Massachusetts Institute of Technology

When STPA Results Surprise You

An industry case study employing STPA, Fault Trees, FMEA, and HAZOP

Dr. John Thomas

Engineering Systems Lab

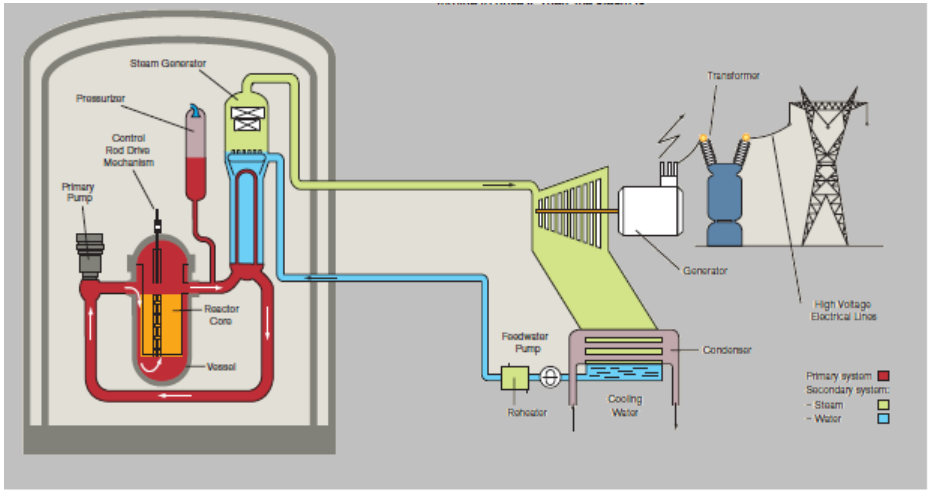
MIT

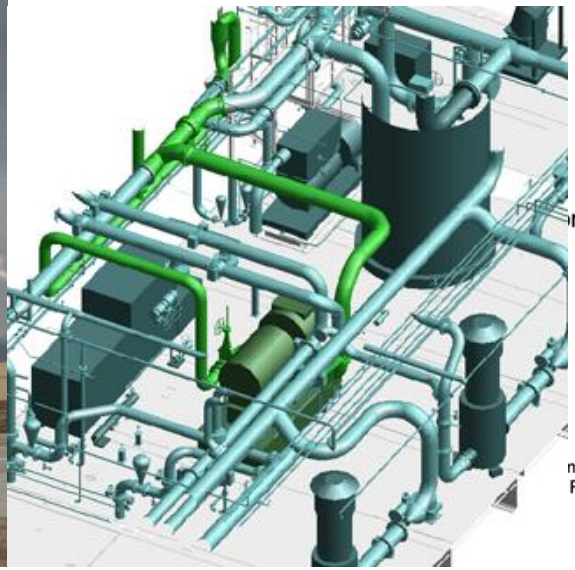
Disclaimer

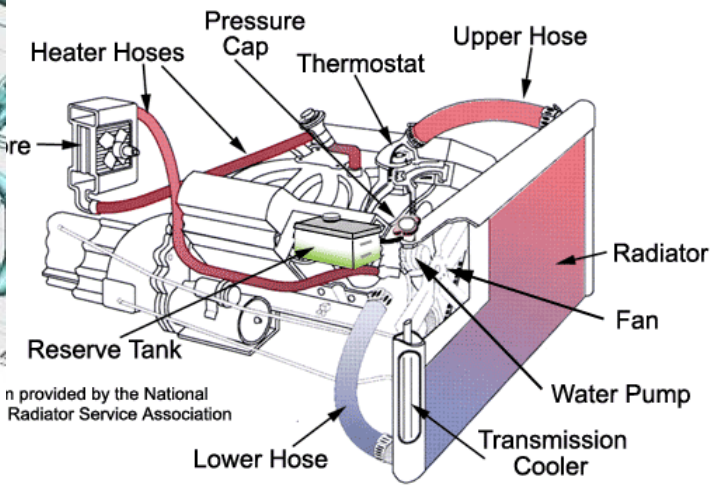
This is a fictional system. It is representative of flaws that have been overlooked in real systems across all industries.

This presentation is not meant to exhaustively demonstrate STPA. The STPA results presented are selected to show key differences between methods.

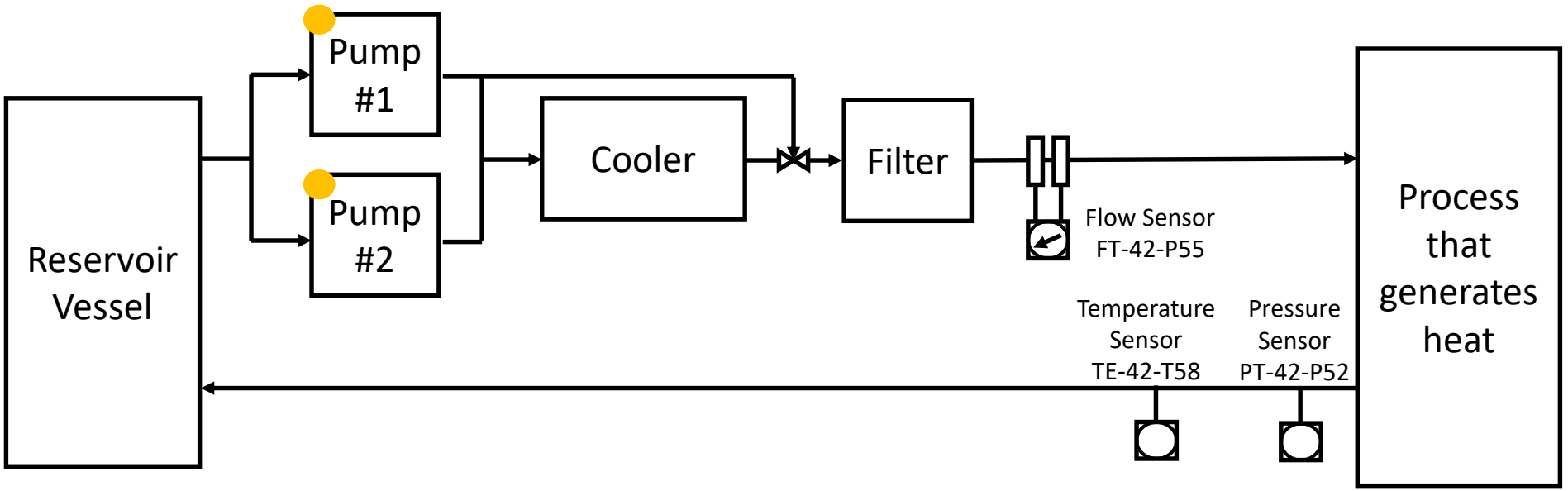
Examples of Cooling systems





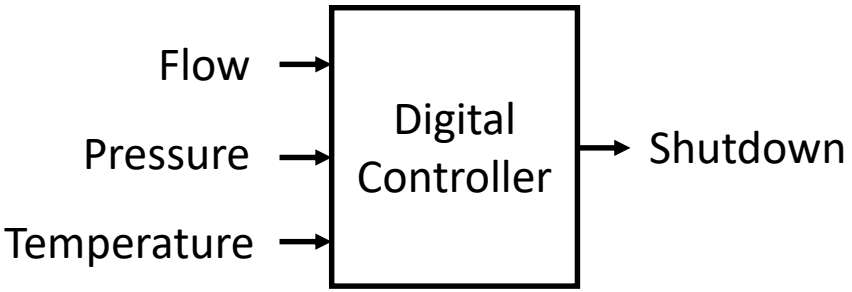


Cooling System (Old System)



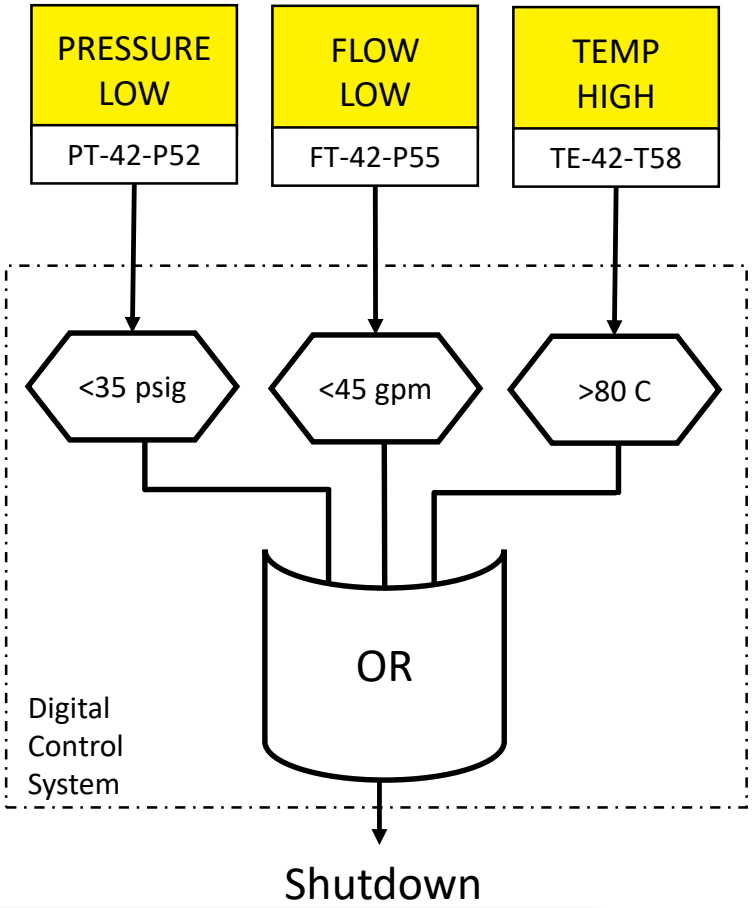
Each pump sized for 100% capacity
Second pump on standby

Manual Control (Maintenance)



Loss of Cooling detection
Old System

- Controller applies a threshold to each sensor
  - Pressure below 35 psig
  - Flow below 45 gpm
  - Temp above 80 C
- Shutdown any time inadequate cooling condition is indicated
  - Low pressure
  - Low flow
  - High temp



Problem: Inadvertent Shutdown (from single sensor failure)
~$1m economic loss **each time**

Digital Modification

Purpose:

- To resolve the problems associated with the existing control systems, each existing system is replaced with a new, state-of-the-art, Digital Control System (DCS).
- These new systems employ, as a minimum, redundant input signal devices, redundant digital signal processors, and redundant output devices.

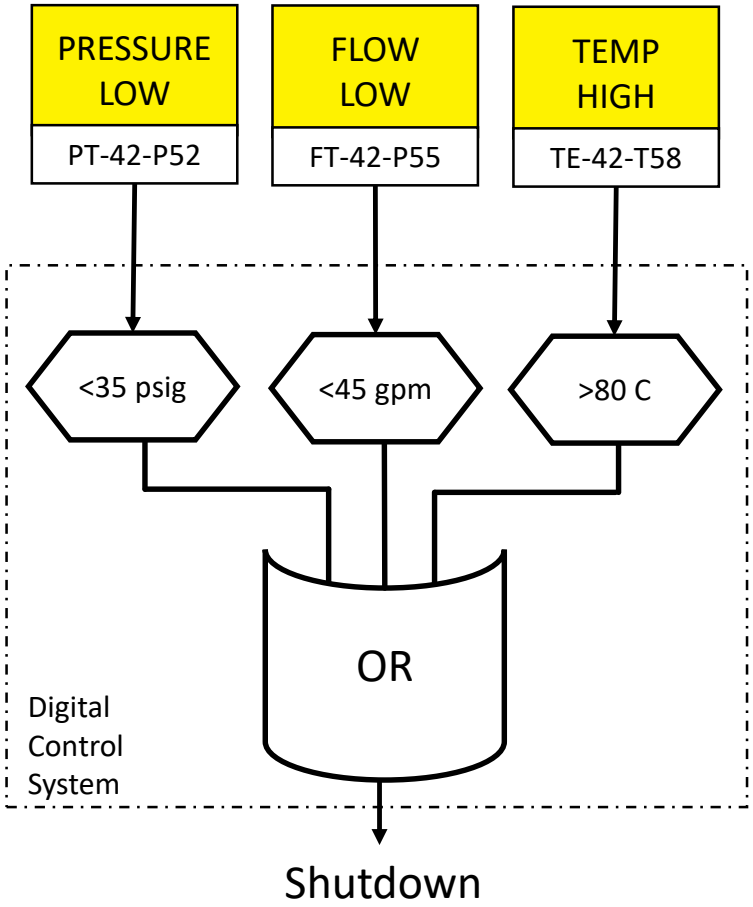
System Requirements Spec:

- DCS will include, among other parameters, protection from **loss of cooling**, which will be measured by low cooling flow, low cooling pressure, or high cooling temperature. DCS will provide automatic Shutdown on loss of cooling.
- The system will identify faulted instruments and will have protection from actuation of any of the shutdown features, including cooling flow, due to a faulted instrument. The system will send a shutdown signal if all instruments for a given parameter are faulted.

