Massachusetts Institute of Technology

STPA (System-Theoretic Process Analysis)

A Systems Approach to Safety (and Security)

Dr. John Thomas

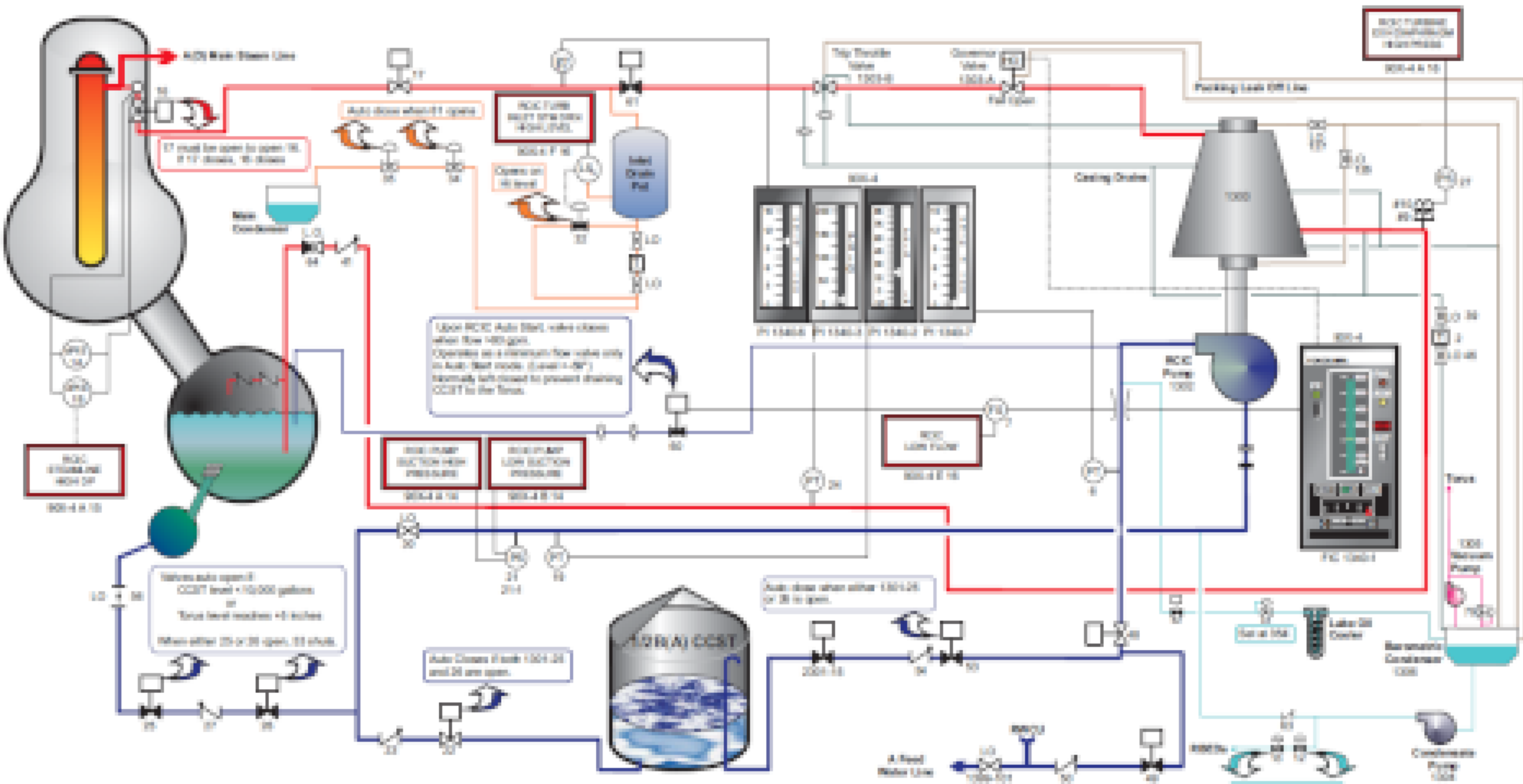
Engineering Systems Lab

MIT

JThomas4@mit.edu

System Models

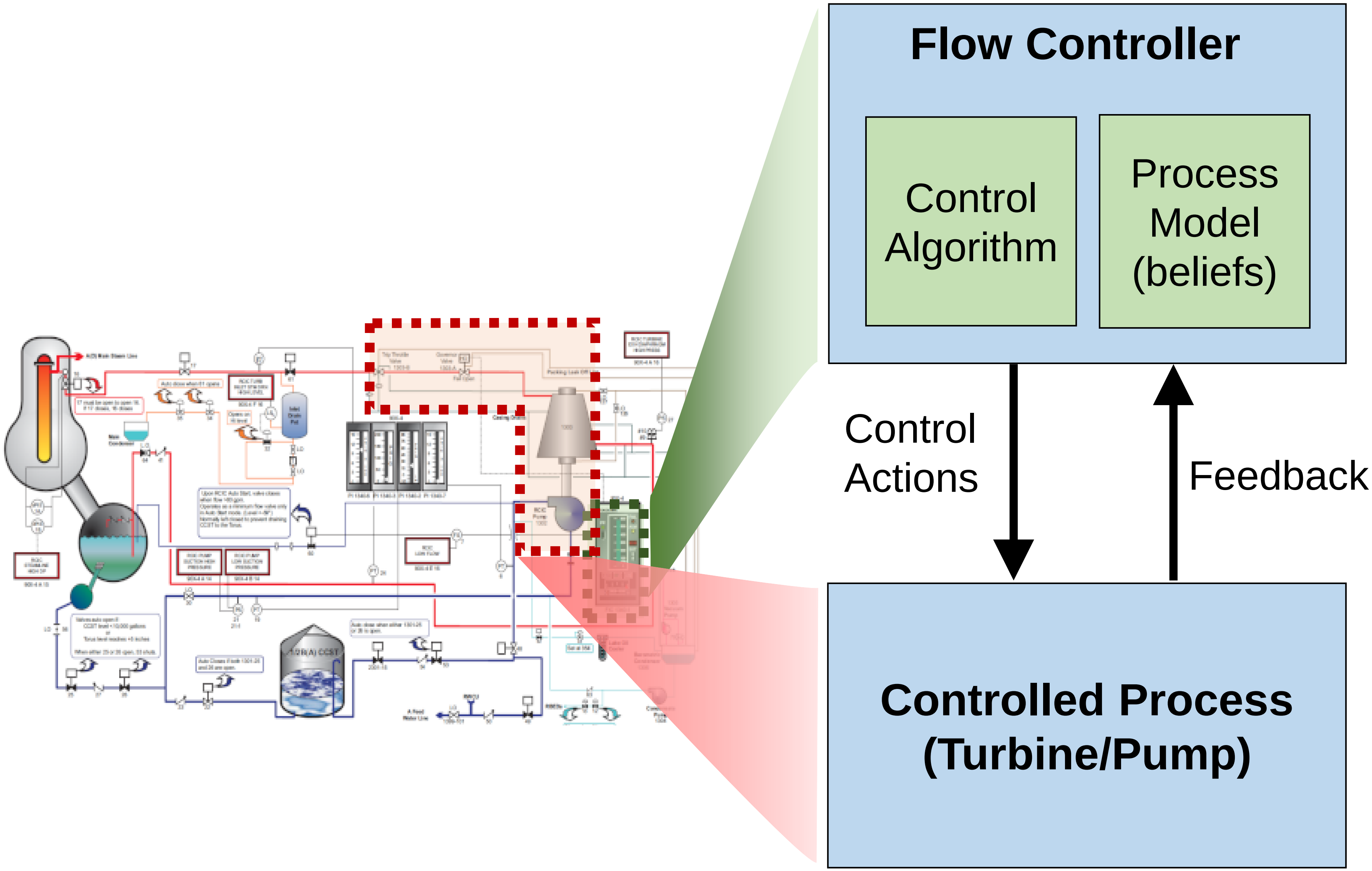
Example: Piping and Instrumentation Diagram (P&ID)



Emphasizes physical flows

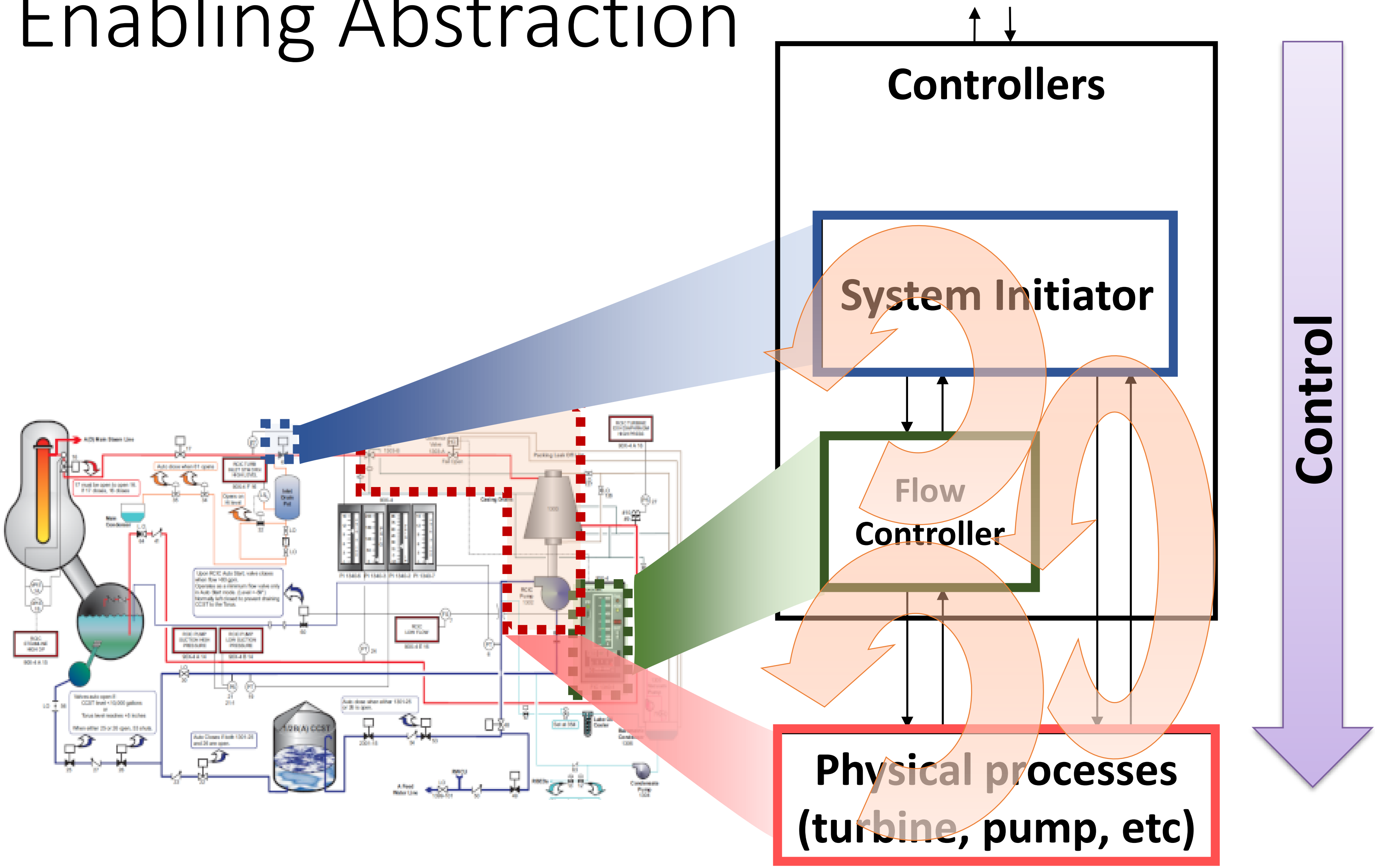
Does not emphasize Digital I&C behavior or Human Interactions

