV open is not hazardous if no rupture (row 1, 9)
- If MSIV kept open during SGTR, will cause all hazards
- If kept open, causes H-2, H-3 during steamline or feedwater rupture

Tools can automatically populate table using these 3 rules

	1	2	3	4	5	6
	Control Action	**Condition of Steam Generator Tube**	**Condition of Main Feedwater Pipe**	**Condition of Main Steamline**	**Operation of other support systems**	**Not Providing Control Action is Hazardous?**
1	*Close MSIV*	Not Ruptured	Not Ruptured	Not Ruptured	Adequate	No
2		Ruptured	Not Ruptured	Not Ruptured	Adequate	H-1, H-2, H-3, H-4
3		Not Ruptured	Ruptured	Not Ruptured	Adequate	H-2, H-3
4		Not Ruptured	Not Ruptured	Ruptured	Adequate	H-2, H-3
5		Ruptured	Ruptured	Not Ruptured	Adequate	H-1, H-2, H-3, H-4
6		Not Ruptured	Ruptured	Ruptured	Adequate	H-2, H-3
7		Ruptured	Not Ruptured	Ruptured	Adequate	H-1, H-2, H-3, H-4
8		Ruptured	Ruptured	Ruptured	Adequate	H-1, H-2, H-3, H-4
9		Not Ruptured	Not Ruptured	Not Ruptured	Adequate	No
10		Ruptured	Not Ruptured	Not Ruptured	Inadequate	H-1, H-2, H-3, H-4
11		Not Ruptured	Ruptured	Not Ruptured	Inadequate	H-2, H-3
12		Not Ruptured	Not Ruptured	Ruptured	Inadequate	H-2, H-3
13		Ruptured	Ruptured	Not Ruptured	Inadequate	H-1, H-2, H-3, H-4
14		Not Ruptured	Ruptured	Ruptured	Inadequate	H-2, H-3
15		Ruptured	Not Ruptured	Ruptured	Inadequate	H-1, H-2, H-3, H-4
16		Ruptured	Ruptured	Ruptured	Inadequate	H-1, H-2, H-3, H-4

Context table for *Close MSIV* control action

	1	2	3	4	5	6	7	8
	Control Action	**Condition of Steam Generator Tube**	**Condition of Main Feedwater Pipe**	**Condition of Main Steamline**	**Operation of other support systems**	**Control Action Hazardous?**	**Control Action Hazardous if Too Late?**	**Control Action Hazardous if Too Early?**
1	*Close MSIV*	Not Ruptured	Not Ruptured	Not Ruptured	Adequate	H-4	H-4	H-4
2		Ruptured	Not Ruptured	Not Ruptured	Adequate	No	H-1, H-2, H-3, H-4	H-3, H-4
3		Not Ruptured	Ruptured	Not Ruptured	Adequate	No	H-2, H-3, H-4	No
4		Not Ruptured	Not Ruptured	Ruptured	Adequate	No	H-2, H-3, H-4	No
5		Ruptured	Ruptured	Not Ruptured	Adequate	No	H-1, H-2, H-3, H-4	H-3, H-4
6		Not Ruptured	Ruptured	Ruptured	Adequate	No	H-2, H-3, H-4	No
7		Ruptured	Not Ruptured	Ruptured	Adequate	No	H-1, H-2, H-3, H-4	H-3, H-4
8		Ruptured	Ruptured	Ruptured	Adequate	No	H-1, H-2, H-3, H-4	H-3, H-4
9		Not Ruptured	Not Ruptured	Not Ruptured	Inadequate	H-2, H-4	H-2, H-4	H-2, H-4
10		Ruptured	Not Ruptured	Not Ruptured	Inadequate	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
11		Not Ruptured	Ruptured	Not Ruptured	Inadequate	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
12		Not Ruptured	Not Ruptured	Ruptured	Inadequate	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
13		Ruptured	Ruptured	Not Ruptured	Inadequate	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
14		Not Ruptured	Ruptured	Ruptured	Inadequate	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
15		Ruptured	Not Ruptured	Ruptured	Inadequate	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
16		Ruptured	Ruptured	Ruptured	Inadequate	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4