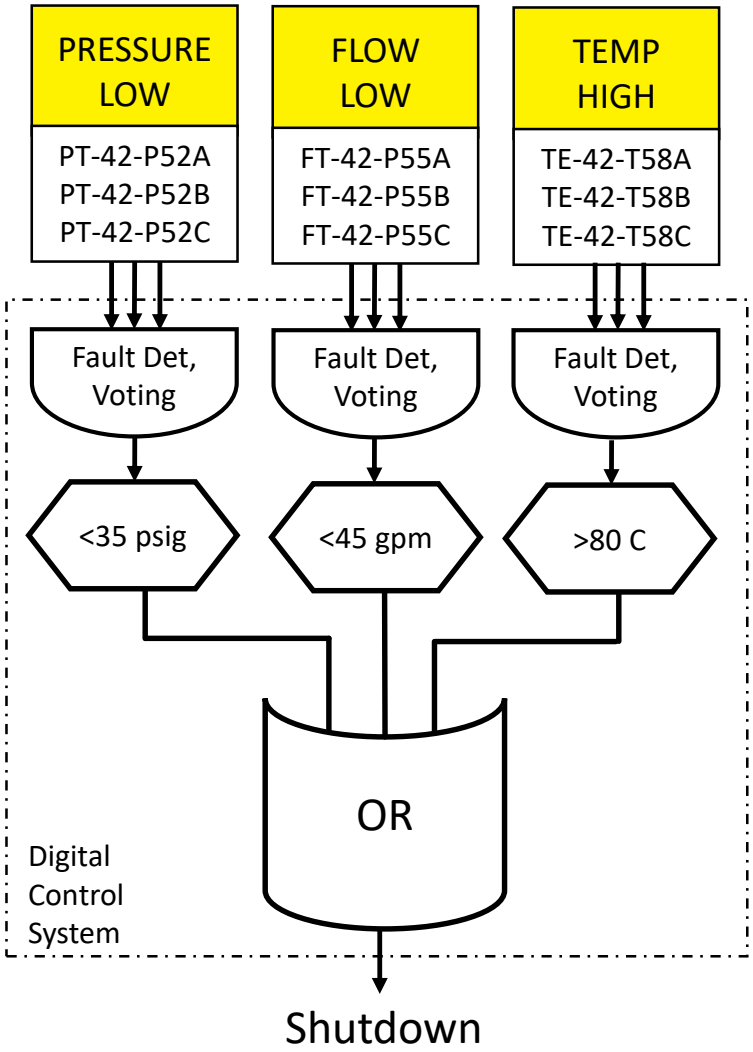
Cost to upgrade: ~$1m
Worth it to prevent an Inadvertent Shutdown!

Loss of Cooling detection

Old System



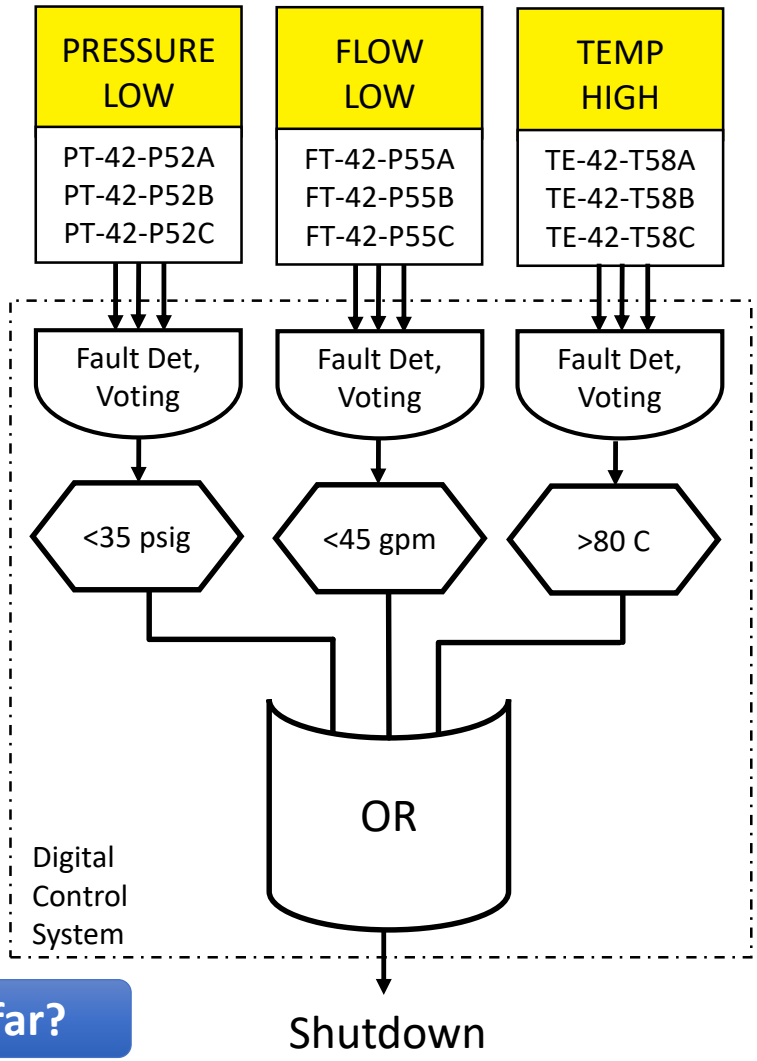
New System



Loss of Cooling detection:
New System

Fault detection and voting

- The Digital Controller will detect faulted instruments and automatically remove them from the logic.
- The logic is designed to identify a faulted instrument by measuring the output either high or low outside the calibrated range.
- 1oo3 logic is used: When one instrument is faulted, it is automatically bypassed by the logic. Bypassing an instrument automatically changes the voter logic to use the remaining two instruments. If a second instrument is faulted, it is also automatically bypassed and the voter logic uses the remaining valid instrument. Finally, if all three instruments are faulted, the logic is designed to send a shutdown signal.
- The setpoints for detection of faulted instrument are 3.8 mA low and 20.32 mA high.



Does this make sense so far?

HAZOP (actual)

- 120 person-hours total


HAZOP WORKSHEET (generator Cooling Circuit)

HAZOP Excerpt (simplified)

Parameter	Guideword	Deviation	Cause	Effect	Protective Systems
Temperature	Higher	Temp. above 84 C	Coolant Blockage, Process overheating, etc.	Damage to Equipment, Loss of Production, etc.	DCS logic, 3x temp sensors
Temperature	Lower	Temp. below 50 C	Process underheating, etc.	No meaningful effect (low temp is good)	
Flow	Higher	Flow above 50 gpm	Both pumps on simultaneously	No meaningful effect (high flow is good)	
Flow	Lower	Flow below 45 gpm	Coolant Blockage, etc.	Damage to Equipment, Loss of Production, etc.	DCS logic, 3x flow sensors

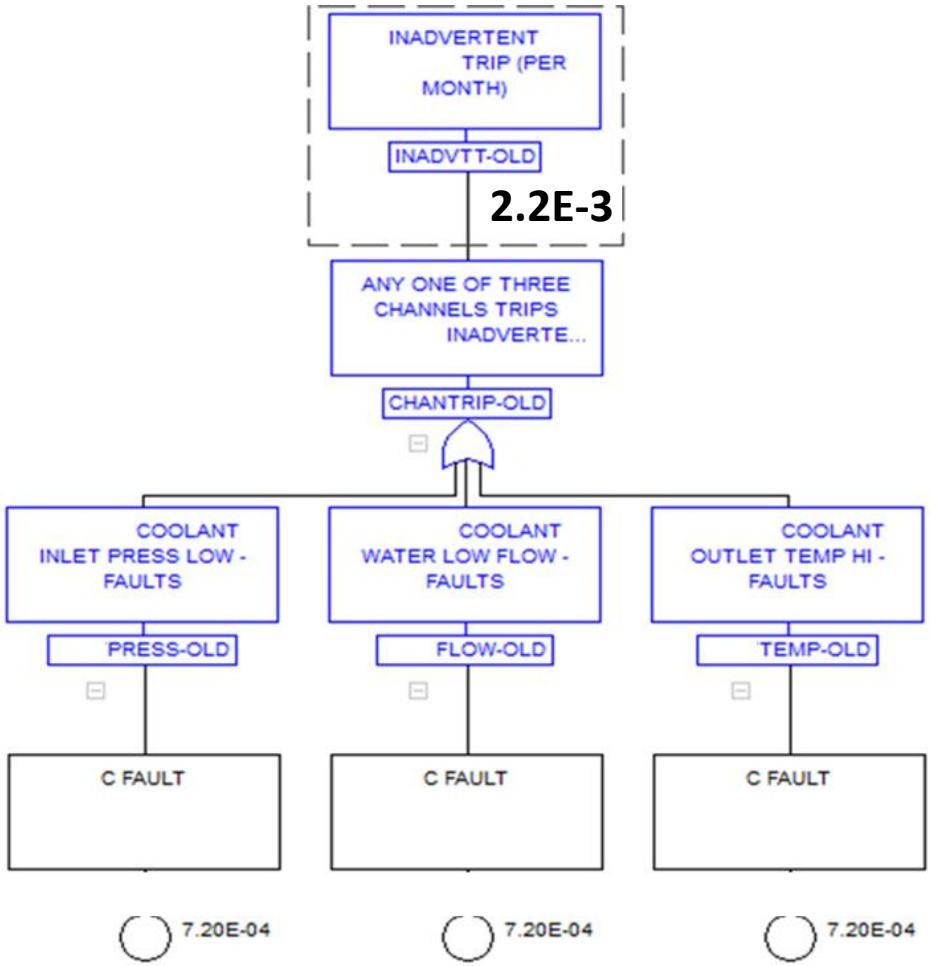
Actual HAZOP: 120 person-hours total

FMEA Excerpt (simplified)