Enabling Abstraction Control Structure



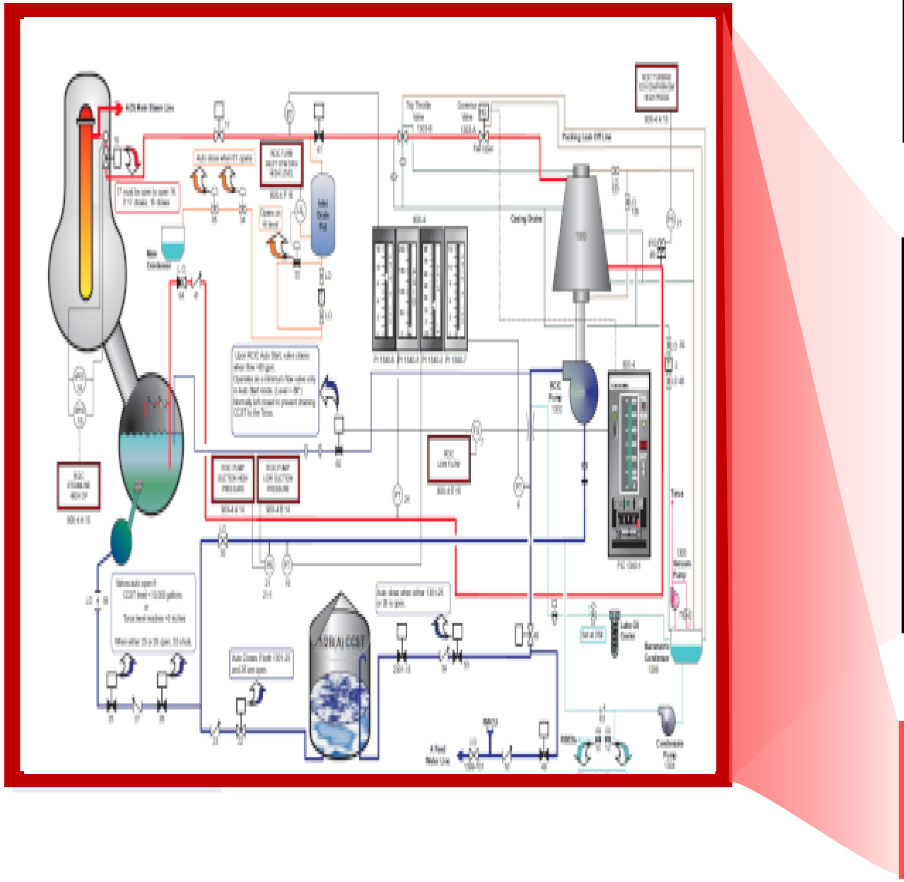
Thomas, 2020

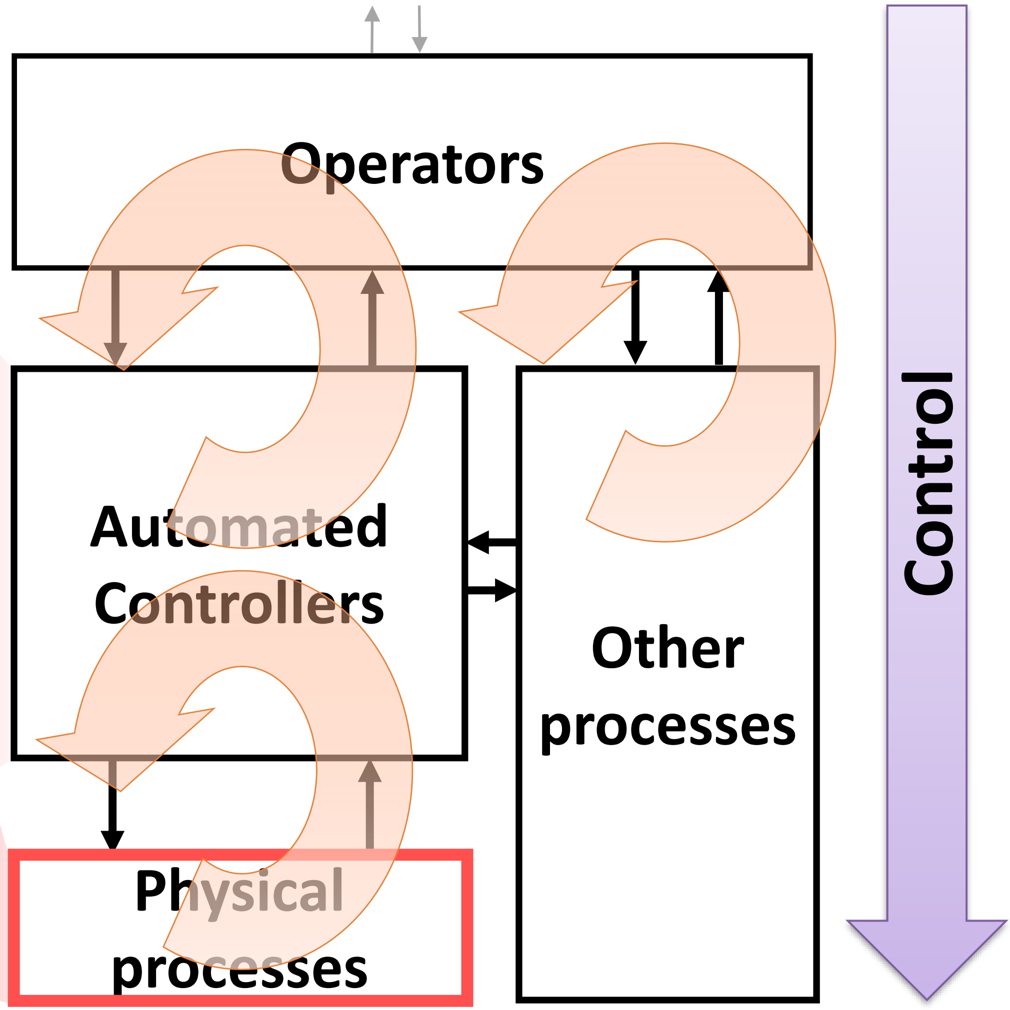
Enabling Abstraction



Thomas, 2020

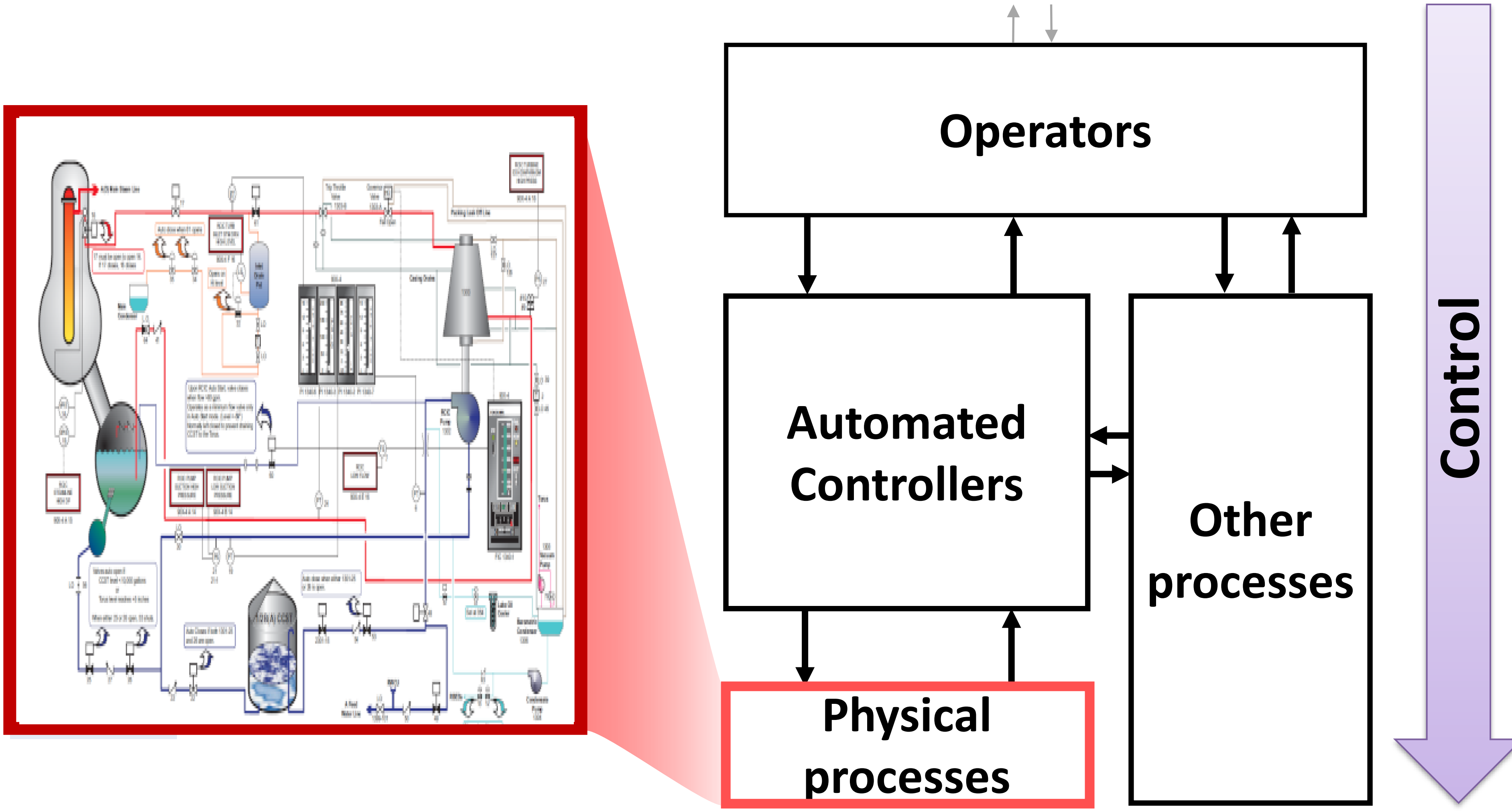
Abstraction





Thomas, 2017

Abstraction



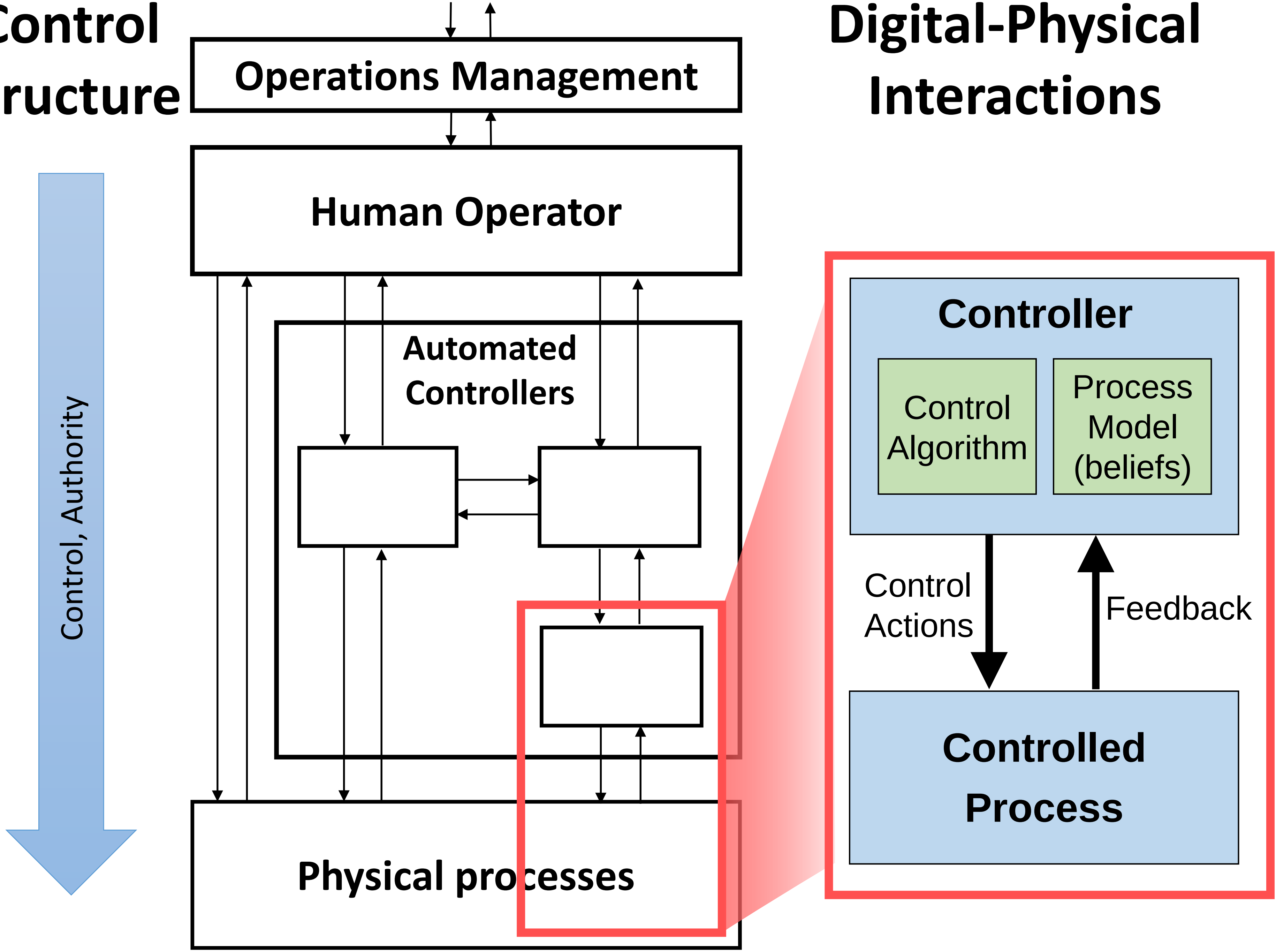
Component view

Systems view

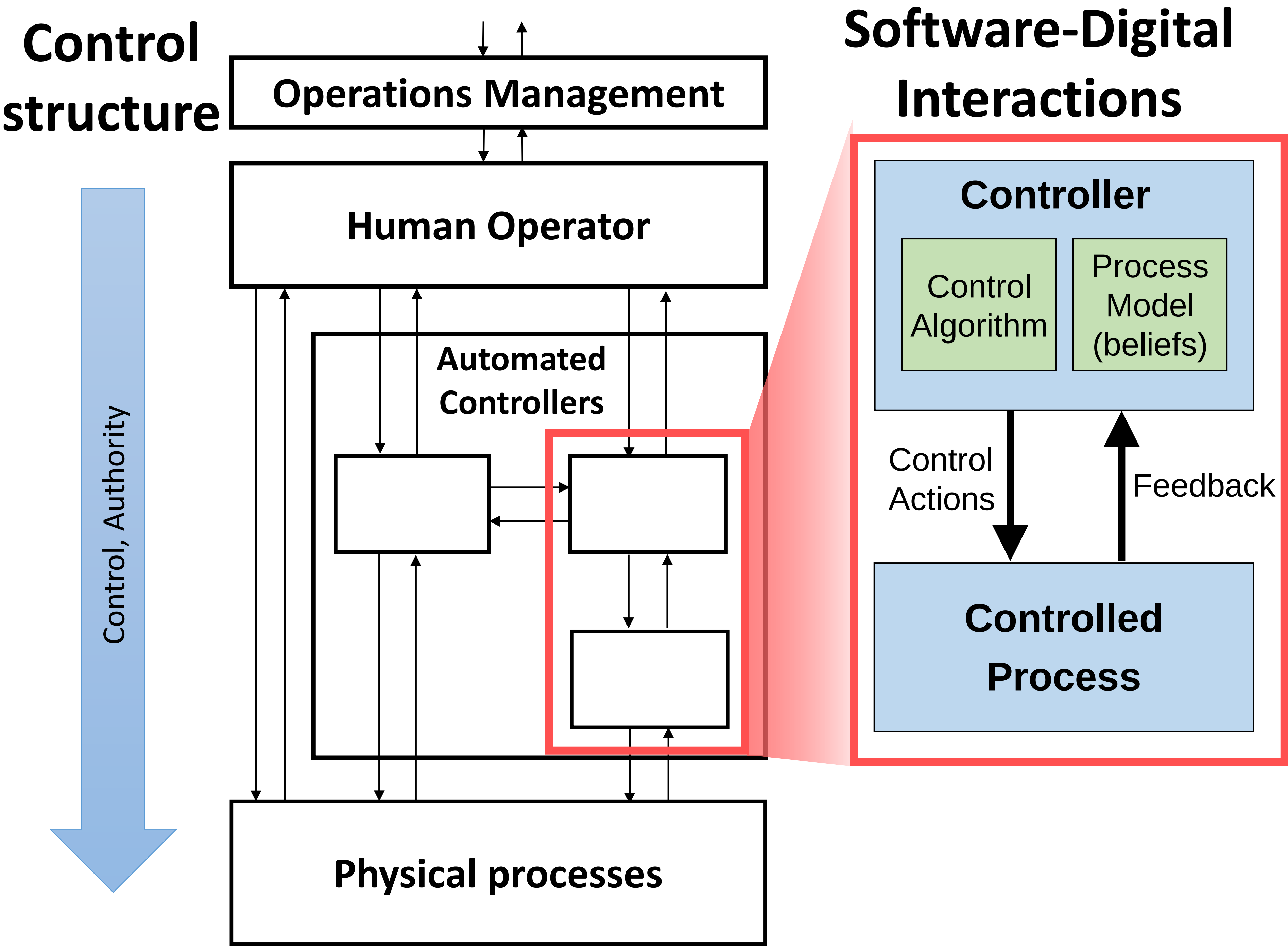
Thomas, 2017

Control structure

Digital-Physical Interactions



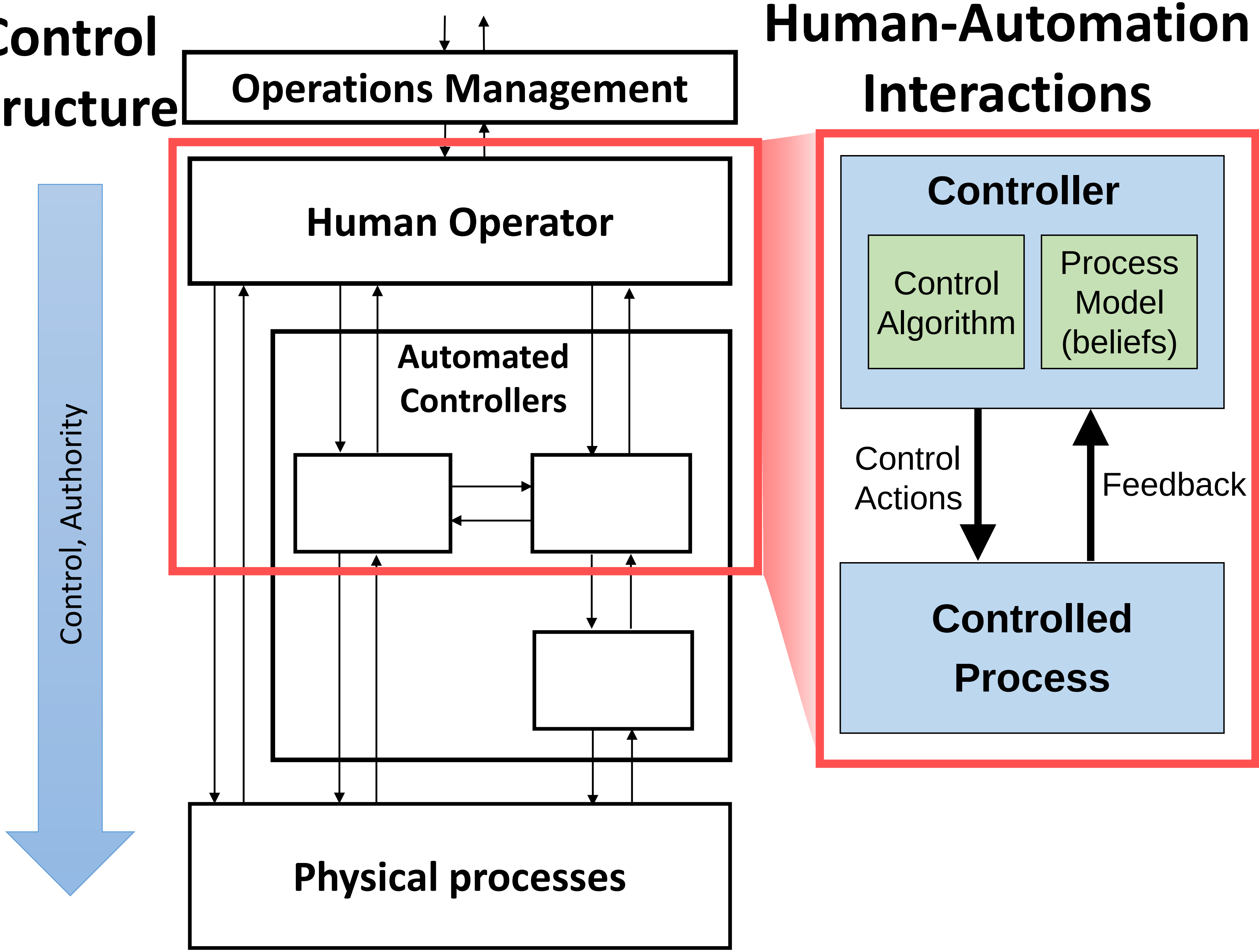
(John Thomas, 2017)



(John Thomas, 2017)

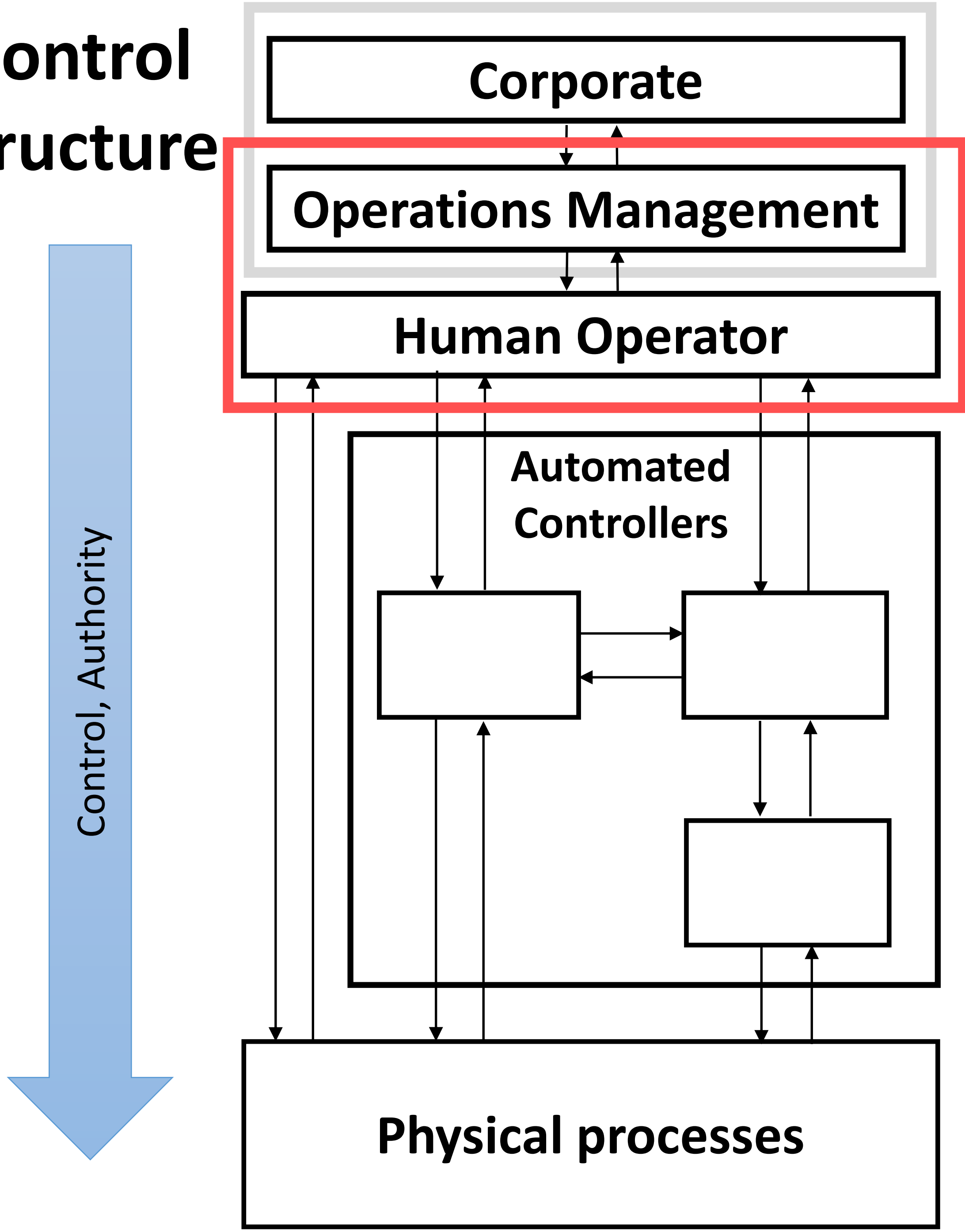
Control structure

Human-Automation Interactions

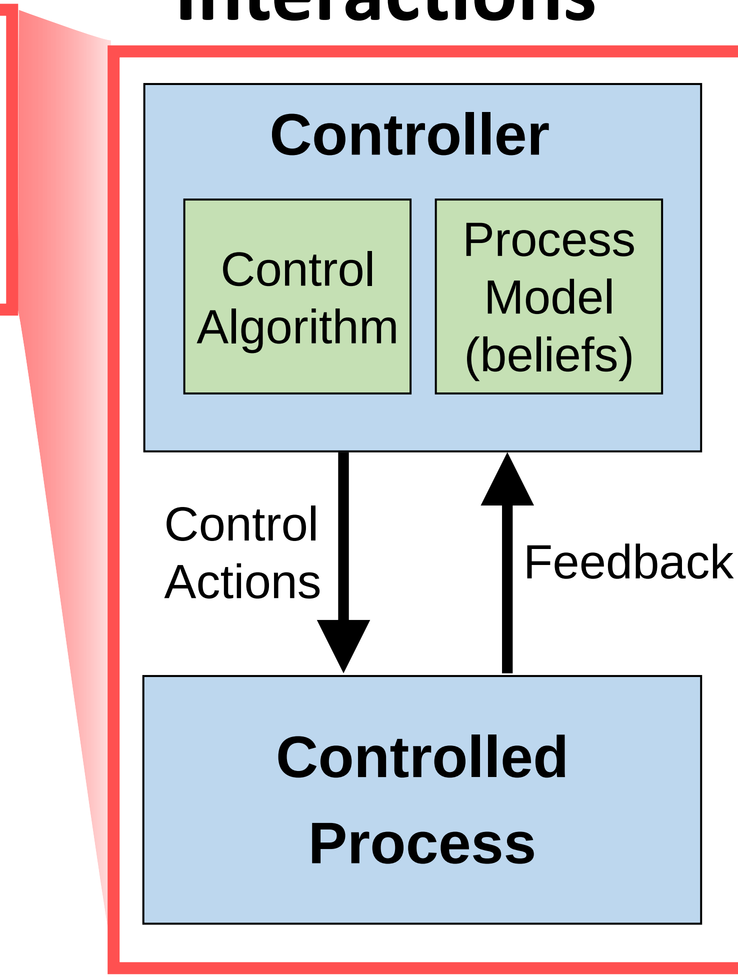


(John Thomas, 2017)

Control structure



Human-Human Interactions



(John Thomas, 2017)

Classification of Causal Factors

You are creating control structures all the time,
whether it's deliberate or not and whether you analyze them or not!

Principles from Control Theory

- Four conditions required to effect control over a system:

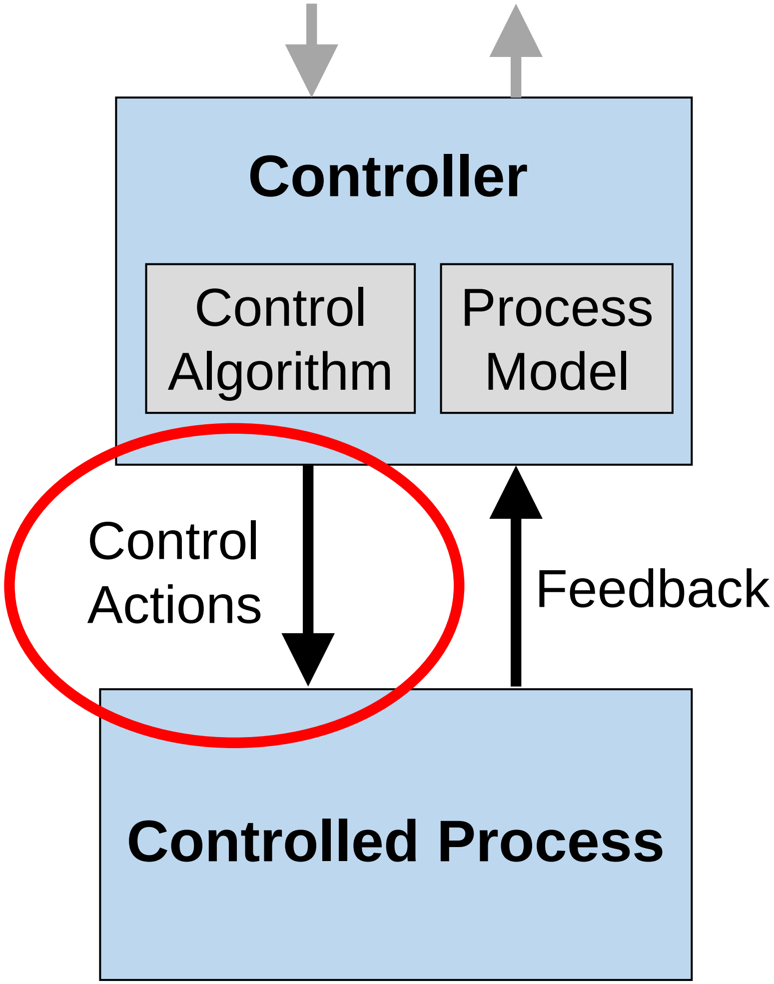
Goal Condition: The controller must have a goal or goals (e.g., to maintain a setpoint)

Action Condition: The controller must be able to affect the system state

Observability Condition: The controller must be able to ascertain the state of the system.

Model Condition: The controller must have (or contain) a model of the system

Ashby, 1957

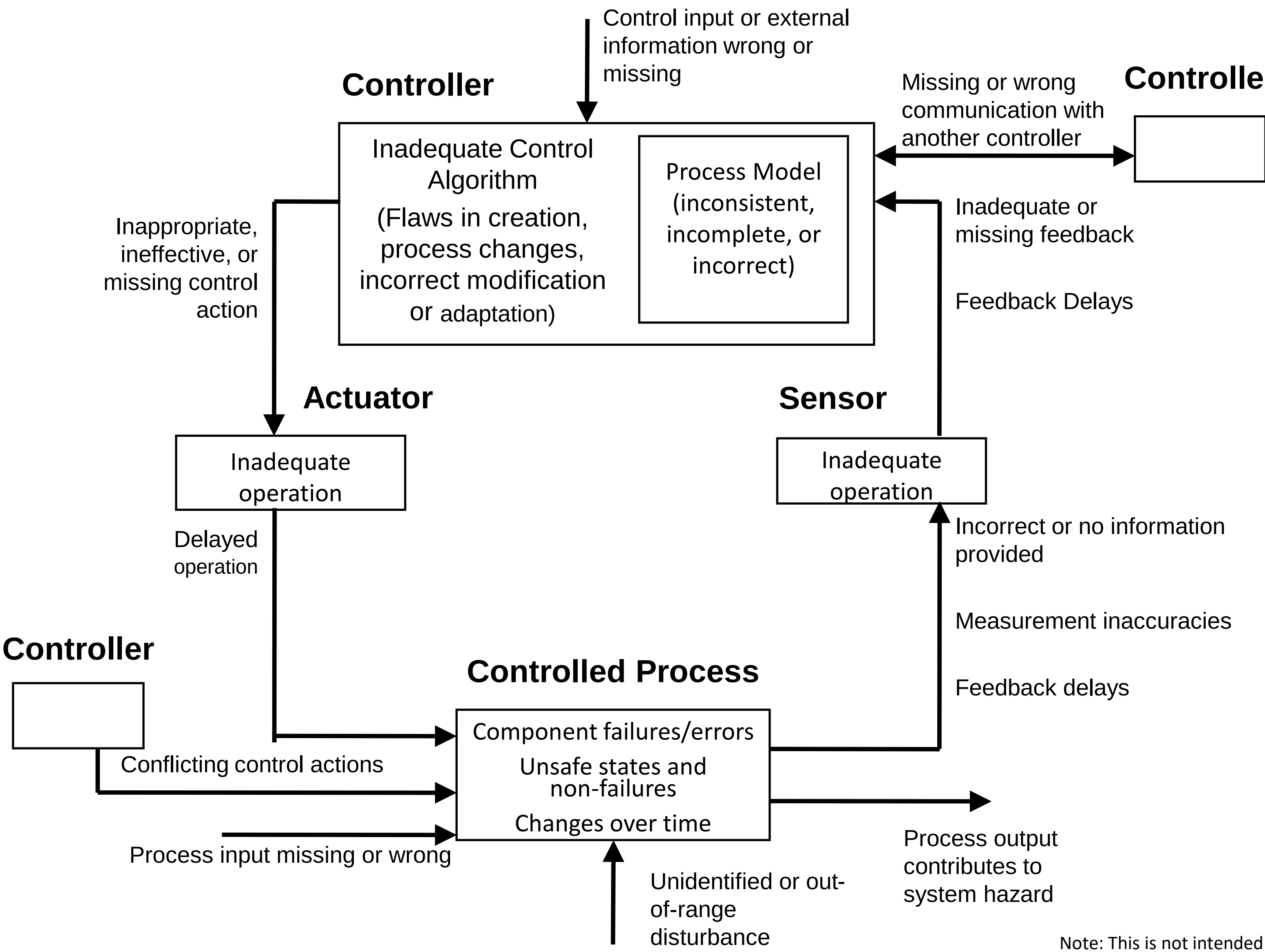


Four types of **unsafe control actions**:

1) Control actions required for safety are not given
2) Unsafe ones are given
3) Potentially safe control actions but given too early, too late
4) Control action stops too soon or applied too long

(Leveson, 2012)

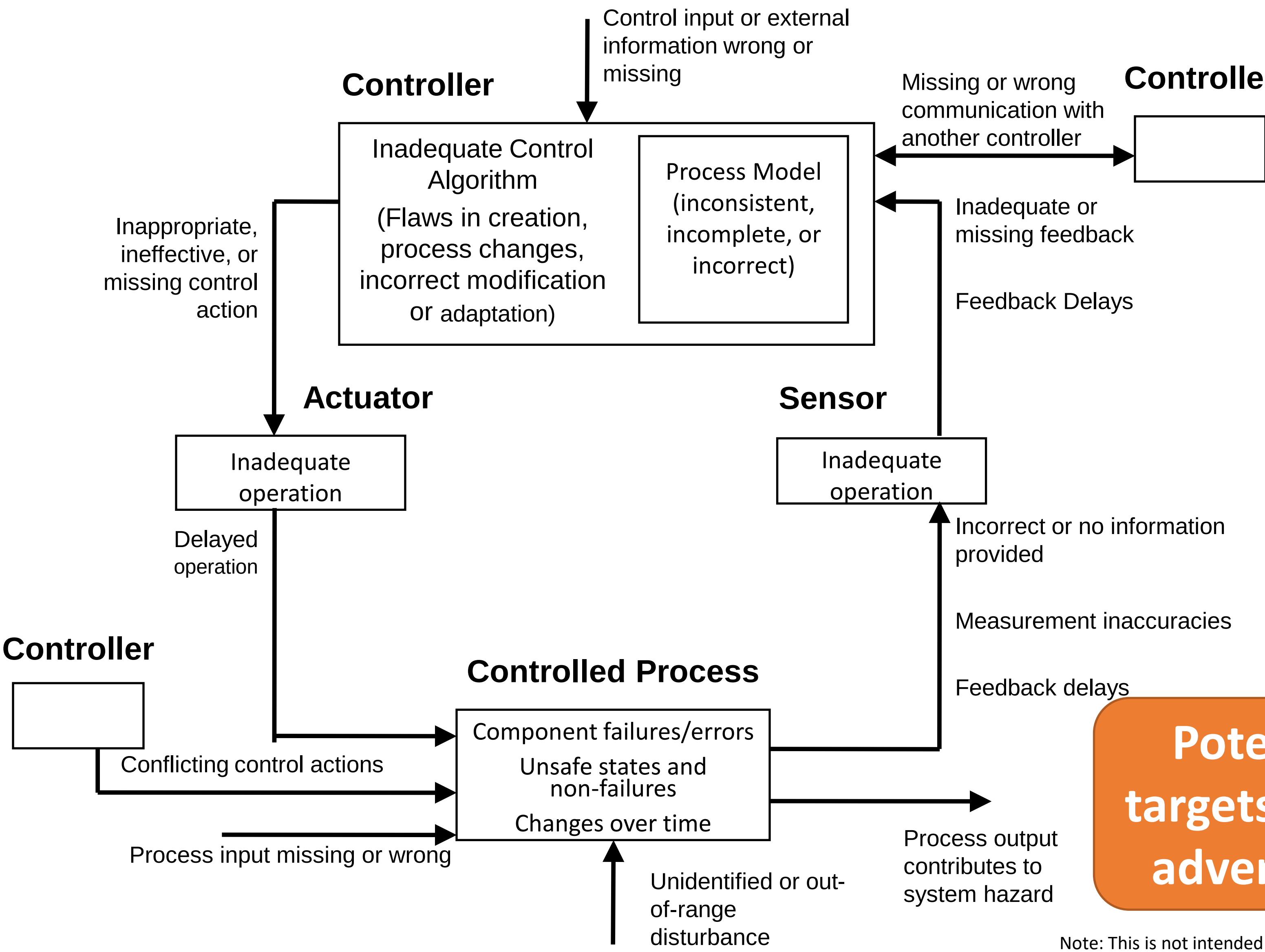
Some Factors in Causal Scenarios



(Leveson, 2012)

Note: This is not intended to be complete, but it provides a starting point. You will need to tailor the specific factors relevant to your application.

