EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Systems Theoretic Process Analysis (STPA) Applied to a Nuclear Power Plant Control System

Ray Torok
rtorok@epri.com

Bruce Geddes
bgeddes@southern-engineering.net

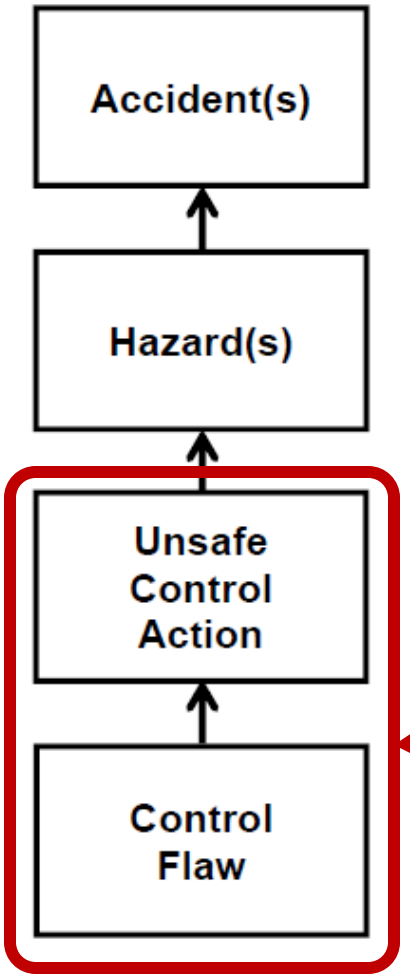
MIT STAMP Workshop
March 26-28, 2013

EPRI Project to Develop Guidance on Hazard Analysis of Digital I&C Systems

- Plants experiencing unexpected/undesired behaviors
  - Failure modes missed or misunderstood
  - Bad things can happen in complex systems, even when all components behave as designed (i.e., no failures)
  - Traditional failure analysis methods are limited; typically look for single failures and their effects on the plant
- Project seeks more effective methods. Looked at:
  - FMEA (Functional or Design Failure Modes & Effects Analysis)
  - FTA (Fault Tree Analysis)
  - HAZOP (Hazard and Operability Analysis)
  - STPA (Systems Theoretic Process Analysis)
  - PGA (Purpose Graph Analysis)

Need approach that is practical and effective for nuclear plants

STPA Overview



An undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environment pollution, and so on). (Reference 19)

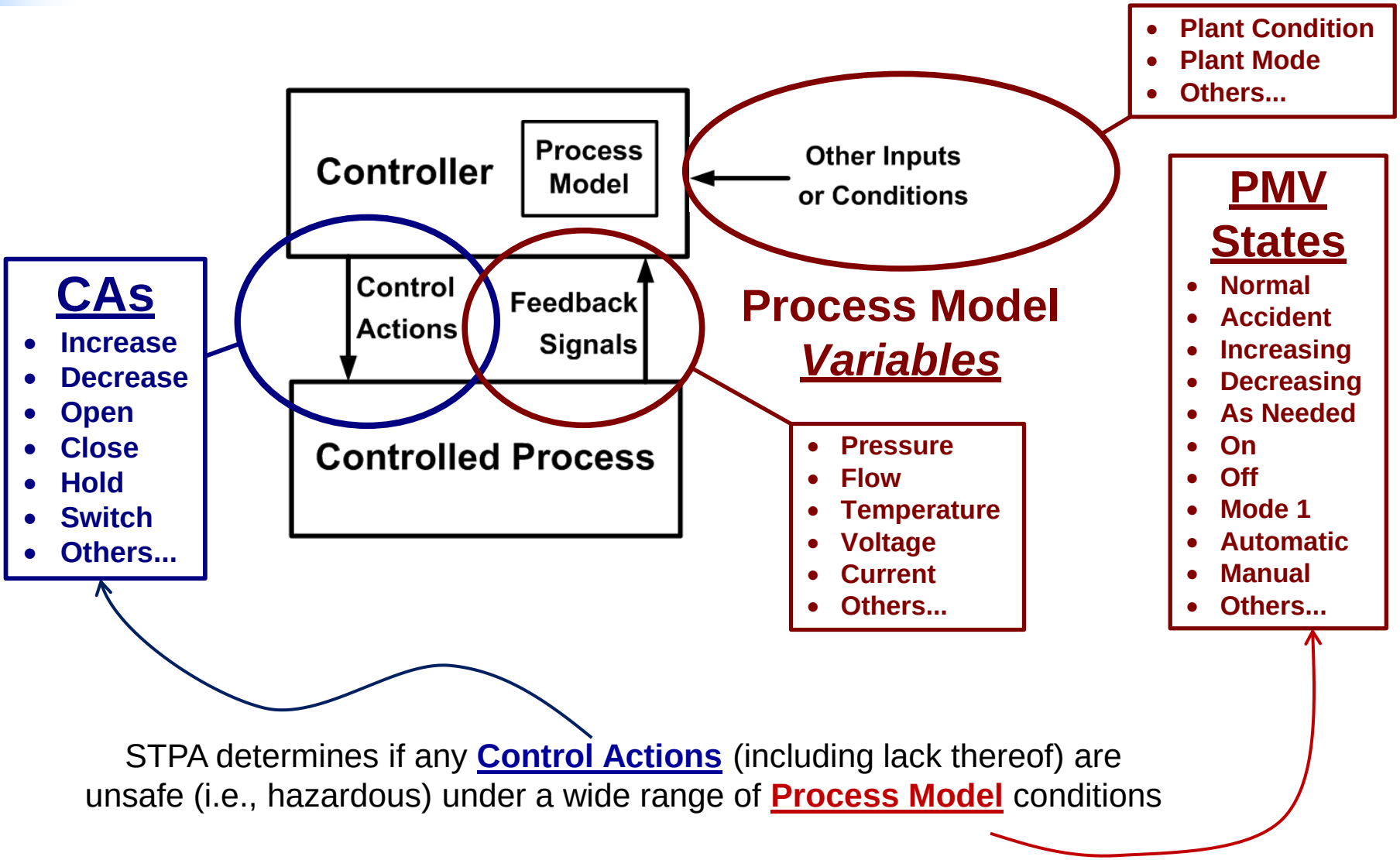
A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss). (Reference 19)

A controller command that violates a safety constraint.

