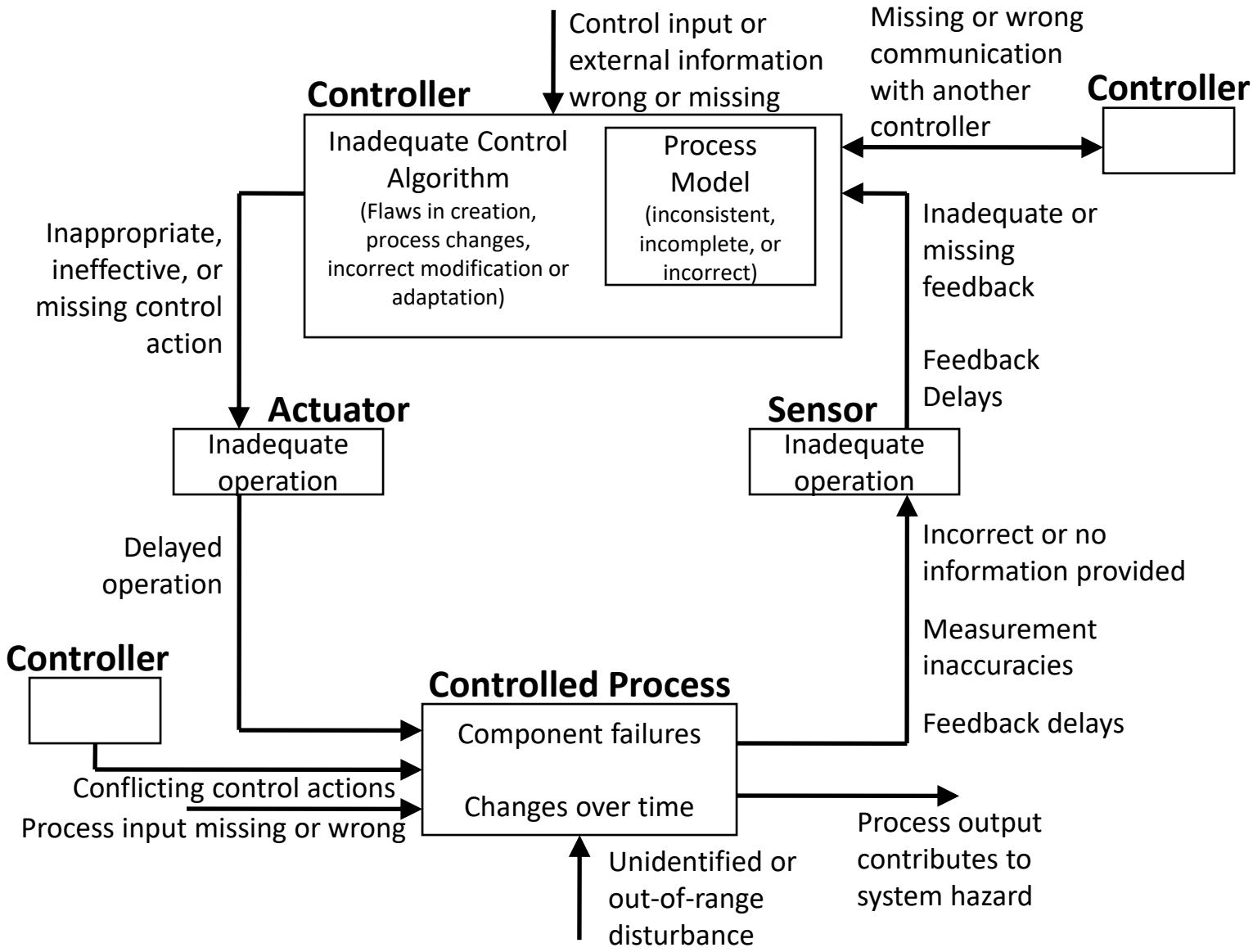
A New Process for Building STPA causal scenarios

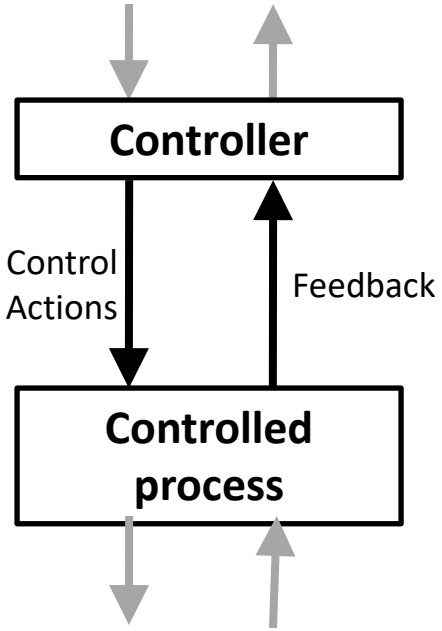
John Thomas

Old STPA Step Scenario Approach

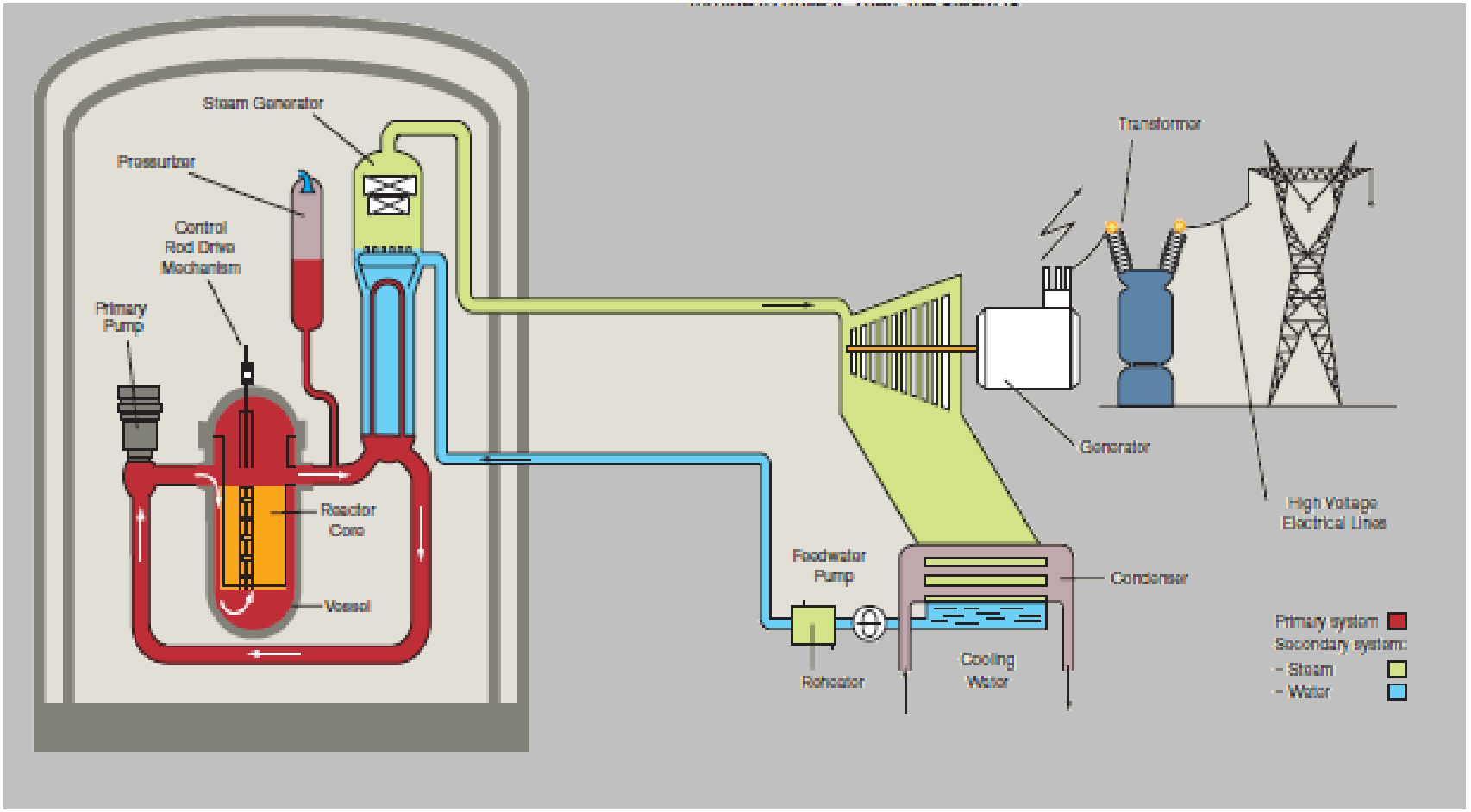


New Scenario-Building Process

- Goals
  - Dramatically improve efficiency of STPA
  - Start with high-level scenarios (quick, easy)
    - Then refine as needed
  - Provide a way to prove the high-level analysis is complete
  - Automatically generate complete set of basic scenarios if possible
    - (it is, given results from previous STPA steps!)



New Evolutionary Power Reactor

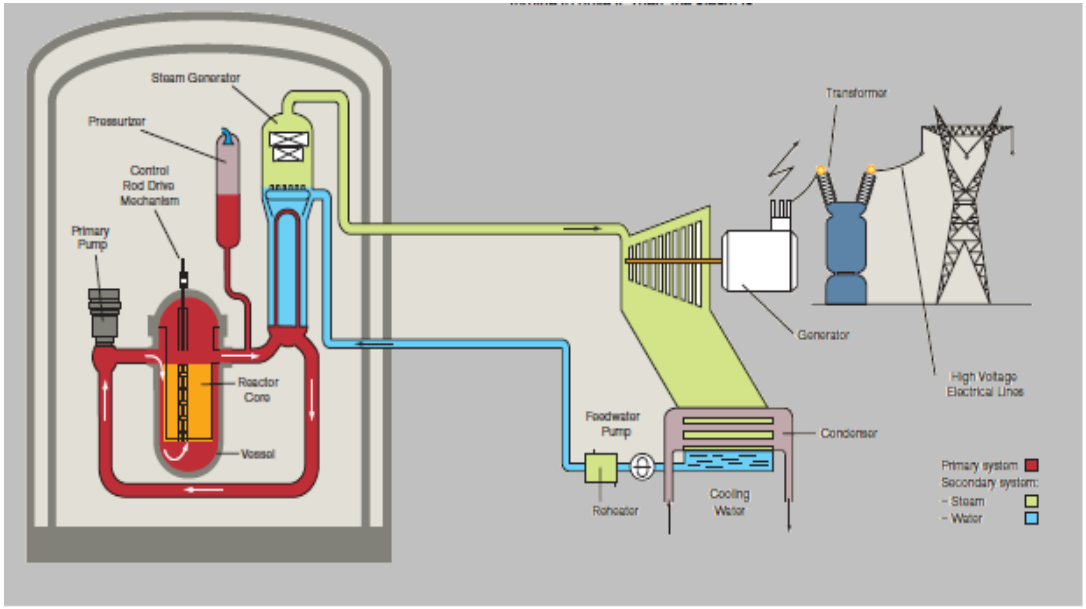


* Image from AREVA Brochure

Accidents (Losses)

- A-1: Death or injury to people
- A-2: Environmental damage
- A-3: Equipment loss/damage
- A-4: Loss of electricity generation

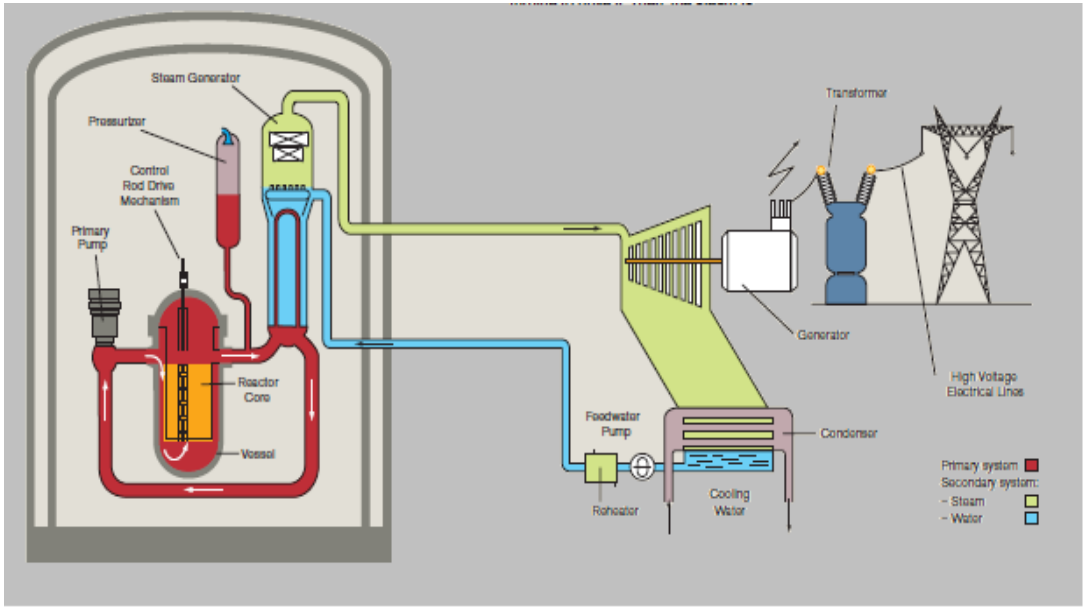
Broad view of "Safety"