Some Factors in Causal Scenarios



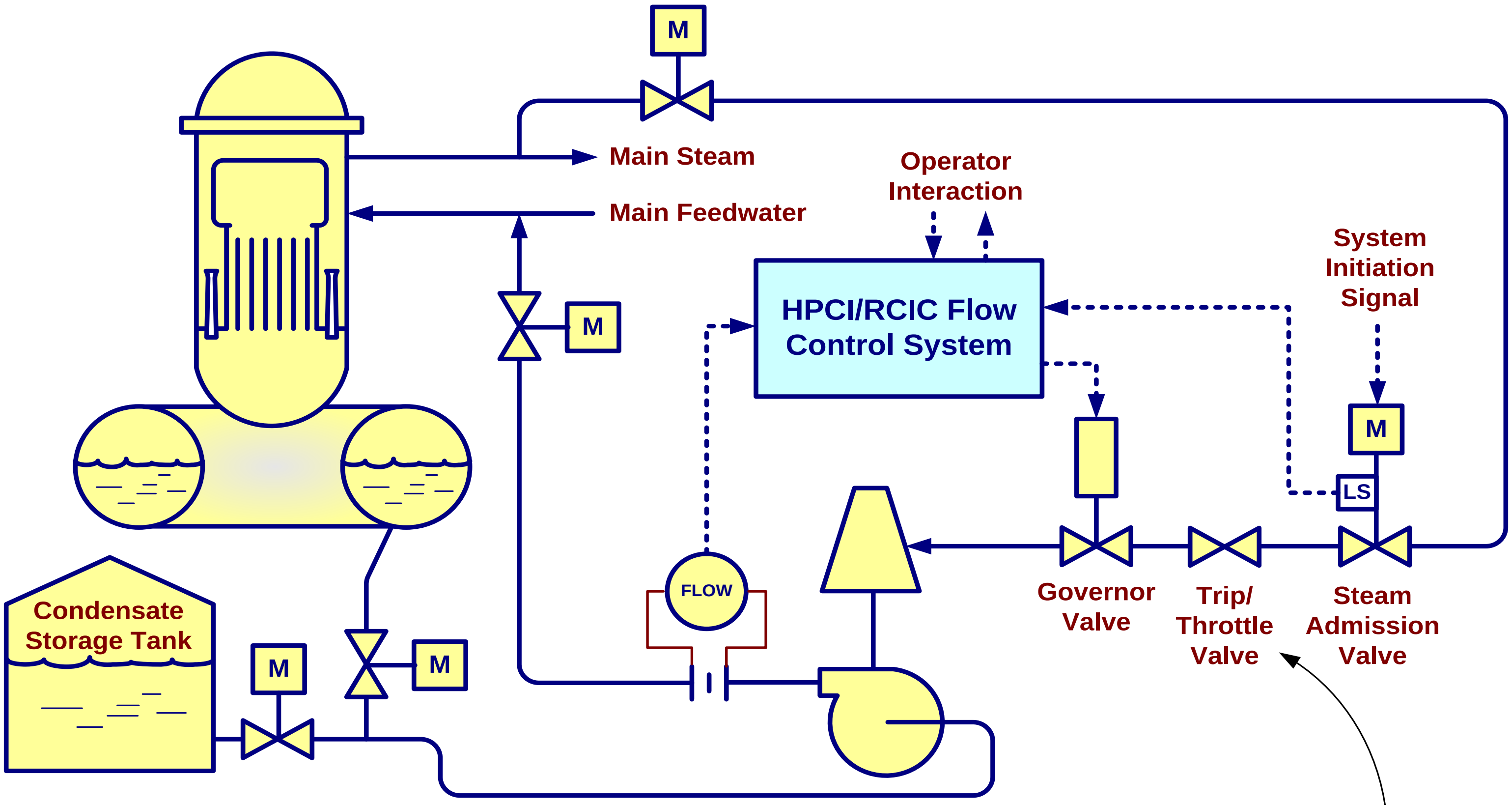
Potential targets for an adversary?

(Leveson, 2012)

Note: This is not intended to be complete, but it provides a starting point. You will need to tailor the specific factors relevant to your application.

Nuclear HPCI/RCIC Example

Nuclear HPCI Example

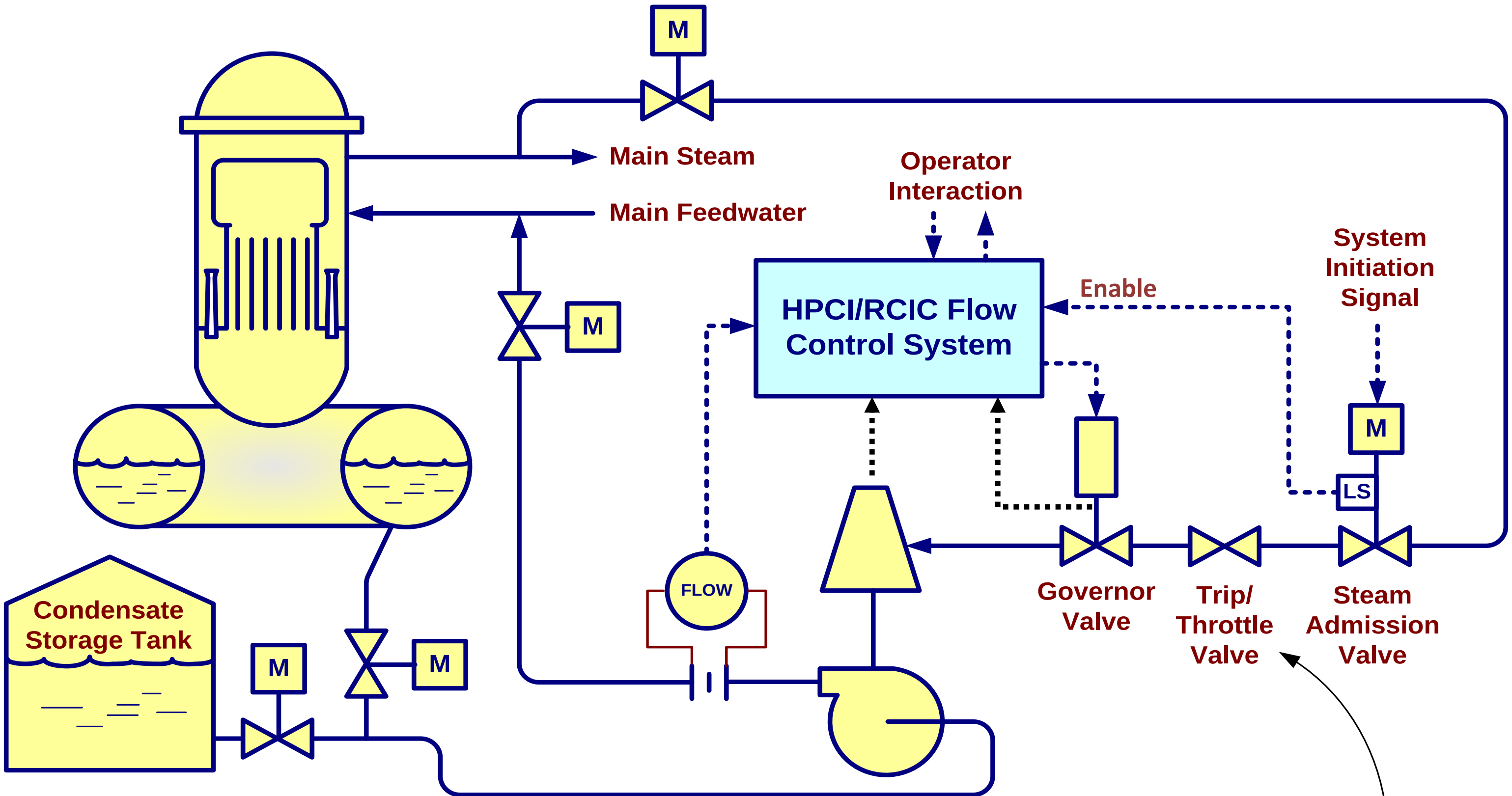


<u>System Initiation Signals</u>
(Open Steam Admission Valve & Process Valves)
1. Low Reactor Level (-48")
2. High Drywell Pressure (HPCI only; +2 psig)

<u>System Isolation Signals</u>
(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

<u>Turbine Trip Signals</u>
(Close Trip/Throttle Valve)
1. <u>Any system isolation signal</u>
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)

HPCI Flow Control System (simplified)

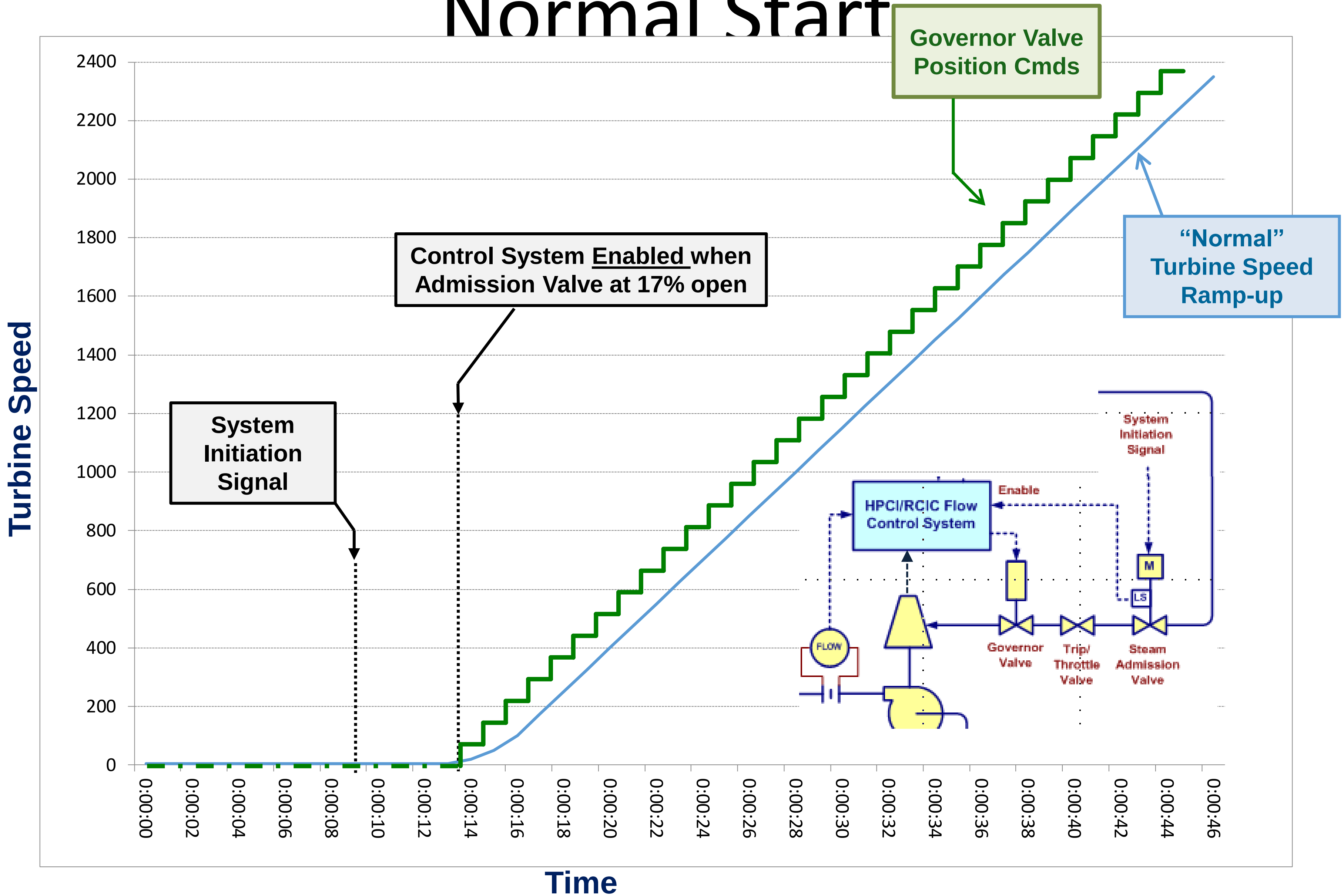


System Initiation Signals
(Open Steam Admission Valve & Process Valves)
1. Low Reactor Level (-48")
2. High Drywell Pressure (HPCI only; +2 psig)

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

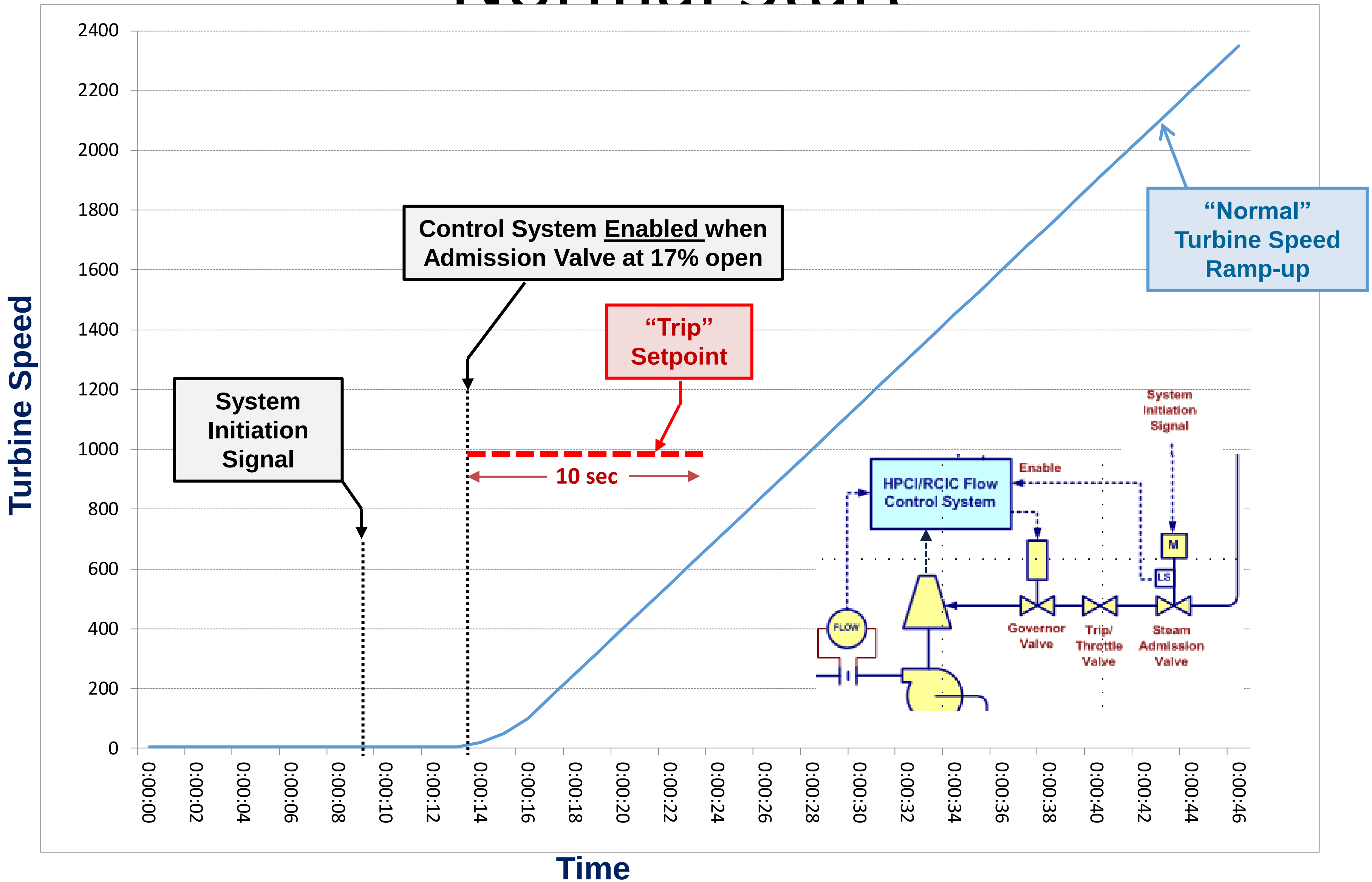
Turbine Trip Signals
(Close Trip/Throttle Valve)
1. Any system isolation signal
2. High Steam Exhaust Pressure (150 psi)
3. High Reactor Level (+46")
4. Low pump suction pressure (15" Hg)
5. Turbine overspeed
6. Manual (local or remote)

Normal Start



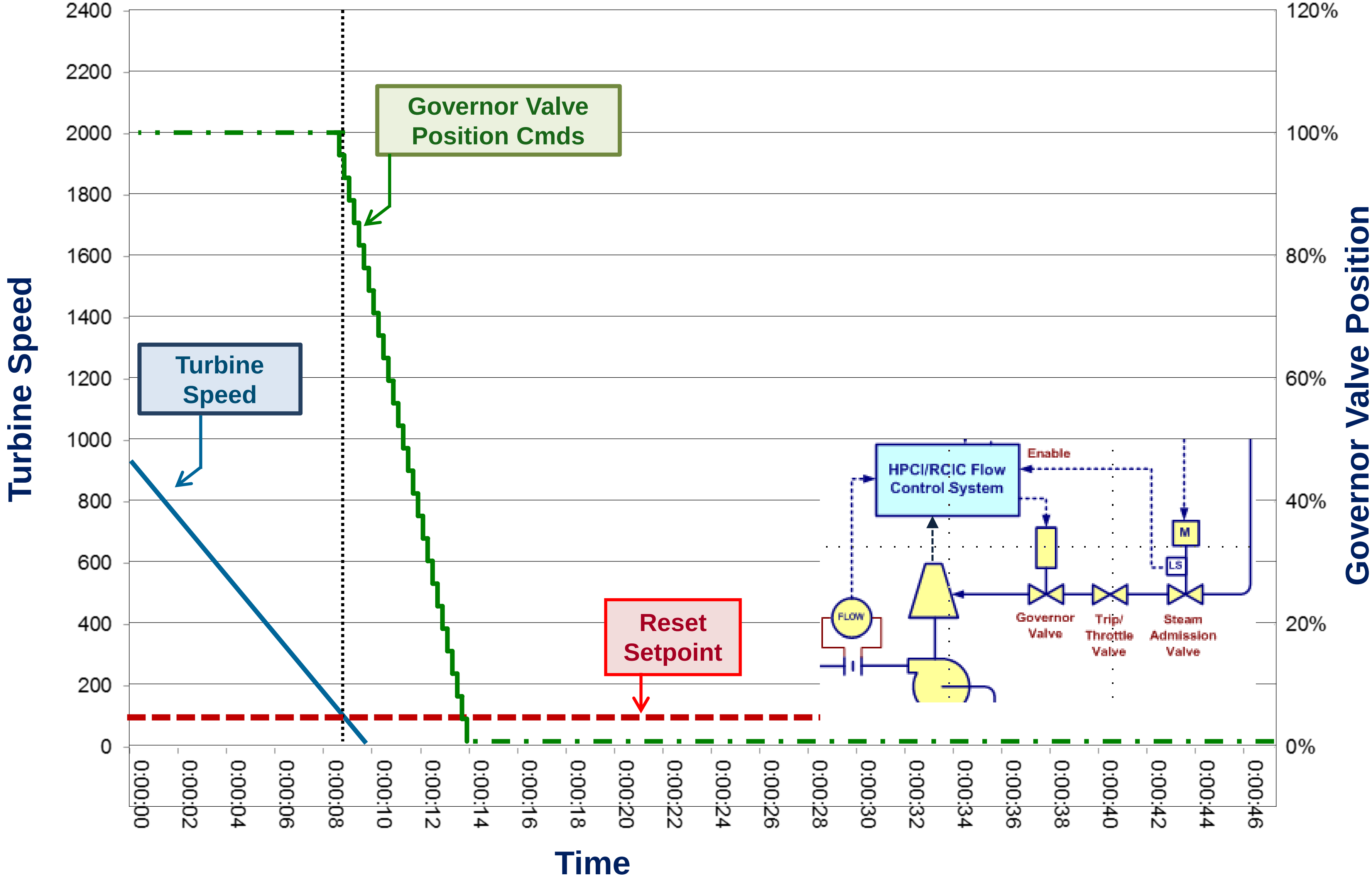
This is a simplified recreation, not actual data

Normal Start



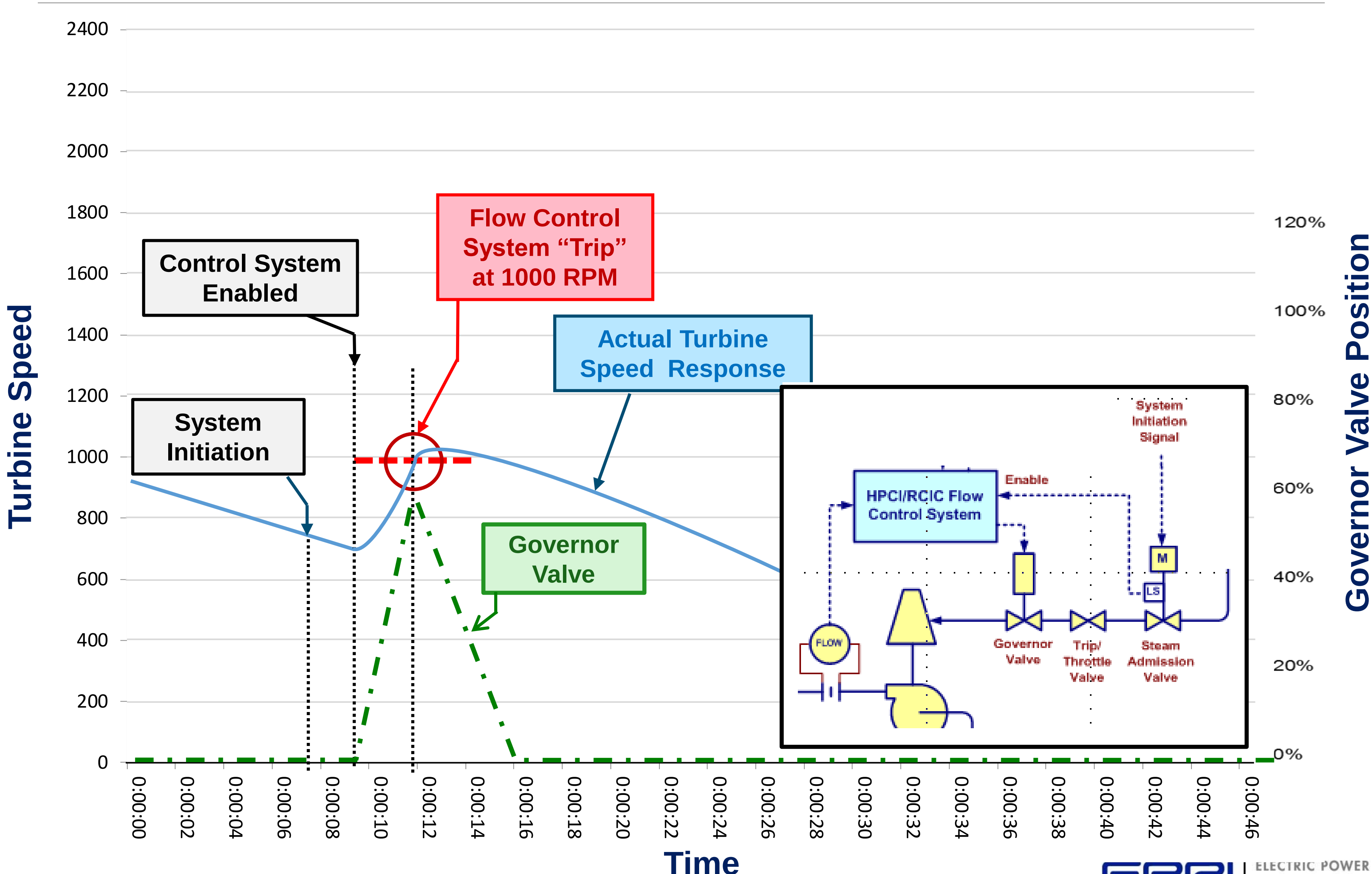
This is a simplified recreation, not actual data