STPA systematically reveals the presence of Control Flaws and the potential for Unsafe Control Actions

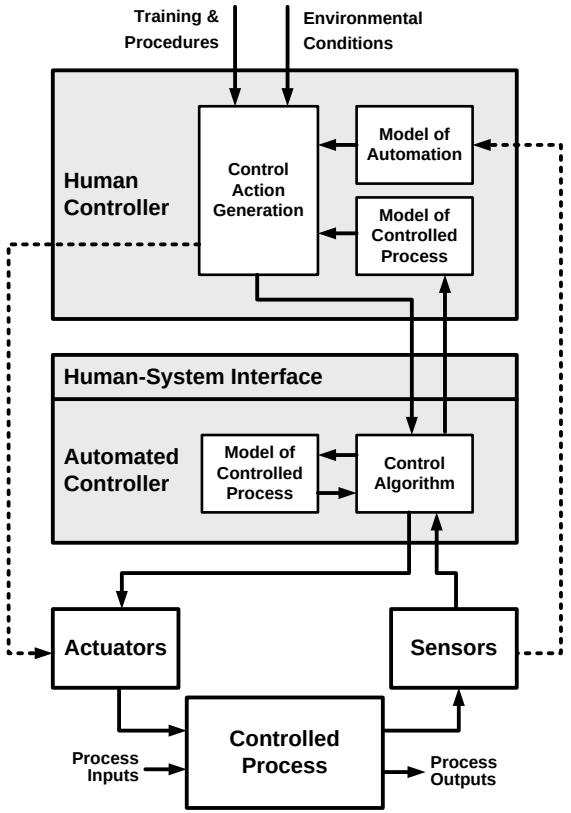
See Figure 5-1

Control Actions in the Context of the Process Model



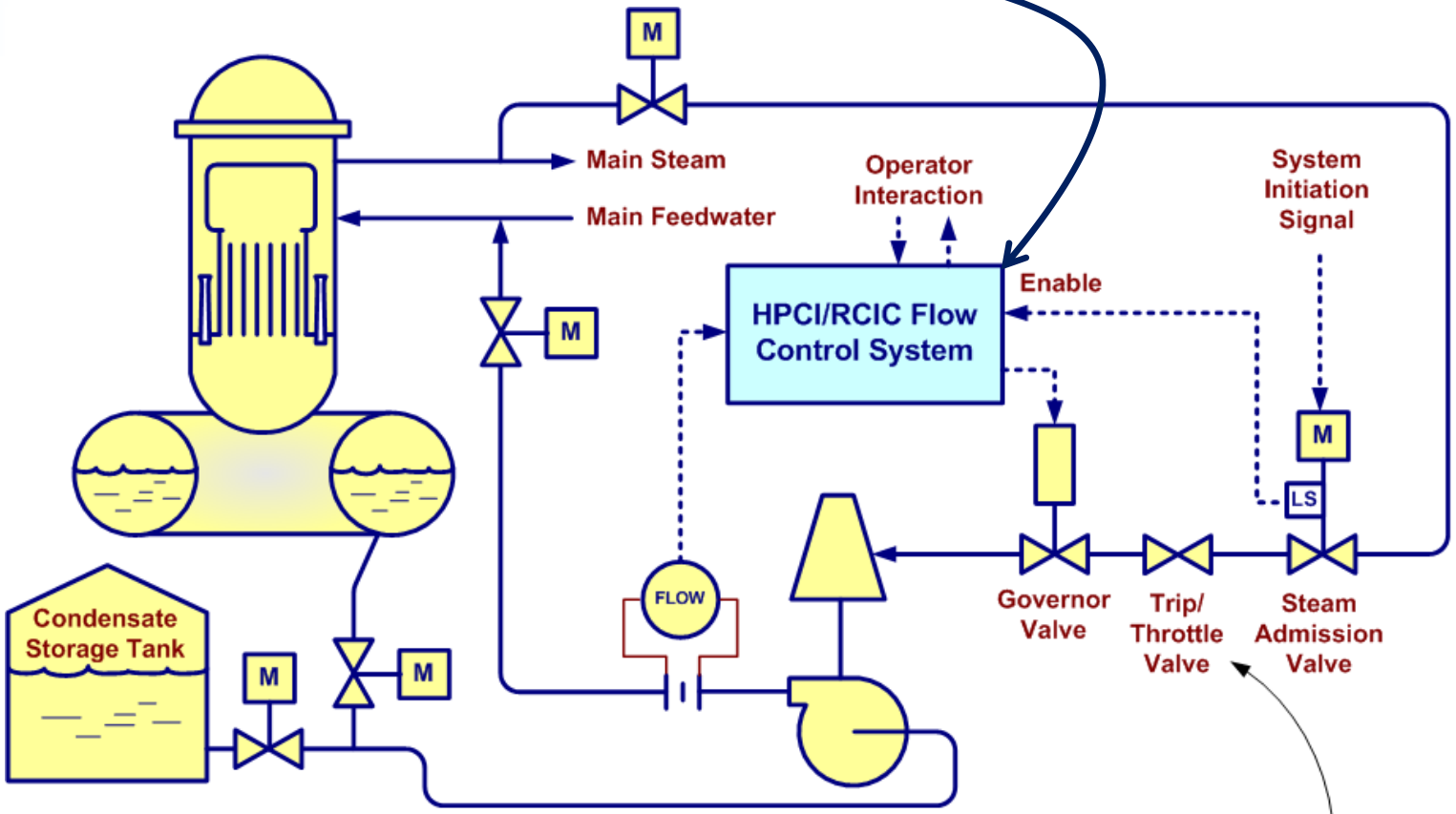
STPA determines if any **Control Actions** (including lack thereof) are unsafe (i.e., hazardous) under a wide range of **Process Model** conditions