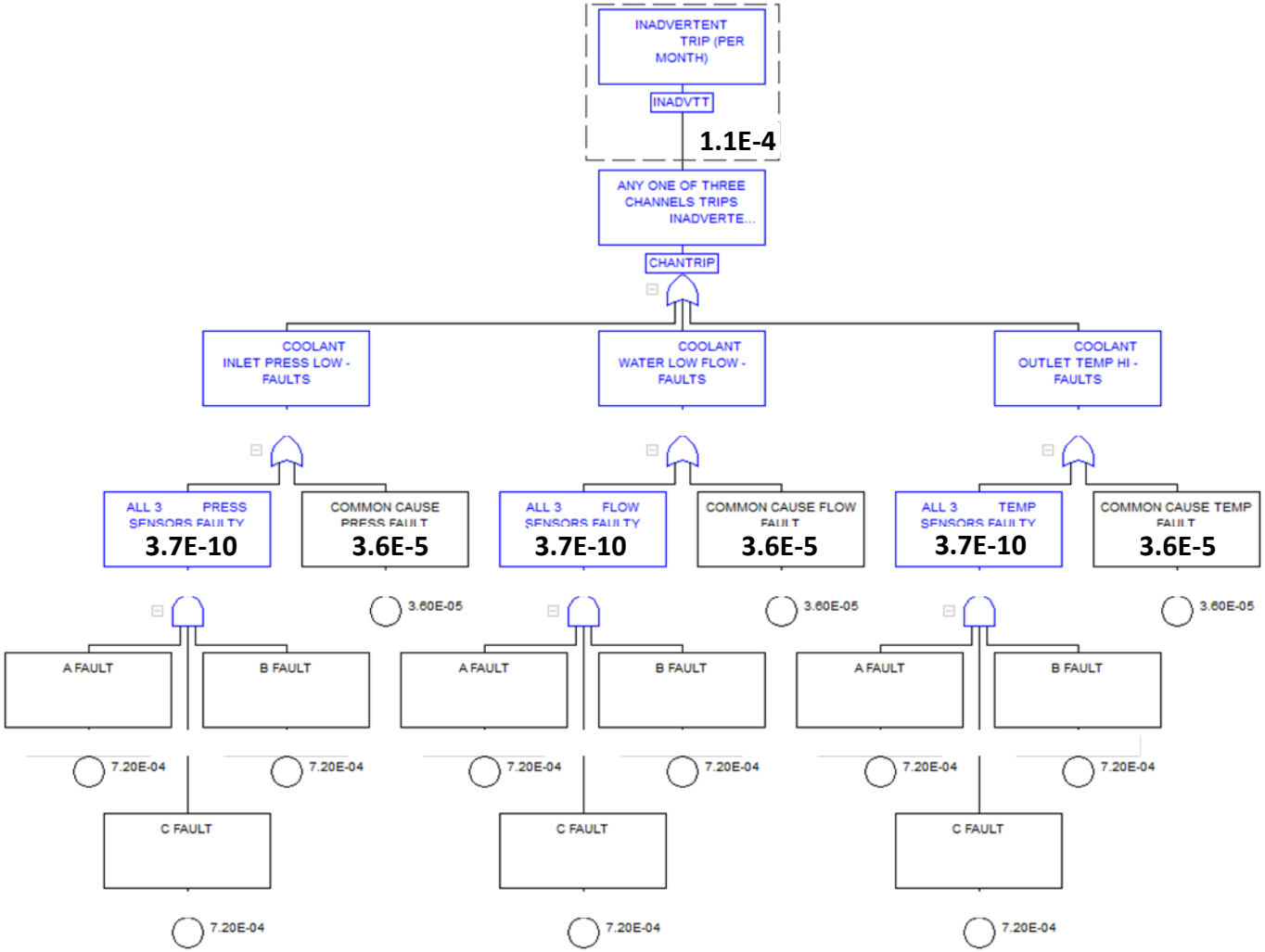
Component	Failure Mode	Failure Mechanism	Effect	Mitigations
Temperature Sensor TE-42-T58	Fail high	[…]	Unnecessary shutdown by DCS (false positive)	3x Temp Sensors, DCS logic protects from single or dual sensor failures
Temperature Sensor TE-42-T58	Fail low	[…]	Undetected loss of cooling: Damage to equipment, Loss of production (false negative)	3x Temp Sensors, DCS logic protects from single or dual sensor failures
Flow Sensor FT-42-P55	Fail high	[…]	Undetected loss of cooling: Damage to equipment, Loss of production (false negative)	3x Flow Sensors, DCS logic protects from single or dual sensor failures
Flow Sensor FT-42-P55	Fail low	[…]	Unnecessary shutdown by DCS (false positive)	3x Flow Sensors, DCS logic protects from single or dual sensor failures

Actual FMEA: 200+ pages, 1,000+ person-hours

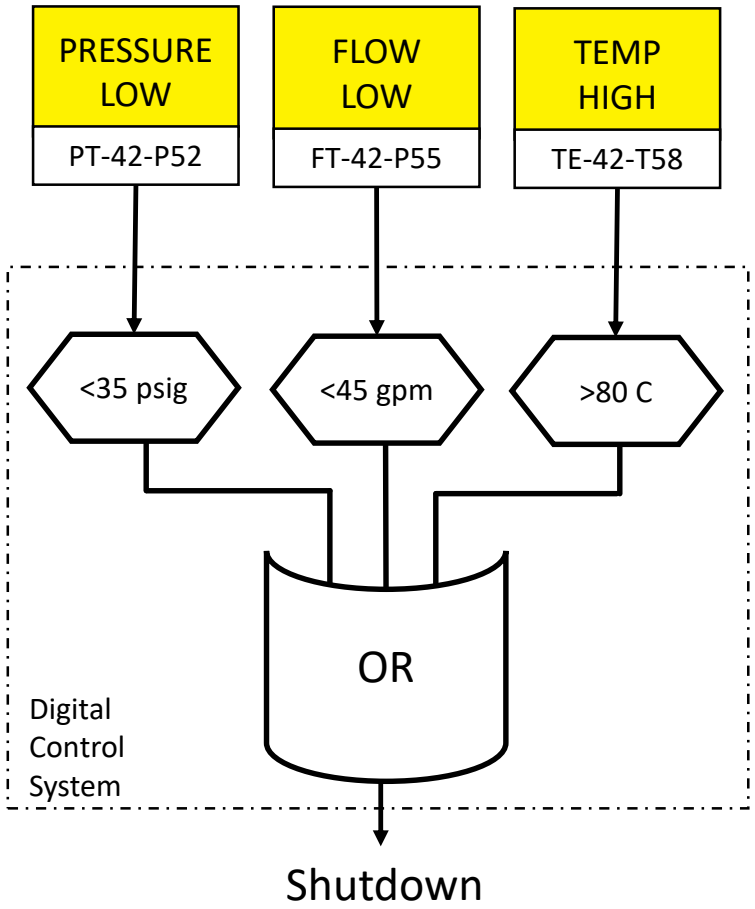
Loss of Stator Cooling detection
Old System



Loss of Cooling detection:
New System



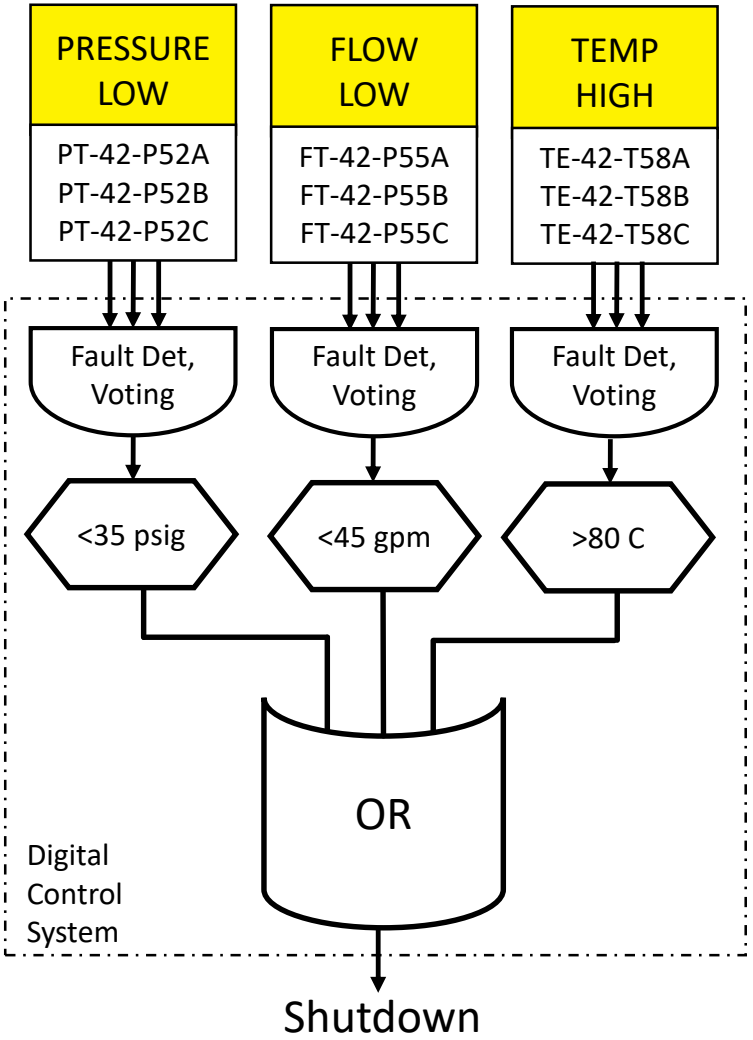
Old System



$P(IS/m) = 2.2 \times 10^{-3}$

(~Once in 38 years)

New System

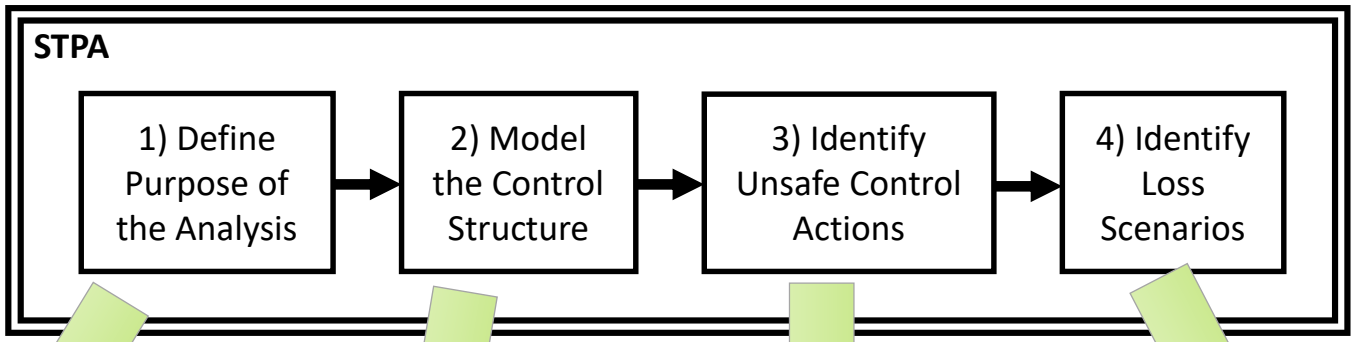


$P(IS/m) = 1.1 \times 10^{-4}$

(~Once in 757 years)

IS = Inadvertent Shutdown

Let's try STPA!