Normal shutdown



This is a simplified recreation, not actual data

Operating Experience Event (No Component Failures)

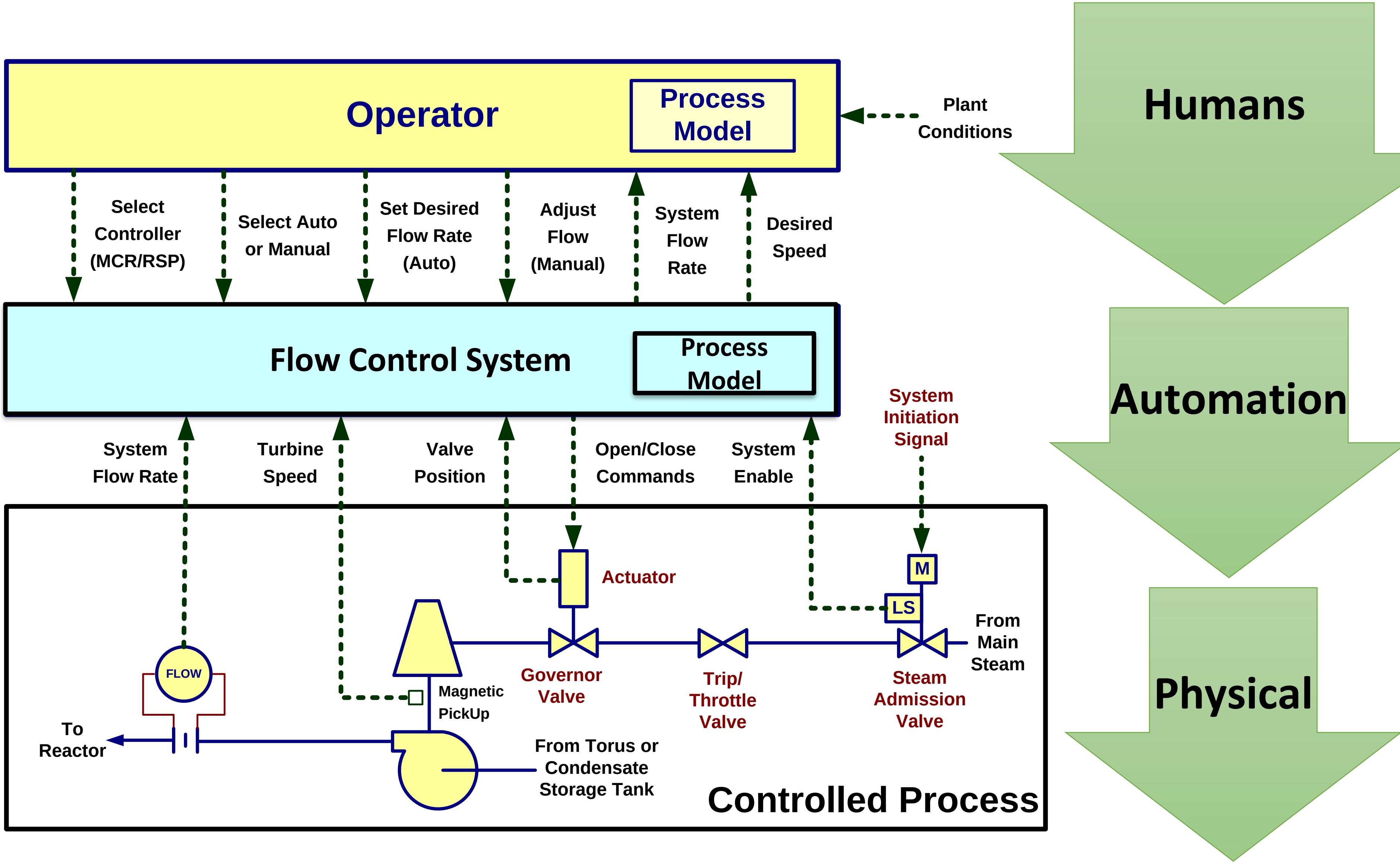


This is a simplified recreation, not actual data

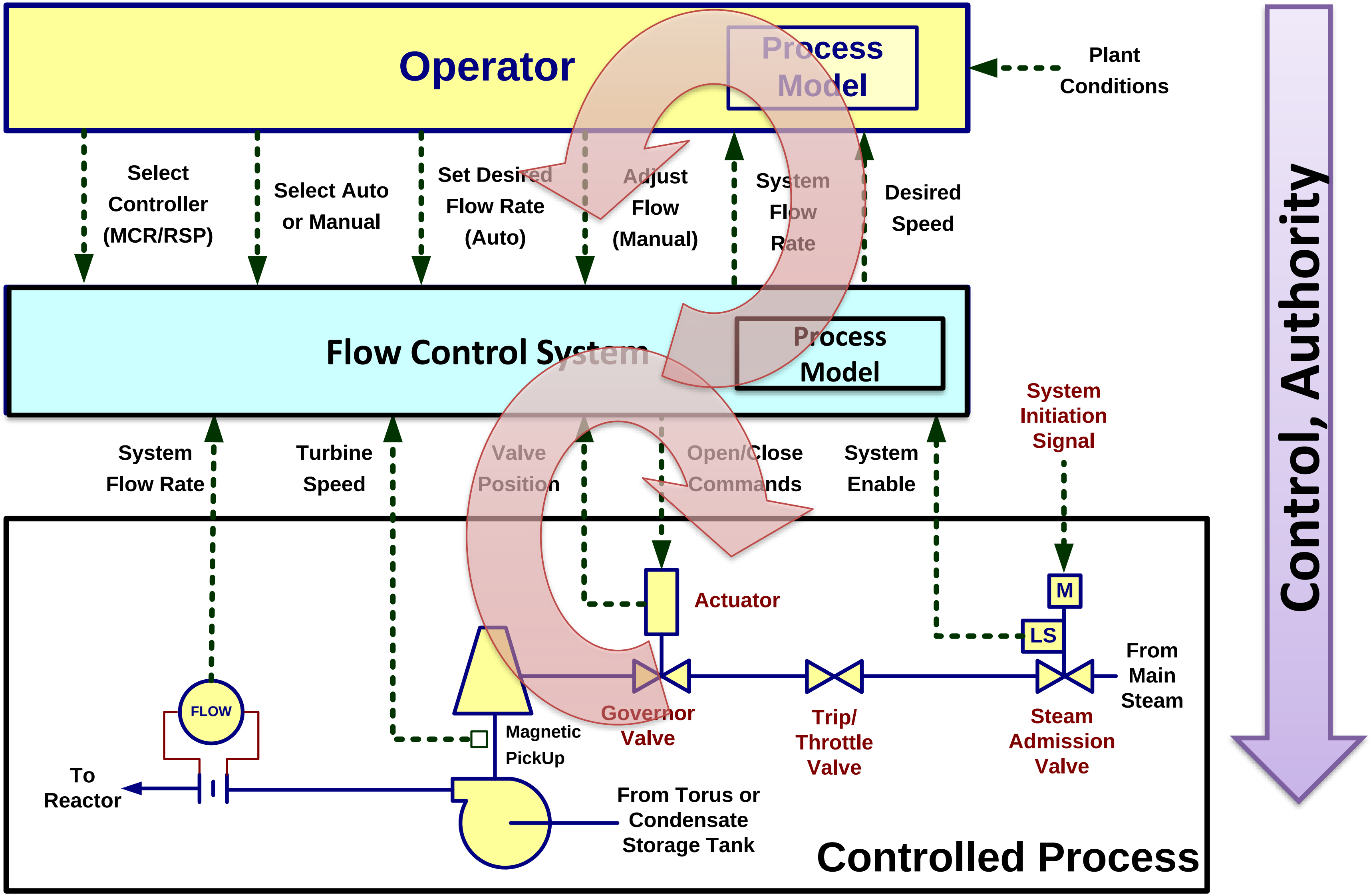
ELECTRIC POWER RESEARCH INSTITUTE

STPA: A systems view

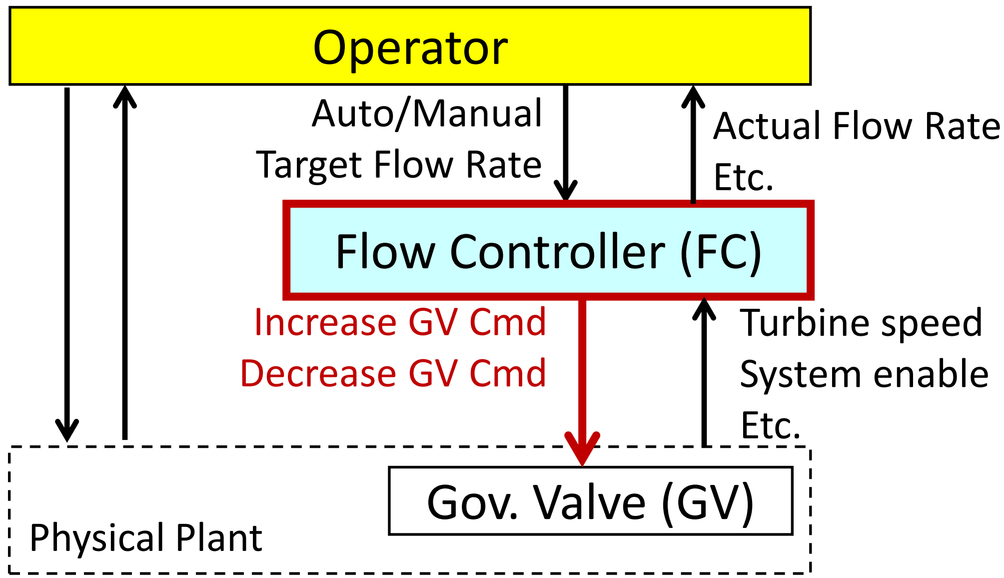
STPA Control Structure (simplified)



Control Structure (simplified)



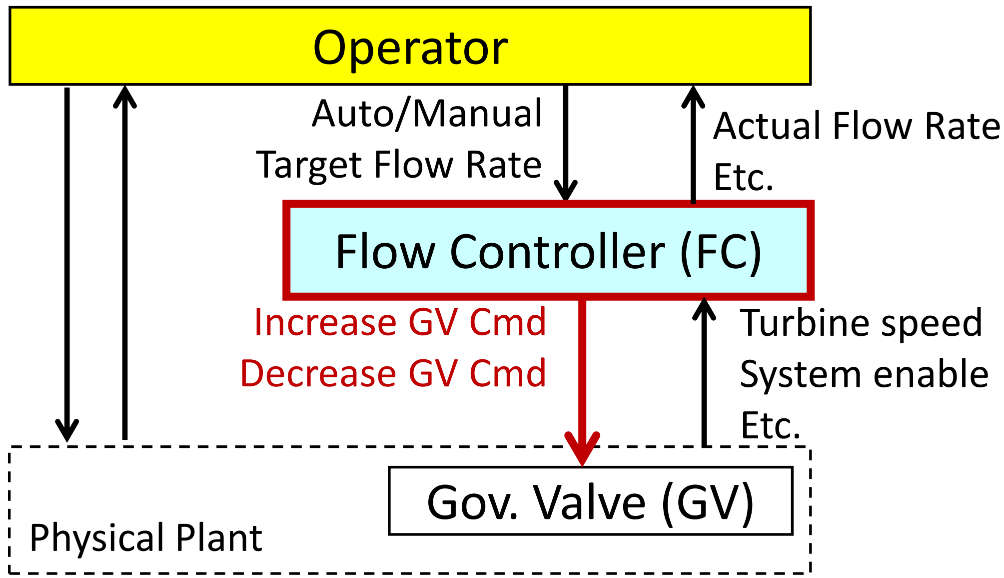
STPA Step 3: Unsafe Control Actions (UCA)



	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped Too Soon / Applied too long
Increase GV Position	[…]	[…]	[…]	[…]
Decrease GV Position	[…]	FCS provides Decrease Gov Cmd when ______	[…]	[…]

John Thomas, 2020

STPA Step 3: Unsafe Control Actions (UCA)



	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped Too Soon / Applied too long
Increase GV Position	[…]	[…]	[…]	[…]
Decrease GV Position	[…]	FCS provides Decrease Gov Cmd when emergency cooling is needed (system initiated)	[…]	[…]

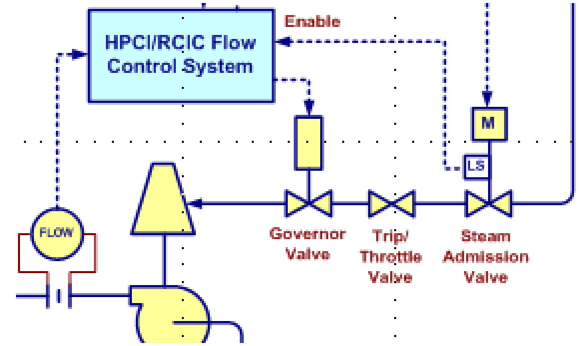
John Thomas, 2020

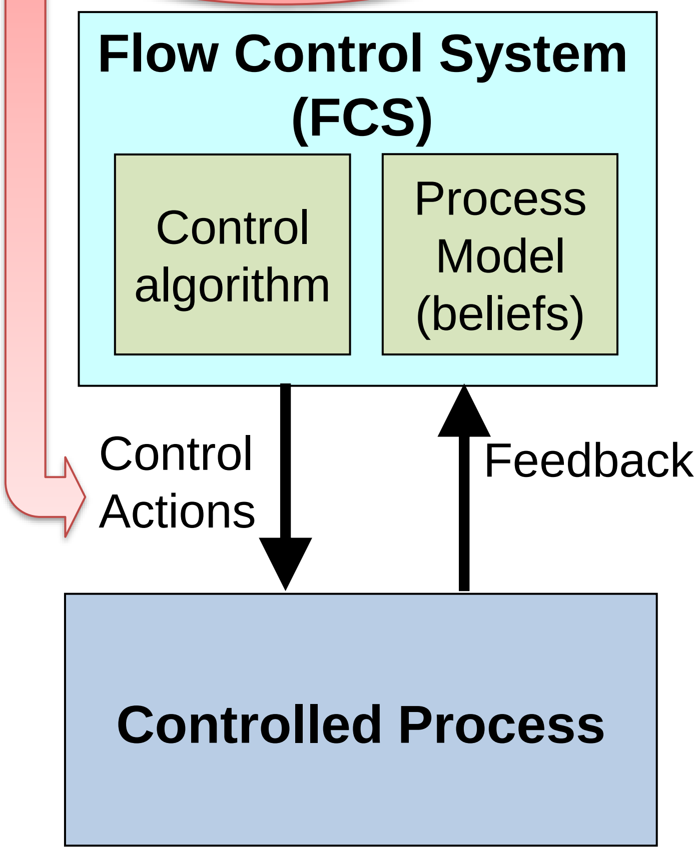
Asking the right questions

Loss: Loss of life, equipment damage, environmental loss

Question: What FCS control actions can cause those losses?

UCA: FCS provides Close Gov Cmd when <u>emergency cooling is needed (system initiated)</u>

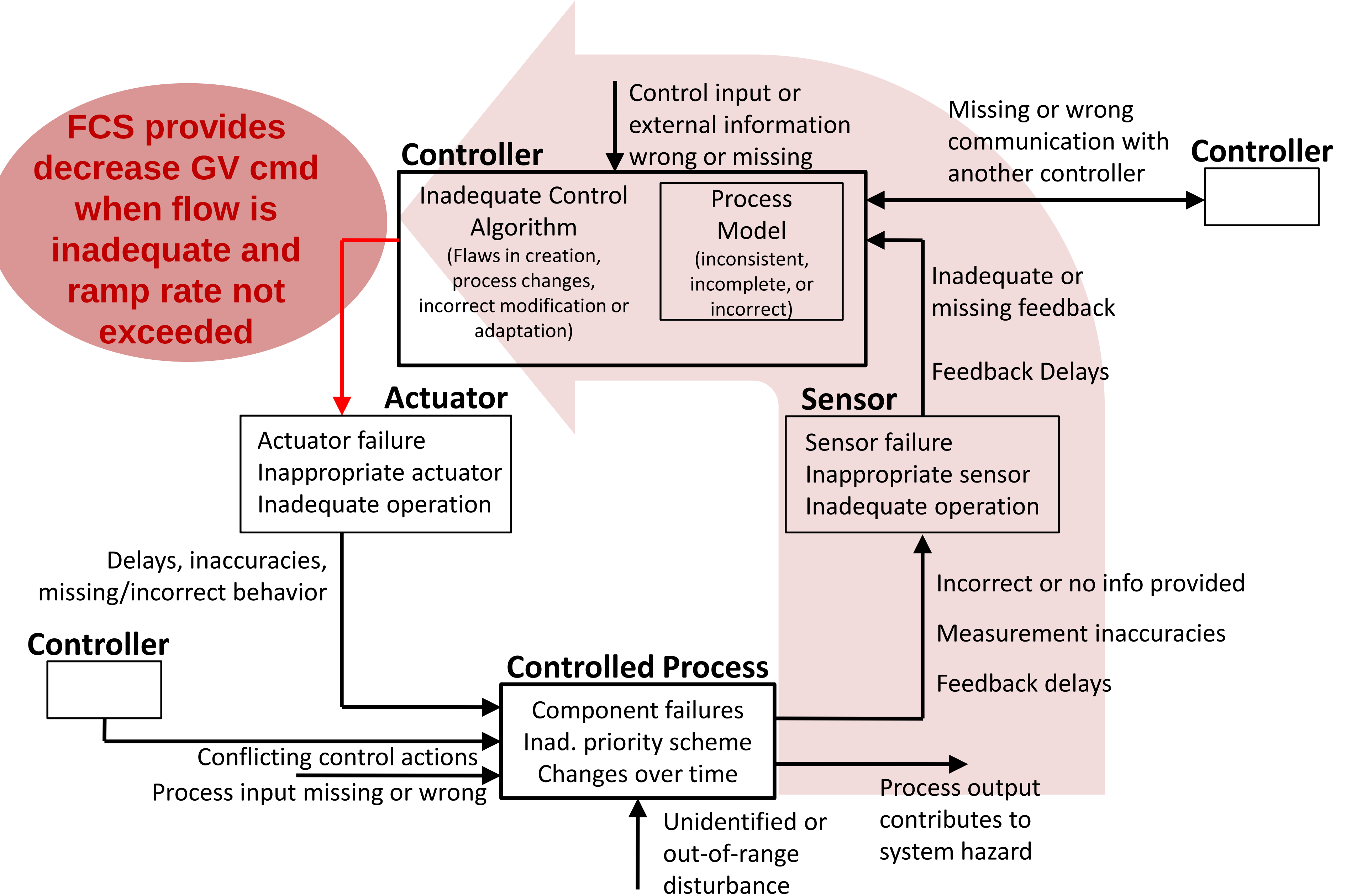




Why might this happen?

John Thomas, 2019

Potential control flaws



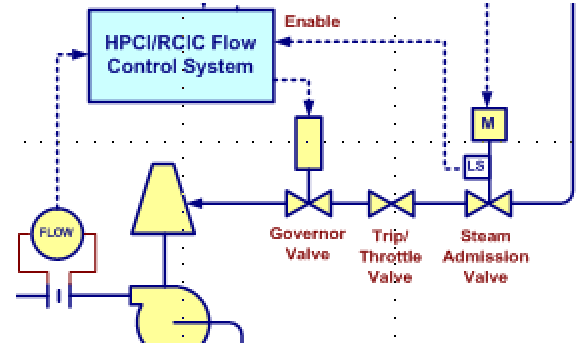
(John Thomas, 2017)

Asking the right questions

Loss: Loss of life, equipment damage, environmental loss

Question: What FCS control actions can cause those losses?

UCA: FCS provides Close Gov Cmd when emergency cooling is needed (system initiated)



Question: What FCS beliefs would cause it to provide Close Gov Cmd when emergency cooling is needed?

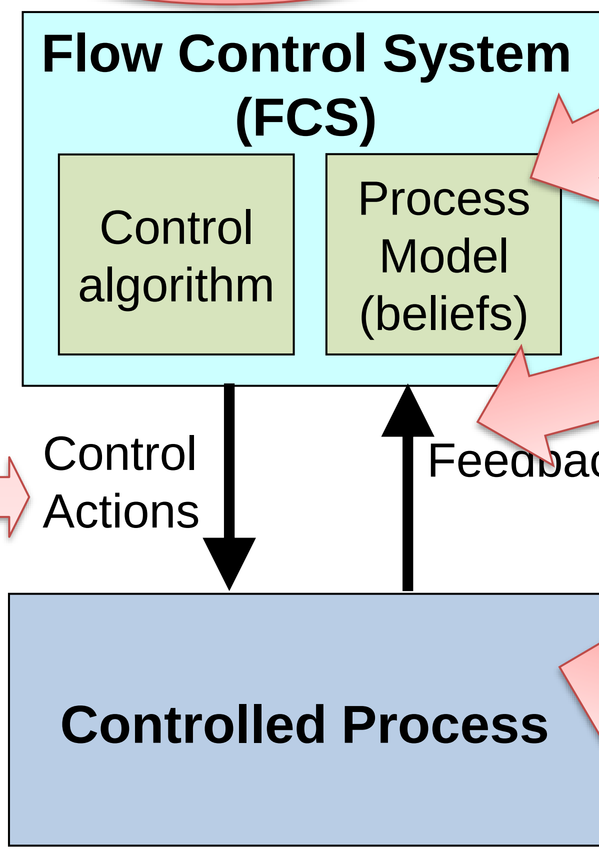
PM: FCS incorrectly believes ramp rate exceeded

Question: What FCS inputs would cause FCS to incorrectly believe ramp rate exceeded?

FB: Turbine speed > 1000rpm within X sec of Enable

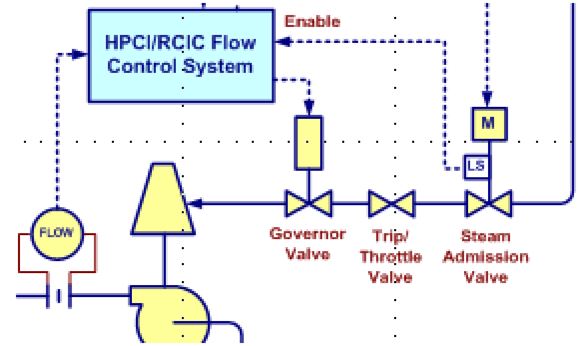
Question: What would cause Speed > 1000rpm within X sec of Enable?

CP: LS setpoint too high, Governor already open, turbine rolling start, etc.



John Thomas, 2019

Asking the right questions



Loss: Loss of life, equipment damage, environmental loss

Question: What FCS control actions can cause those losses?

UCA: FCS provides Close Gov Cmd when emergency cooling is needed (system initiated)

Question: What FCS beliefs would cause it to provide Close Gov Cmd when emergency cooling is needed?

PM: FCS incorrectly believes ramp rate exceeded

Question: What FCS inputs would cause FCS to incorrectly believe ramp rate exceeded?

FB: Turbine speed > 1000rpm within X sec of Enable

Question: What would cause Speed > 1000rpm within X sec of Enable?

CP: LS setpoint too high, Governor already open, turbine rolling start, etc.

Flow Control System (FCS)

Control algorithm

Process Model (beliefs)

Control Actions

Feedback

Controlled Process

This unanticipated flaw caused >$10M USD losses.

No random failures!

No component failures!

John Thomas, 2019

Testing the methods we use

- The existing hazard analysis had not anticipated this flaw
- Now we know about this specific flaw—modify the design and add it to the existing hazard analysis
  - Not good enough!
- Need a method that can discover these flaws **before** they are encountered!