STPA Procedure



1. Identify System Boundary
2. Identify Accidents (Losses)
3. Identify System-Level Hazards
4. Draw the Control Structure
5. Create the Process Model
   a) List Process Model Variables
6. Identify Hazardous Control Actions
   a) Identify Control Actions
   b) Postulate Control Action Behaviors:
      - Control Action is Provided, Not Provided, Provided Too Soon, Provided Too Late, or Stopped Too Soon
   c) Determine if Control Action Behaviors are Hazardous in various contexts expressed by the Process Model Variables
7. Identify Potential Causes of Hazardous Control Actions
8. Remove or Mitigate Hazards

Step 1: HPCI Flow Control System

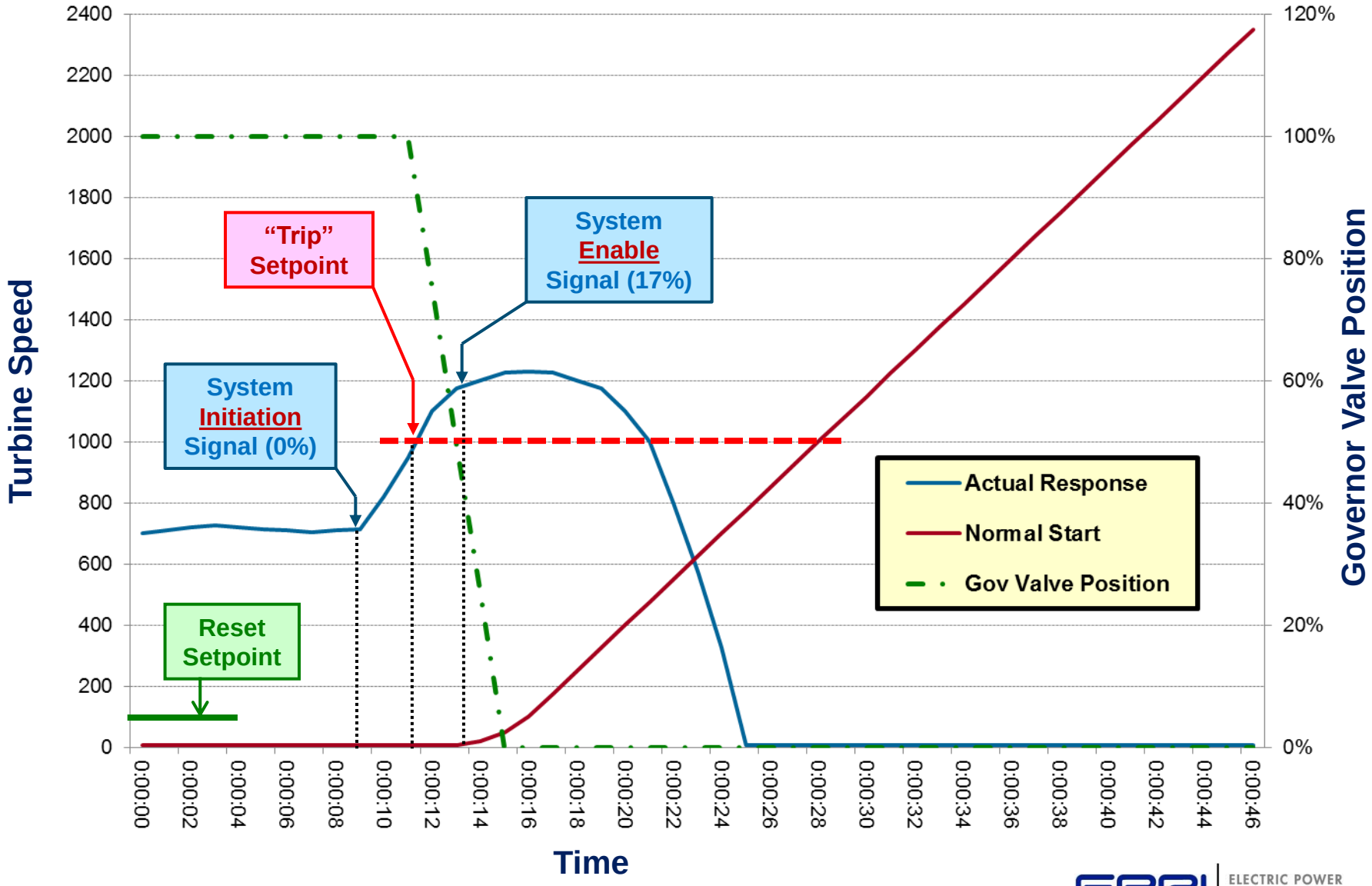


System Initiation Signals
(Open Steam Admission Valve & Process Valves)
1. Low Reactor Level (-48")
2. High Drywell Pressure (HPCI only; +2 psig)