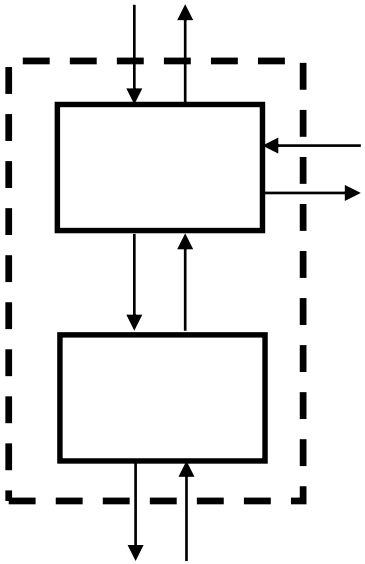


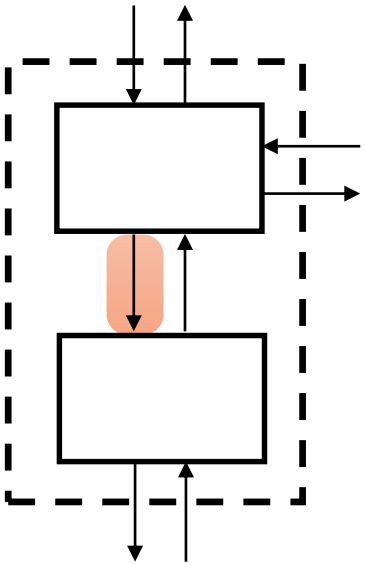
Identify Losses, Hazards

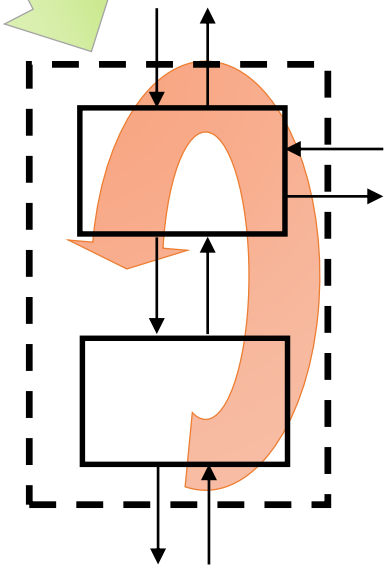
Define System boundary

Environment

System







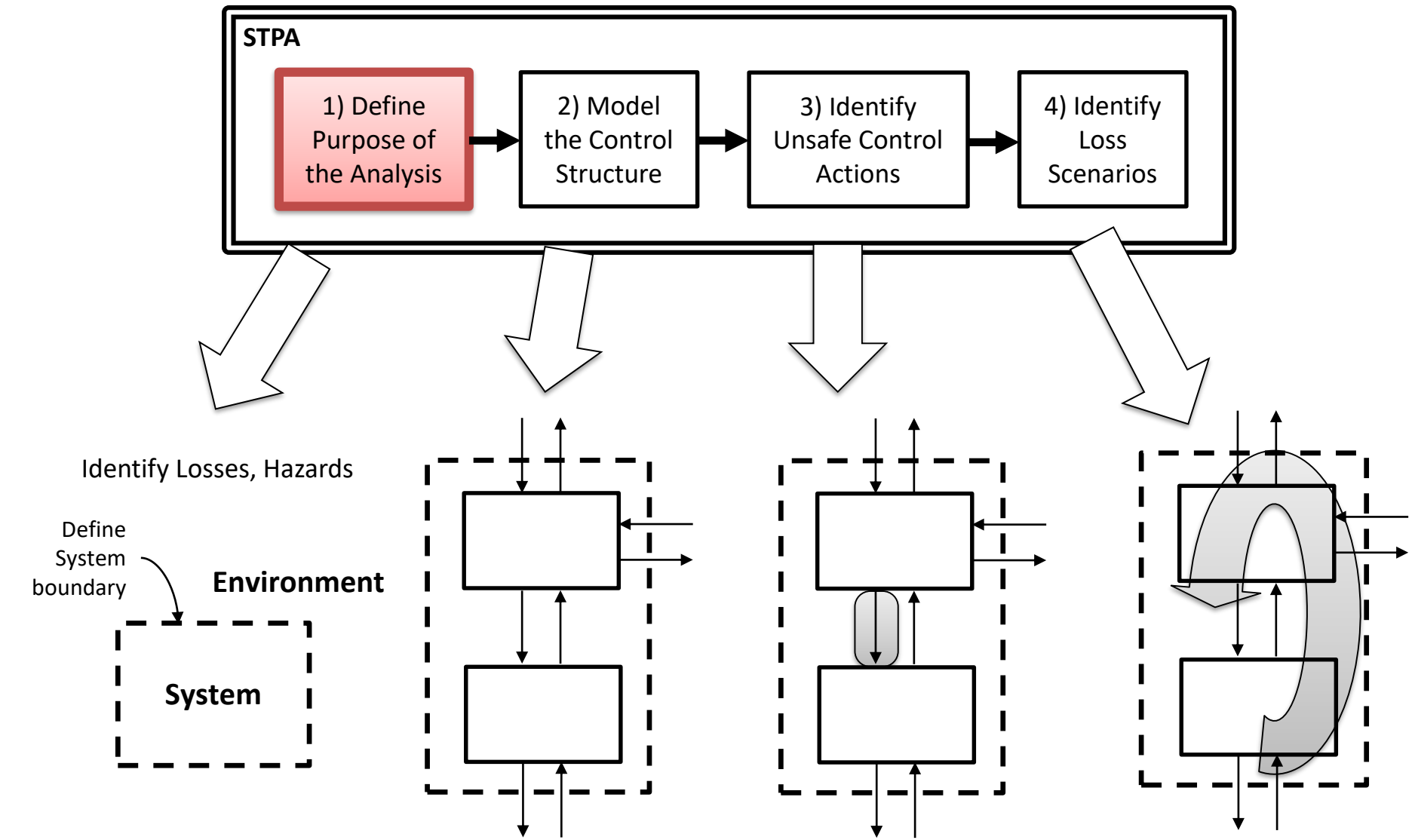
Losses to prevent

Model

Behavior to prevent

How could behavior occur

(Leveson and Thomas, 2018)

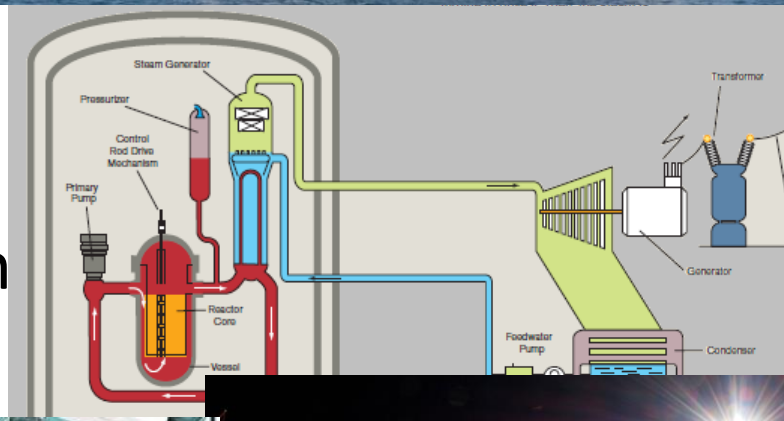


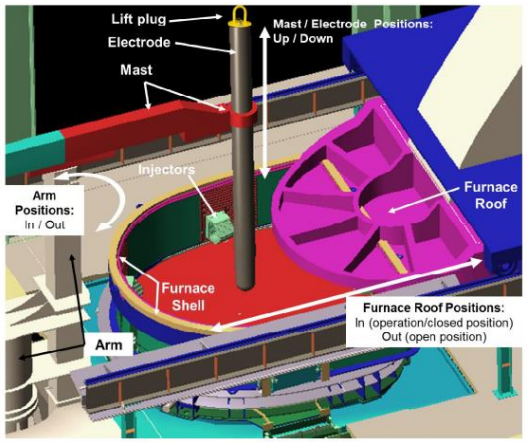
(Leveson and Thomas, 2018)

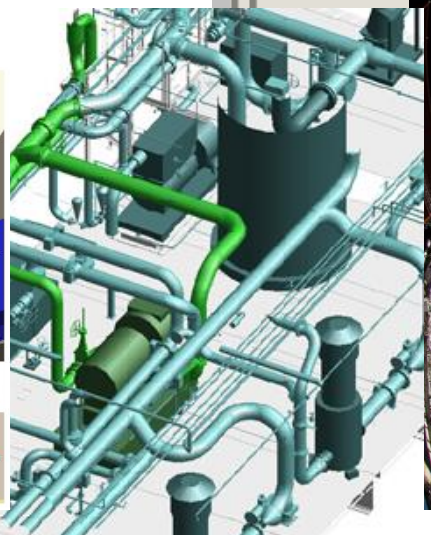
STPA Losses

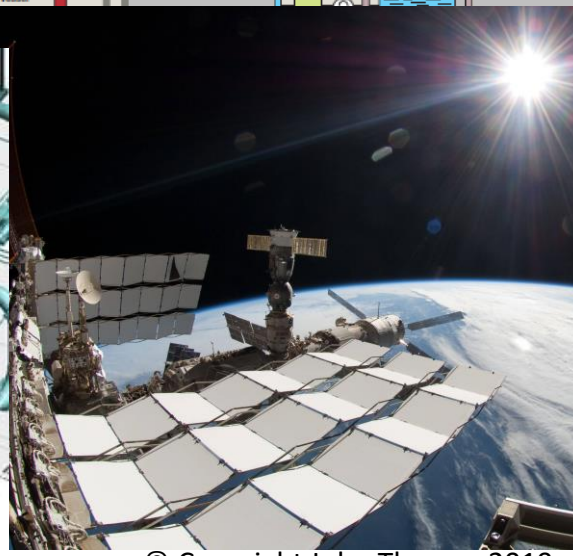
Example Losses

- L-1: Loss of life or injury
- L-2: Equipment damage
- L-3: Environmental contamination
- L-4: Loss of mission
- Etc.