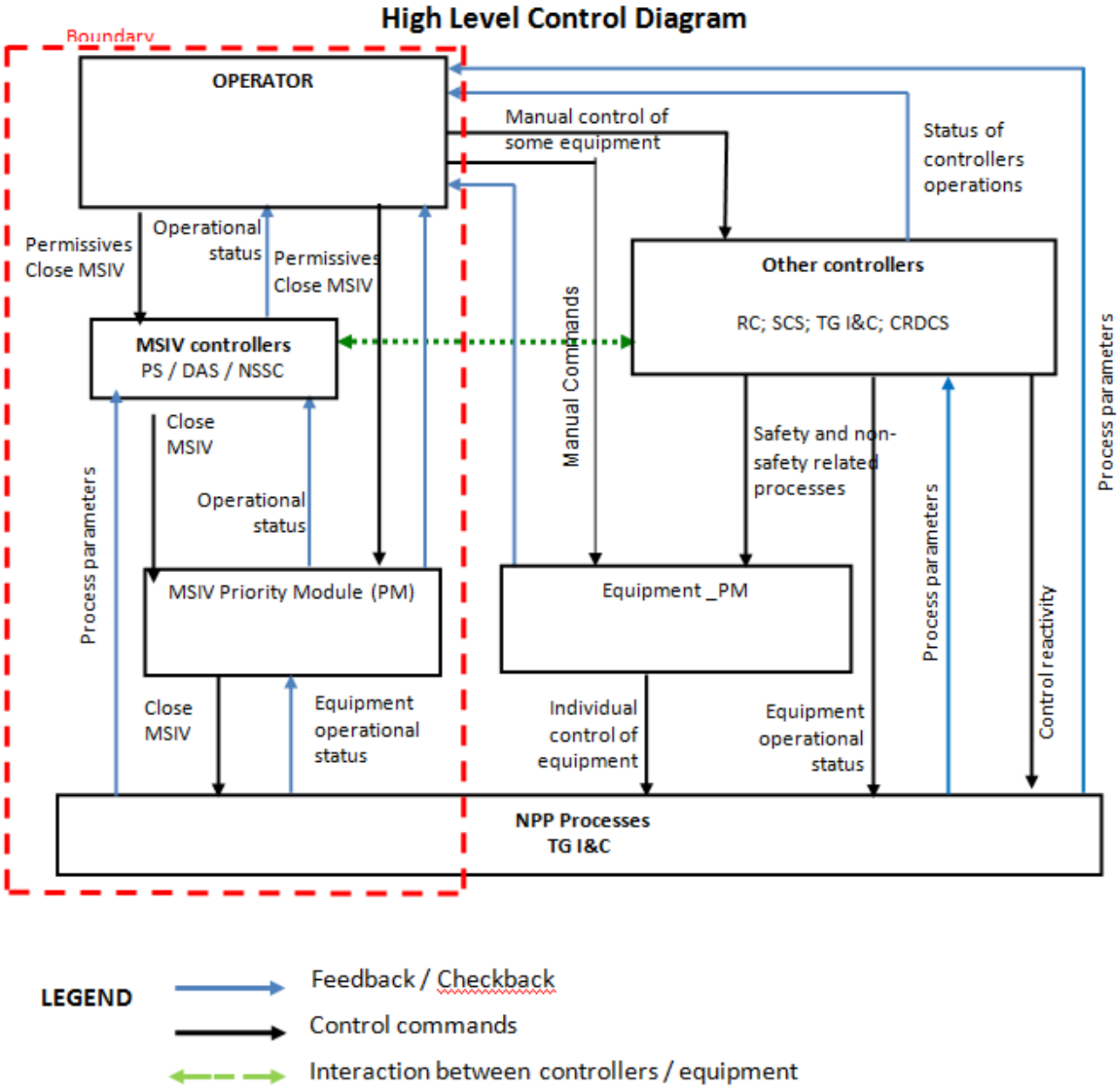
Accidents (Losses)

- A-1: Death or injury to people
- A-2: Environmental damage
- A-3: Equipment loss/damage
- A-4: Loss of electricity generation

Safety and security goals are the same!



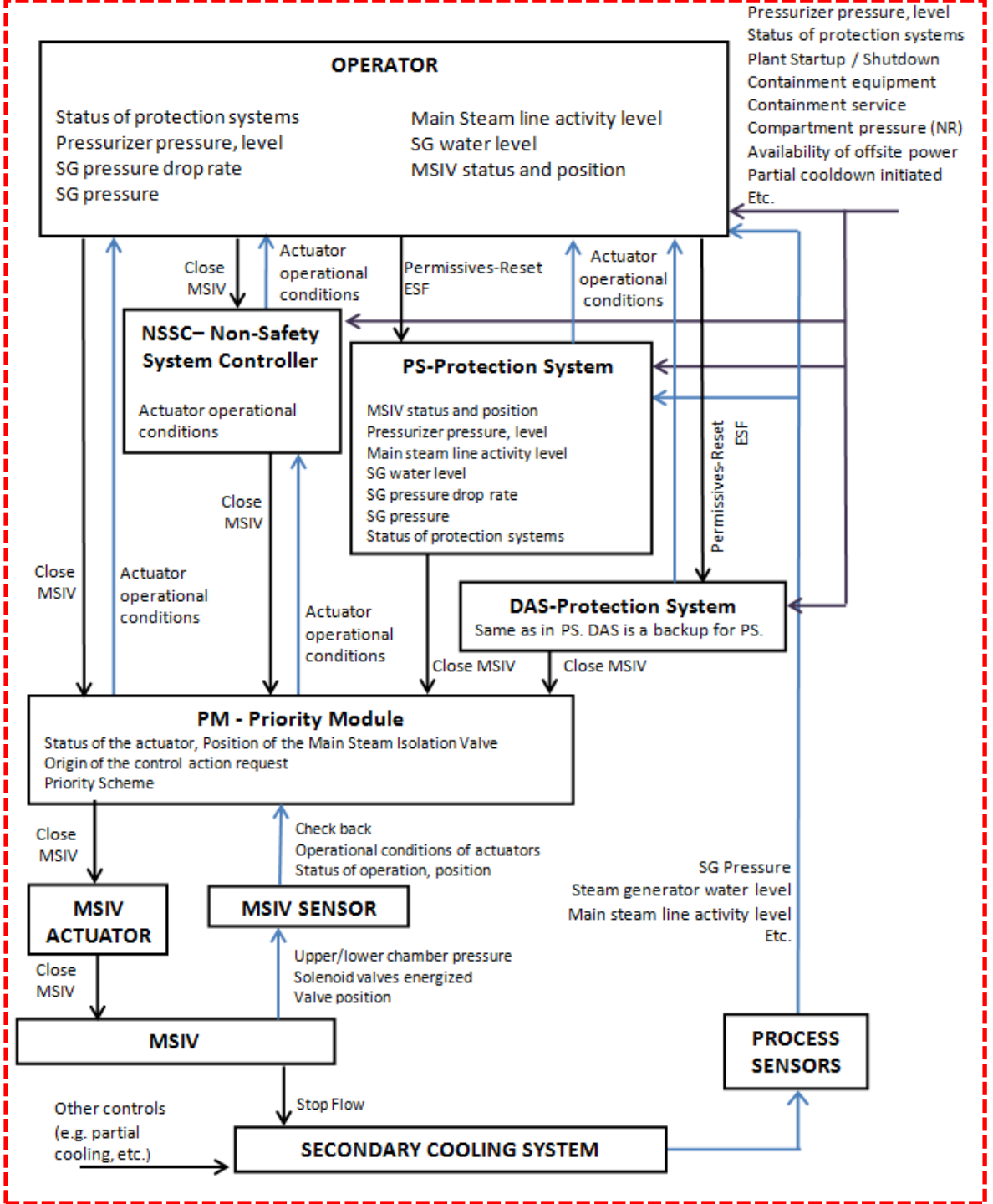
System Control Structure



More Detailed Control Structure

System Responsibilities

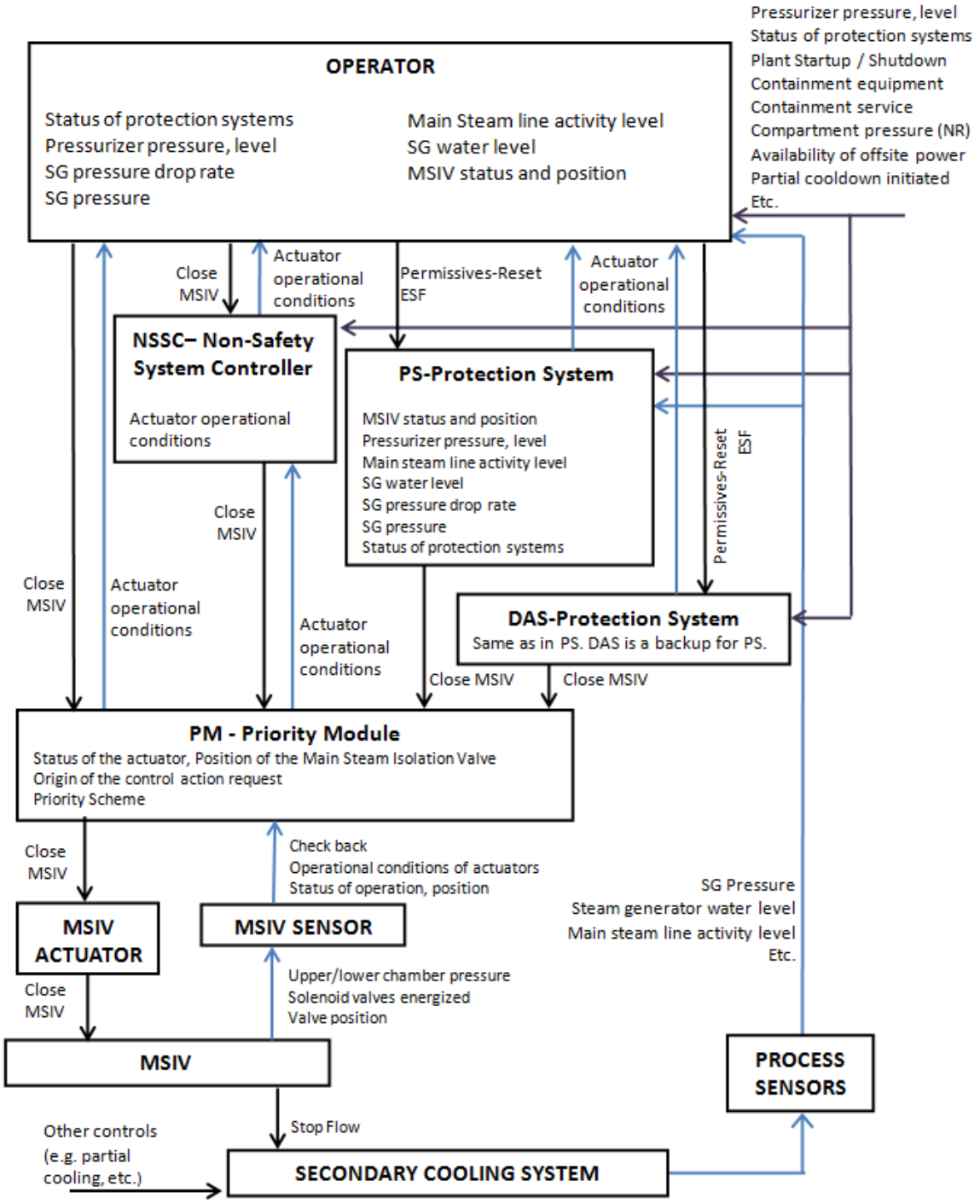
- Allow secondary cooling flow during normal operation
- Stop secondary cooling flow during certain emergency conditions



Unsafe Control Actions

UCA:
NSSC provides Close MSIV cmd when there is no rupture

Safety problem or security problem?