System Isolation Signals
(Trip Turbine & Close Process Valves)
1. High Steam Line Flow
2. High Area Temperature
3. Low Steam Line Pressure (HPCI only)
4. Low Reactor Pressure (RCIC only)
5. Manual

Turbine Trip Signals
(Close Trip/Throttle Valve)
1. Any system isolation signal
2. High Steam Exhaust Pressure (150 psi)
3. High Reactor Level (+46")
4. Low pump suction pressure (15" Hg)
5. Turbine overspeed
6. Manual (local or remote)

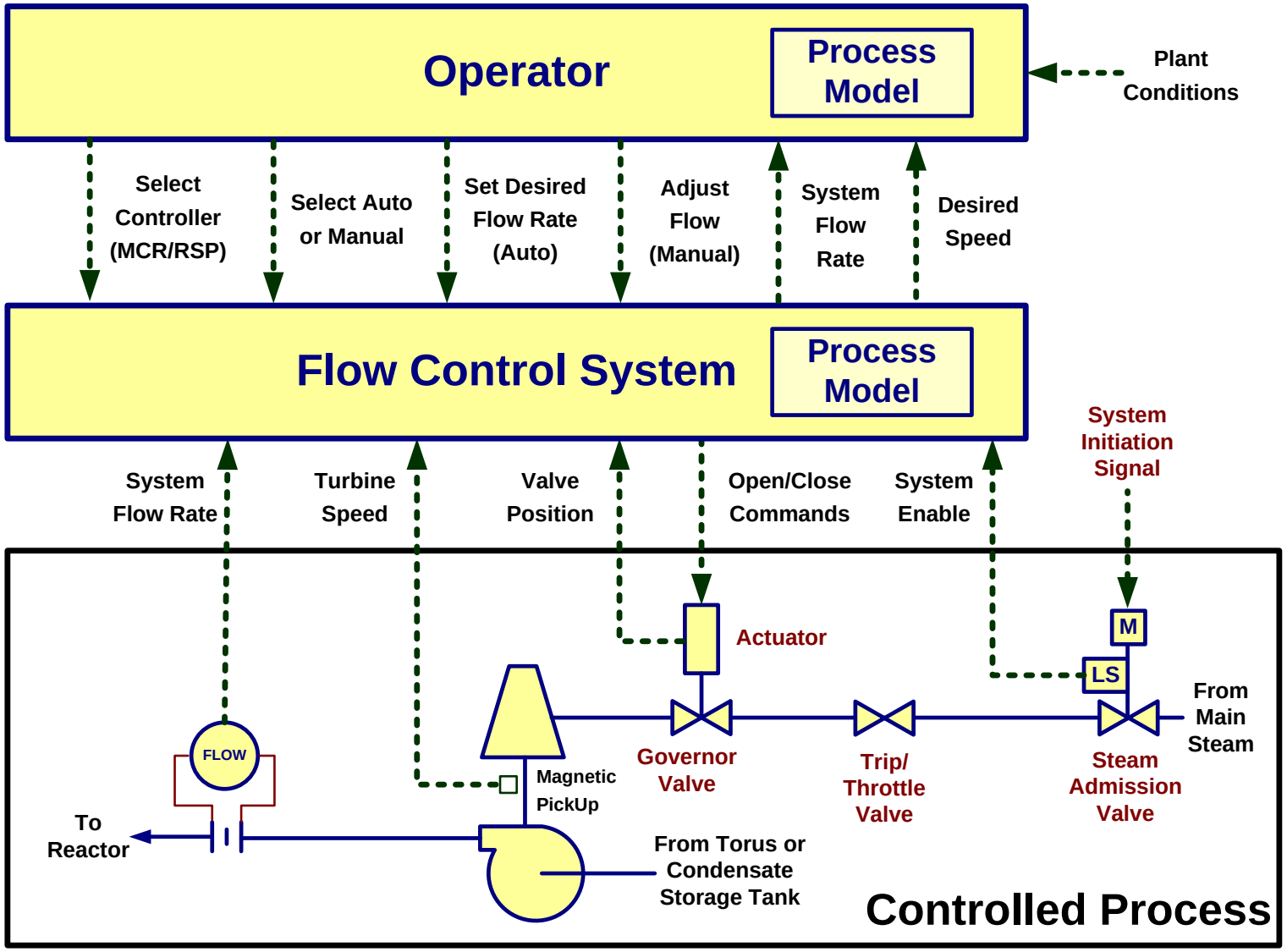
Operating Experience (No Component Failures)