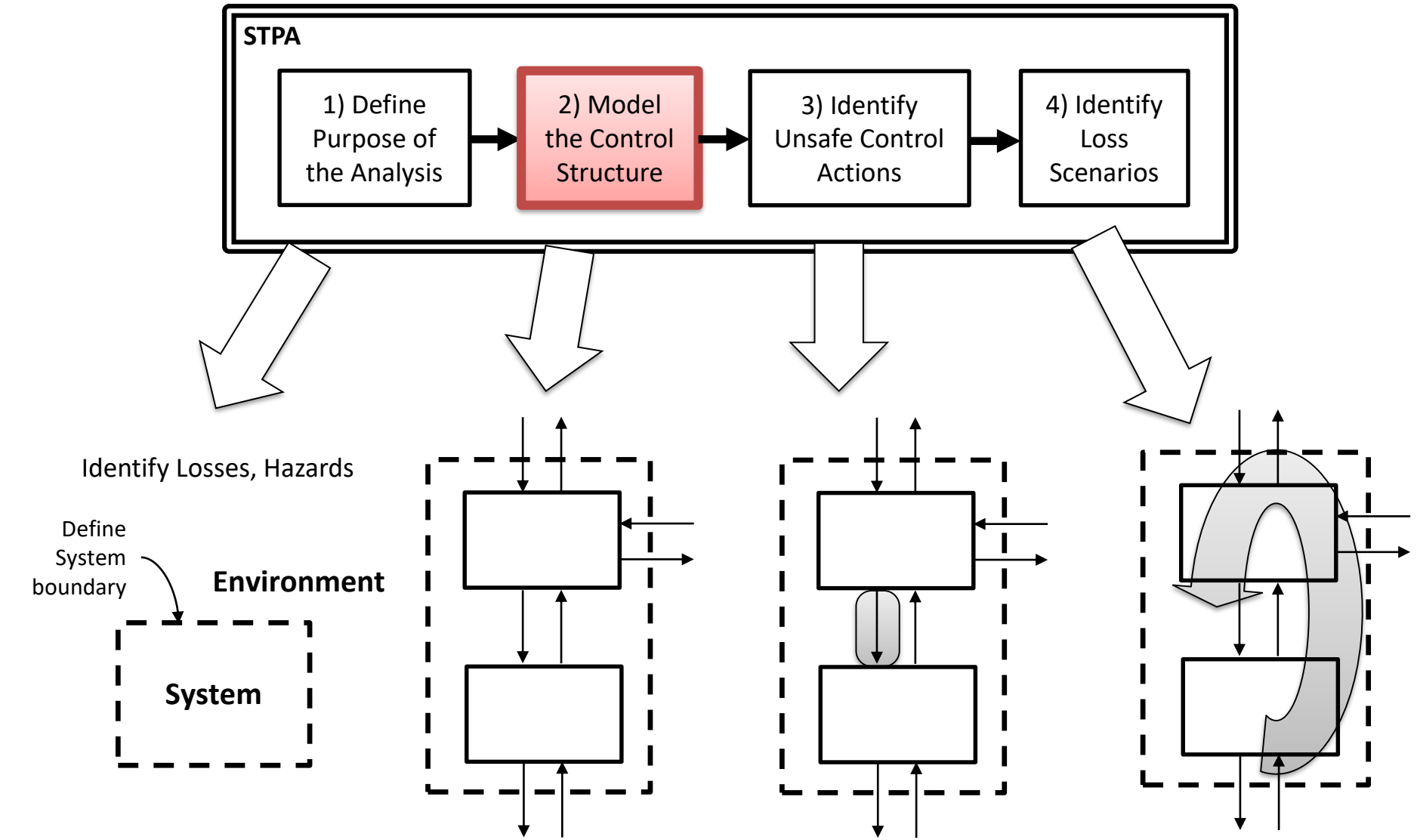






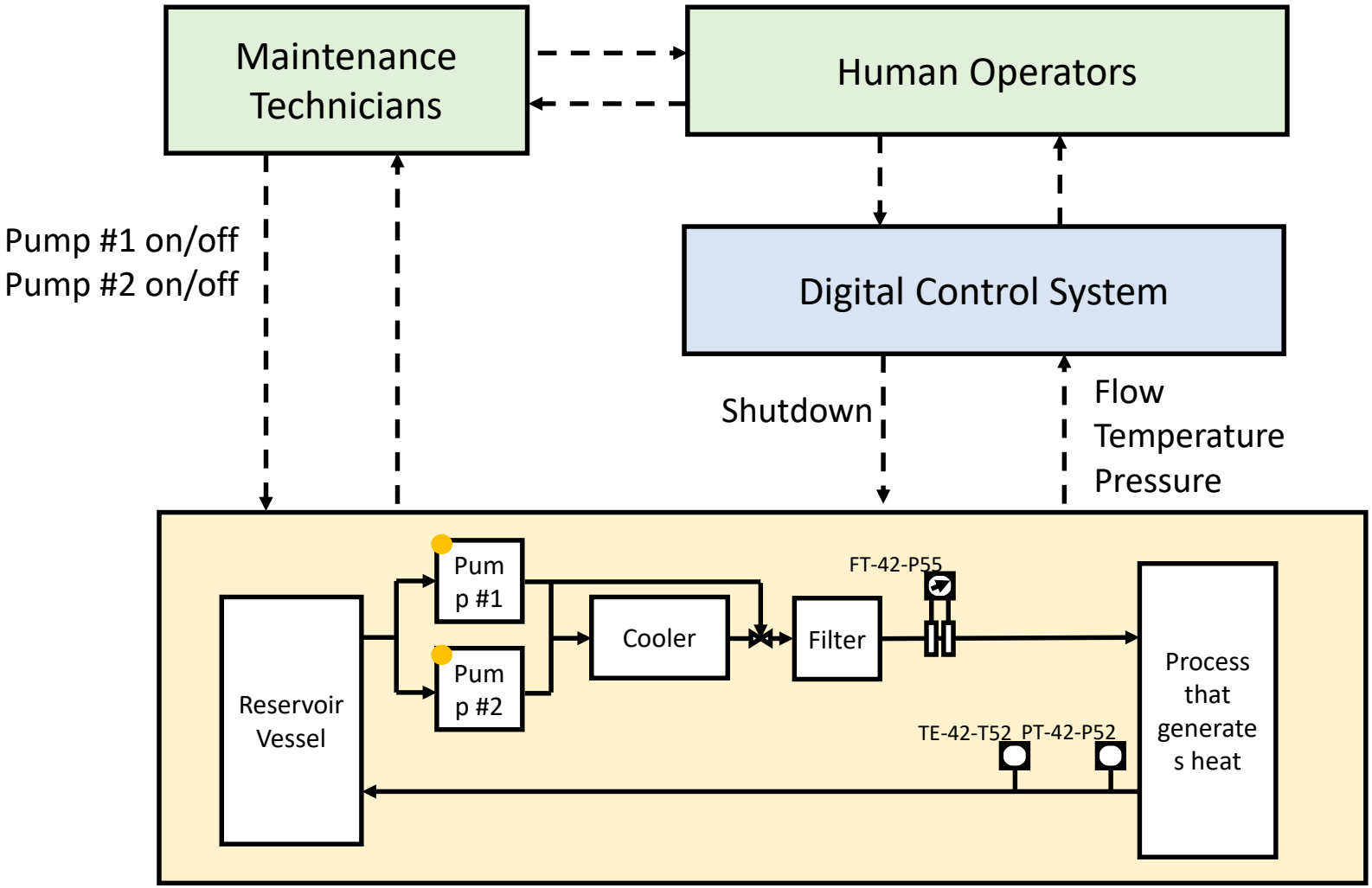


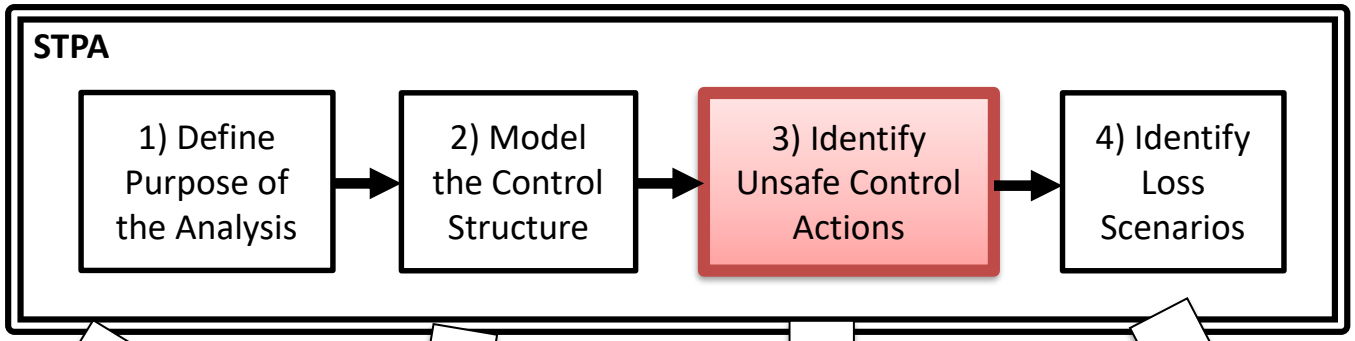
(John Thomas, 2014)



(Leveson and Thomas, 2018)

Control Structure



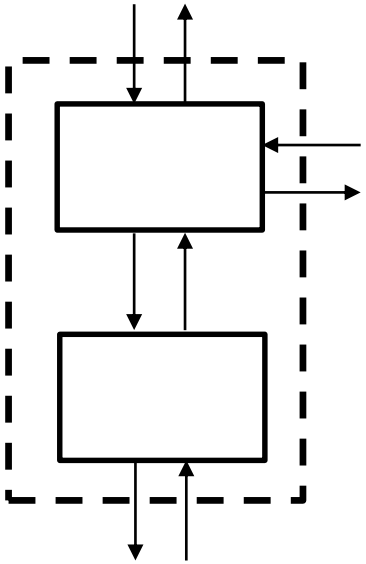


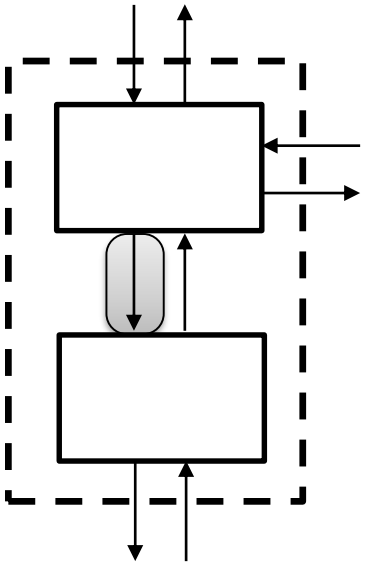
Identify Losses, Hazards

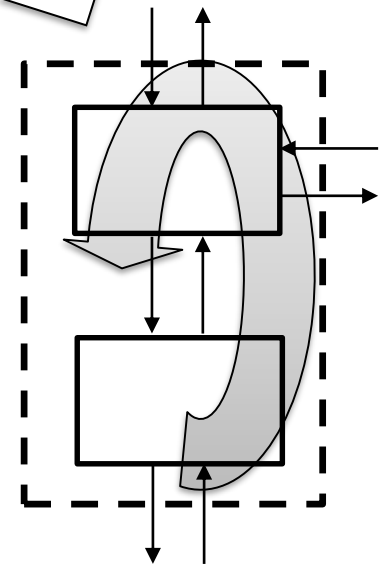
Define System boundary

Environment

System





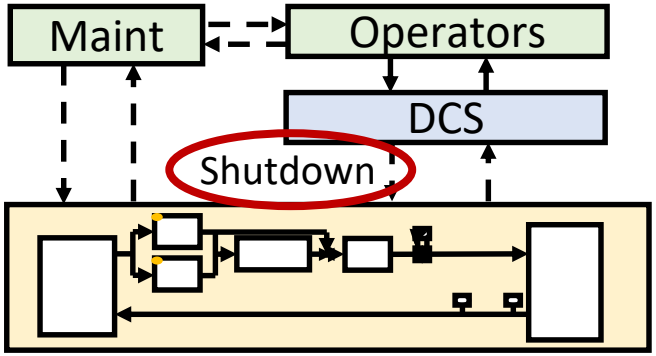


(Leveson and Thomas, 2018)

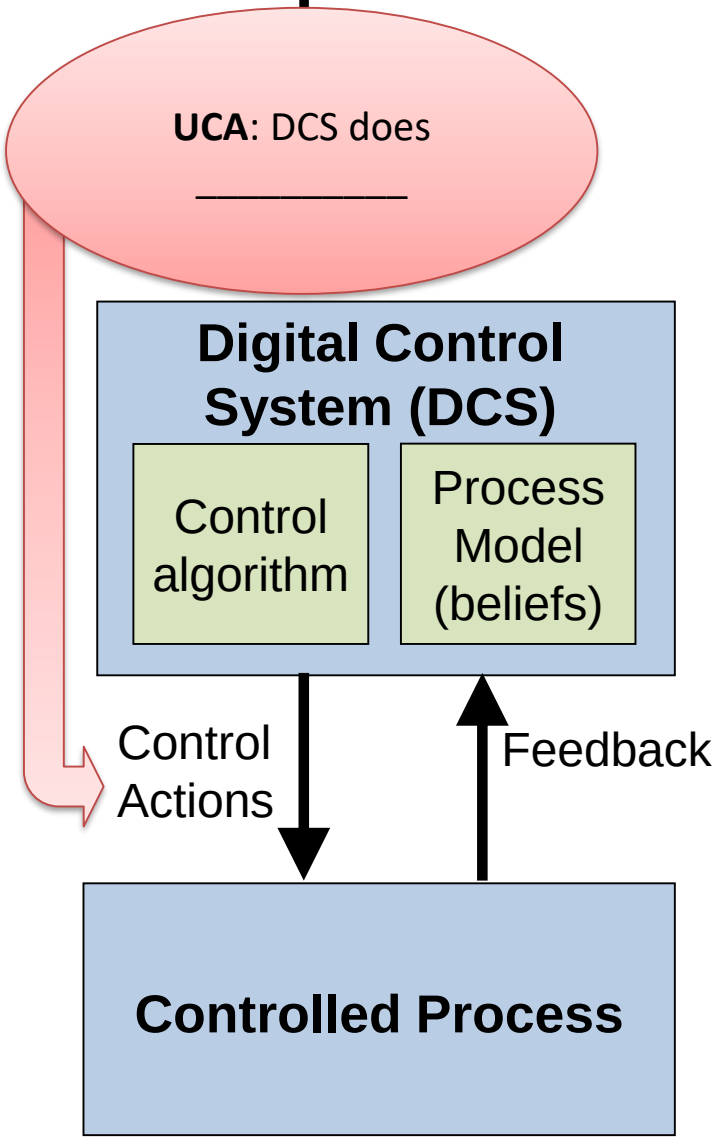
Asking the right questions

Loss: Loss of Mission (unnecessary shutdown)

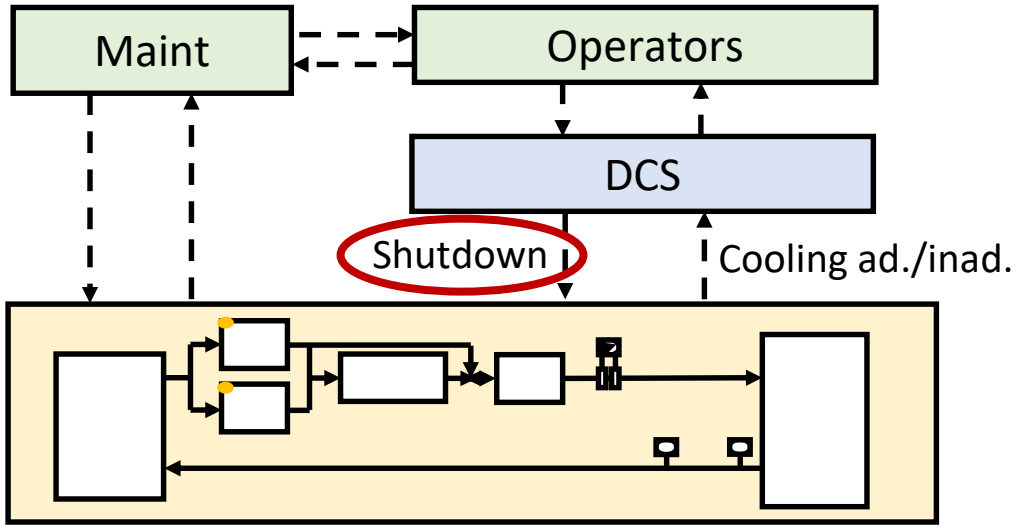
Question: What DCS control actions can cause unnecessary shutdown?