Simplified context table for *Close MSIV* control action provided

	1	2	3	4	5	6	7	8
	Control Action	**Condition of Steam Generator Tube**	**Condition of Main Feedwater Pipe**	**Condition of Main Steamline**	**Operation of other support systems**	**Control Action Hazardous?**	**Control Action Hazardous if Too Late?**	**Control Action Hazardous if Too Early?**
1	*Close MSIV*	Not Ruptured	Not Ruptured	Not Ruptured	Adequate	**Yes**	**Yes**	**Yes**
2		Ruptured	*	*	Adequate	No	**Yes**	**Yes**
3		Not Ruptured	Ruptured	Not Ruptured	Adequate	No	**Yes**	No
4		Not Ruptured	Not Ruptured	Ruptured	Adequate	No	**Yes**	No
5		Not Ruptured	Ruptured	Ruptured	Adequate	No	**Yes**	No
6		*	*	*	Inadequate	**Yes**	**Yes**	**Yes**

*** means "doesn't matter"**
Helps to simplify the table

Summary of UCAs identified

Control Action	Unsafe Control Actions			
	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order Causes Hazard	Stopped Too Soon or Applied Too Long
Close MSIV	Close MSIV not provided when there is a rupture in the S/G tube, main feedwater, or main steam line and the support systems are adequate [H-2, H-1, H-3]	Close MSIV provided when there is a rupture and other support systems are inadequate [H-1, H-2, H-3] Close MSIV provided when there is no rupture [H-4]	Close MSIV provided too early (while SG pressure is high): SG pressure may rise, trigger relief valve, abrupt steam expansion [H-2, H-3] Close MSIV provided too late after SGTR: contaminated coolant released into secondary loop, loss of primary coolant through secondary system [H-1, H-2, H-3]	N/A

Conflicts automatically detected

- Rows 10-16
  - Context: rupture is present but other support systems are not operating or inadequate
  - Hazardous to keep MSIV open
    - May contaminate secondary system, cause overcooling transient, etc.
  - Hazardous to close MSIV
    - Isolates the only operational cooling system
  - Conflict should be addressed. For example, best to keep MSIV open depending on type of rupture to provide limited cooling until operators find a solution?

Automatically generated model-based requirements

Provide 'Close MSIV valve' command

Steam Generator Tube =	Not Ruptured
	Ruptured
Condition of Main Feedwater Pipe =	Not Ruptured
	Ruptured
Condition of Main Steamline =	Not Ruptured
	Ruptured
Operation of other support systems =	Adequate
	Inadequate

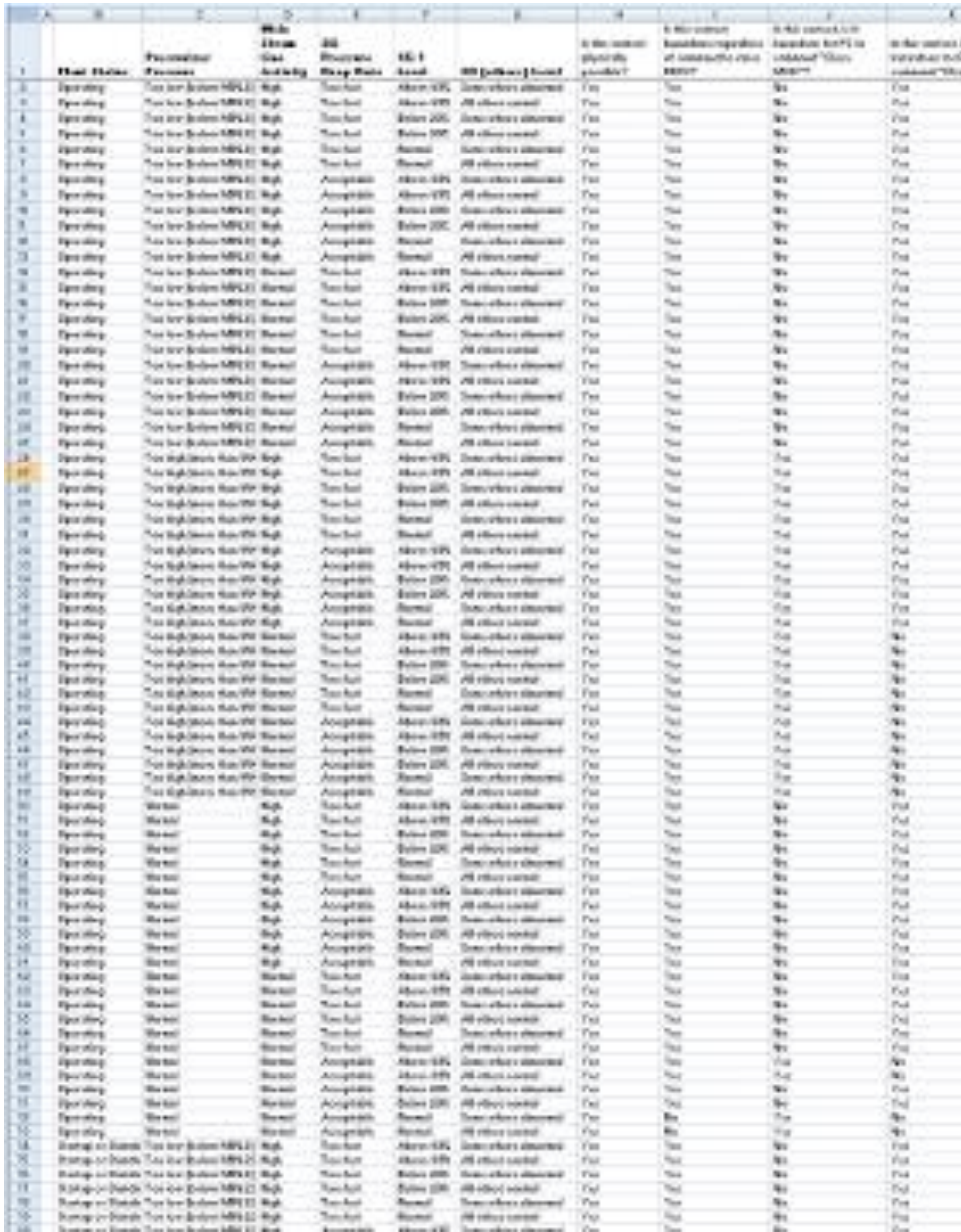
T	T	T	F	F	F	F	T	T	T	F	F	F
F	F	F	T	T	T	T	F	F	F	T	T	T
T	F	F	T	T	F	F	T	F	F	T	F	F
F	T	T	F	F	T	T	F	T	T	F	T	T
F	T	F	T	F	T	F	F	T	F	F	T	F
T	F	T	F	T	F	T	T	F	T	T	F	T
T	T	T	T	T	T	T	F	F	F	F	F	F
F	F	F	F	F	F	F	T	T	T	T	T	T