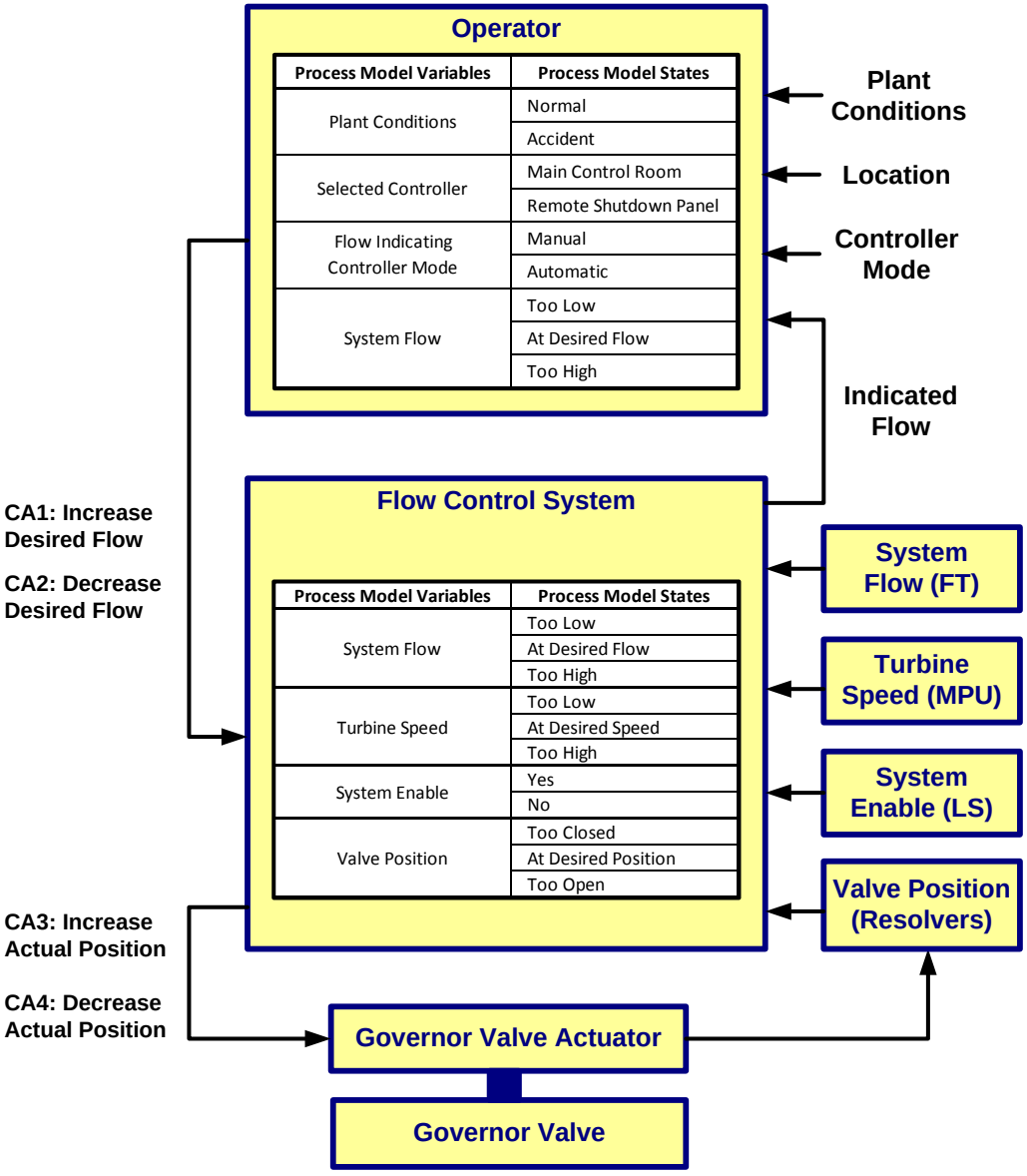
Steps 2 & 3: Identify Accidents & Hazards

		Accidents				
		A1	A2	A3	A4	A5
Hazards		Radiation Exposure	Contaminated Enviroment	Equipment Damage	Injury or Death	Lost Generation
H1	Reactor Exceeds Limits			X		X
H2	Radioactive Material Release	X	X			
H3	Equipment Operated Beyond Limits			X	X	
H4	Inadvertent Equip. Operation During Maintenance				X	
H5	Reactor Shutdown					X

Step 4: Draw Control Structure



Step 5: Develop Process Model



Step 5(a): List Process Model Variables (PMV)

Control Actions		Process Model Variables	Process Model States
CA3	Increase Valve Position	PMV1 Plant Conditions	Normal
			Accident
		PMV2 Valve Position	Too Closed
			As Needed
			Too Open
		PMV3 Turbine Speed	Too Low
			As Needed
			Too High
		PMV4 System Flow	Too Low
			As Needed
			Too High
		PMV5 System Enable	Yes
			No
CA4	Decrease Valve Position	PMV1 Plant Conditions	Normal
			Accident
		PMV2 Valve Position	Too Closed
			As Needed
			Too Open
		PMV3 Turbine Speed	Too Low
			As Needed
			Too High
		PMV4 System Flow	Too Low
			As Needed
			Too High
		PMV5 System Enable	Yes
			No

Postulated Control Action Behaviors

1. Control Action Is ***Provided***
2. Control Action Is ***Not Provided***
3. Control Action Is ***Provided Too Early***
4. Control Action Is ***Provided Too Late***
5. Control Action Is ***Stopped Too Soon***

Structure of a Hazardous Control Action (HCA):

Governor	**Provides**	**Increase Valve Position**	**when Turbine Speed is Too High**
Source	Behavior	Control Action	Context

Step 6: Identify Hazardous Control Actions (HCA)

Controller:	HPCI-RCIC Flow Control System		H1	Reactor Exceeds Limits
Control Action:	CA3	Increase Governor Valve Position	H2	Radioactive Release
			H3	Equipment Damage
Postulated Behavior:	Providing (the increase valve position command) (Is CA Behavior Hazardous?)		H4	Personnel Injury or Death
			H5	Reactor Shutdown