UCA: DCS does _____

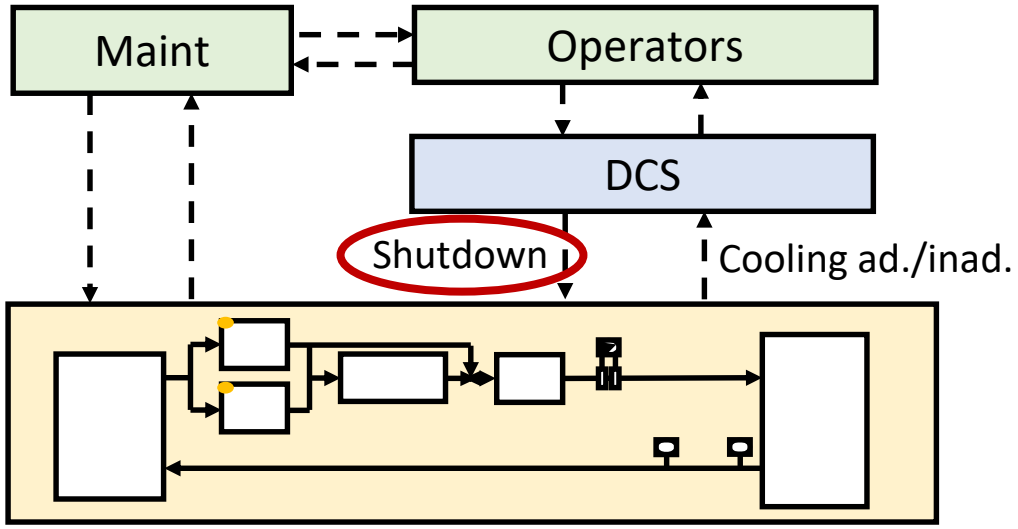


Unsafe Control Actions



	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped Too Soon / Applied too long
Shutdown Cmd				

Unsafe Control Actions

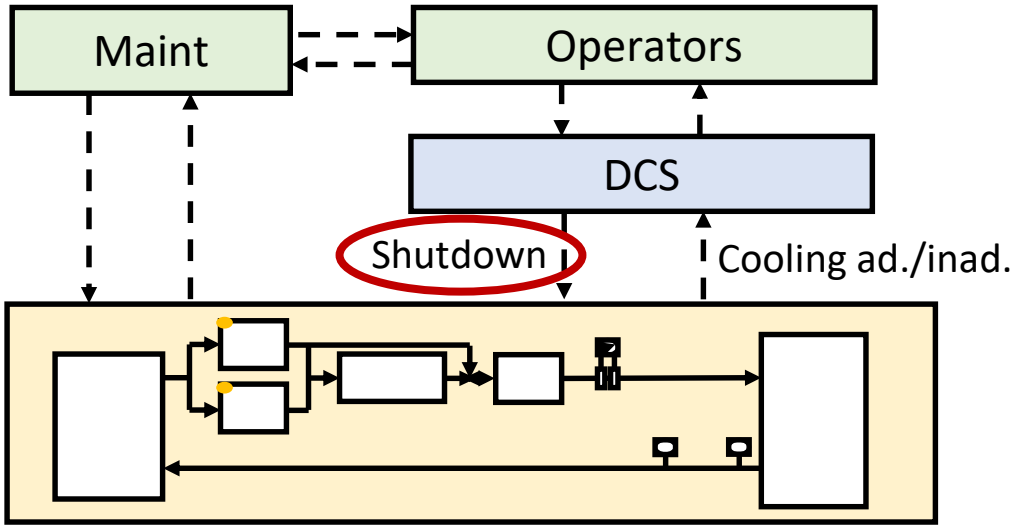


L-1: Loss of life or injury
L-4: Loss of mission (unnecessary shutdown)

	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped Too Soon / Applied too long
Shutdown Cmd	**Controller does not provide Shutdown Cmd when _____**	**Controller provides Shutdown Cmd when _____**	**Controller provides Shutdown Cmd before _____ Controller provides Shutdown Cmd after _____**	**Controller continues providing Shutdown Cmd too long after_____**

Note: This short example is incomplete, for demonstration only!

Unsafe Control Actions



	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped Too Soon / Applied too long
Shutdown Cmd	**Controller does not provide Shutdown Cmd when cooling is inadequate* [H-1]**	**Controller provides Shutdown Cmd when cooling is adequate* [H-2]**	**[…]**	**[…]**

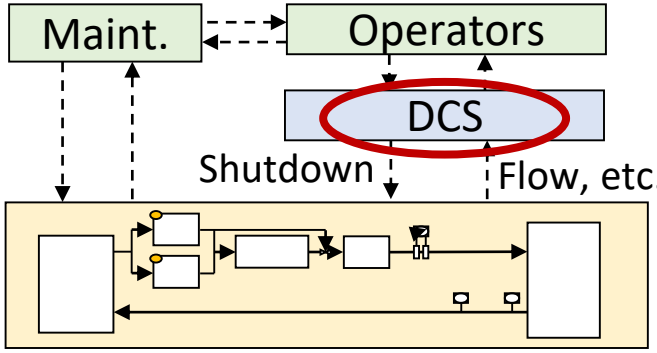
Cooling is inadequate* = low pressure OR low flow OR high temp

Note: This short example is incomplete, for demonstration only!

Asking the right questions

Loss: Loss of Mission (unnecessary shutdown)

Question: What DCS control actions can cause unnecessary shutdown?



UCA: DCS provides Shutdown Cmd when cooling is adequate*

Question: What DCS beliefs would cause it to provide Shutdown Cmd when cooling is adequate?

Digital Control System (DCS)

Control algorithm

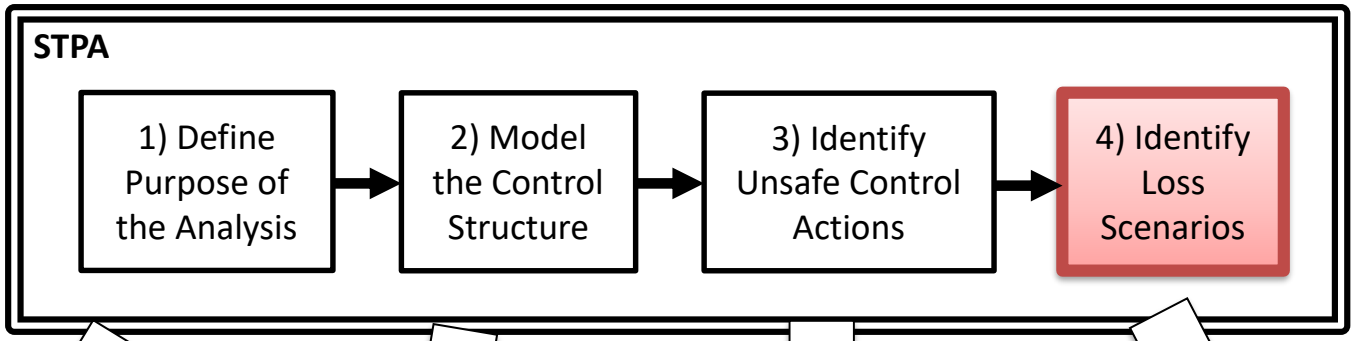
Process Model (beliefs)

Process Model: DCS believes _____

Control Actions

Feedback

Controlled Process

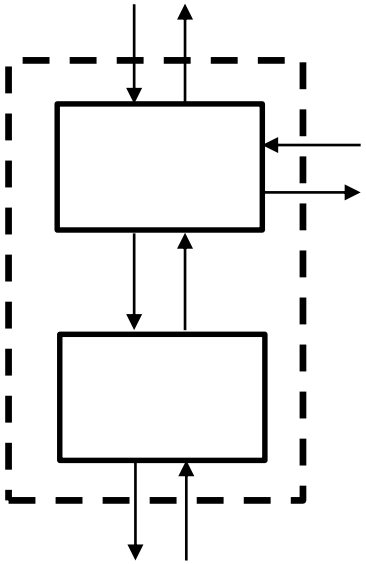


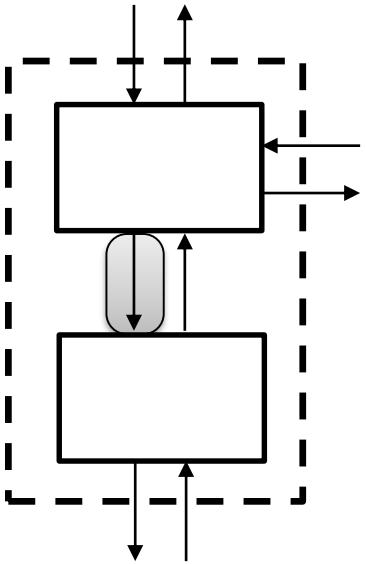
Identify Losses, Hazards

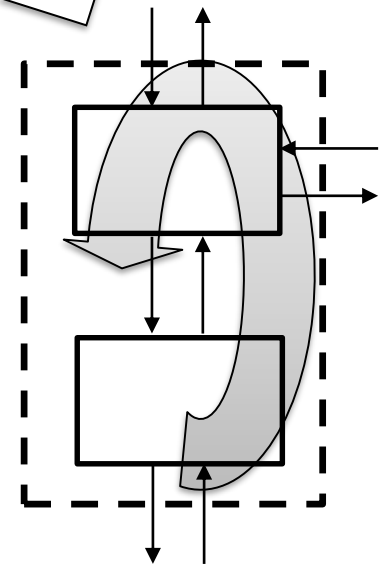
Define System boundary

Environment

System

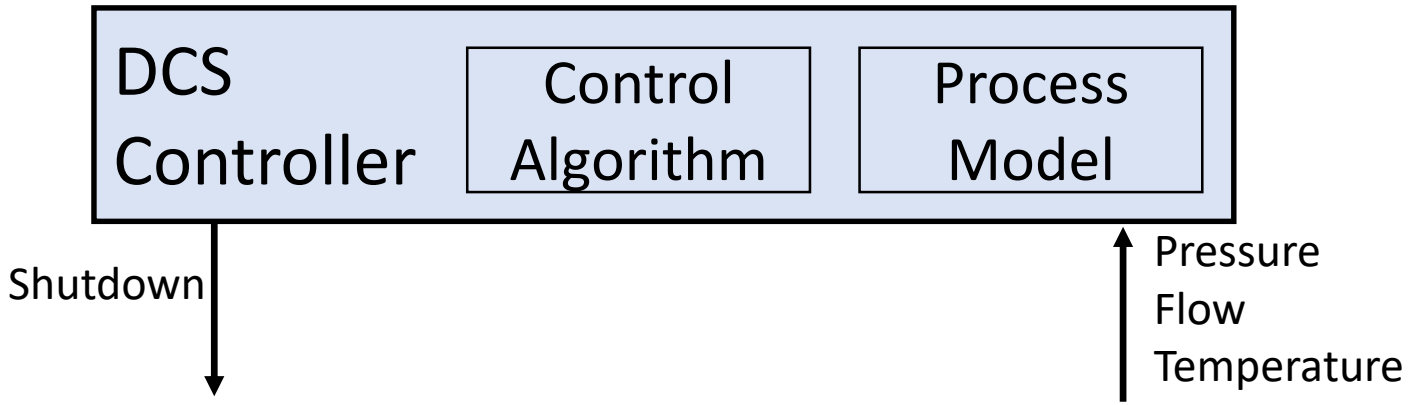






(Leveson and Thomas, 2018)

Controller Analysis (Let's do this together!)



DCS output

UCA-2: DCS provides Shutdown Cmd when cooling is adequate* [H-2]

DCS process model

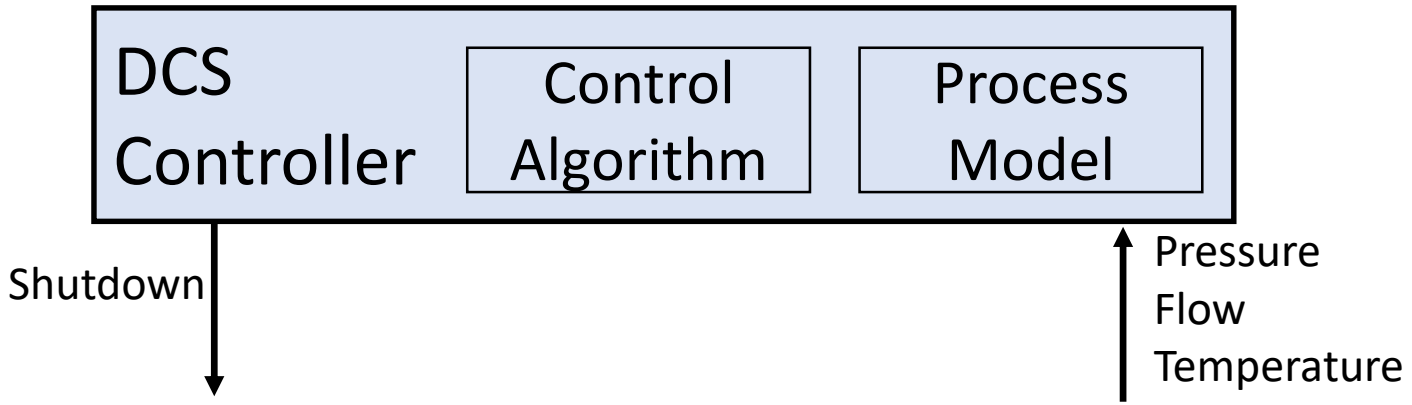
PM-1: Controller believes pressure is too low [UCA-2]

DCS input

F-1: All three pressure sensors report low pressure [PM-1]
< 15.2mA, aka < 45gpm

Note: This short example is incomplete, for demonstration only!

Controller Analysis (Let's do this together!)