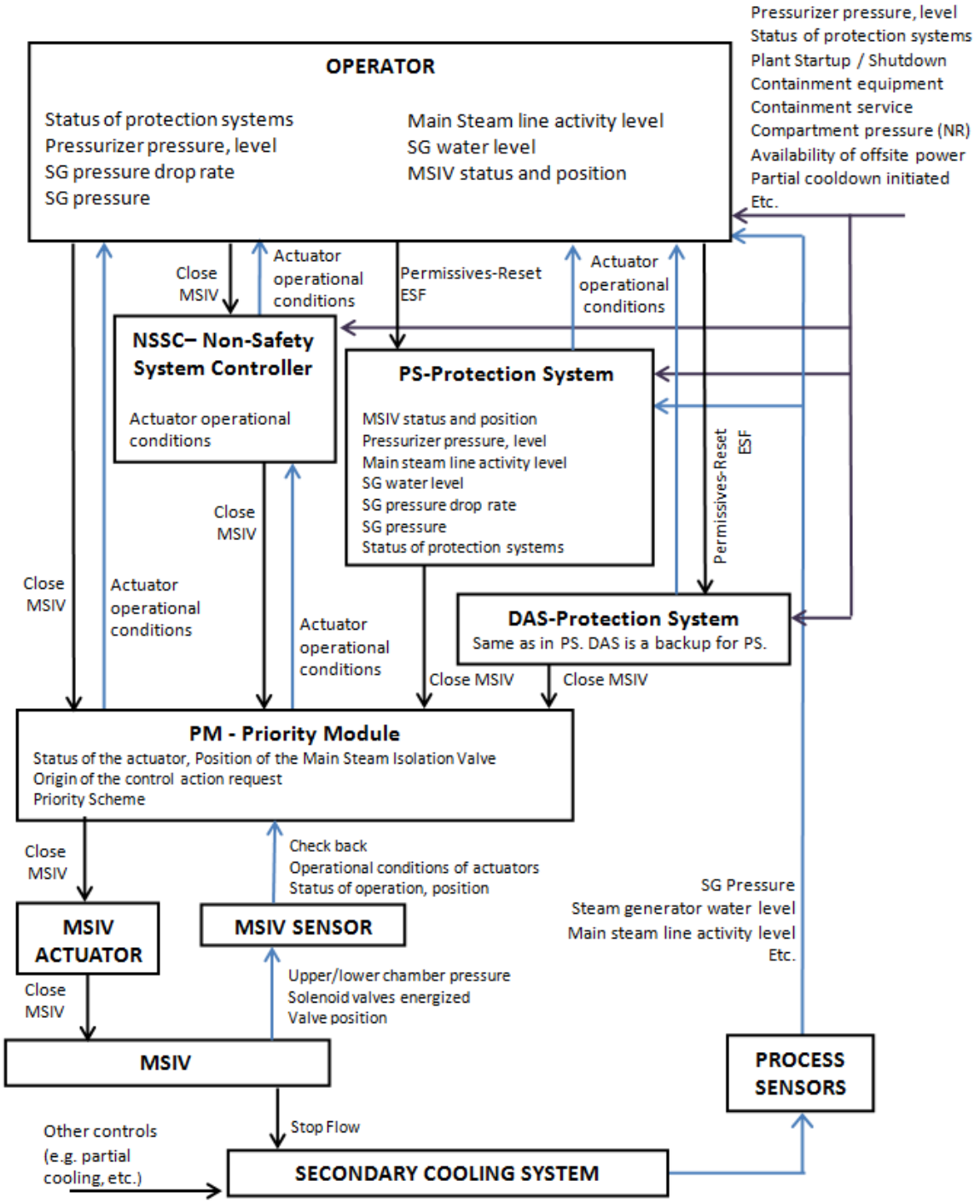
Summary of Unsafe Control Actions

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	NSSC does not provide Close MSIV 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]	NSSC provides Close MSIV when there is a rupture and other support systems are inadequate [H-1, H-2, H-3] **NSSC provides Close MSIV when there is no rupture** [H-4]	NSSC provides Close MSIV too early (while SG pressure is high): SG pressure may rise, trigger relief valve, abrupt steam expansion [H-2, H-3] NSSC provides Close MSIV 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

Unsafe Control Actions

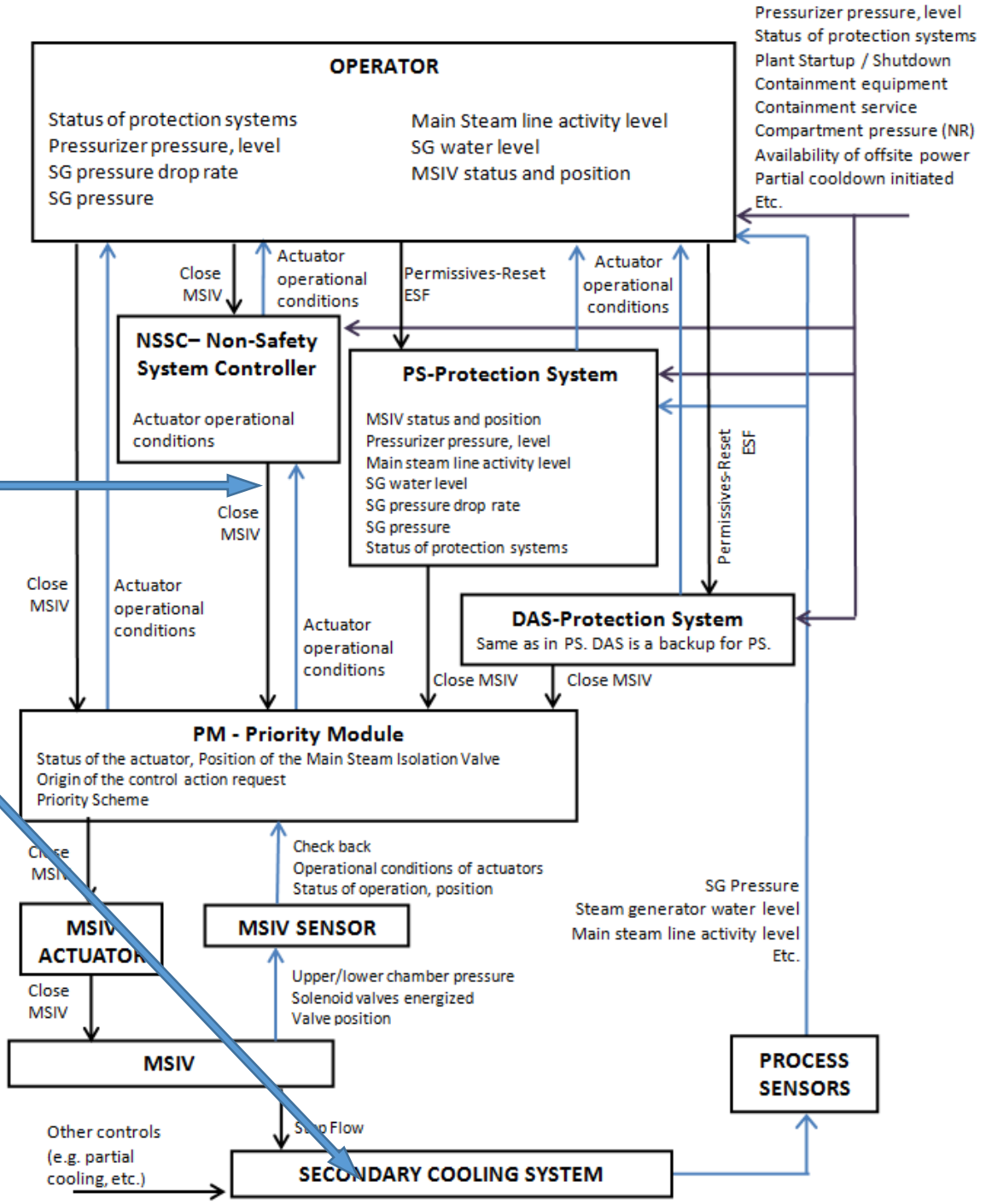
UCA:
NSSC provides Close MSIV command when there is no rupture

How to build scenarios from this?



Unsafe Control Actions

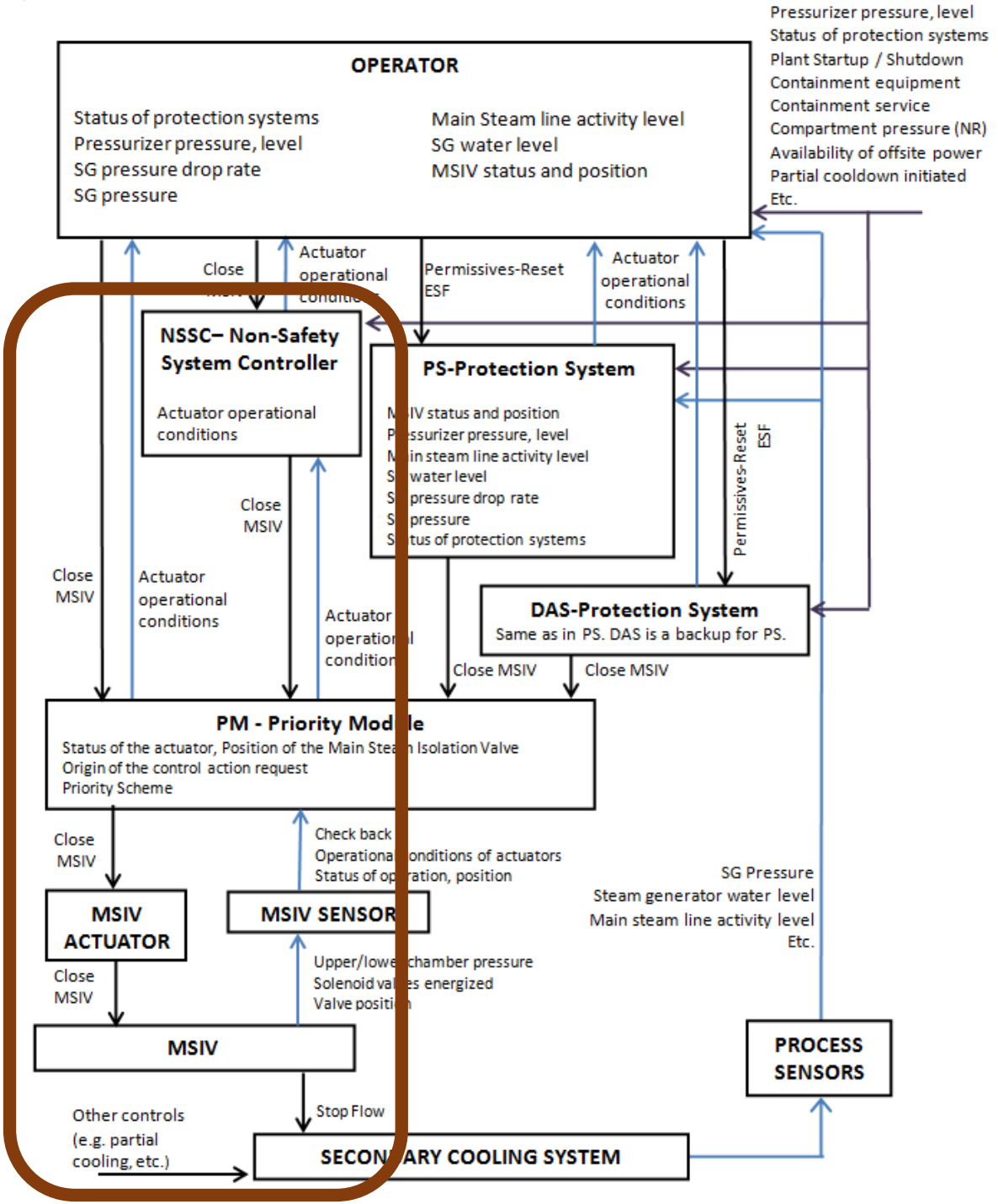
UCA:
NSSC provides Close MSIV cmd when there is no rupture



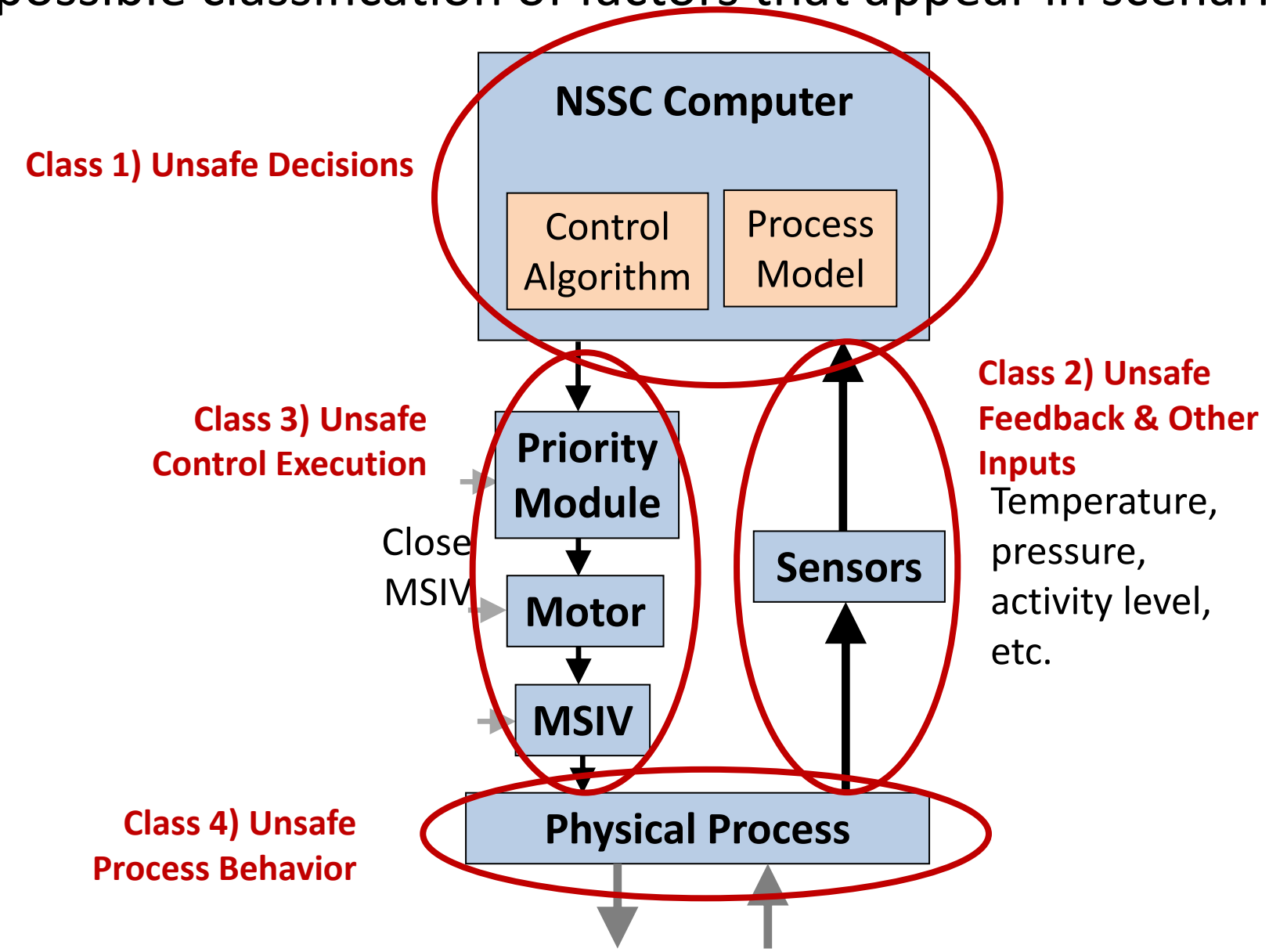
More Detailed Control Structure

The UCA text is describing conditions in this region.