Row	Process Model Variables					Analysis Results			
	PMV1 Plant Conditions	PMV2 Valve Position	PMV3 Turbine Speed	PMV4 System Flow	PMV5 System Enable	Is Situation Already Hazardous?	Is CA Behavior Hazardous?	Related Hazards	Comments (Situational Context)
1	Accident	Too open	Too high	Too high	Yes	Yes	Yes	H3	Leads to Rx overfill
2					No	Yes	No Response	H1, H2	Accident and no enable
3				Too low	Yes	Yes	Maybe	H3	Increase flow, but overspeed?
4					No	Yes	No Response	H1, H2	Accident and no enable
5				As needed	Yes	No	Yes	H3	Leads to Rx overfill
6					No	Yes	No Response	H1, H2	Accident and no enable
7			Too low	Too high	Yes	Yes	Yes	H3	Leads to Rx overfill
8					No	Yes	No Response	H1, H2	Accident and no enable
9				Too low	Yes	Yes	Maybe	H3	Increase flow, but valve damage?
10					No	Yes	No Response	H1, H2	Accident and no enable
11				As needed	Yes	No	Yes	H3	Leads to Rx overfill
12					No	Yes	No Response	H1, H2	Accident and no enable
13				Too high	Yes	Yes	Yes	H3	Leads to Rx overfill
14					No	Yes	No Response	H1, H2	Accident and no enable

Step 6: Reduced List of Hazardous Control Actions

Hazardous Control Actions										Hazard
Flow control system <u>provides</u> increase governor valve position (CA3) when:										
1	there is an accident	and valve position is	*	and turbine speed is	*	and system flow is	*	and system enable is	No[1]	H1, H2
2	there is an accident	and valve position is	too open or as needed	and turbine speed is	too high or as needed	and system flow is	*	and system enable is	Yes	H3
3	there is an accident	and valve position is	too closed	and turbine speed is	too high or as needed	and system flow is	*	and system enable is	Yes	H3
4	there is an accident	and valve position is	too closed	and turbine speed is	too low	and system flow is	too high or as needed	and system enable is	Yes	H3
5	there is <u>not</u> an accident	and valve position is	*	and turbine speed is	too high	and system flow is	too high	and system enable is	Yes[2]	H1
6	there is <u>not</u> an accident	and valve position is	*	and turbine speed is	too high	and system flow is	*	and system enable is	No[3]	H3
Flow control system <u>does not provide</u> increase governor valve position (CA3) when:										
7	there is an accident	and valve position is	*	and turbine speed is	*	and system flow is	too low	and system enable is	*[4]	H1, H2

<u>Notes</u>

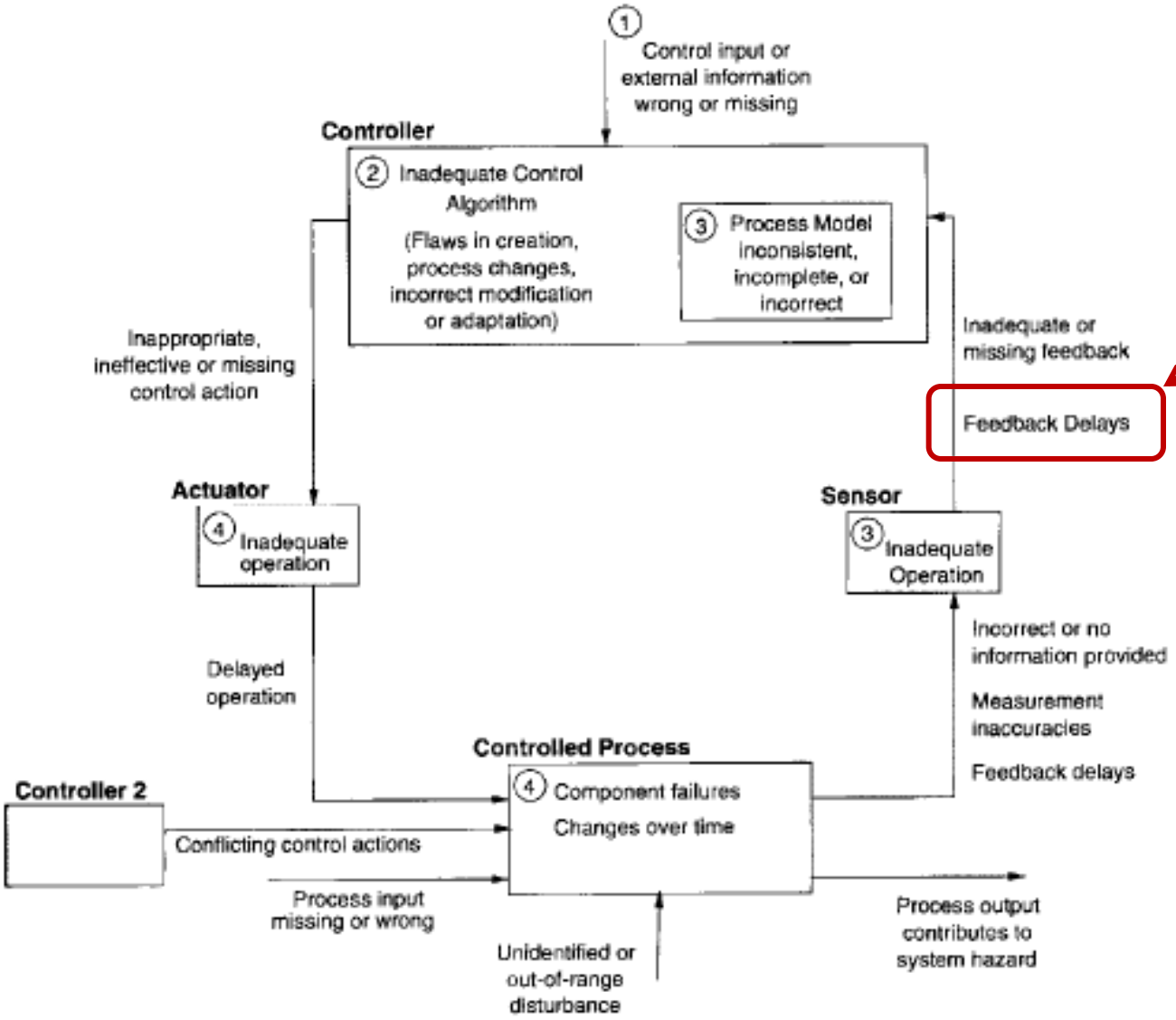
1. Flow control system does not respond at all when there is an accident and no system enable

2. Increasing the governor valve position (CA3) worsens the effect of a spurious system actuation

3. Might be a Hazardous Control Action if it causes turbine speed to reach a limit when turbine speed is already too high and there is no system enable (possible due to a leaky steam admission valve?)