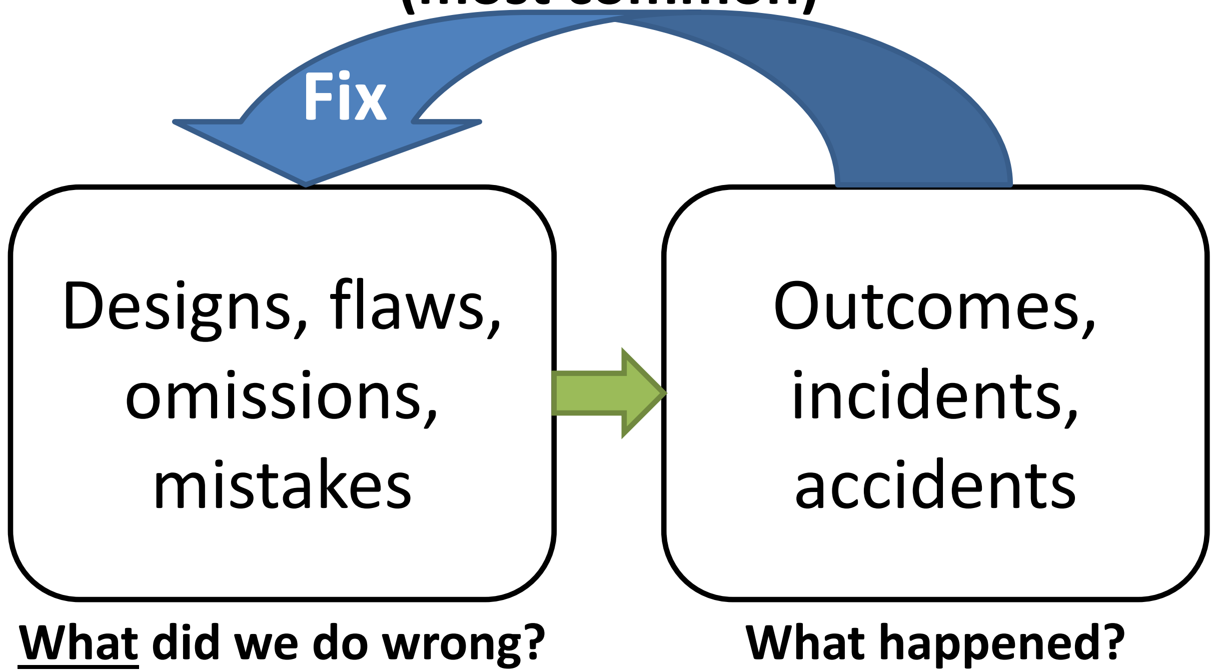
- Multiple blind tests conducted
  - STAMP / STPA
  - HAZOP
  - FTA
  - FMEA
  - Others

- Result
  - Most component failures were identified by every method
  - Only the STPA approach reliably identified these DI&C flaws in design & assumptions
  - STPA selected for new guidance for Nuclear DI&C engineering

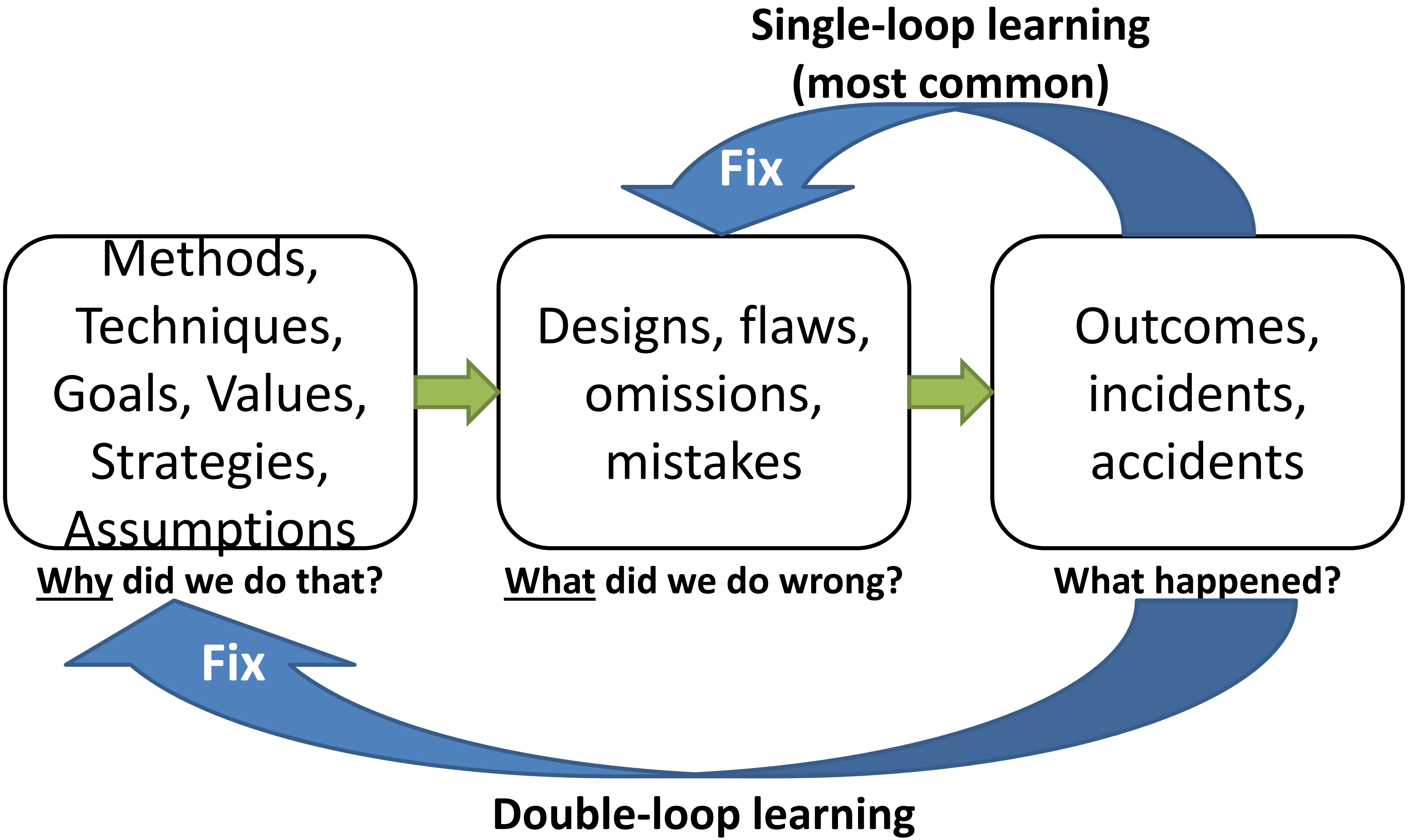
Blind testing: STPA works
Discuss effectiveness & efficiency

Single- vs. Double-Loop Learning

Single-loop learning (most common)



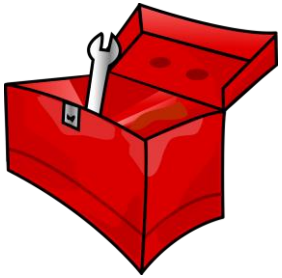
Single- vs. Double-Loop Learning



John Thomas, 2019

Every model and every method has limitations!

	Strengths	Limitations
STPA	?	?
FMEA	?	?
FTA	?	?
PRA	?	?



Massachusetts Institute of Technology

STPA: Cooling System Case Study

Dr. John Thomas
Engineering Systems Lab
MIT

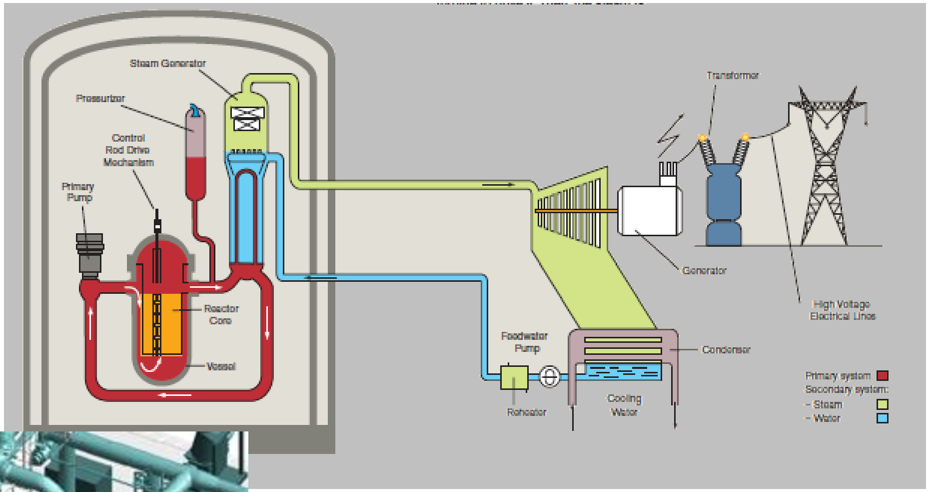
Disclaimer

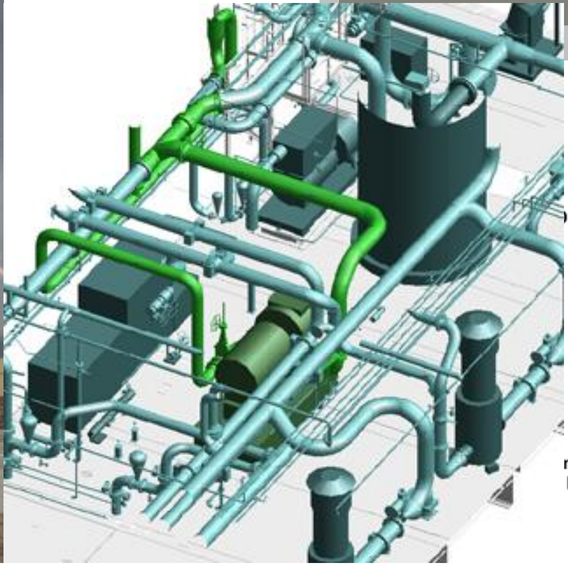
This exercise comes from a real system

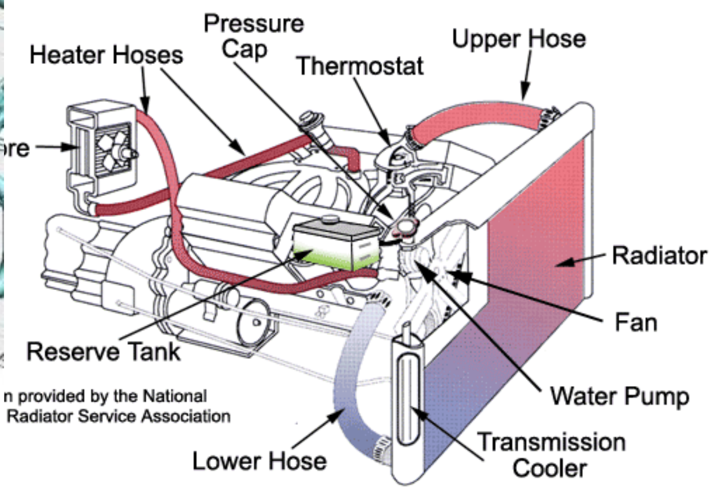
BUT

Details had to be sufficiently changed or generalized in order to study in this class.

Examples of Cooling Systems







Old Cooling System 1.0

Purpose

- Cooling System 1.0 provides cooling for a critical process[1] that generates heat during the operation of […].
- If we ever lose cooling, the cooling system must trigger a shutdown of […] and in order to prevent unacceptable losses.

[1] This could be any process that generates heat, such as electrical power generation processes.

Old Cooling System 1.0

Concept of Operation

- Provides cooling of [heat generation systems]
- Includes protection from **loss of cooling**, which will command an automatic shutdown of [heat generation systems].
- Loss of cooling is measured by
  - Low cooling flow, OR
  - Low cooling pressure, OR
  - High cooling temperature

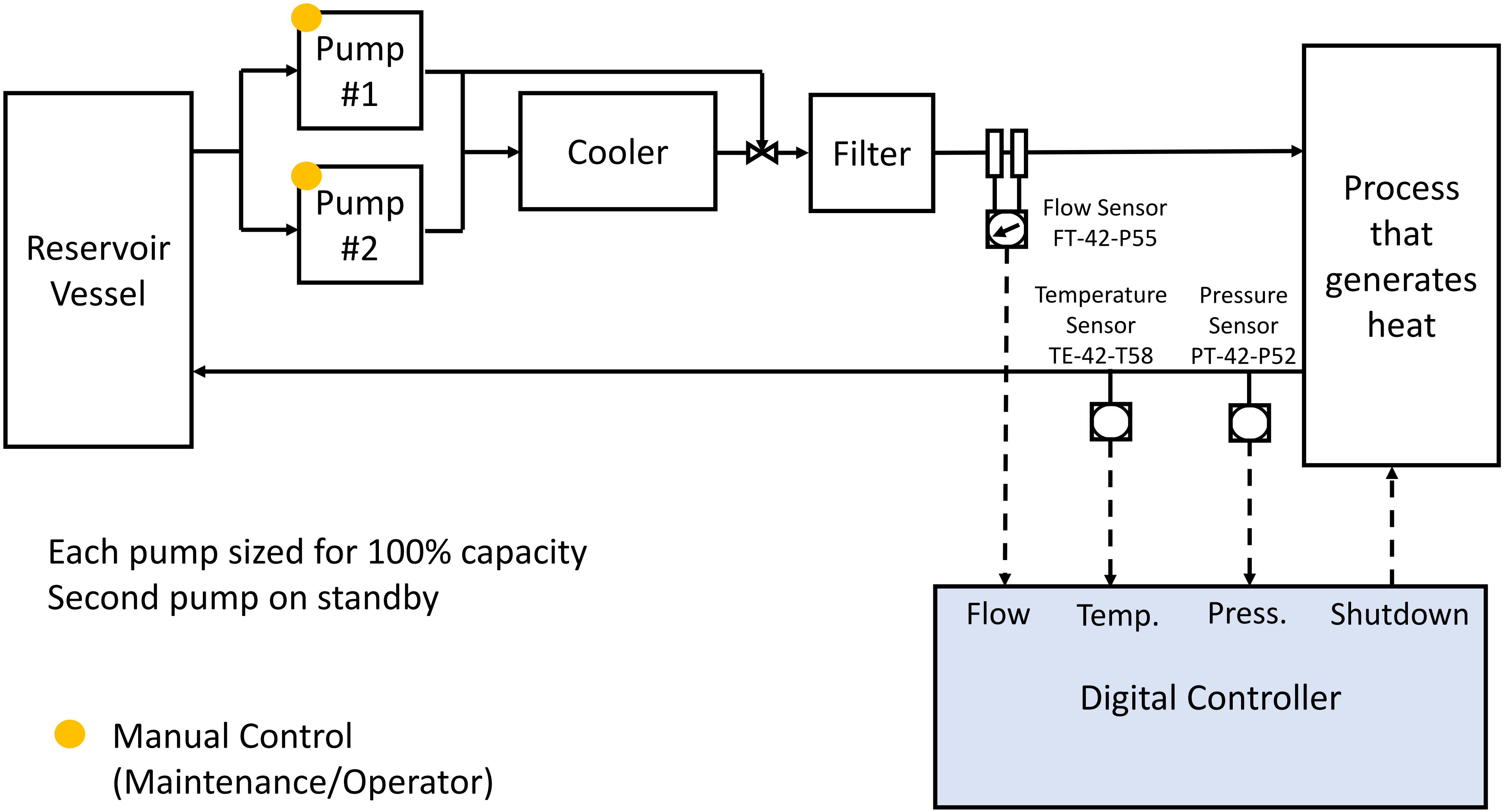
Old Cooling System 1.0

History of Operation

- Cooling System 1.0 was originally built 40 years ago. It has been operating ever since without any unsafe behaviors, such as a loss of cooling without a shutdown.
- The design includes single points of failure that have lead to reliability, performance, and maintenance issues over the last 40 years, such as inadvertent shutdowns.

[1] This could be any process that generates heat, such as electrical power generation processes.

Old Cooling System 1.0 P&ID

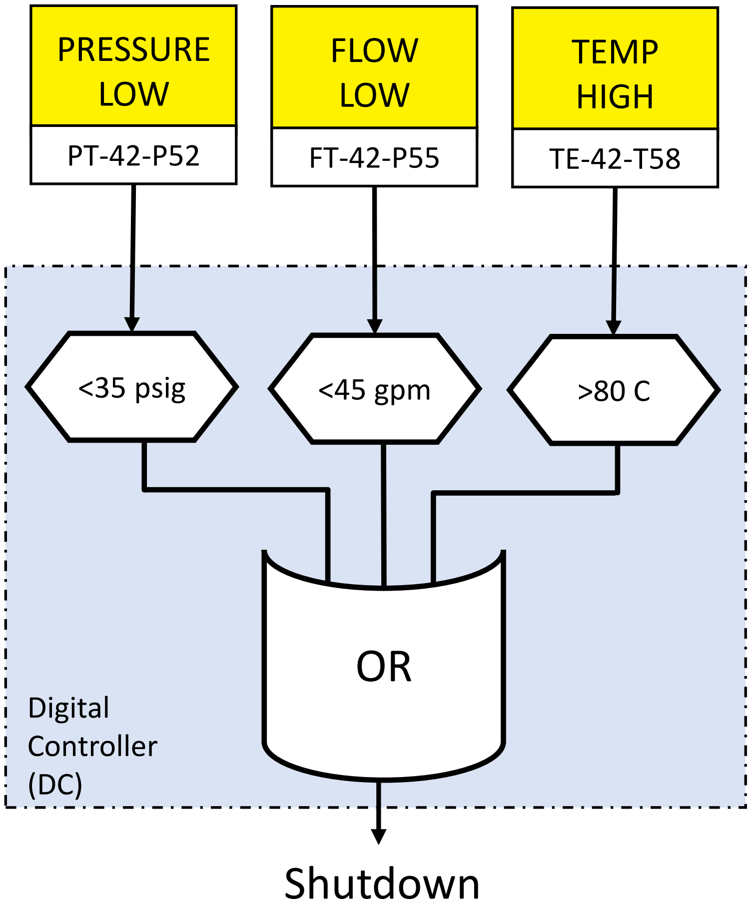


Each pump sized for 100% capacity
Second pump on standby

● Manual Control (Maintenance/Operator)

Old Cooling System 1.0 Digital Logic

- Digital Controller must shutdown [heat generation processes] any time inadequate cooling is detected



Problem: Inadvertent Shutdown (from single sensor failure)
An inadvertent shutdown causes ~$1m production loss **each time**

Let’s design a new upgrade!

Leadership has decided to commission a modification to improve reliability by eliminating single points of failure. The new system will include redundant input signal devices, redundant digital signal processors, and redundant output devices.

New Cooling System 2.0

Same as 1.0

Cooling System 2.0 Concept of Operation:

- System will provide automatic Shutdown on loss of cooling.
- Loss of cooling is measured by
  - Low cooling flow, OR
  - Low cooling pressure, OR
  - High cooling temperature

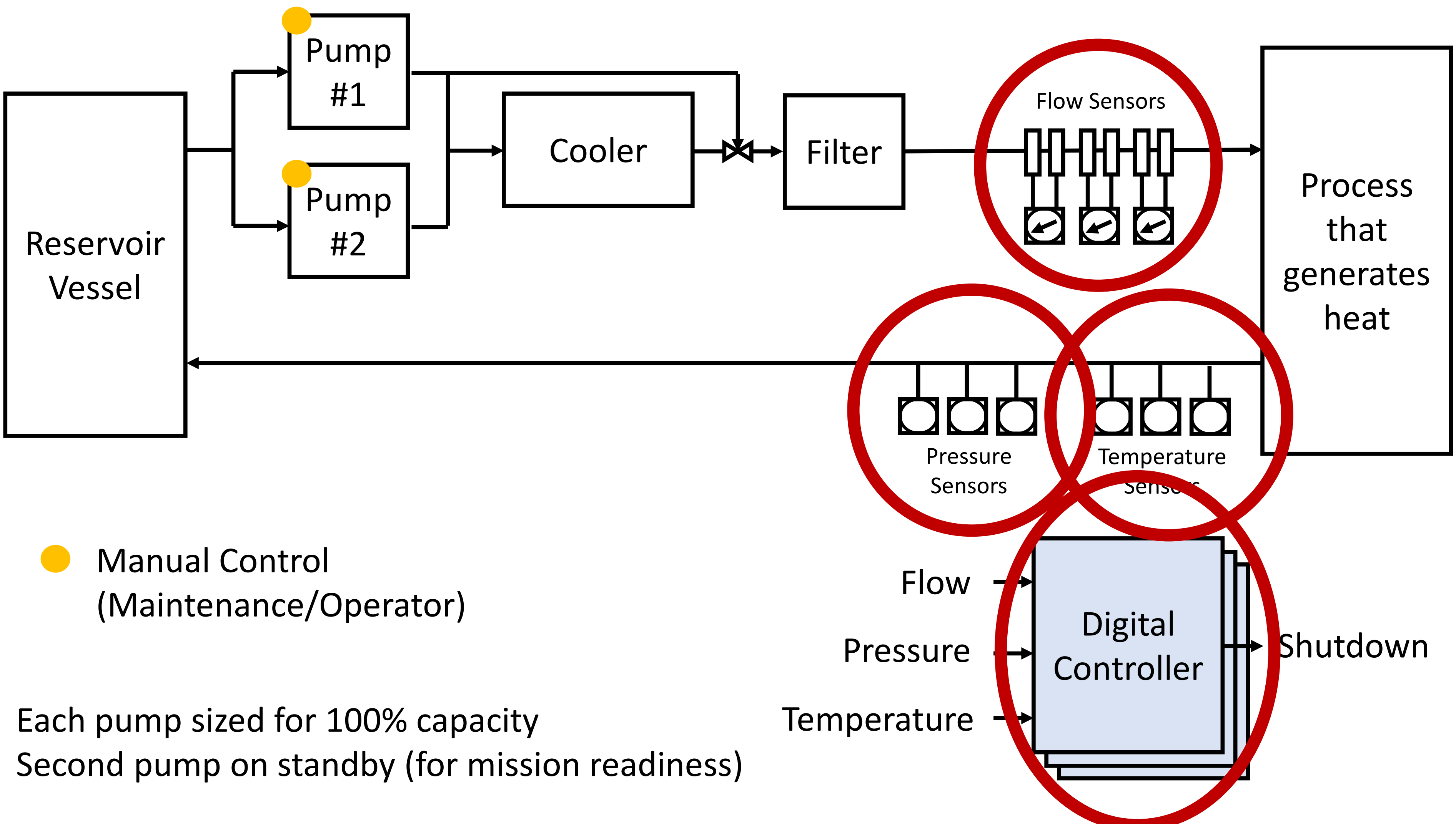
New in 2.0

- All instruments are triple redundant
- System will identify faulted instruments and will protect from inadvertent shutdown due to a faulted instrument.
  - If all 3 instruments for a channel are faulted, the system will send a shutdown command.