The UCA is saying that these conditions can work together to cause an overall system Hazard.



A possible classification of factors that appear in scenarios



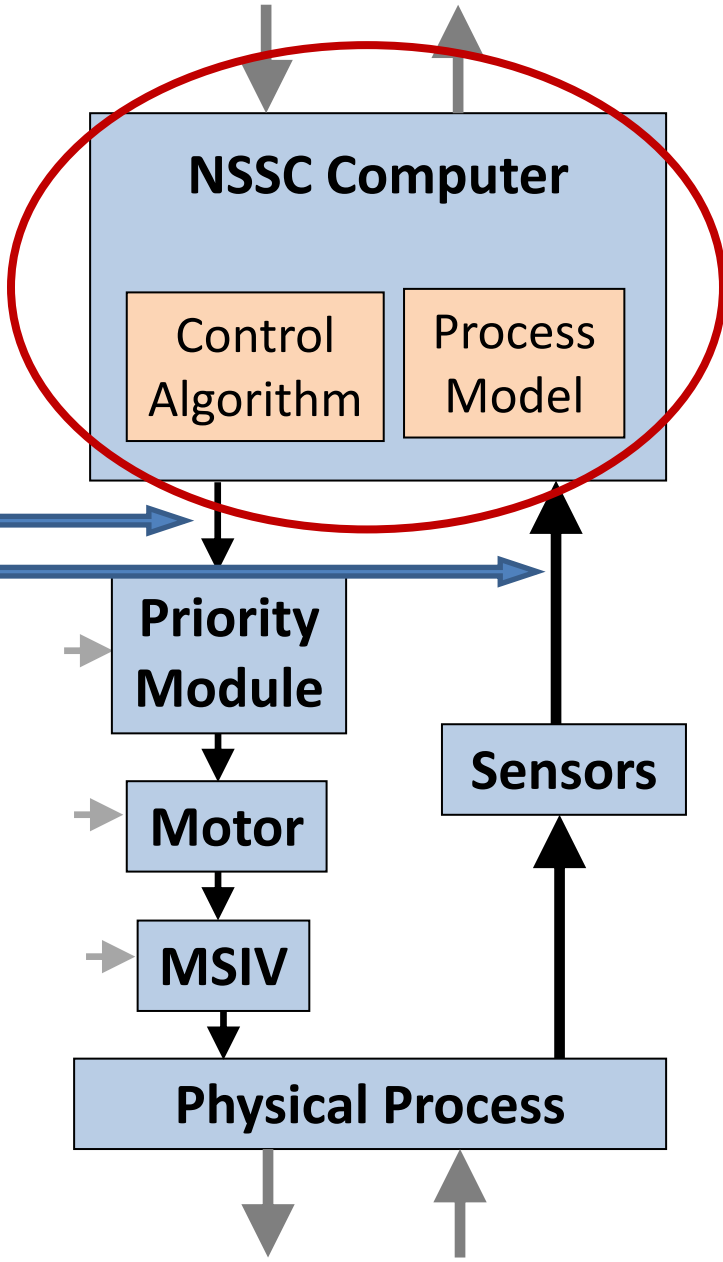
We can define 4 general classes or regions of interest
All must be considered when building scenarios

Building Scenarios
Top-down

UCA: NSSC provides Close MSIV when there is no rupture […]

Class 1 Basic Scenario: Unsafe Decisions

- NSSC provides close command
- There is no rupture indication



There may be several different causes that could explain this. We may need to consult SMEs who know the system but not STPA. We can use this basic scenario to generate SME questions, find the specific causes, and refine this scenario in more detail.

Generated question: What could cause the NSSC Computer to close the MSIV when no rupture is indicated?

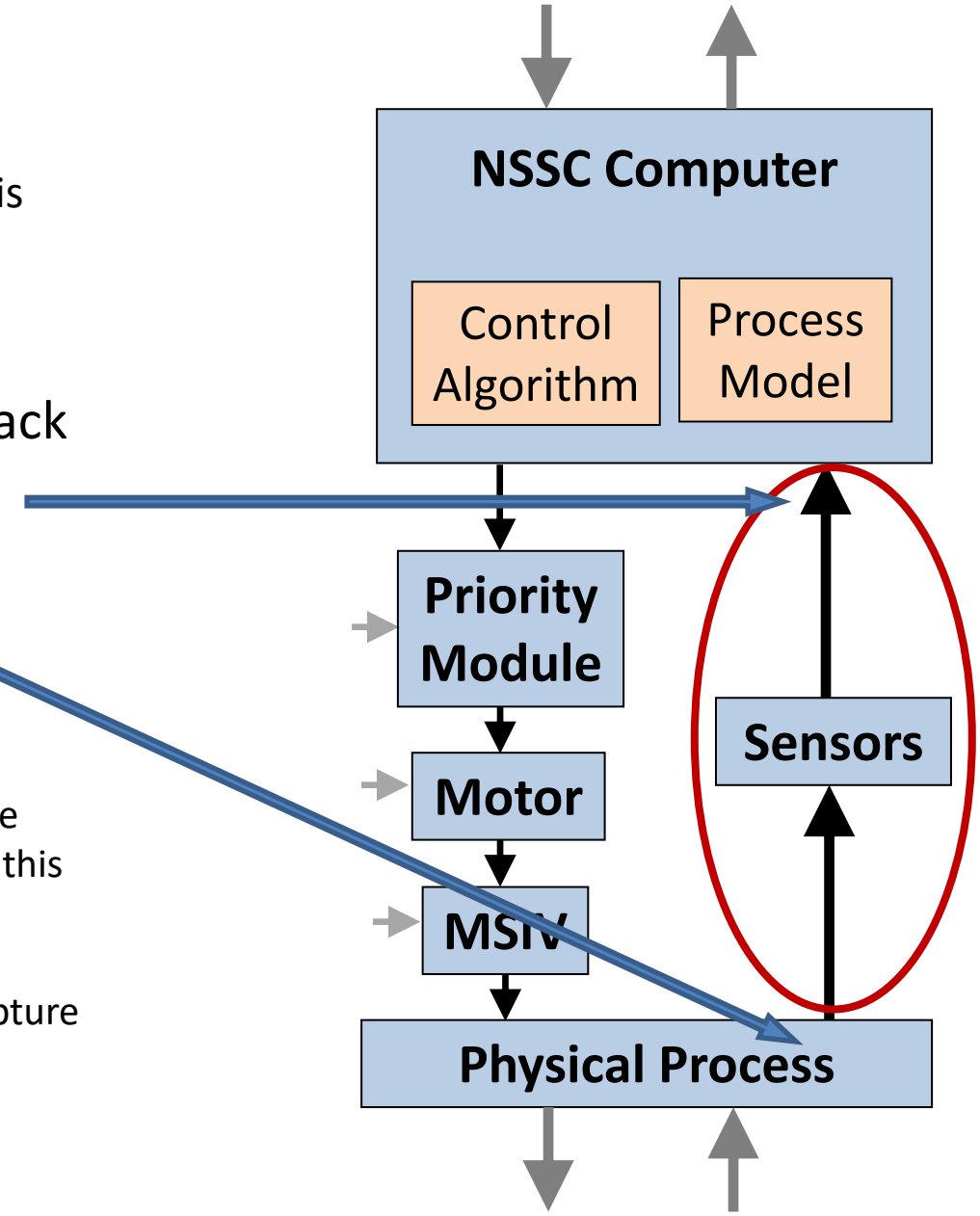
- Potential emergency conditions that override normal behavior?
- Any default behaviors that may trigger Close MSIV?
- Etc.

Building Scenarios Top-down

UCA: NSSC provides Close MSIV when there is no rupture […]

Class 2 Basic Scenario: Unsafe Feedback

- NSSC receives rupture indication
- There is no rupture



The UCA may be caused by unsafe feedback (Class 2). We can use this basic scenario to generate SME questions, find the specific causes, and refine this scenario in more detail.

Generated question: What could cause a digital rupture indication when there is no rupture?

- How can this happen due to a failure?
- How can this happen without any failure?

Building Scenarios Top-down

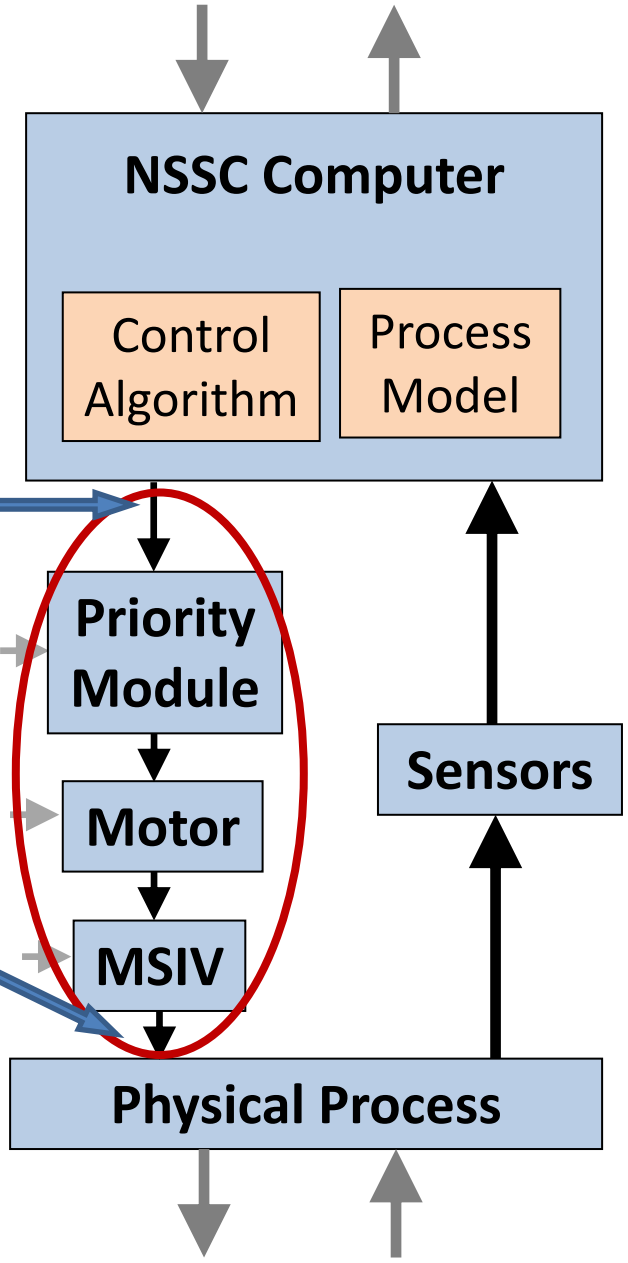
Class 3 Basic Scenario: Unsafe Control Execution

- NSSC does not send close command
- MSIV closes

The command may be safe (do not close MSIV), but the outcome may not be safe (MSIV closes anyway). This is Class 3.

There may be several different causes that could explain this. We can generate questions to consult SMEs.

Generated question: What could cause the MSIV to close without a close command?