DCS output

UCA-2: Controller provides Shutdown Cmd when cooling is adequate* [H-2]

DCS process model

PM-1: Controller believes Pressure is too low

PM-2: Controller believes Flow is too low

PM-3: Controller believes Temperature is too high

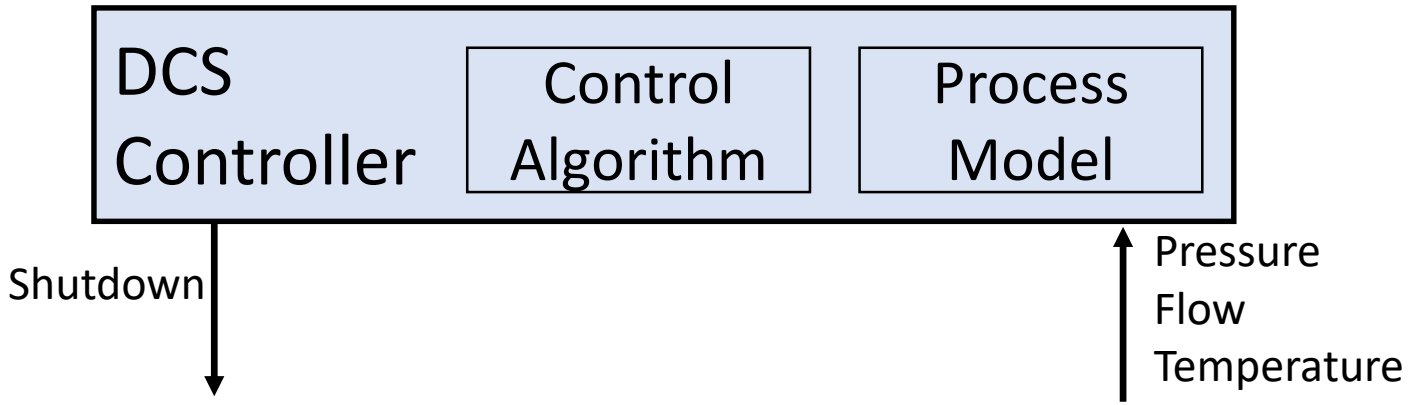
PM-4: Controller believes all three Flow sensors are faulted

DCS input

F-1: ?

Note: This short example is incomplete, for demonstration only!

Controller Analysis (Let's do this together!)



DCS output

UCA-2: Controller provides Shutdown Cmd when cooling is adequate* [H-2]

DCS process model

PM-1: Controller believes Pressure is too low

PM-2: Controller believes Flow is too low

PM-3: Controller believes Temperature is too low

PM-4: Controller believes all three Flow sensors are faulted

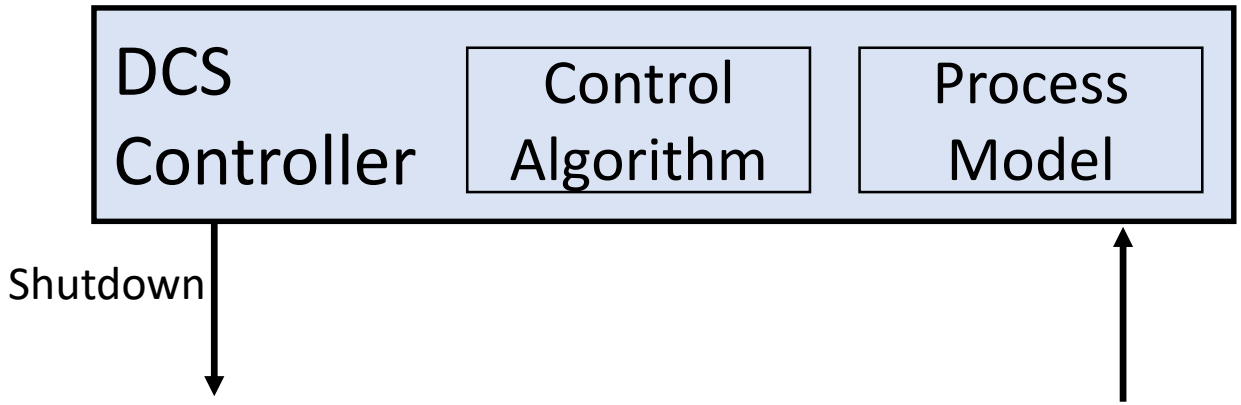
DCS input

F-1: All three flow sensors report out of range low
<3.8mA, aka < 0 gpm

F-2: All three flow sensors report out of range high
>20.38mA, aka ? gpm

Note: This short example is incomplete, for demonstration only!

Controller Analysis (Let's do this together!)



DCS output | **DCS process model** | **DCS input**

UCA-2: Controller provides Shutdown Cmd when cooling is adequate* [H-2]

PM-4: Controller believes all three flow sensors have failed [UCA-2]

F-2: All three flow sensors out of range high [PM-4]
>20.38mA, aka X gpm

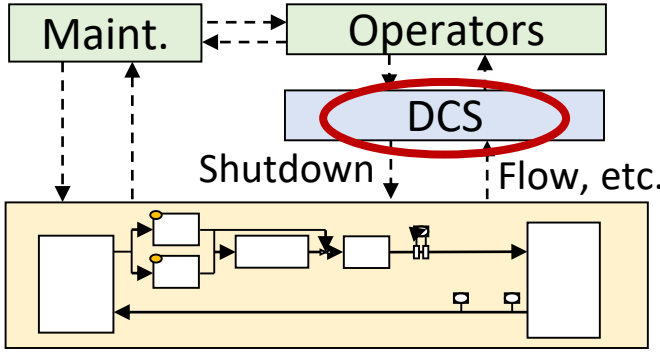
New question: What's X?

(Need to make sure it won't happen inadvertently!)

Note: This short example is incomplete, for demonstration only!

Asking the right questions

Loss: Loss of Mission (unnecessary shutdown)



Question: What DCS control actions can cause unnecessary shutdown?

UCA: DCS provides Shutdown Cmd when cooling is adequate*

Question: What DCS beliefs would cause it to provide Shutdown Cmd when cooling is adequate?

Digital Control System (DCS)

Control algorithm

Process Model (beliefs)

PM: DCS believes all flow sensors are faulted

Question: What DCS inputs would cause DCS to incorrectly believe all flow sensors are faulted?

FB: All Flow Sensors report > 20.32mA (X gpm)

Control Actions

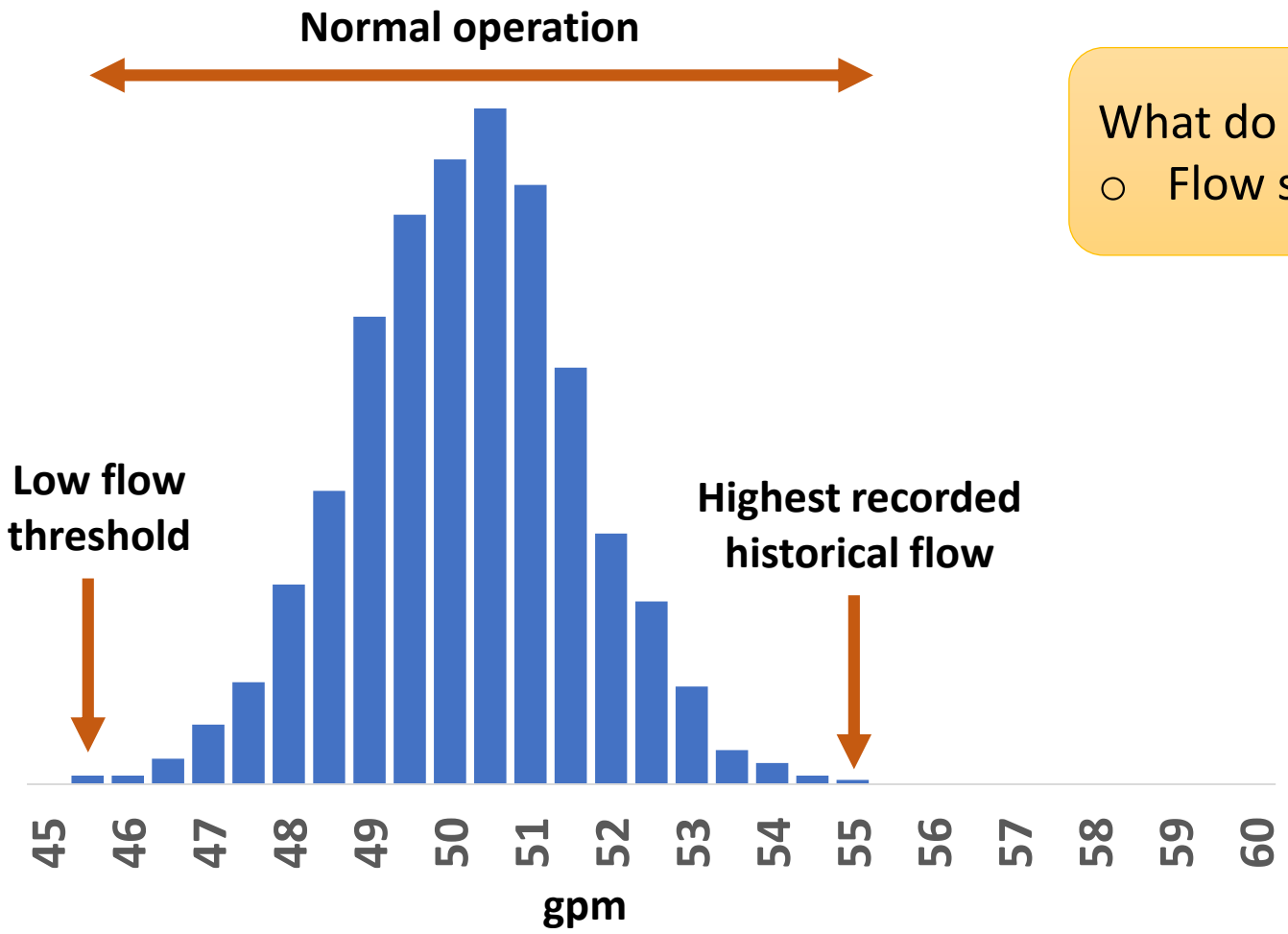
Feedback

Question: What would cause all flow sensors > X gpm when cooling is adequate?

Controlled Process

CP: _____

What is the flow sensor max range?
Answer based on historical data:

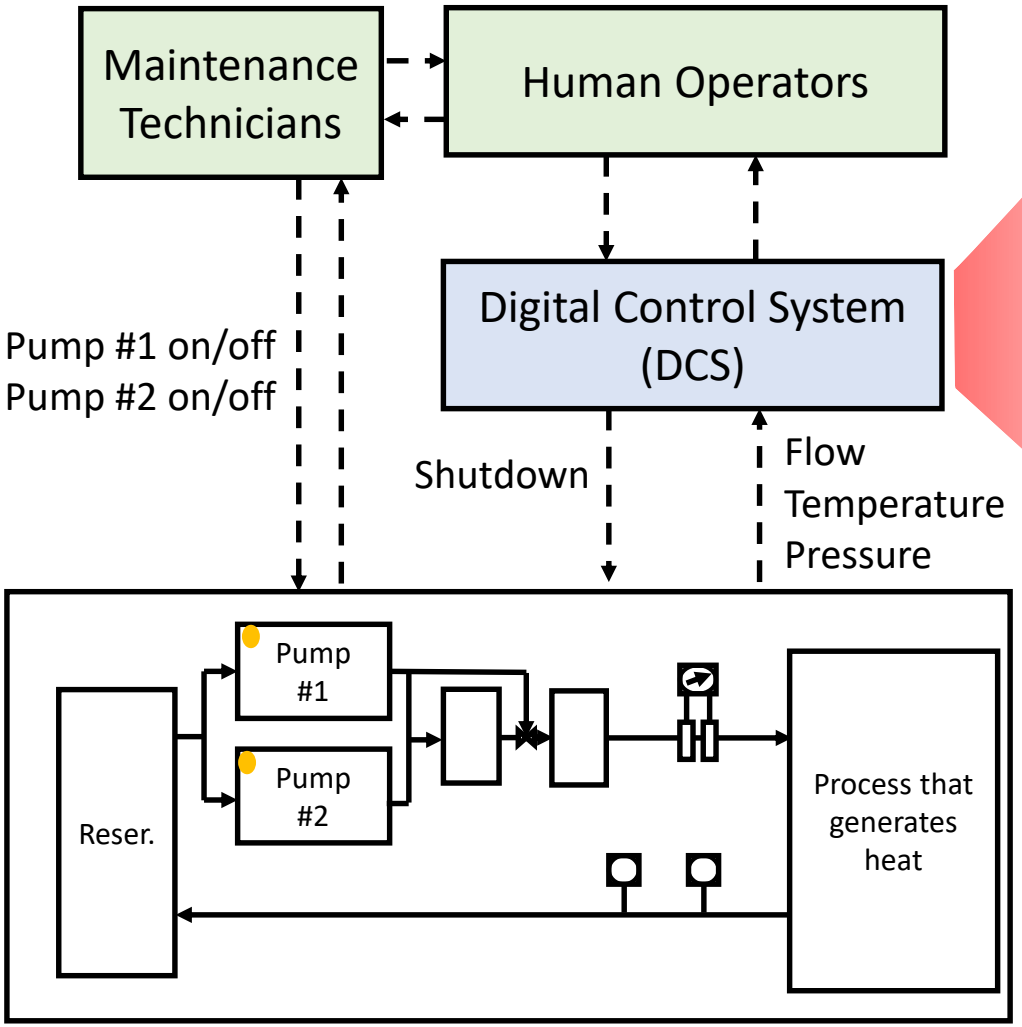


What do you think they chose?