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

Cooling System 2.0 P&ID

- Essentially identical to 1.0, but with more redundancy

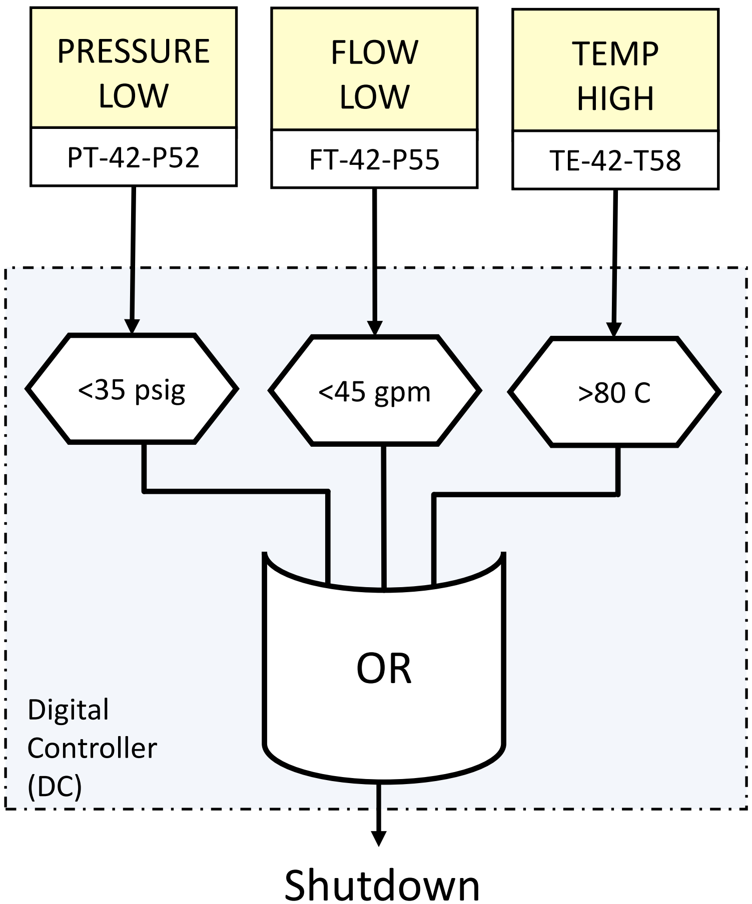


Each pump sized for 100% capacity
Second pump on standby (for mission readiness)

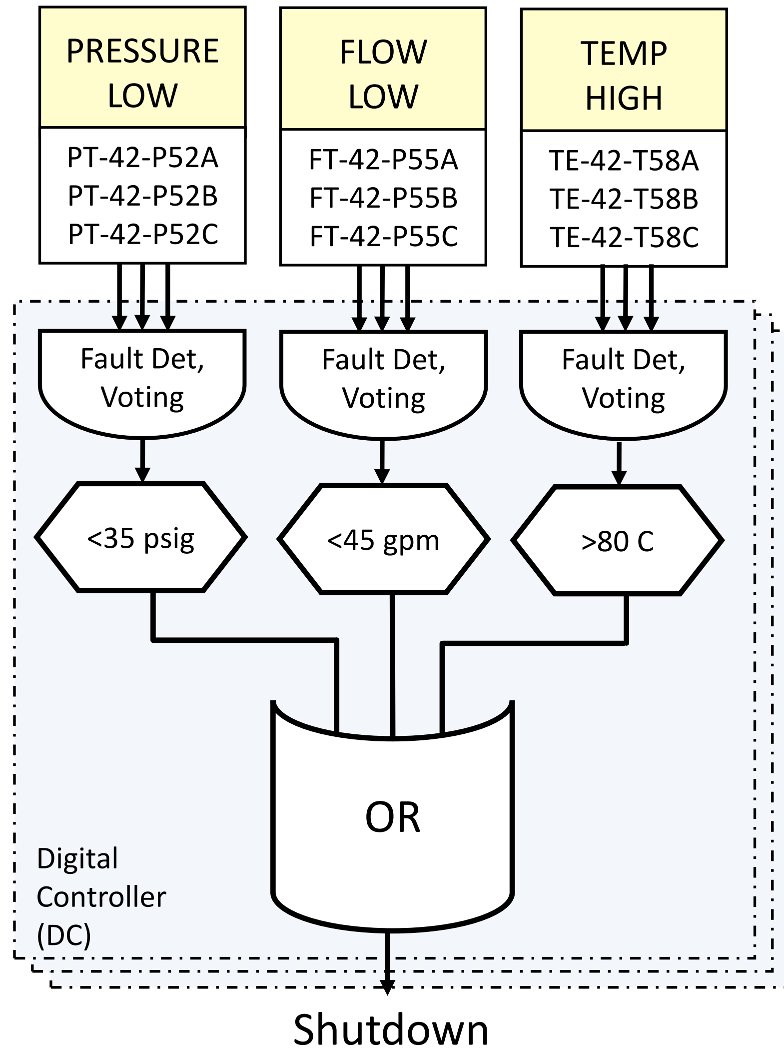
Changes in Red

Digital Controller

System 1.0



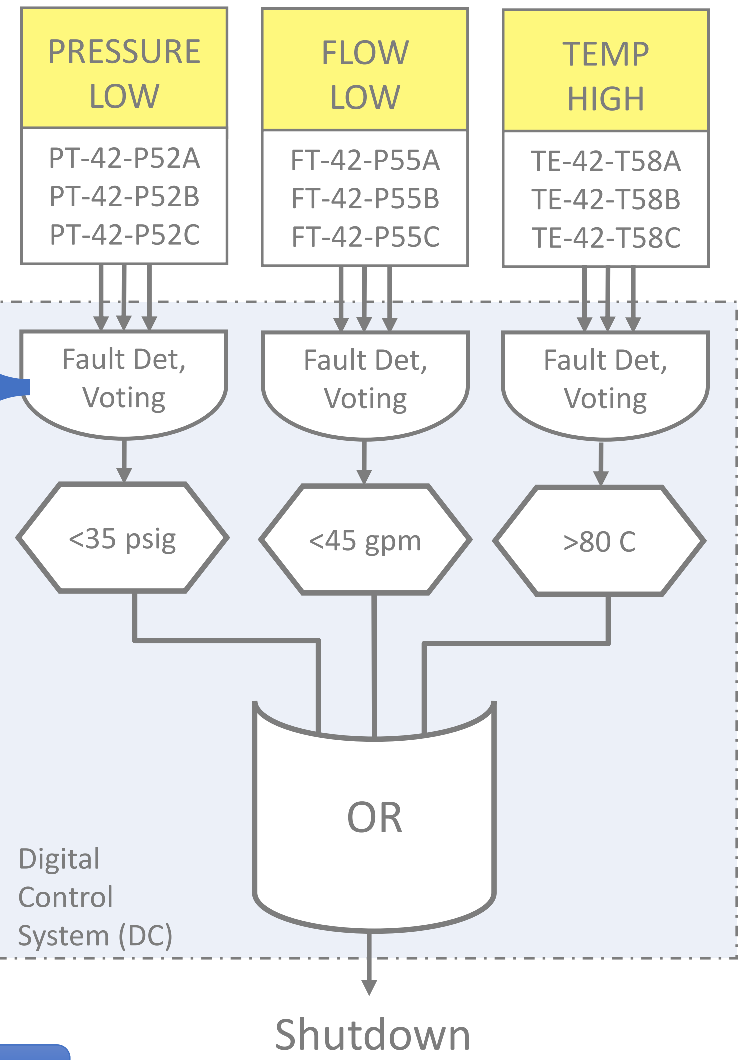
System 2.0



Digital Controller (DC) 2.0

Typical fault detection and voting

- Voting:
  - Median select of non-faulted sensors
- 1oo3 logic on each channel:
  - One instrument faulted:
    Use the remaining two instruments
  - Two instruments faulted:
    Use the third valid instrument
  - All three instruments faulted:
    Send a shutdown signal
- Detecting faulted instruments:
  - … it is outside the valid range (high or low). Setpoints for detection of faulted instrument are 3.8 mA (low) and 20.32 mA (high).
  - … it's value differs from median select of non-faulted sensors



Does this make sense so far?

Let’s evaluate the new system

- Let’s try:
  - Component view and conclusions

    vs.
  - Systems view and conclusions

Component view

- Analyze each component in isolation.
- Identify component failures or deviations.
- Identify and address the weakest components
- Aggregate component conclusions to make an overall conclusion

FMEA Excerpt (simplified)

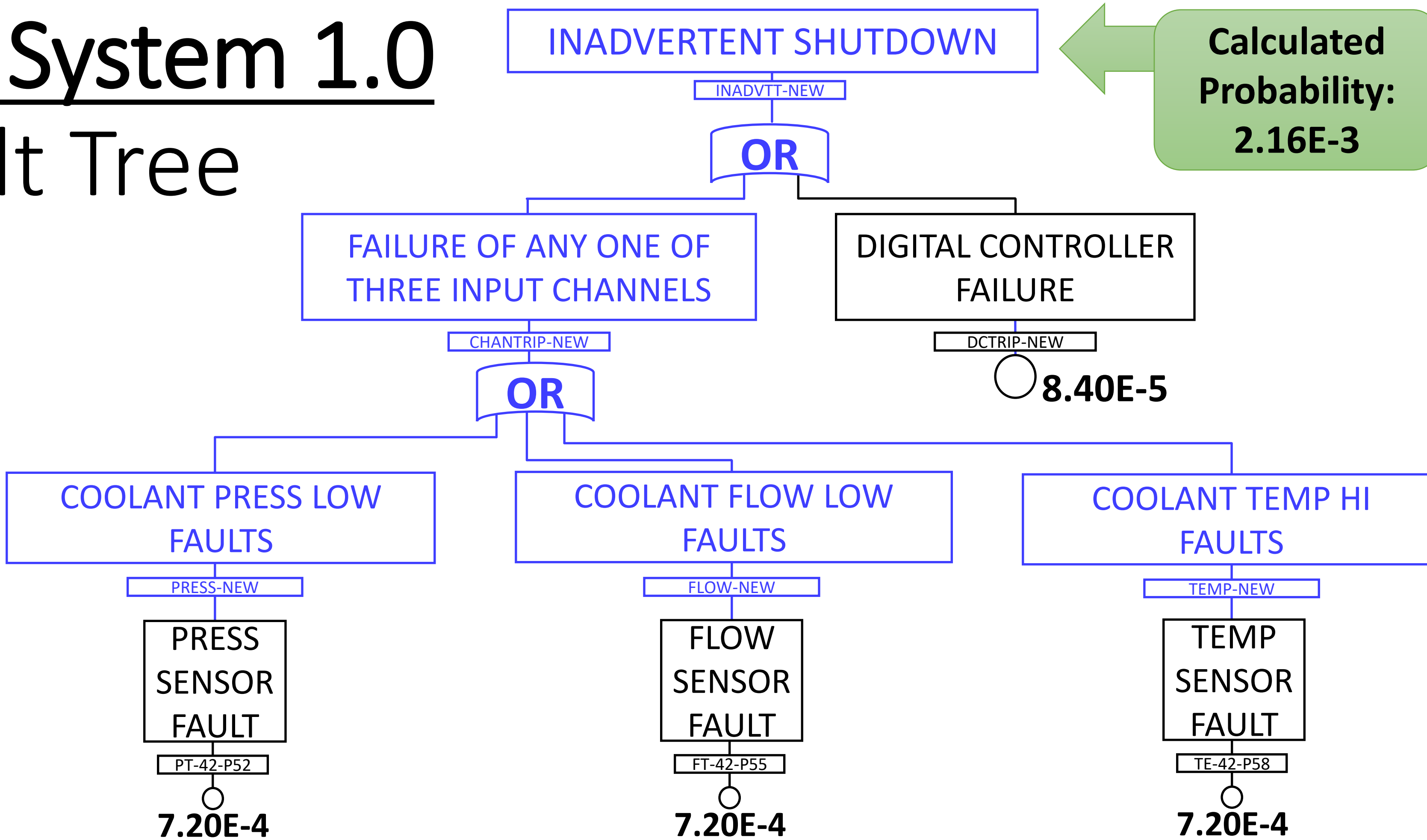
Component	Failure Mode	Failure Mechanism	Effect	Mitigations
Temperature Sensor TE-42-T58	Fail high	[…]	Unnecessary shutdown by DC (false positive)	3x Temp Sensors, DC logic protects from single or dual sensor failures
Temperature Sensor TE-42-T58	Fail low	[…]	Undetected loss of cooling: Damage to equipment,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

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

Simplified FMEA shown here. Full FMEA includes Failure Mode, Failure Mechanism, Cause, Symptoms, Local Effects, Method of Detection, Inherent Compensating Feature, Effect on System, Criticality, and other fields.

Old System 1.0

Fault Tree

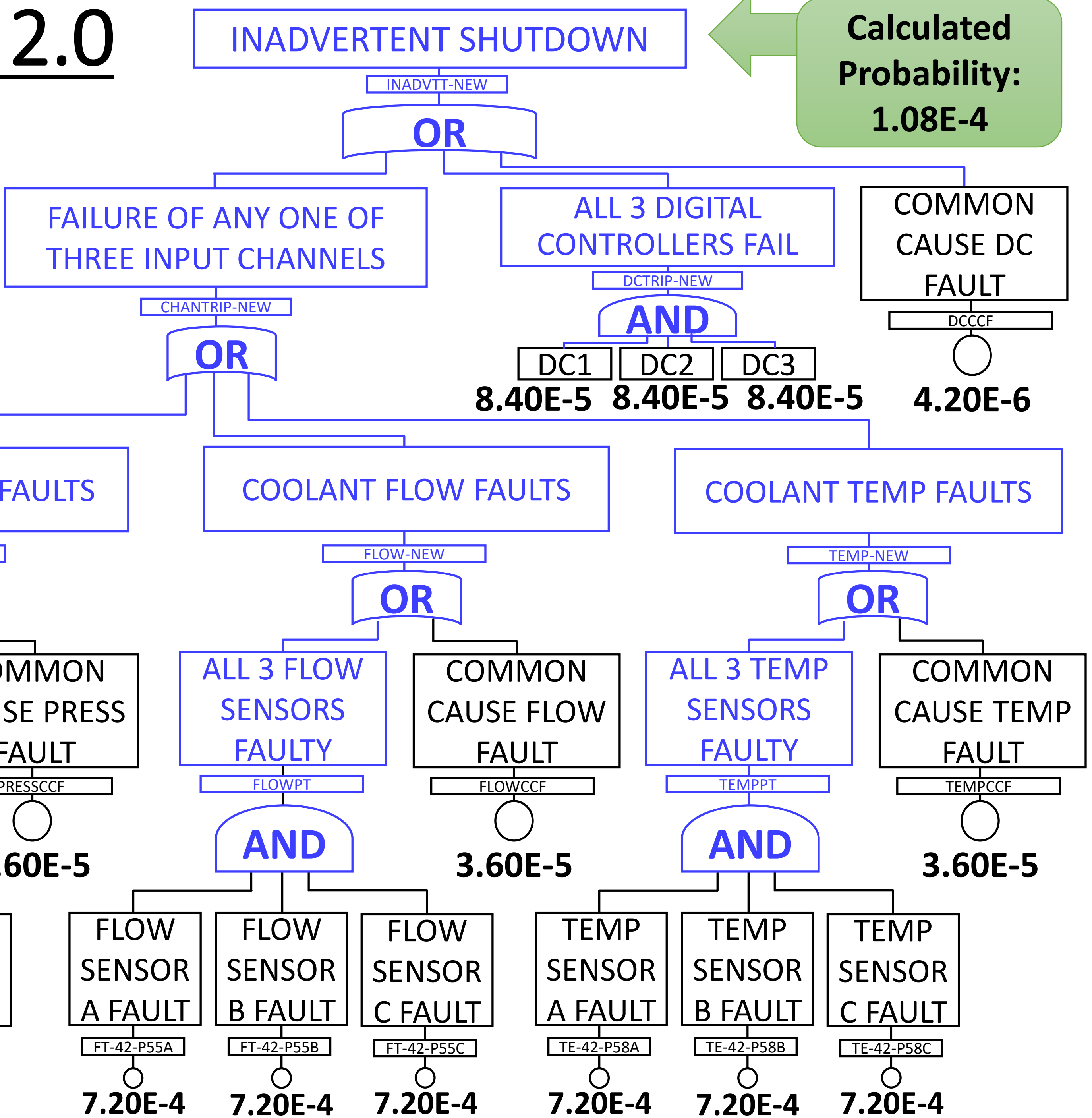


Simplified fault tree shown here. Full fault tree and additional nodes / combinations are not shown.

New System 2.0

Fault Tree

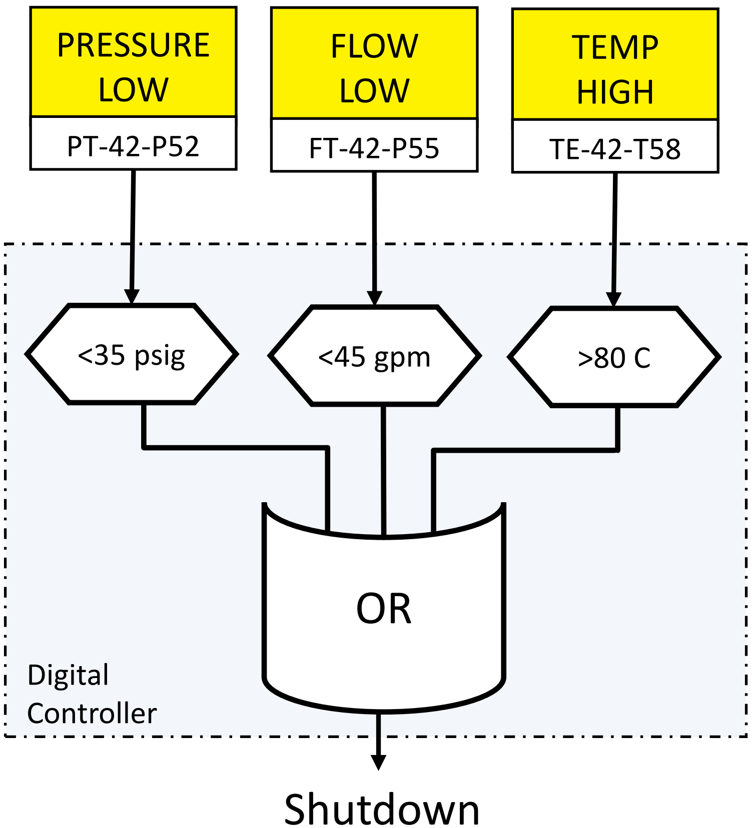
(with CCF)



Simplified fault tree shown here. Full fault tree and additional nodes / combinations are not shown.

FTA Conclusions

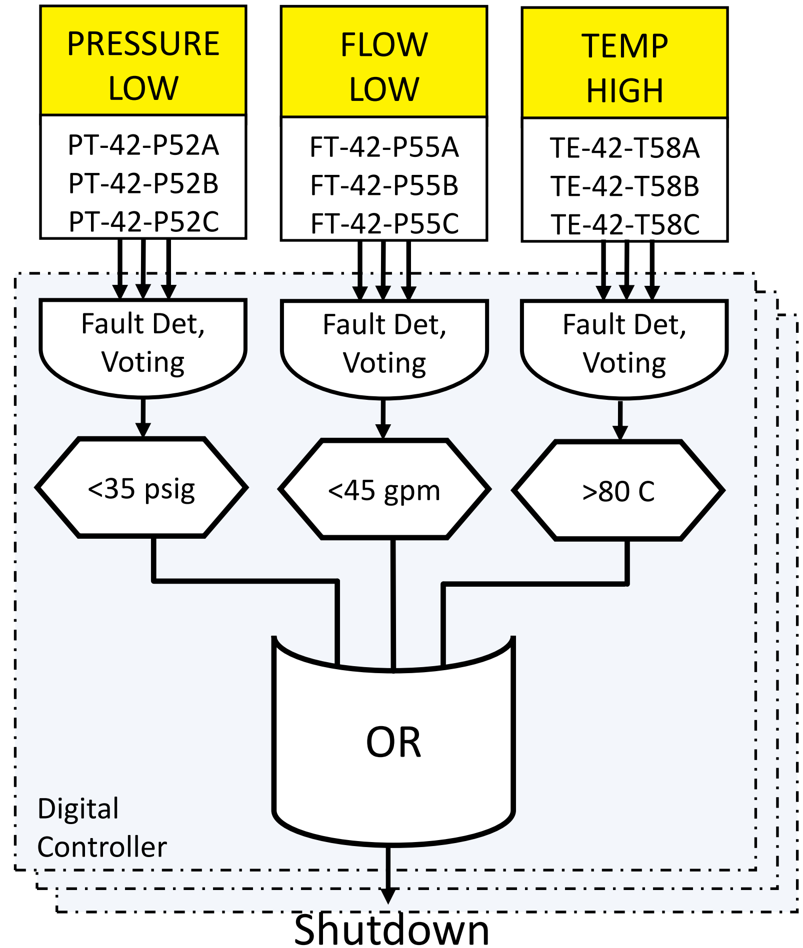
Old System



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

(~Once in 38 years)

New System



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

(~Once in 757 years)

IS = Inadvertent Shutdown

Conclusions from Component View

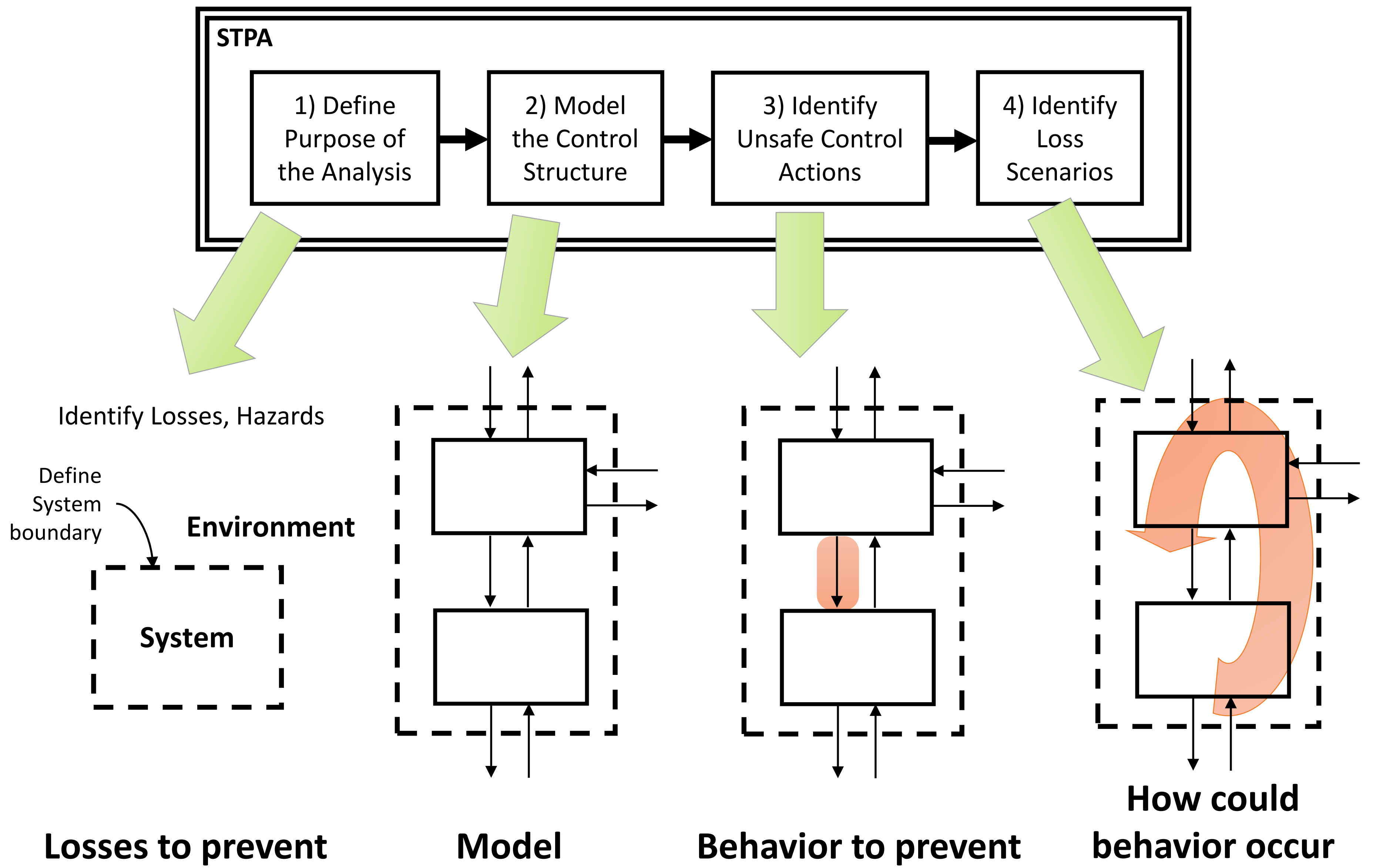
- The new system with triple redundancy will be **~10x more reliable** than the old system with single points of failure.
- The new system will pay for itself due to the **lower rate of inadvertent shutdowns** (false positives).
- A weak link in new system is the failure rate of the dual-redundant pumps[1]. Solution: **more frequent preventative maintenance** of the pumps.

[1] The pumps and many other components are not shown on previous slides for simplicity.