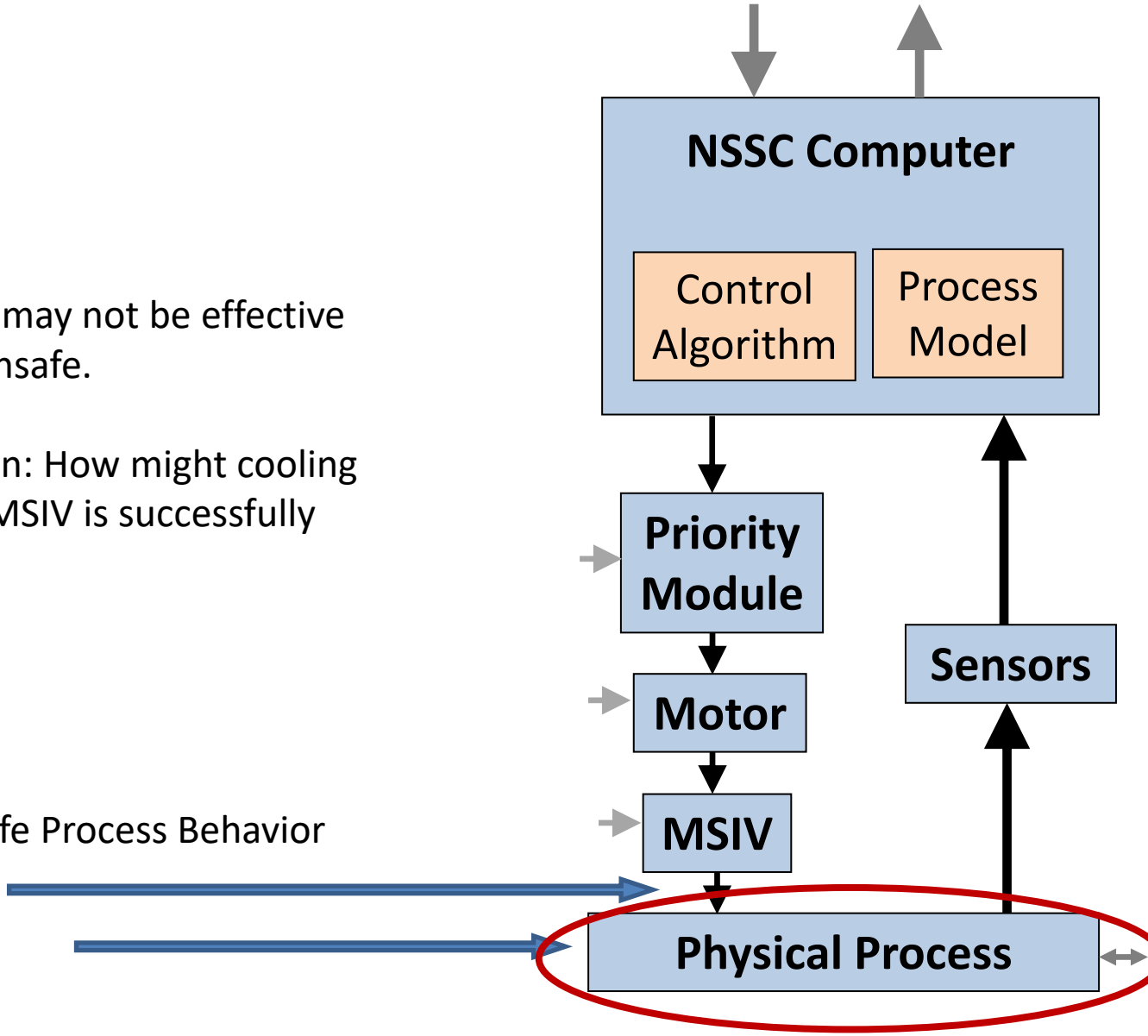
Building Scenarios Top-down

Even if the MSIV is open, it may not be effective if the process behavior is unsafe.

Example generated question: How might cooling still be inadequate even if MSIV is successfully opened?

Class 4 Basic Scenario: Unsafe Process Behavior

- MSIV open
- Cooling not provided



Building Scenarios
Top-down

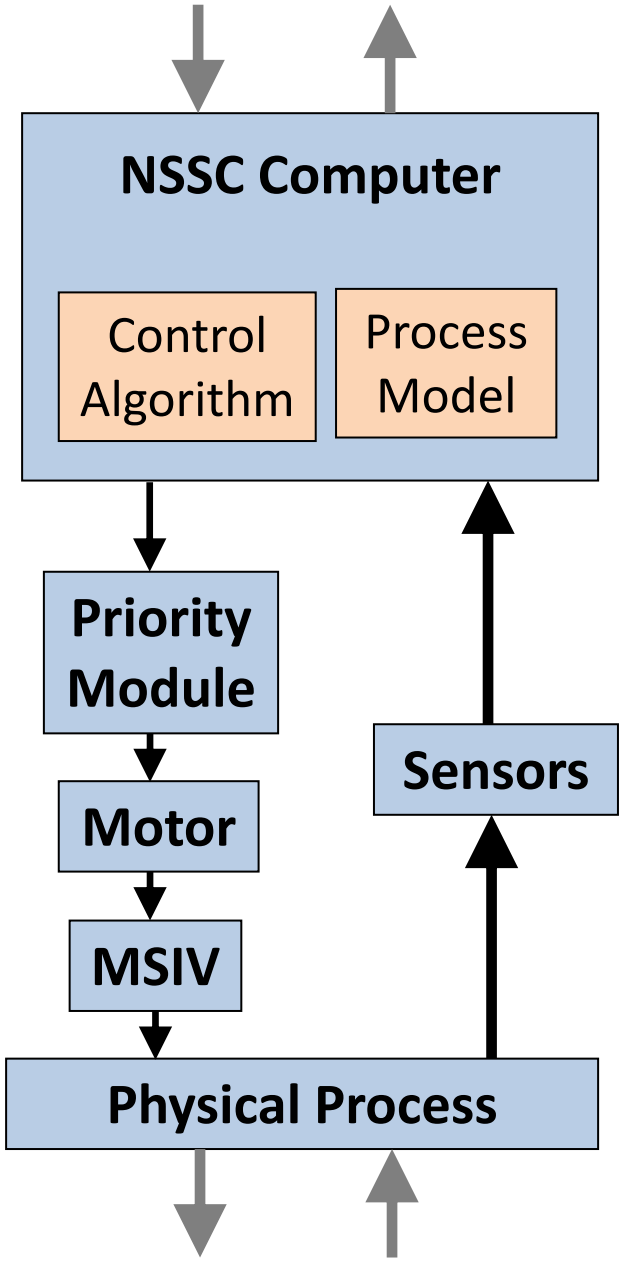
All classes should be considered when building scenarios:

Class 1) Unsafe Decisions
- NSSC provides close command
- There is no rupture indication

Class 2) Unsafe Feedback & Other Inputs
- NSSC receives rupture indication
- There is no rupture

Class 3) Unsafe Process Behavior
- MSIV not closed
- Cooling not provided

Class 4) Unsafe Control
- NSSC does not provide close command
- MSIV closes



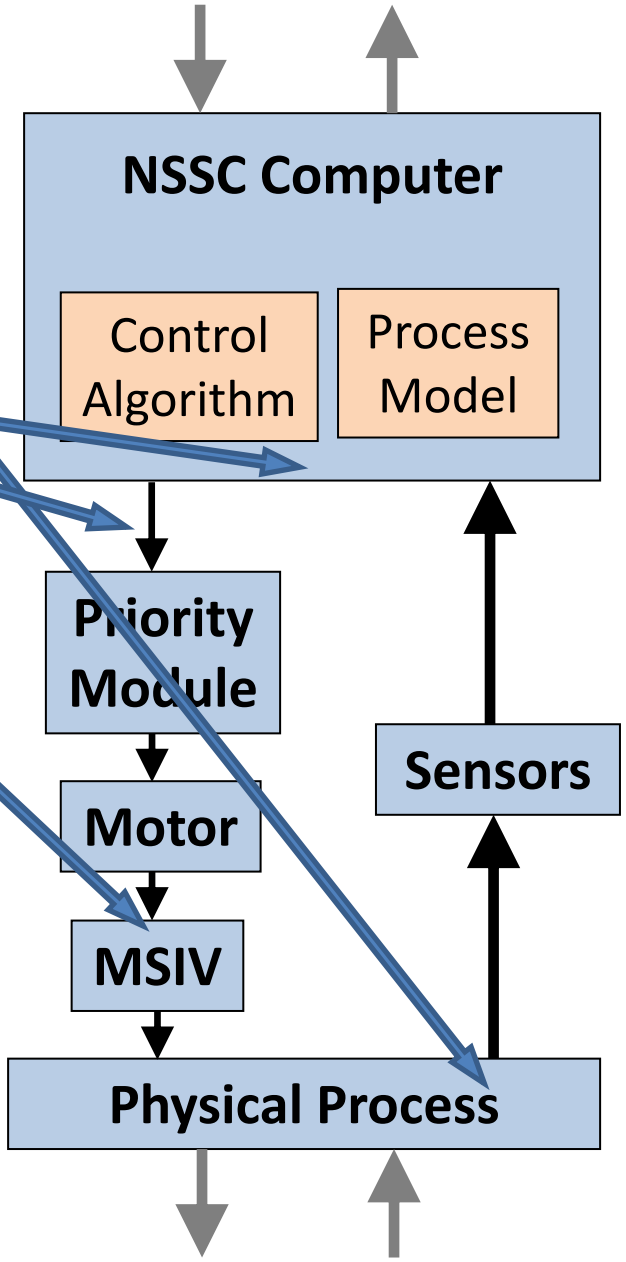
Building Scenarios

Top-down

UCA:

NSSC provides Close cmd to MSIV when there is no rupture

1. Inappropriate Decisions
   - NSSC provides close command
   - There is no rupture indication
2. Inadequate Feedback & Other Inputs
   - NSSC receives rupture indication
   - There is no rupture
3. Inadequate Process Behavior
   - MSIV not closed
   - Cooling not provided
4. Inadequate Control
   - NSSC does not provide close command
   - MSIV closes

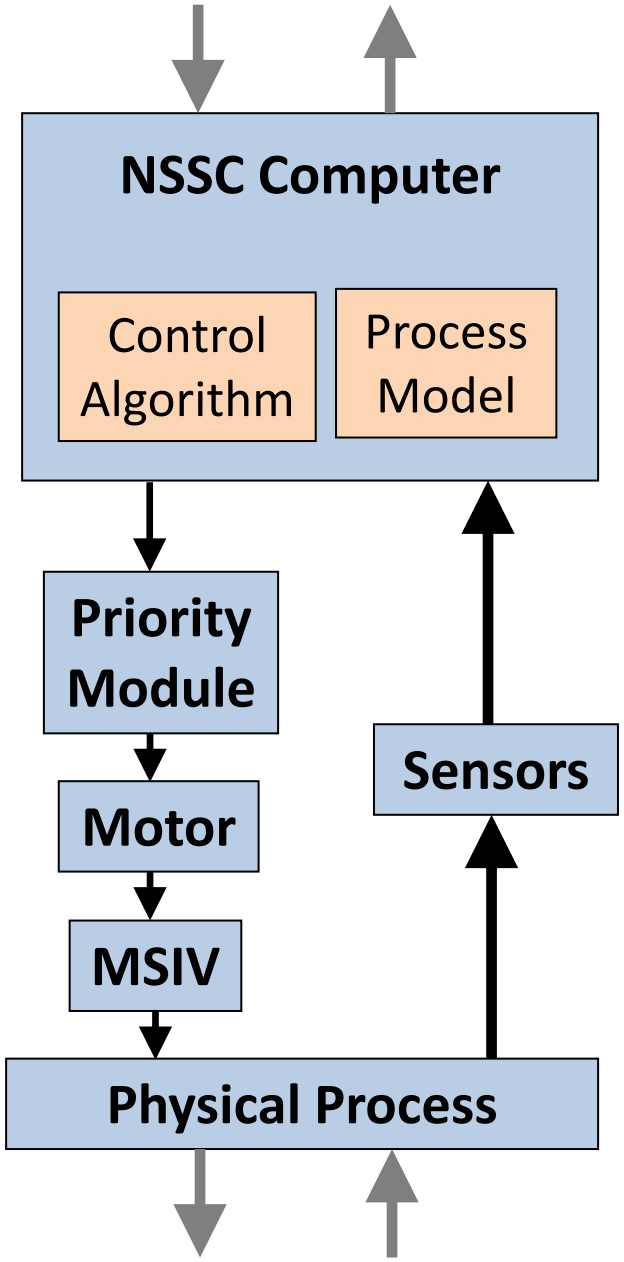


Building Scenarios

Top-down

UCA:
NSSC provides Close cmd to MSIV when there is no rupture

1. Inappropriate Decisions
   - NSSC provides close command
   - There is no rupture indication
2. Inadequate Feedback & Other Inputs
   - NSSC receives rupture indication
   - There is no rupture
3. Inadequate Process Behavior
   - MSIV not closed
   - Cooling not provided
4. Inadequate Control
   - NSSC does not provide close command
   - MSIV closes