- Flow sensor max: ? gpm

Historical flow data (sampled regularly over many years)

Faulted Instrument Detection

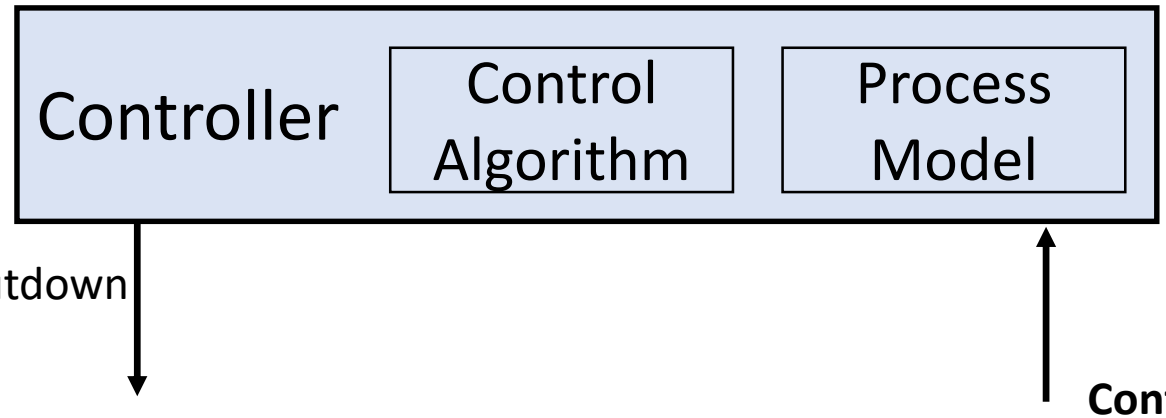


DCS requirements for faulted instrument detection:

Shall detect faulted instrument when signal is:

- <3.8 mA (<0gpm)
- >20.32 mA (>60gpm)

Controller Analysis (Let's do this together!)



Controller output

UCA-2: Controller provides Shutdown Cmd when cooling is adequate [H-2]

Controller process model

PM-4: Controller believes all 3 flow sensors are faulted

Controller input

F-3: all 3 flow sensors indicate high out of range [>20mA; 60gpm]

- **This will occur any time both pumps are running (planned every 9 months)**

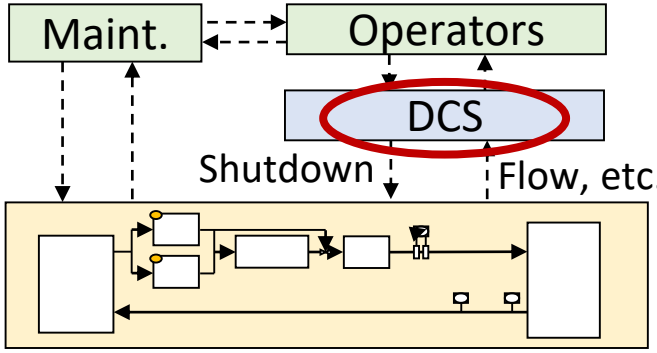
Aha! The design is flawed—components interacting exactly as designed will inadvertently shutdown the system!

This will occur even if all component requirements are met, no components fail, and all human procedures are followed!

Note: This short example is incomplete, for demonstration only!

Asking the right questions

Loss: Loss of Mission (unnecessary shutdown)



Question: What DCS control actions can cause unnecessary shutdown?

UCA: DCS provides Shutdown Cmd when cooling is adequate*

Question: What DCS beliefs would cause it to provide Shutdown Cmd when cooling is adequate?

AHA!

This will occur any time both pumps are running (planned every 9 months)

Digital Control System (DCS)

Control algorithm

Process Model (beliefs)

PM: DCS believes all flow sensors are faulted

Question: What DCS inputs would cause DCS to incorrectly believe all flow sensors are faulted?

FB: All Flow Sensors report >20.32mA, aka >60 gpm

Control Actions

Feedback

Question: What would cause all flow sensors > 60 gpm when cooling is adequate?

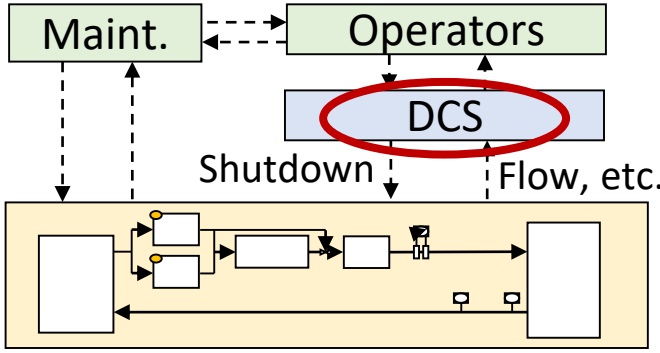
Controlled Process

CP: Both pumps turned on together (maintenance activity)

John Thomas, 2020

Asking the right questions

Loss: Loss of Mission (unnecessary shutdown)



Question: What DCS control actions can cause unnecessary shutdown?

UCA: DCS provides Shutdown Cmd when cooling is adequate*

Question: What DCS beliefs would cause it to provide Shutdown Cmd when cooling is adequate?

PM: DCS believes all flow sensors are faulted

Question: What DCS inputs would cause DCS to incorrectly believe all flow sensors are faulted?

FB: All Flow Sensors report >20.32mA, aka >60 gpm

Question: What would cause all flow sensors > 60 gpm when cooling is adequate?

CP: Both pumps turned on together (maintenance activity)

New upgrade: Expect ~$1m loss every 9 months <u>with no component failures!</u>

Digital Control System (DCS)

Control algorithm

Process Model (beliefs)

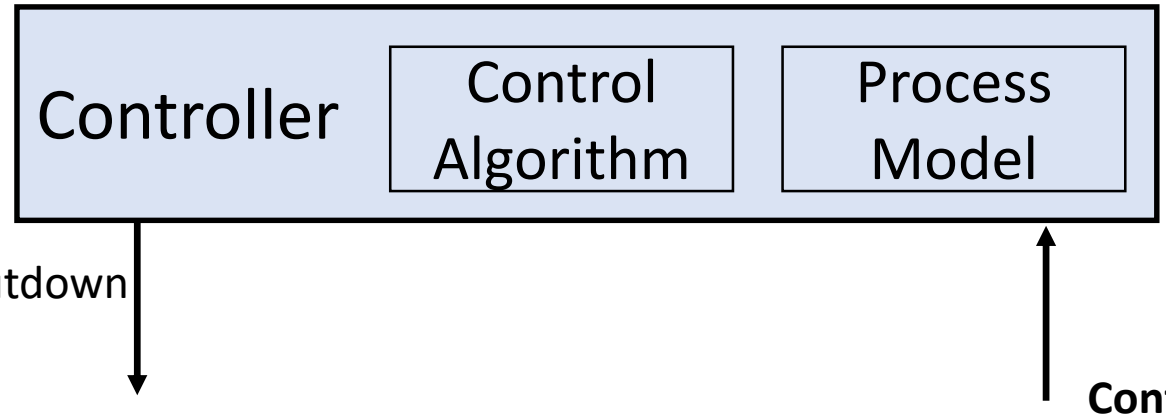
Control Actions

Feedback

Controlled Process

John Thomas, 2020

Controller Analysis (Let's do this together!)



Controller output

UCA-2: Controller provides Shutdown Cmd when cooling is adequate [H-2]

Controller process model

PM-4: Controller believes all 3 flow sensors are faulted

Controller input

F-3: all 3 flow sensors indicate high out of range [>20mA; 60gpm]

- **This will occur any time both pumps are running (planned every 9 months)**

Design solutions?

New requirements?

Maintenance, operator solutions?

Note: This short example is incomplete, for demonstration only!

Hindsight

- These analyses (HAZOP, FMEA, FTA, STPA) were all done blind—without any knowledge of the flaw—by separate teams
- In hindsight and after an incident, we may all find a place to update an old analysis (HAZOP, FMEA, FTA, STPA) to include a newly discovered flaw
- That is not sufficient!
- The challenge we have is NOT whether we can correct omissions in hindsight with full knowledge of the flaws!
- The real challenge—and the real test of any method—is whether the technique consistently discovers these flaws **before an incident**, and before we have the benefit of hindsight!

STPA Consistency

The STPA results have been replicated 7 times

- STPA Team Sizes
  - Ranging from 1 to 4+ people
- STPA Team Backgrounds
  - No prior STPA experience
  - Professionals from process industry
  - Professionals from non-process industries
  - Students with no professional experience
- STPA Training Time
  - Ranging from 2hrs to 30hrs
- STPA Analysis Time
  - Ranging from 30 minutes to 8 hours
- Materials provided to STPA Teams
  - General description of system as available before incidents
  - No knowledge or info about the flaws or the incidents

All teams successfully used STPA to discover the exact flaw and scenario!

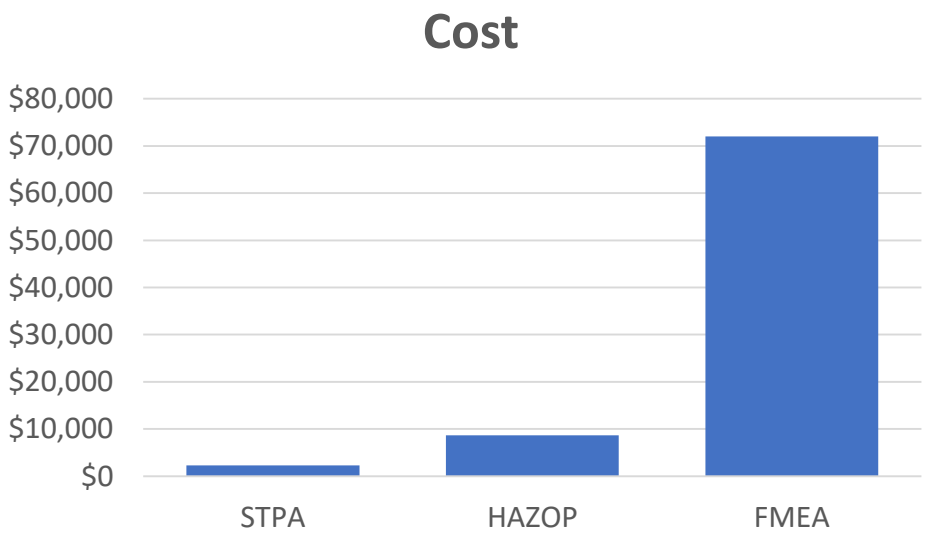
Analysis Method Comparison

- STPA*
  - **Time:** 1 to 32 person-hours
  - **Team:** STPA novices (but trained by STPA expert trainer/facilitator)
  - **Results:** All seven independent STPA teams anticipated the flaw and the incident scenario
- HAZOP*
  - **Time:** 120 person-hours
  - **Team:** Professional HAZOP practitioners from process industry
  - **Results:** HAZOP did not anticipate the flaw
- FMEA*
  - **Time:** 1,000+ person hours
  - **Team:** Industry professionals with FMEA training and prior FMEA experience
  - Note: Considered many more design details than other teams in this study
  - **Results:** FMEA did not anticipate the flaw
- Fault Tree Analysis (FTA)*
  - **Time: [**Not Available]
  - **Team:** Industry FTA professionals with decades of experience and specialization in FTA development
  - **Results:** FTA did not anticipate the flaw

*These results only reflect one data point—this specific research experiment—and are not intended as recommendations. For example, it is NOT recommended to limit STPA to 32 person-hours.

Return on Investment (ROI)

- Let's assume $75/hr labor
- STPA cost for this application: $2,400
- Value added: Identifying and addressing the $1m design flaw
- ROI*: $1m / $2,400 = 416



*These results only reflect one data point—this specific project. Further work is underway to explore the generalizability of these results.

For more information

- Google: “STPA Handbook”
  - How-to guide for practitioners applying STPA
- Website: mit.edu/psas
- Questions? Email me!

  JThomas4@mit.edu