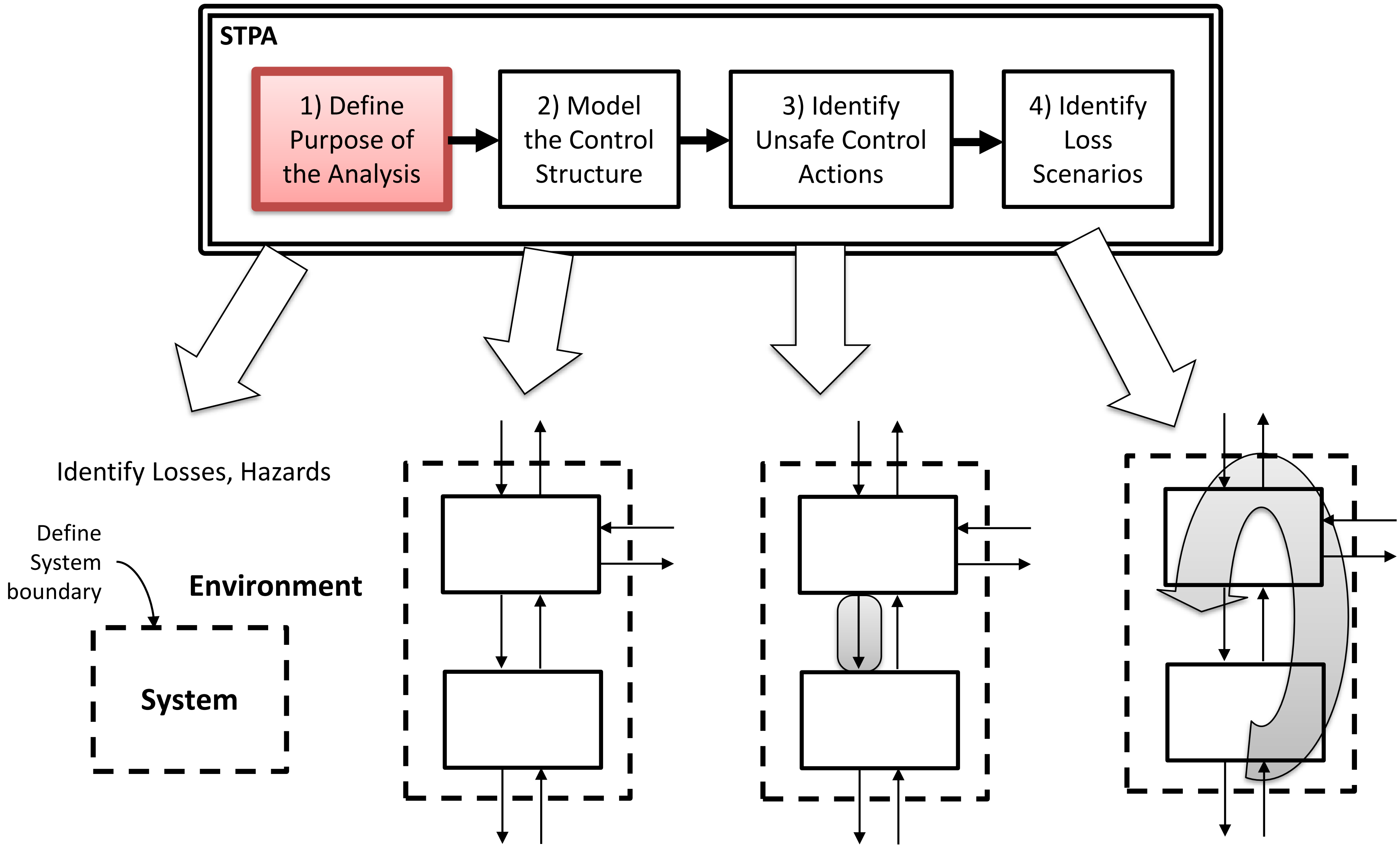
Let's evaluate the new system

- Let's try:
  - Component view and conclusions
    vs.
  - Systems view and conclusions

Let's try STPA!



(Leveson and Thomas, 2018)



(Leveson and Thomas, 2018)

STPA Step 1 Example Results

Losses

- L1: Loss of life or injury
- L2: Damage to equipment & assets
- L3: Loss of mission (production)
- Etc.

System-level Hazards (Plant)

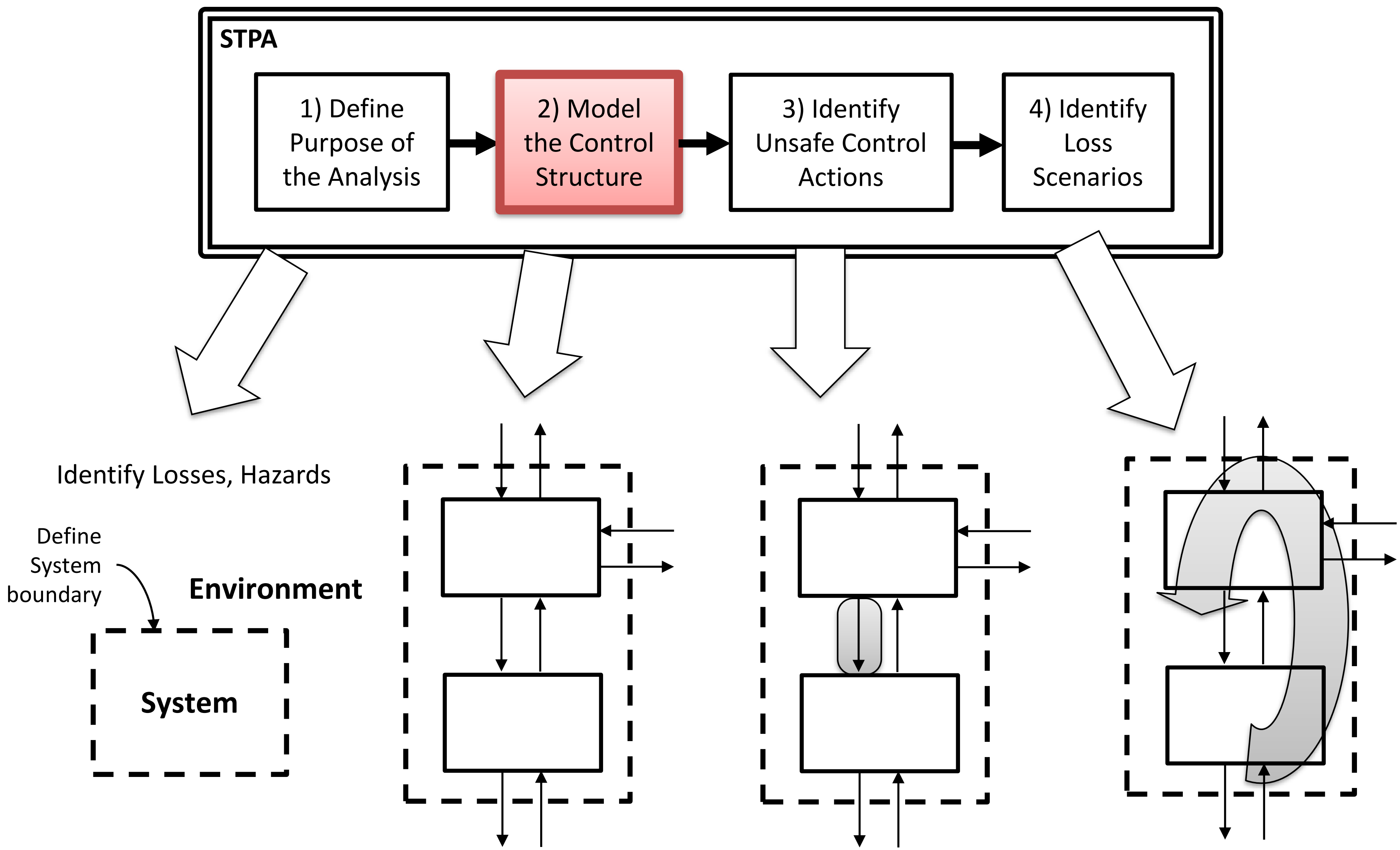
- H-1: **Plant** releases toxic materials [L1,L3]
- H-2: **Plant** is physically damaged [L2,L3]
- H-3: **Plant** unable to perform/produce X [L3]
- Etc.

System-level Hazards (Cooling System)

- C-H1: **Cooling system** unable to provide adequate cooling [H1,H2,H3]
- C-H2: **Cooling system** unable to prevent equipment damage [H2,H3]
- C-H3: **Cooling system** interferes with production [H3]
- Etc.

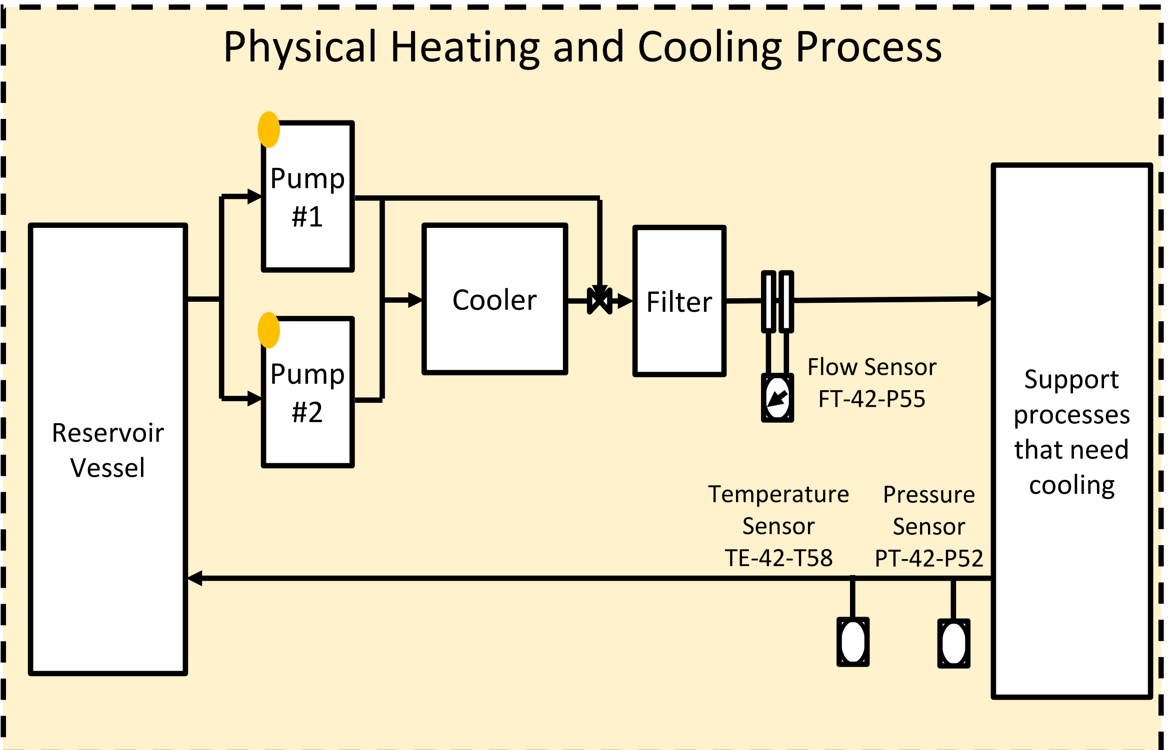
For this short exercise, we need a smaller scope. Our "system" will be the cooling system in these slides.

(John Thomas, 2021)



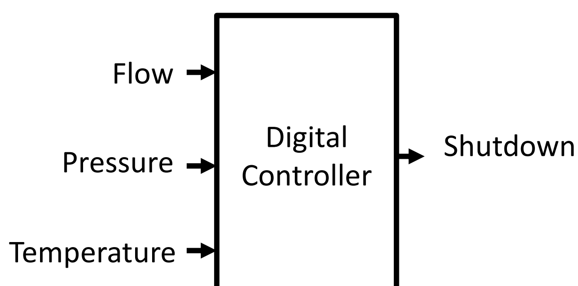
(Leveson and Thomas, 2018)

P&ID



Manual Control (Maintenance)

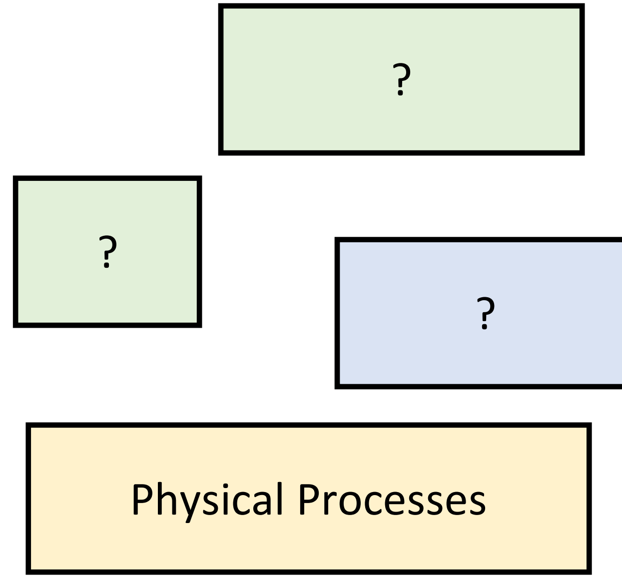
Each pump sized for 100% capacity
Second pump on standby



Exercise note: Stay true to the information provided—start here. When you need additional info, make whatever realistic assumptions you deem reasonable. Use chat for help.

(John Thomas, 2021)

STPA Control Structure



<u>Deliverable:</u> Draw your own control structure

- 3-4 boxes total
- Label the boxes (controllers)
- Draw & label all arrows
- Write goal/responsibility for each controller

Control Structure

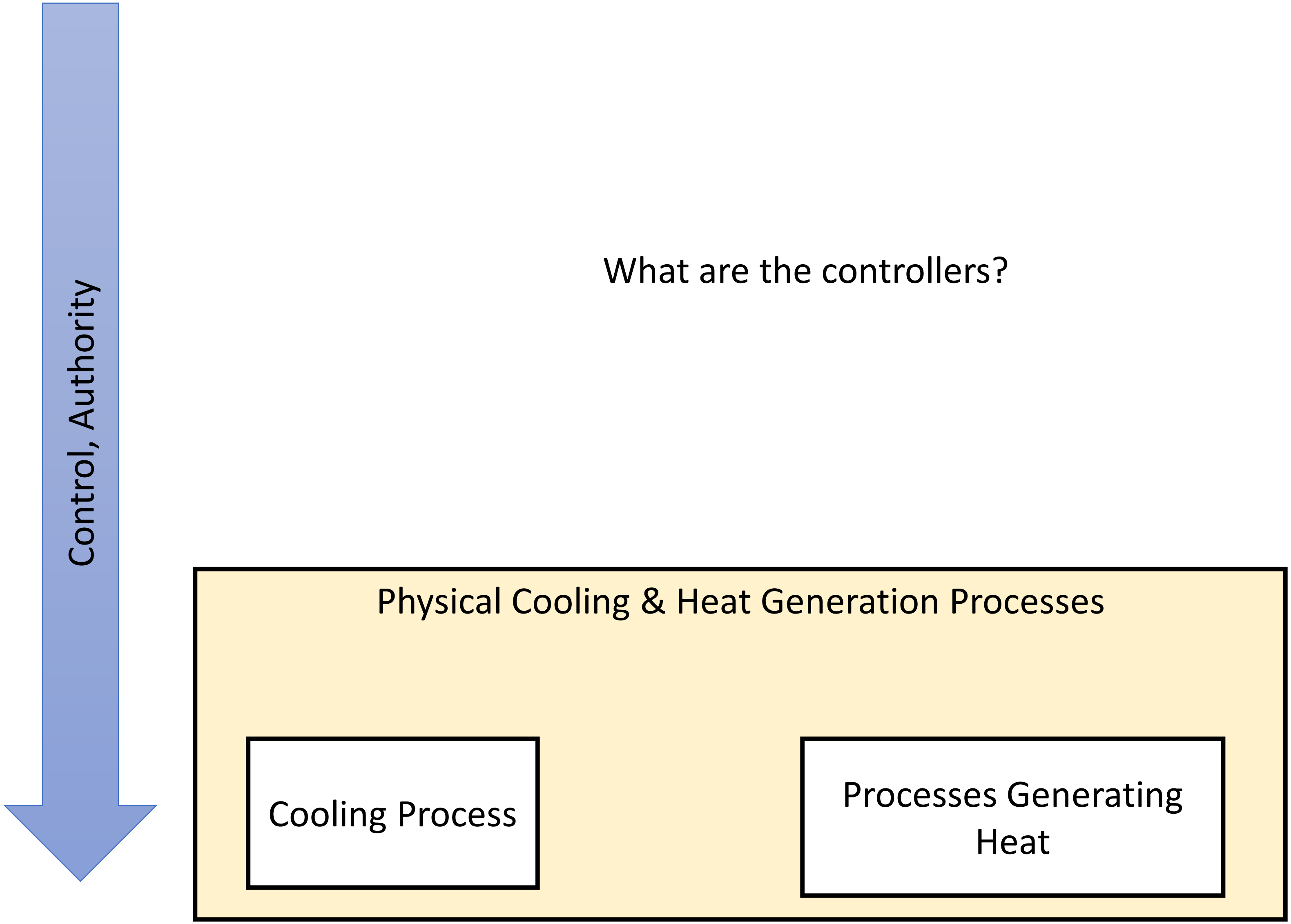
Where do you start?

One place to start is with the controlled processes
(as we did in previous exercises)

What are the controlled processes so far?

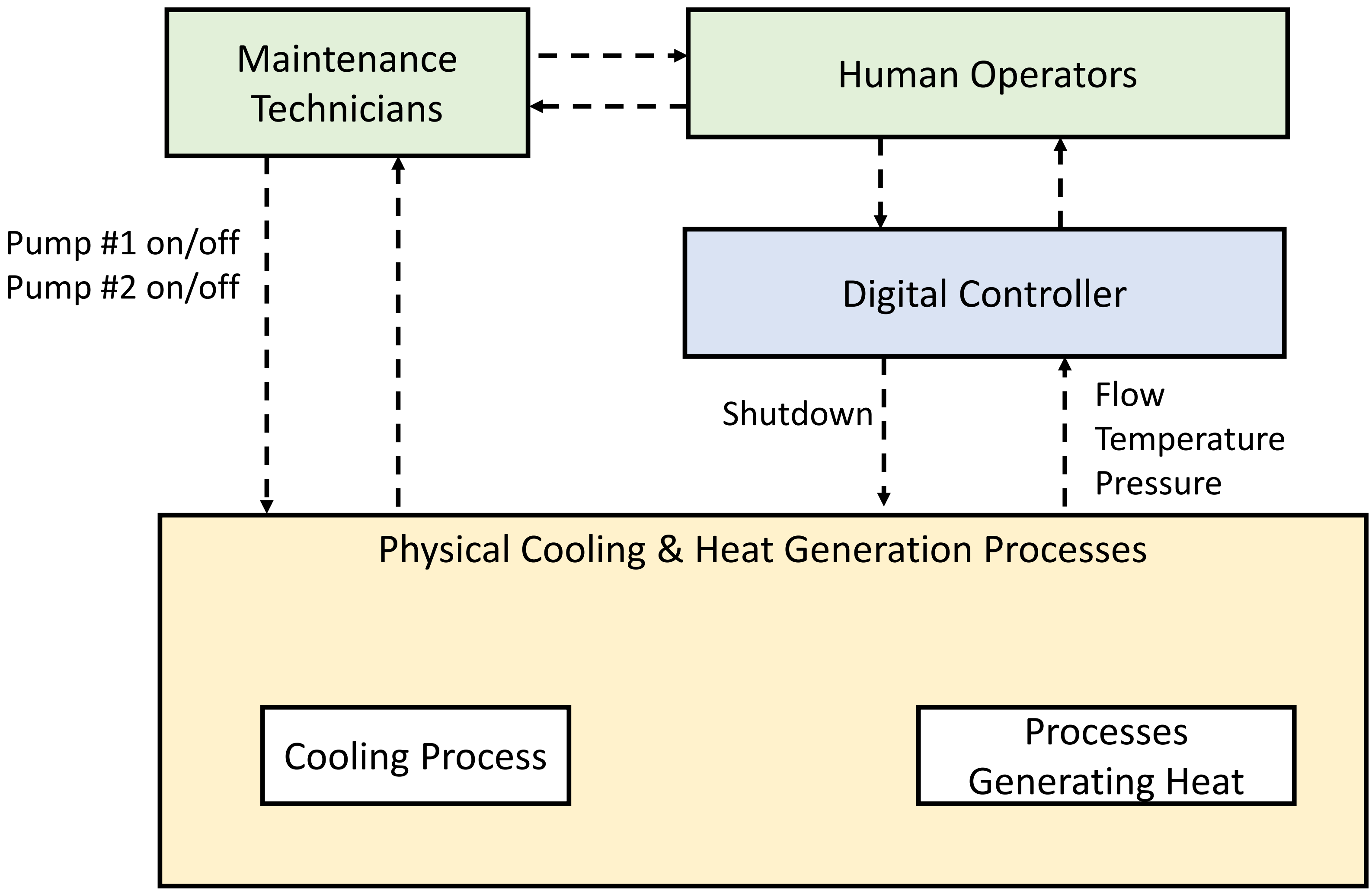
Control Structure

What are the controllers?

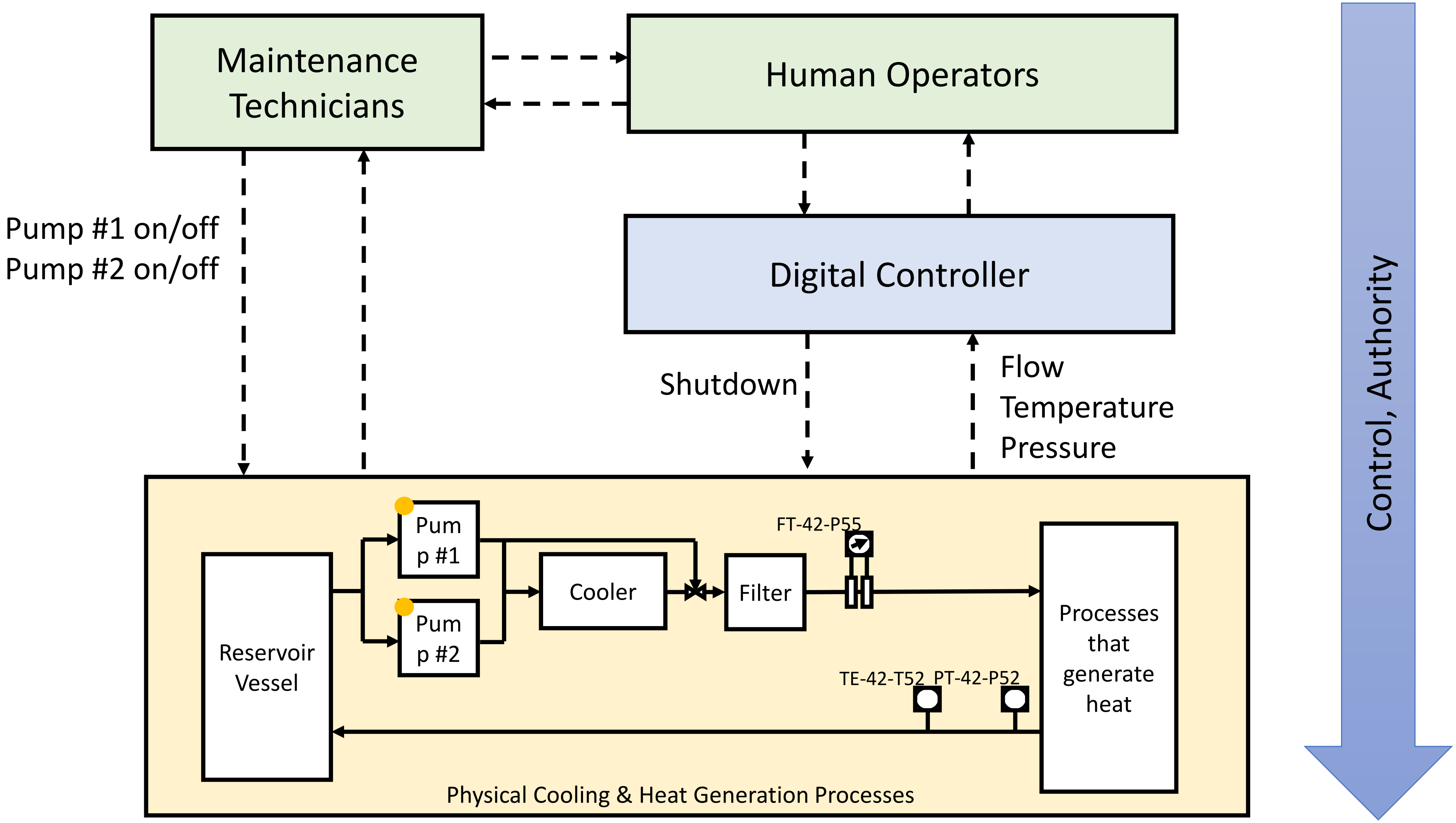


(John Thomas, 2021)