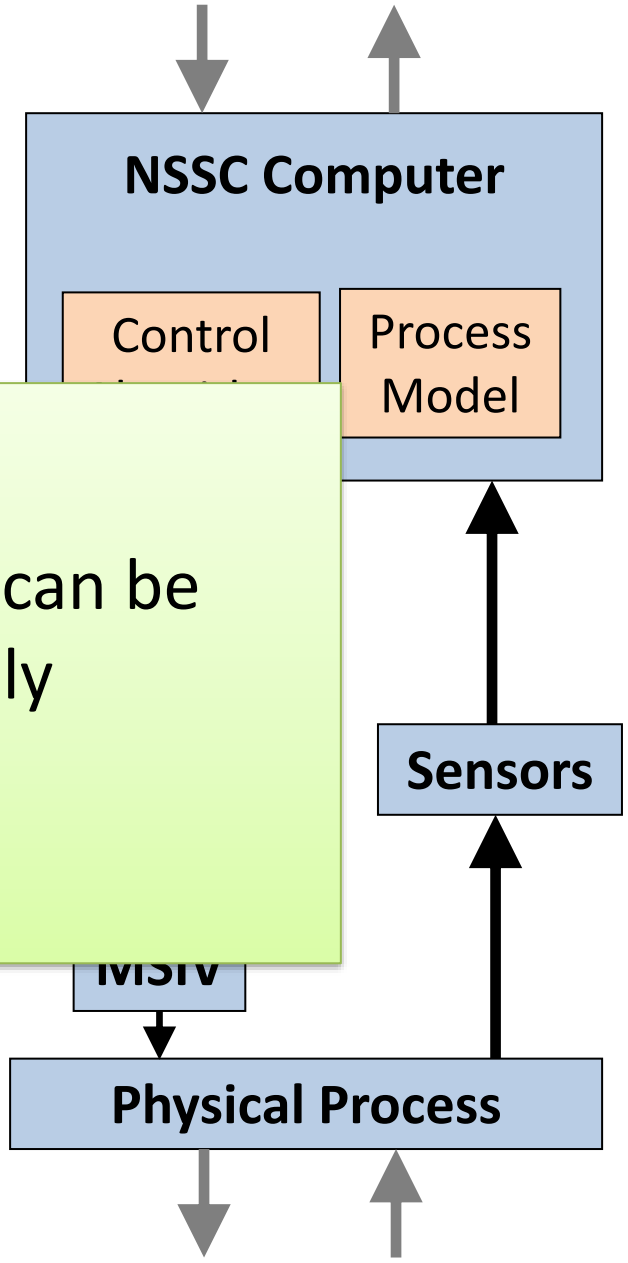


Building Scenarios Top-down

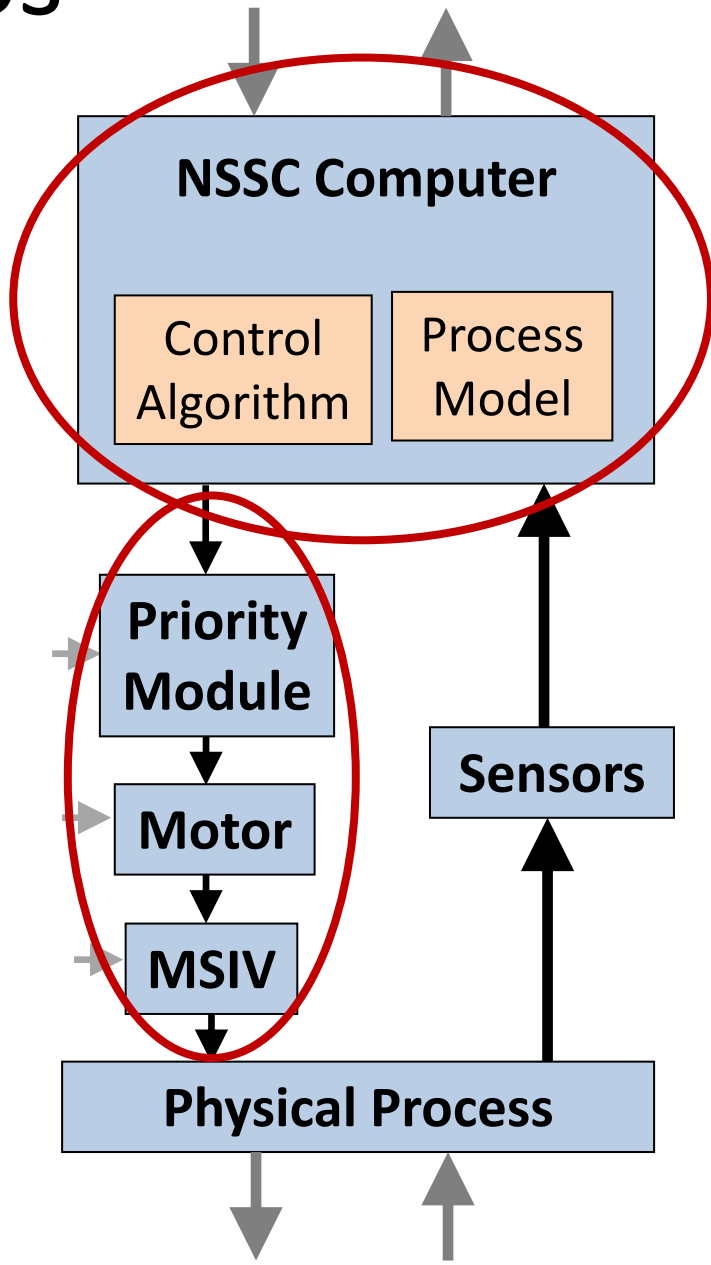
UCA:
NSSC provides Close cmd to MSIV when there is no rupture

1. Inappropriate Decisions
   - NSS
   - The
2. Inade
   - NSS
   - The
3. Inade
   - MSI
   - Cooling not provided
4. Inadequate Control
   - NSSC does not provide close command
   - MSIV closes

All of these basic scenarios can be generated automatically from UCAs!!