4. System flow is too low during an accident, regardless of the states of the other process model variables, including the system enable signal

Control Flaws are Possible Causes of HCAs



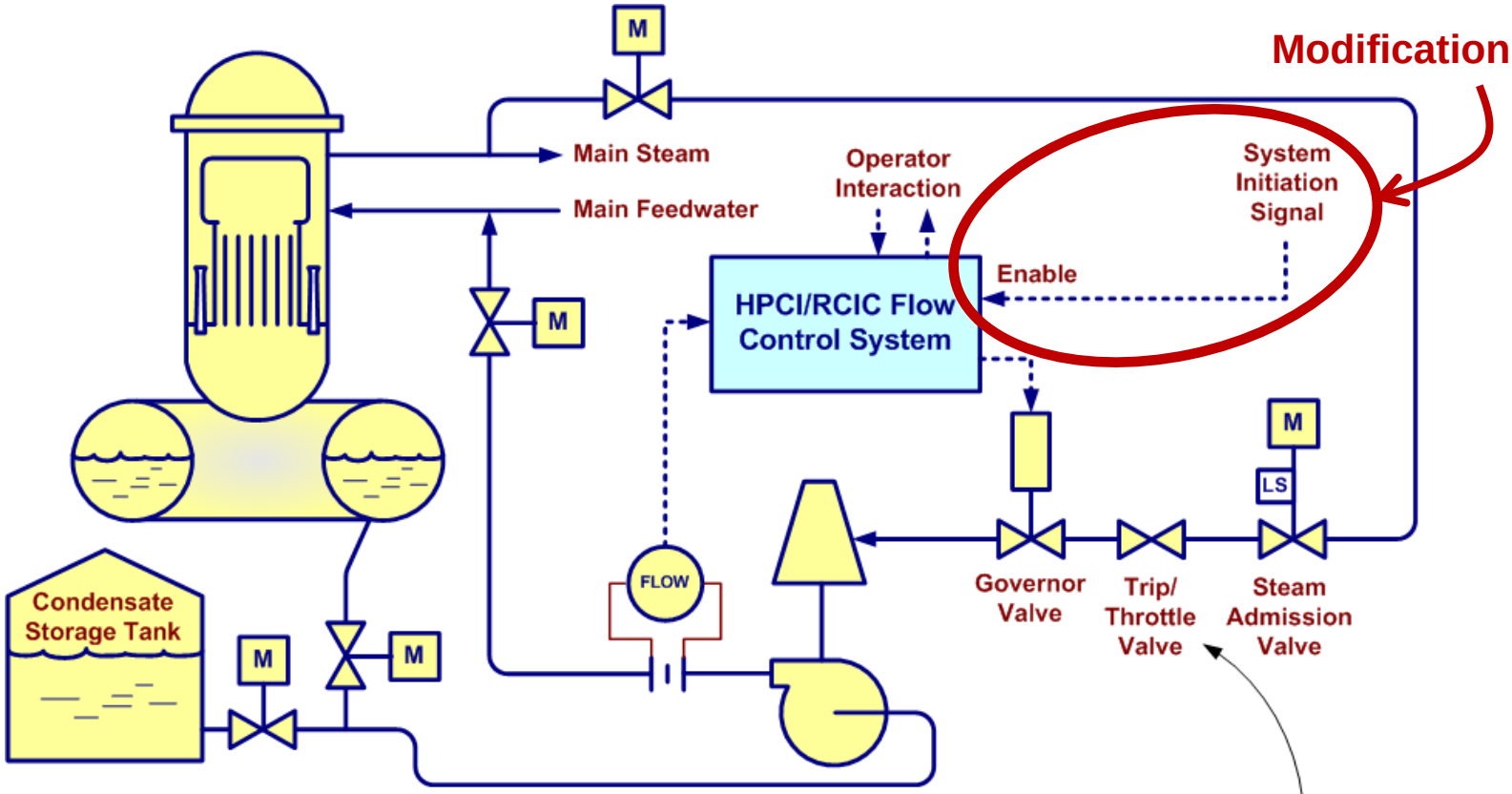
Utility engineers focused on this *Control Flaw*

after the event

Step 7: Identify Potential Causes of HCAs

Hazard: Equipment Operated Beyond Limits (H3)
Controller: HPCI-RCIC Flow Control System
Hazardous Control Action No. 2: "Increase governor valve position" command is provided when: there is an accident and turbine speed is too high, regardless of system flow
Inadequate, Missing or Delayed Feedback
Enable signal sent to controller before there is a valid demand on HPCI/RCIC
enable provided when steam admission valve is not open (broken or misaligned LS)
steam admission valve commanded open when there is no demand on HPCI/RCIC (spurious ESFAS signal)
Enable signal sent to controller when there is a demand on HPCI/RCIC, but delayed
enable provided when steam admission valve is opened, but too late (misaligned LS or LS setpoint too high)
Steam admission valve opens too slowly when commanded by ESFAS Initiation Signal (excessive stem thrust)
steam admission valve commanded open too late when there is a demand on HPCI/RCIC (ESFAS delay)
HPCI/RCIC pump flow rate signal to controller is missing, delayed, incorrect, too infrequent, or has inadequate resolution
Signal corrupted during transmission
sensor failure
sensor design flaw
sensor operates correctly but actual flow rate is outside sensor's operating range
fluid type is not as expected (water vs. steam?)
Governor valve position signal to controller is missing, delayed, incorrect, too infrequent, or has inadequate resolution
Problems with communication path
actual position is beyond sensor's range
sensor reports actuator position and it doesn't match valve position
sensor correctly reports valve position but position doesn't match assumed area/shape