Derived from H-2, H-3
Derived from H-2, H-3
Derived from H-2, H-3
Derived from H-1, H-2, H-3, H-4
Derived from H-1, H-2, H-3, H-4
Derived from H-1, H-2, H-3, H-4
Derived from H-1, H-2, H-3, H-4
Derived from H-2, H-3
Derived from H-2, H-3
Derived from H-2, H-3
Derived from H-1, H-2, H-3, H-4
Derived from H-1, H-2, H-3, H-4
Derived from H-1, H-2, H-3, H-4

Traceability can also be provided from info in context tables

Including more detail with refinement

- What about these gigantic tables?
  - At the end of the day, this information needs to be defined
  - May not have to manually fill out large tables to define it
- STPA is a top-down method
  - Really need to start at high level, add detail through refinement
- How can we start with simpler analysis, then add more detail in a way that is easy to define, understand, and review?



Including more detail with refinement

- Solution:
  - Define how process model variables are inferred
  - Then automatically generate low-level requirements or tables

	1	2	3	4	5
	Control Action	**Condition of Steam Generator Tube**	**Condition of Main Feedwater Pipe**	**Condition of Main Steamline**	**Operation of other support systems**
	Close MSIV				

Condition of Steam Generator Tube inferred to be ...

		ruptured when:		***not ruptured*** when:
Radioactivity sensor =	Normal			T
	Radioactive	T		
Steam generator water level =	Too low			
	Normal			
	Too high		T	F

Condition of Main Feedwater Pipe inferred to be ...

		ruptured when:			***not ruptured*** when:
Steam generator pressure drop rate =	More than X	T			F
	Less than X				
Steam generator pressure =	More than Y				
	Less than Y		T		F
Containment pressure =	More than Z			T	F
	Less than Z				

Condition of Main Steam Line inferred to be ...

		ruptured when:			***not ruptured*** when:
Steam generator pressure drop rate =	More than X	T			F
	Less than X				
Steam generator pressure =	More than Y				
	Less than Y		T		F
Containment pressure =	More than Z			T	F
	Less than Z				

Operation of other support systems inferred to be ...

		adequate when:			***not adequate*** when:
Safety injection system =	Operating	T			F
	Not operating				
Emergency feedwater system =	Operating		T		F
	Not operating				
Emergency cooling system =	Operating			T	F
	Not operating				

* Inference rules based on existing public documentation

Conclusions

- Provides structured way to generate low-level context tables from high-level information
- Top-down approach to identifying UCAs, helps manage complexity
- Provides rigorous process to analyze complex systems using STPA

Note:

- Project focus was on developing methods, not evaluating one particular design
- In practice, the results at each step should be carefully reviewed by nuclear experts