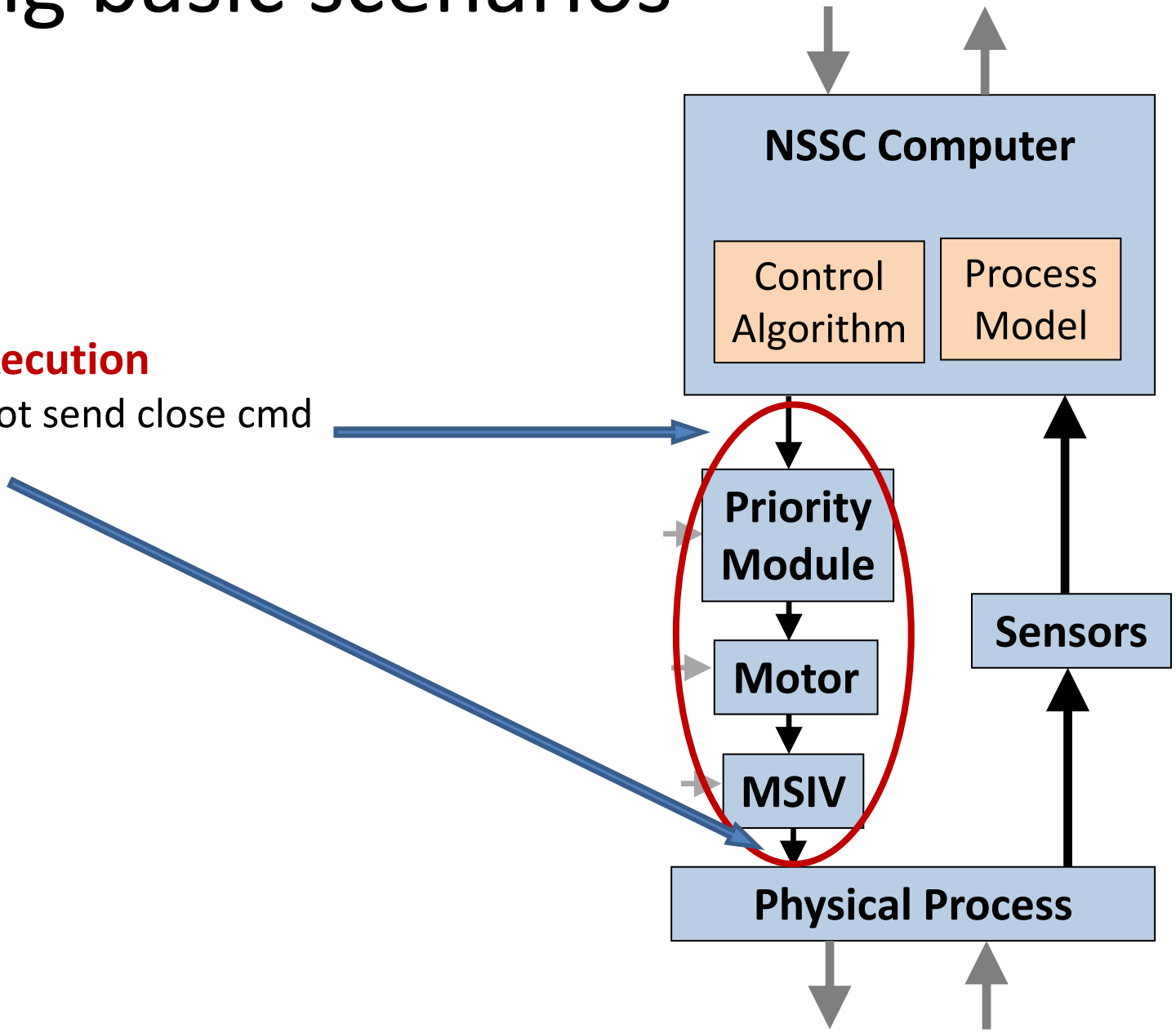
Combining basic scenarios



Combining basic scenarios

Unsafe Control Execution

- NSSC does not send close cmd
- MSIV closes



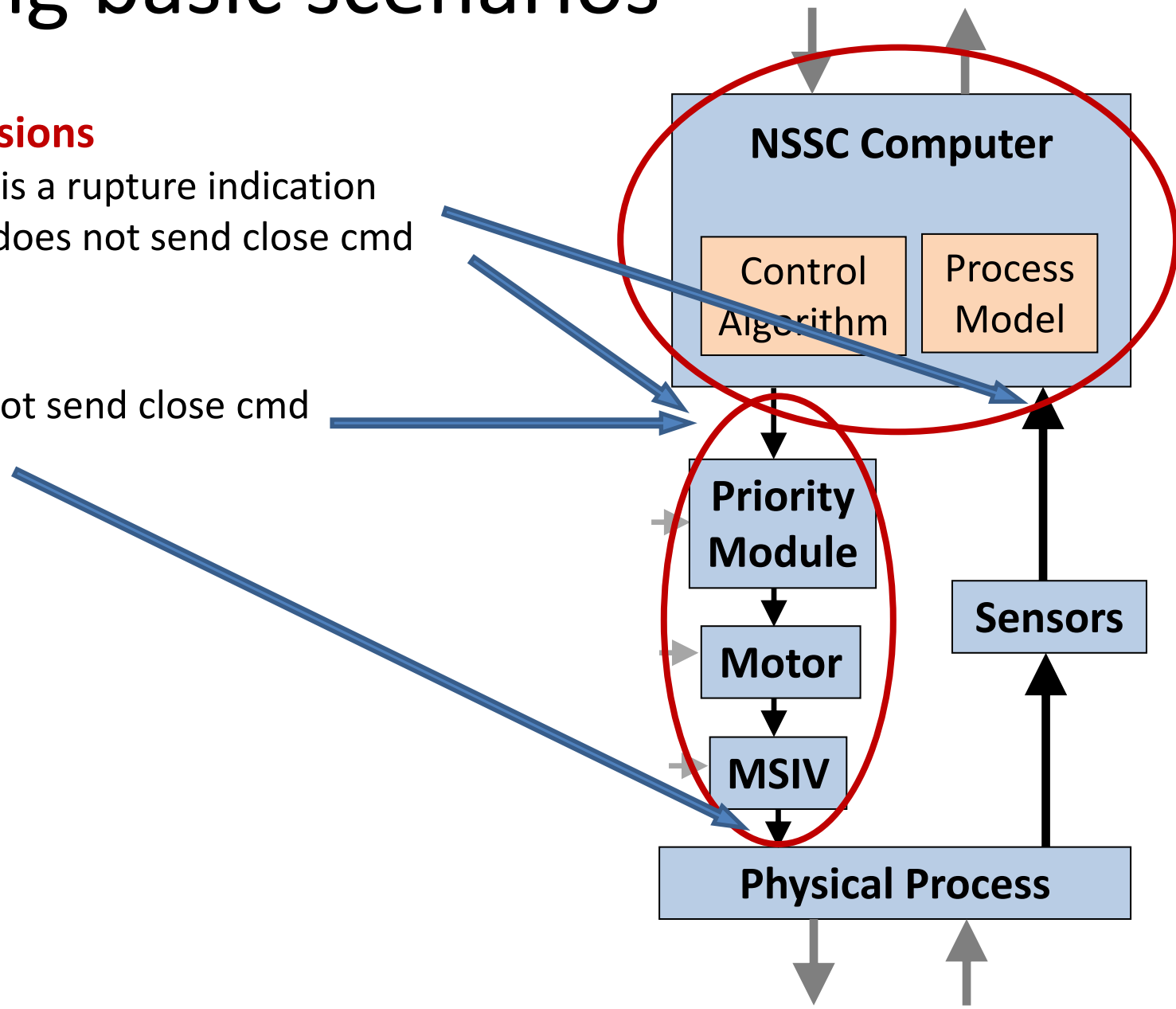
Combining basic scenarios

Unsafe Decisions

- There is a rupture indication
- NSSC does not send close cmd

Unsafe Control

- NSSC does not send close cmd
- MSIV closes



Combining basic scenarios

Unsafe Decisions

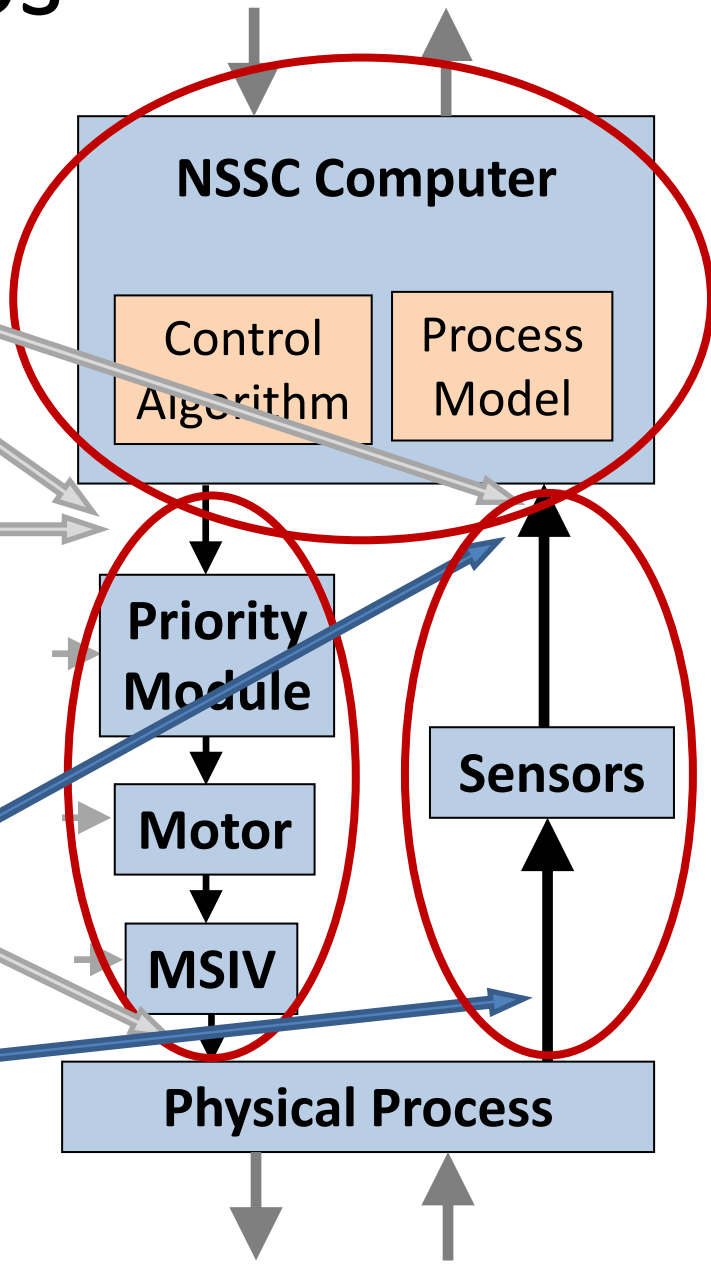
- There is a rupture indication
- NSSC does not send close cmd

Unsafe Control

- NSSC does not send close cmd
- MSIV closes

Unsafe Feedback

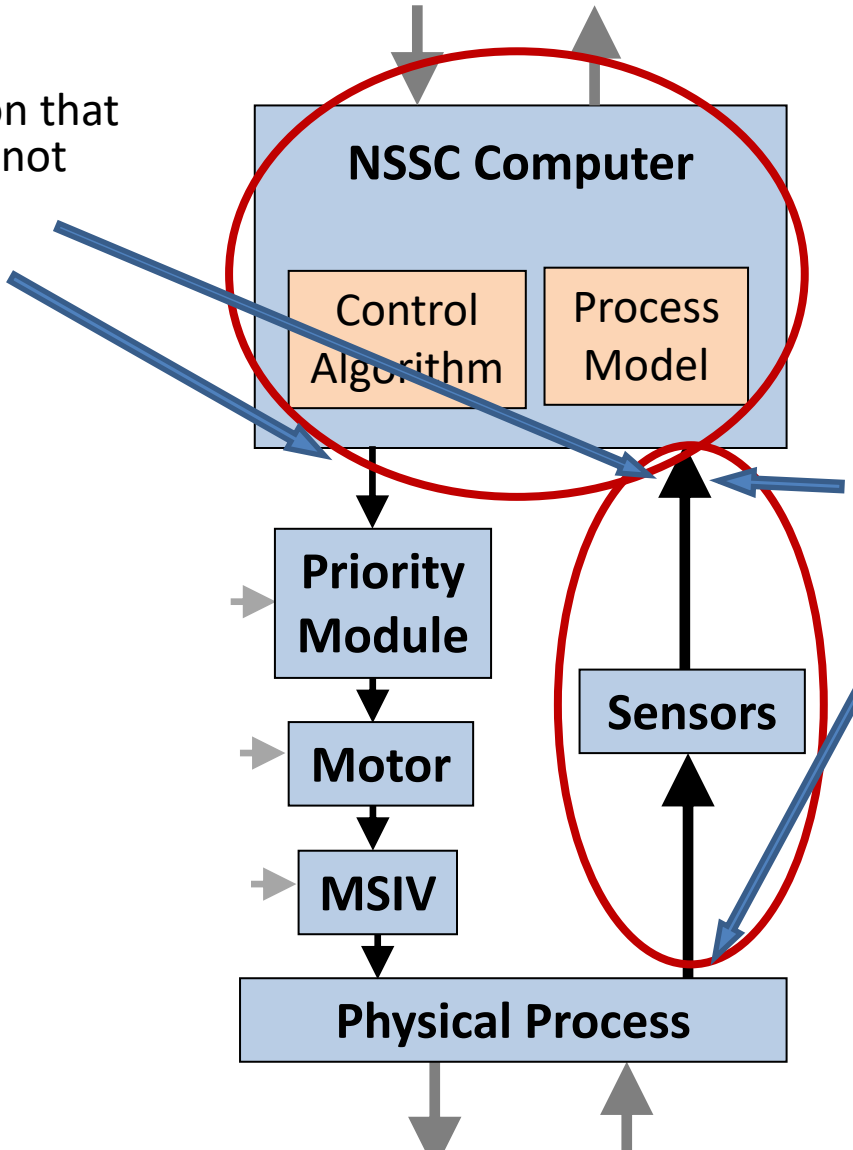
- There is a rupture indication
- There is no rupture



Combining basic scenarios

Unsafe Decisions

- NSSC receives indication that other support systems not operational
- NSSC sends close cmd



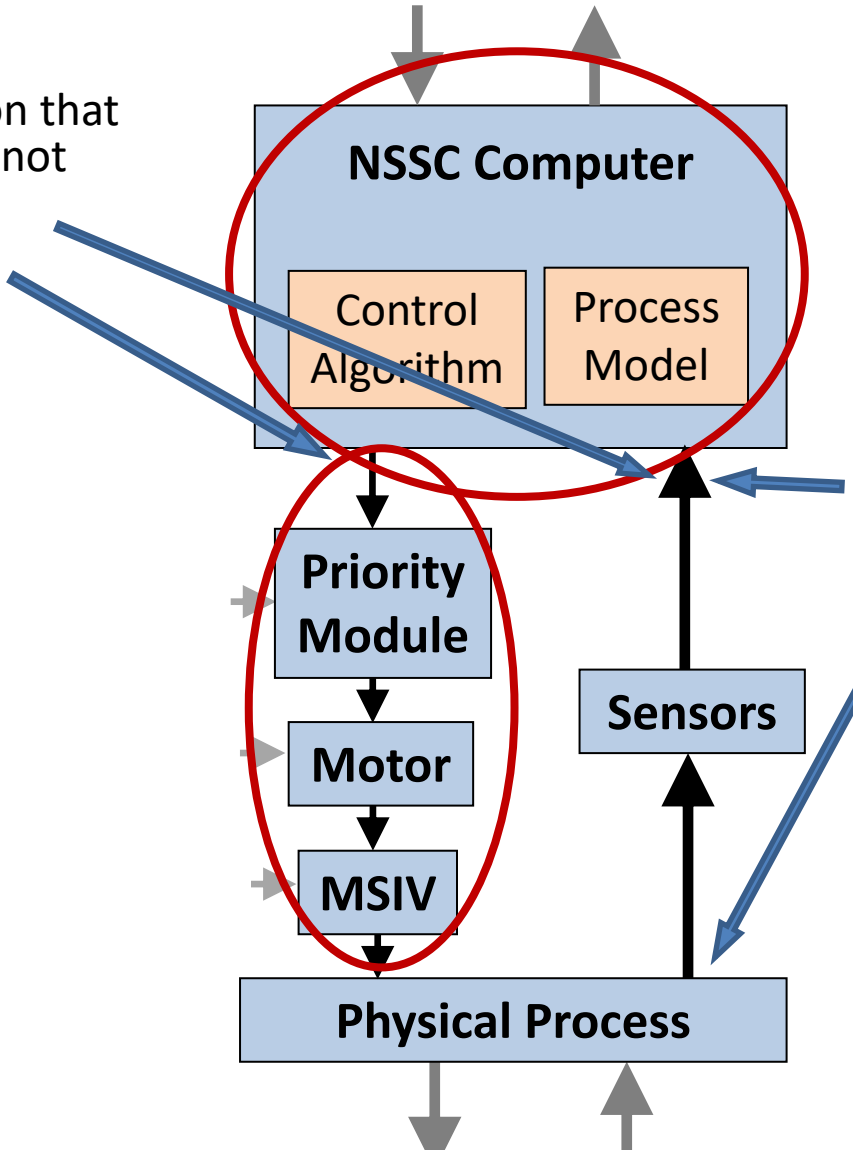
Unsafe feedback

- NSSC receives indication of a rupture
- There is no rupture

Combining basic scenarios

Unsafe Decisions

- NSSC receives indication that other support systems not operational
- NSSC sends close cmd