Step 8: Eliminate, Prevent or Mitigate Hazards

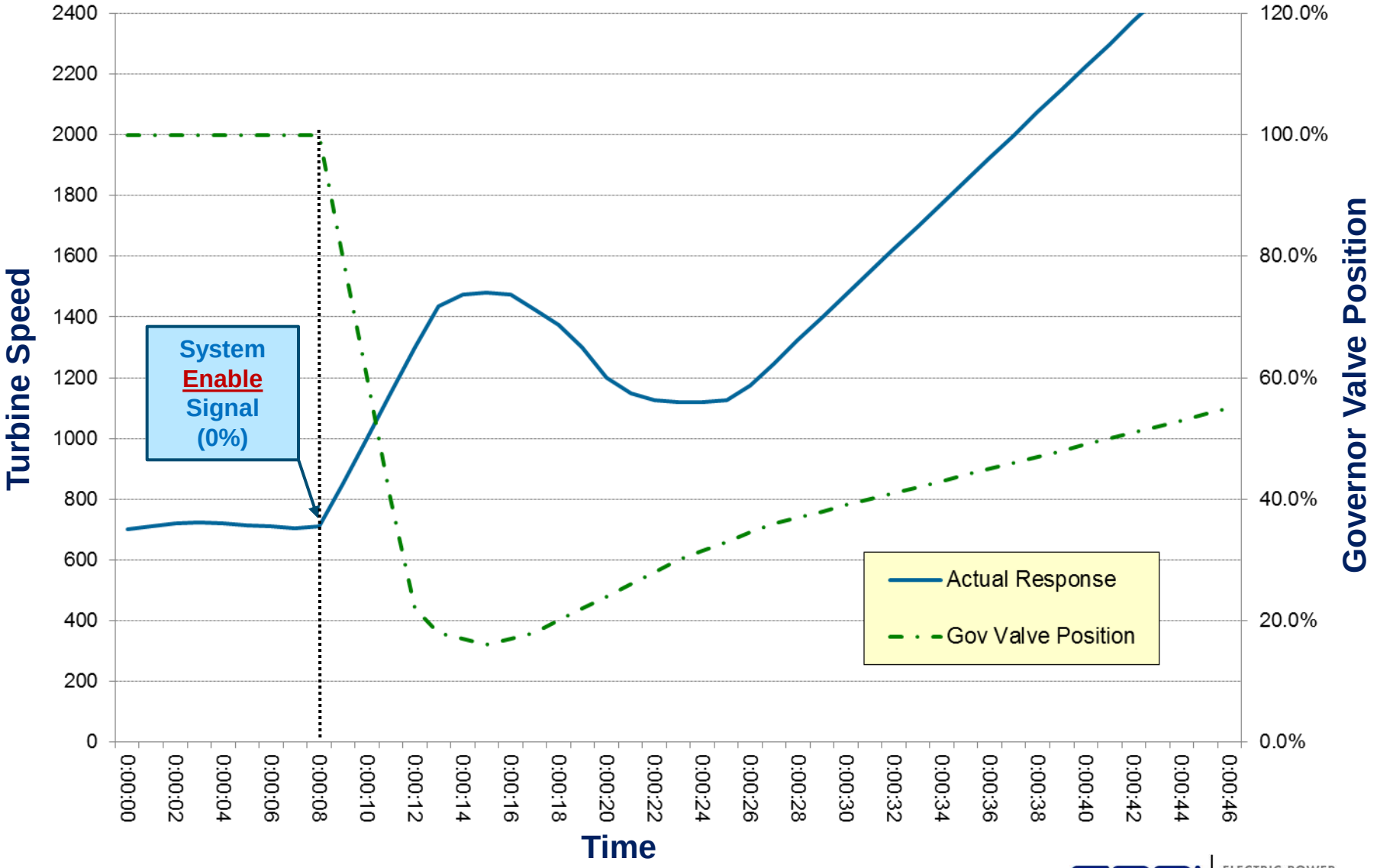


System Initiation Signals
(Open Steam Admission Valve & Process Valves)
1. Low Reactor Level (-48")
2. High Drywell Pressure (HPCI only; +2 psig)

System Isolation Signals
(Trip Turbine & Close Process Valves)
1. High Steam Line Flow
2. High Area Temperature
3. Low Steam Line Pressure (HPCI only)
4. Low Reactor Pressure (RCIC only)
5. Manual

Turbine Trip Signals
(Close Trip/Throttle Valve)
1. Any system isolation signal
2. High Steam Exhaust Pressure (150 psi)
3. High Reactor Level (+46")
4. Low pump suction pressure (15" Hg)
5. Turbine overspeed
6. Manual (local or remote)

Post-Mod Response of Turbine



STPA Strengths & Limitations

- Strengths
  - Can identify misbehaviors even when no “failures”
  - Thorough coverage
  - Addresses misbehaviors due to software problems
  - May help address regulatory concerns
- Limitations
  - Likely to require a facilitator for new users
  - Dependent on analysis boundary
  - Does not pinpoint single failures (a nuclear criterion)
  - Large combinatorial data sets are possible

Together…Shaping the Future of Electricity