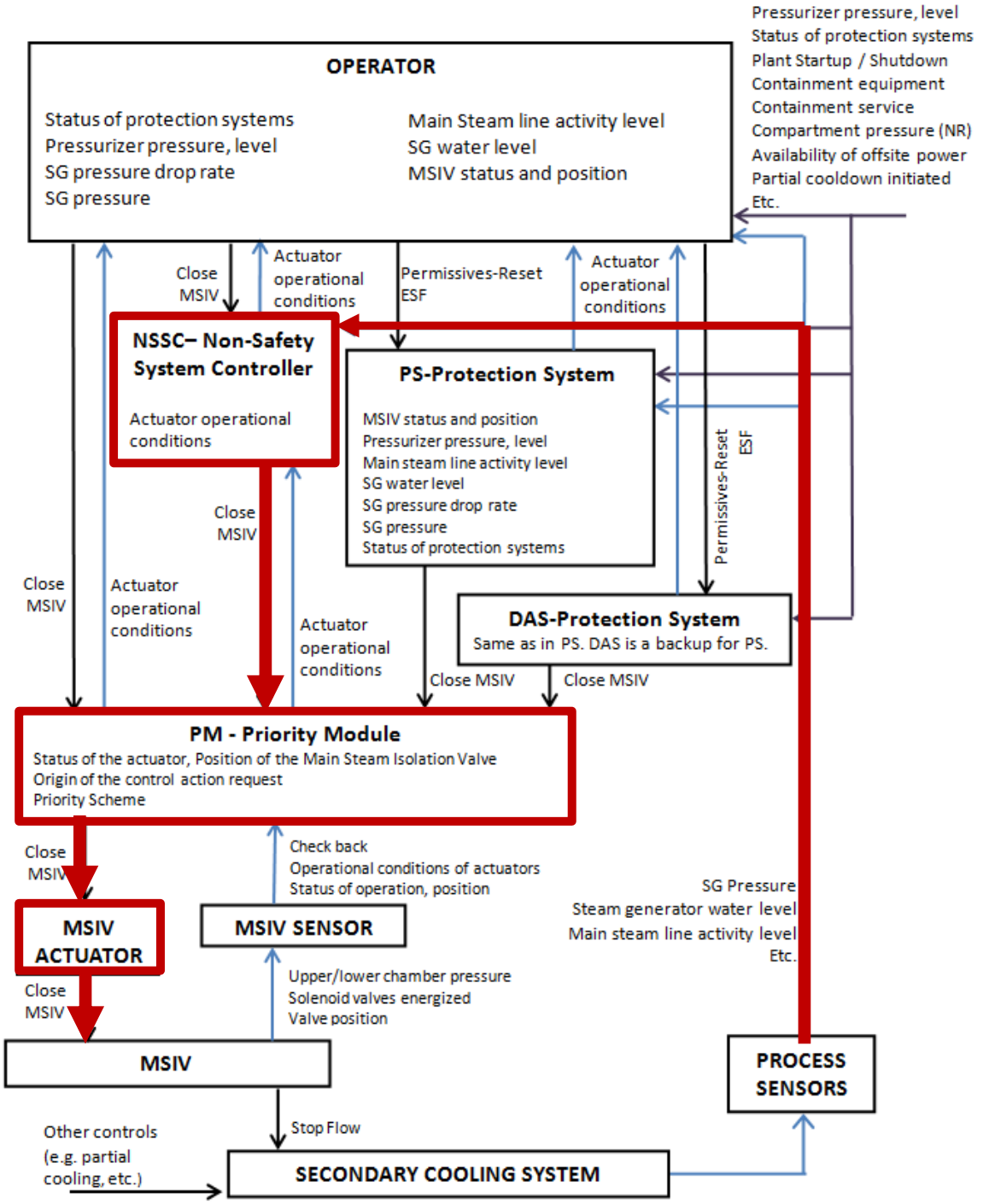


Unsafe feedback

- NSSC receives indication of a rupture
- There is no rupture

Results

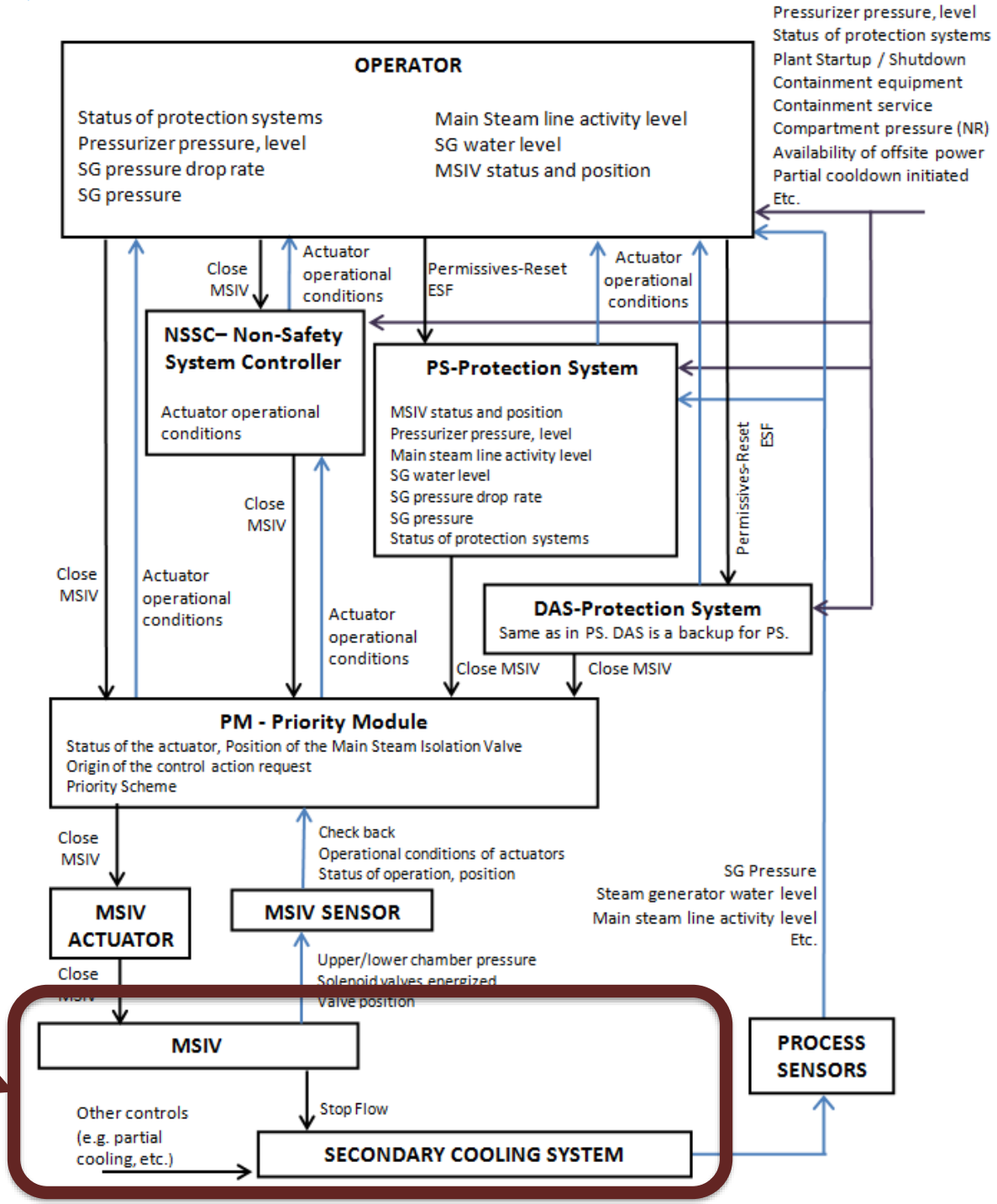
Real safety issue identified



Traditional Security

How do you make this secure?

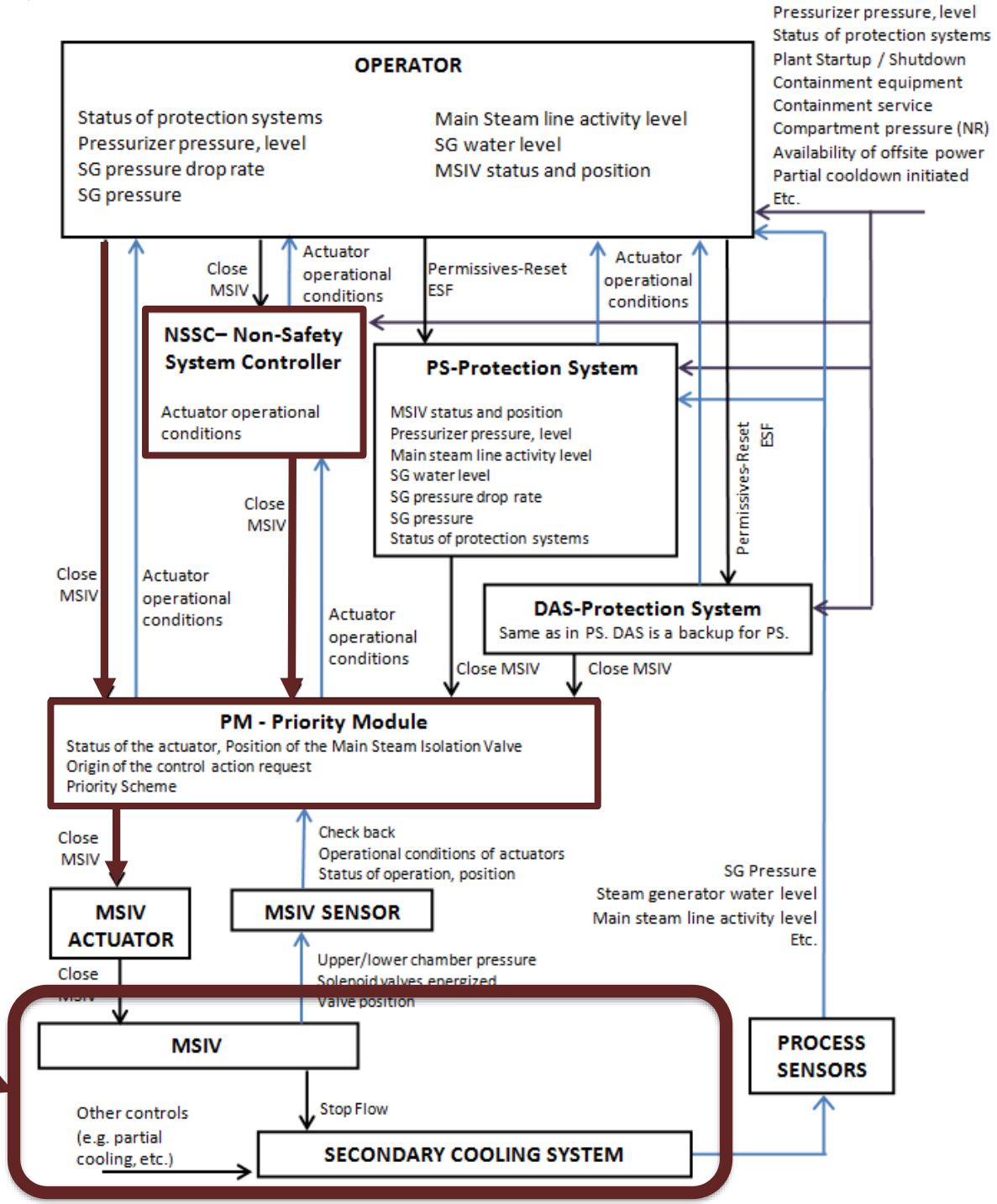
Physical security:
Add physical barriers
"Guards, gates, guns"



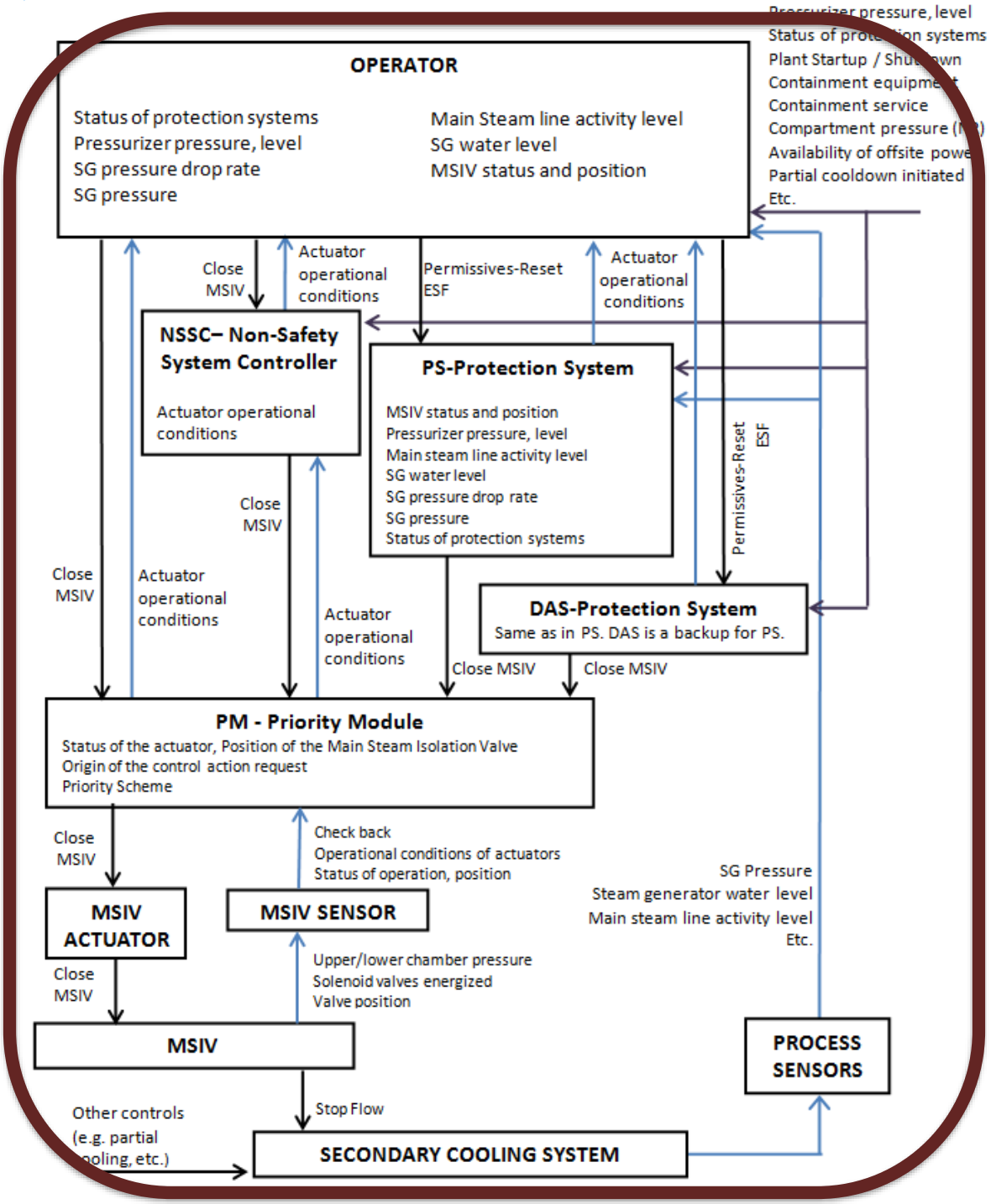
Traditional Security

Cybersecurity:
Protect computers, networks, etc.

Physical security:
Add physical barriers
"Guards, gates, guns"



Traditional Security



Conclusions

- Structured way to build scenarios
- Top-down approach
  - Start with basic scenarios, then add detail to refine them
  - Quicker than 100s of detailed scenarios
  - Focuses on fundamental issues first
- Scenarios can be easily combined
- Basic scenarios can be automatically generated from UCAs!
- Still need human creativity and expertise to refine scenarios, help identify UCAs, etc.