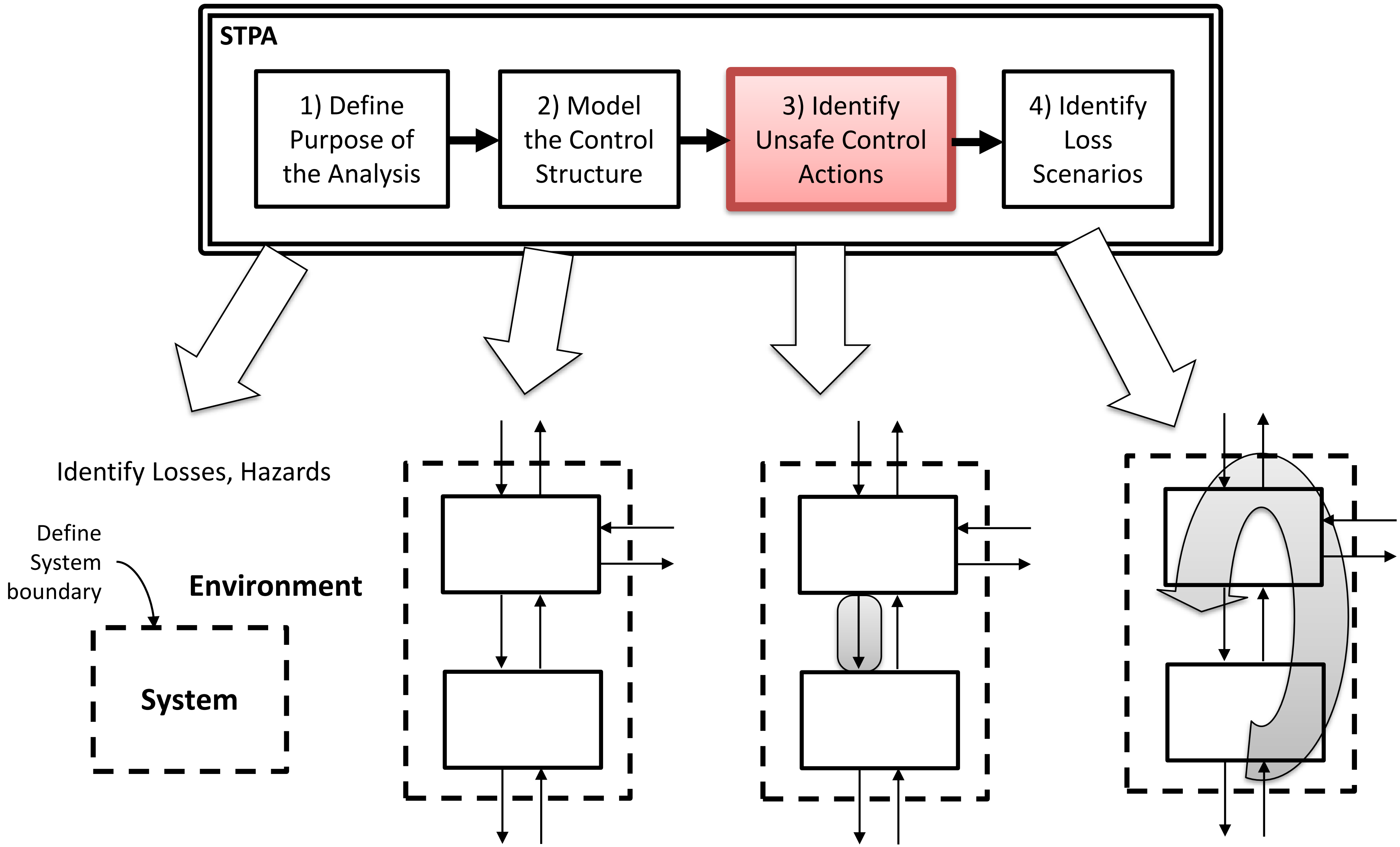
Example Control Structure



Example Control Structure



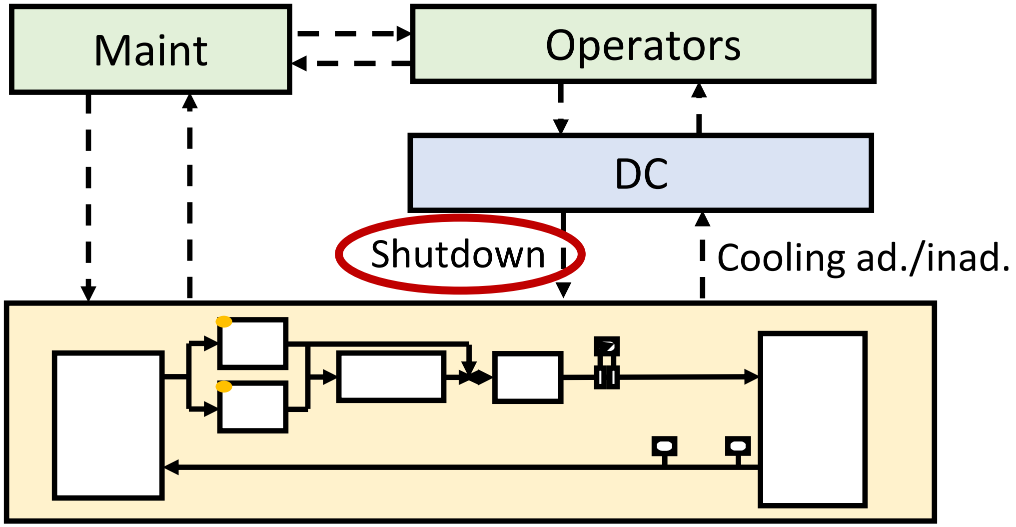
(John Thomas, 2021)



(Leveson and Thomas, 2018)

System-level Hazards

- H1: Cooling system unable to provide adequate cooling [L2,L3]
- H2: Cooling system unable to prevent equipment damage [L2,L3]
- H3: Cooling system interferes with production [L3]



Unsafe Control Actions

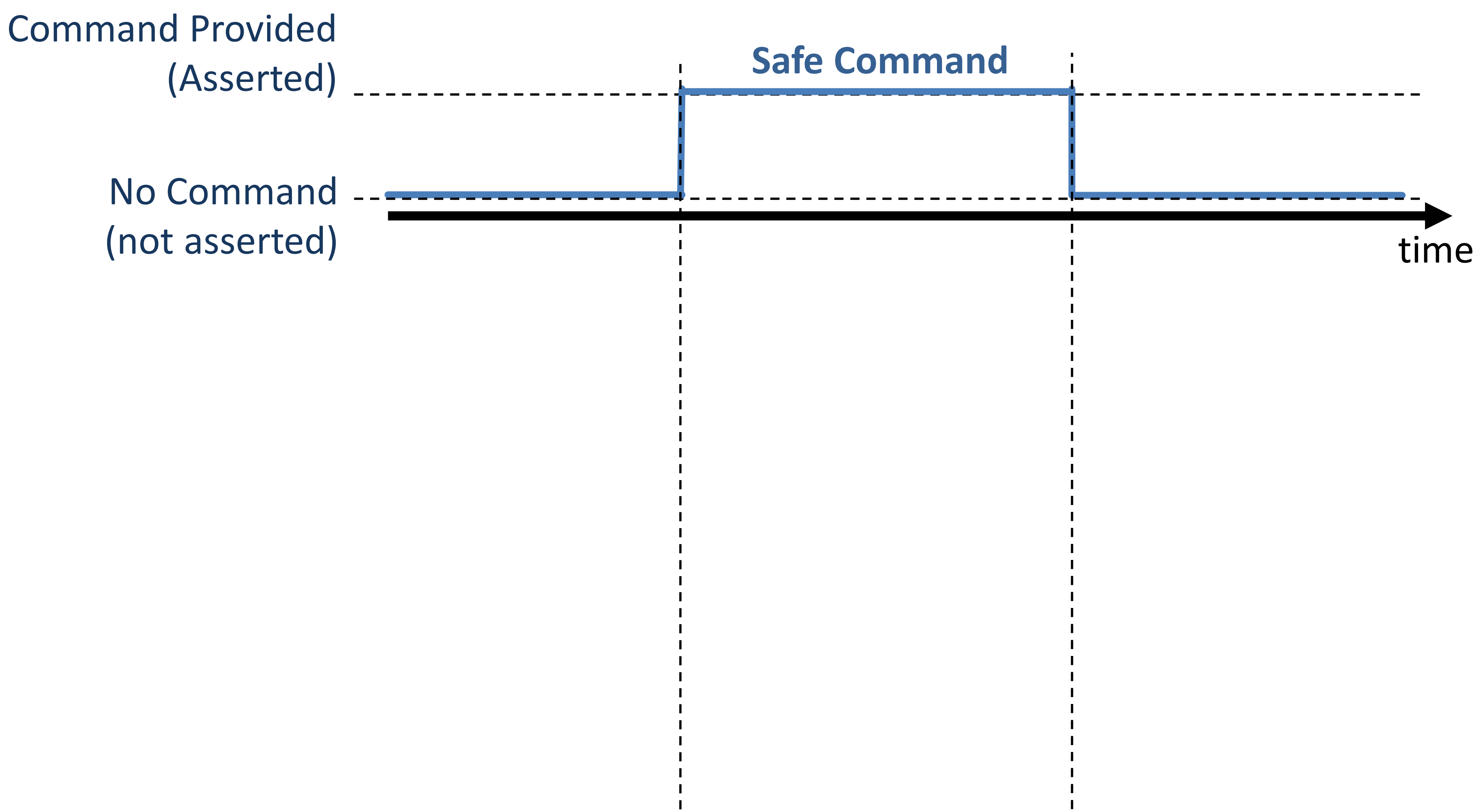
	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped Too Soon / Applied too long
Shutdown Cmd	DC does not provide Shutdown Cmd when ____________	DC provides Shutdown Cmd when ___________	DC provides Shutdown Cmd before ___________ DC provides Shutdown Cmd after ___________	DC stops providing Shutdown Cmd too soon before ______ DC continues providing Shutdown Cmd too long after________

Deliverable: Identify UCAs

(John Thomas, 2021)

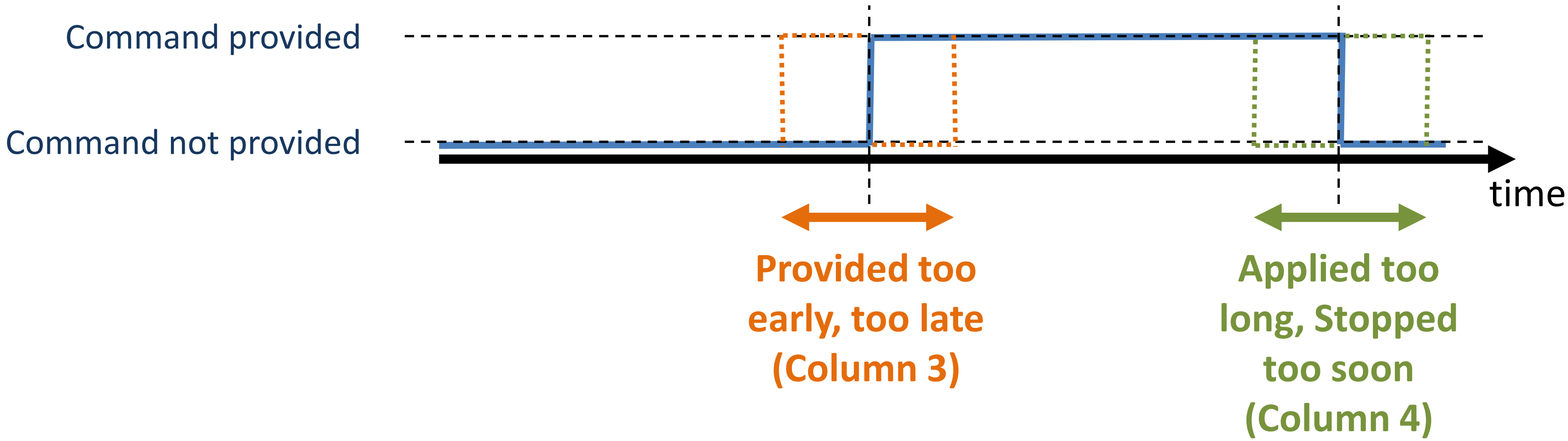
Note: This short example is incomplete, for demonstration only!

Safe Command



(Thomas. 2018)

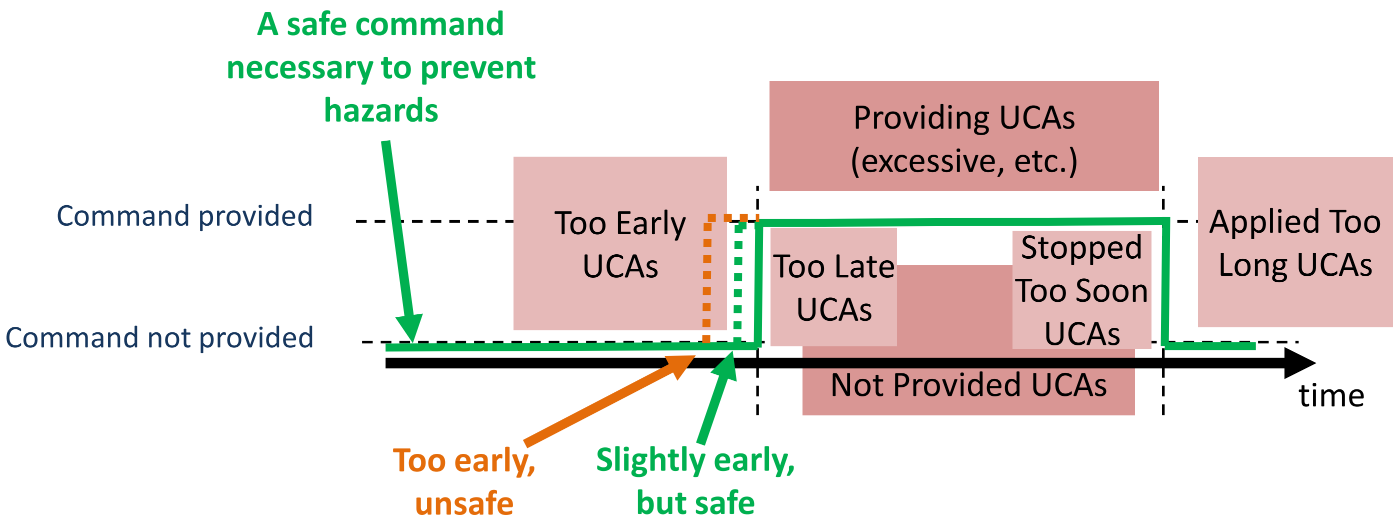
UCA Type 3 vs. Type 4



	1) Not providing causes hazard	2) Providing causes hazard	3) Too Early, Too Late, Order	4) Stopped Too Soon / Applied too long
<command>	?	?	?	?

(Thomas, 2018)

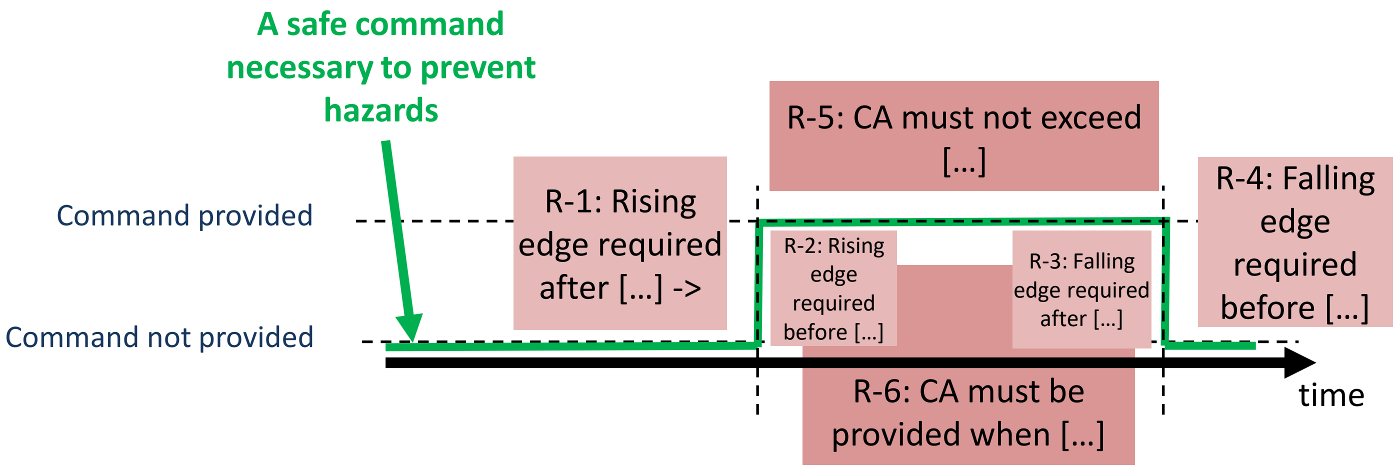
UCA Bounding



The complete set of UCAs will fully bound the necessary safe behavior

(Thomas, 2018)

UCAs -> Requirements

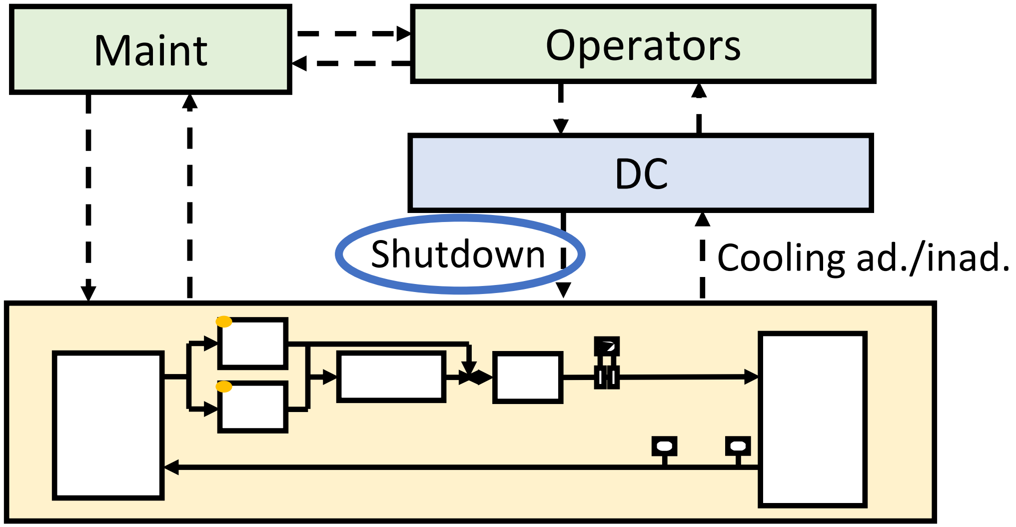


The UCAs will generate a complete set of safety requirements

(Thomas, 2018)

System-level Hazards

- H1: Cooling system unable to provide adequate cooling [L2,L3]
- H2: Cooling system unable to prevent equipment damage [L2,L3]
- H3: Cooling system interferes with production [L3]



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* [H2,3]	Controller provides Shutdown Cmd when cooling is adequate* [H3]	[...]	[...]

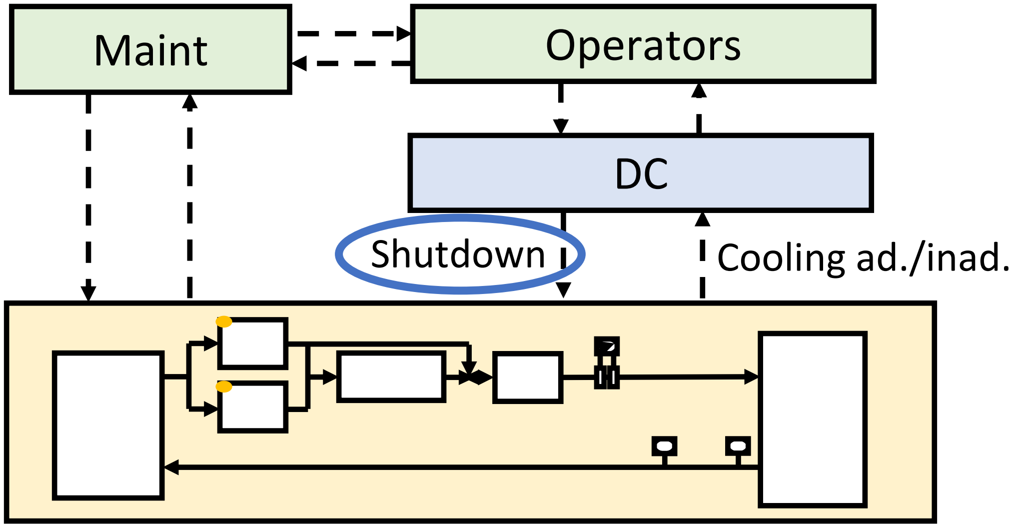
Cooling is inadequate* = low pressure OR low flow OR high temp

(John Thomas, 2021)

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

System-level Hazards

- H1: Cooling system unable to provide adequate cooling [L2,L3]
- H2: Cooling system unable to prevent equipment damage [L2,L3]
- H3: Cooling system interferes with production [L3]



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* [H2,3]	Controller provides Shutdown Cmd when cooling is adequate* [H3]	Controller provides Shutdown Cmd too late after equipment is damaged. [H2] Controller provides Shutdown Cmd too early before […]	Controller stops providing Shutdown Cmd too soon before Shutdown can be completed/latched [H2] Controller continues providing Shutdown Cmd too late after system & conditions are reset [H3]

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

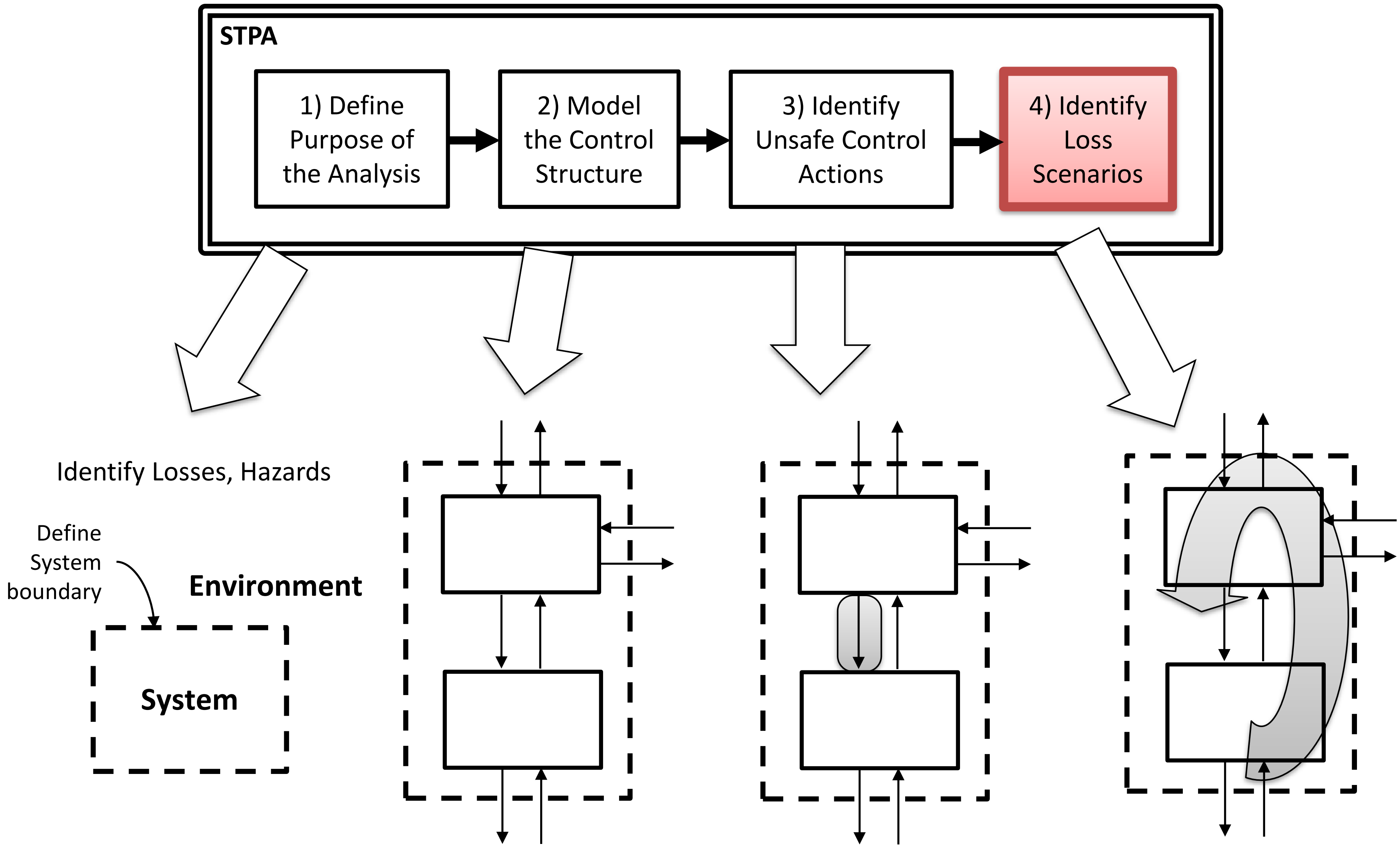
(John Thomas, 2021)

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

Component Safety Requirements / Constraints

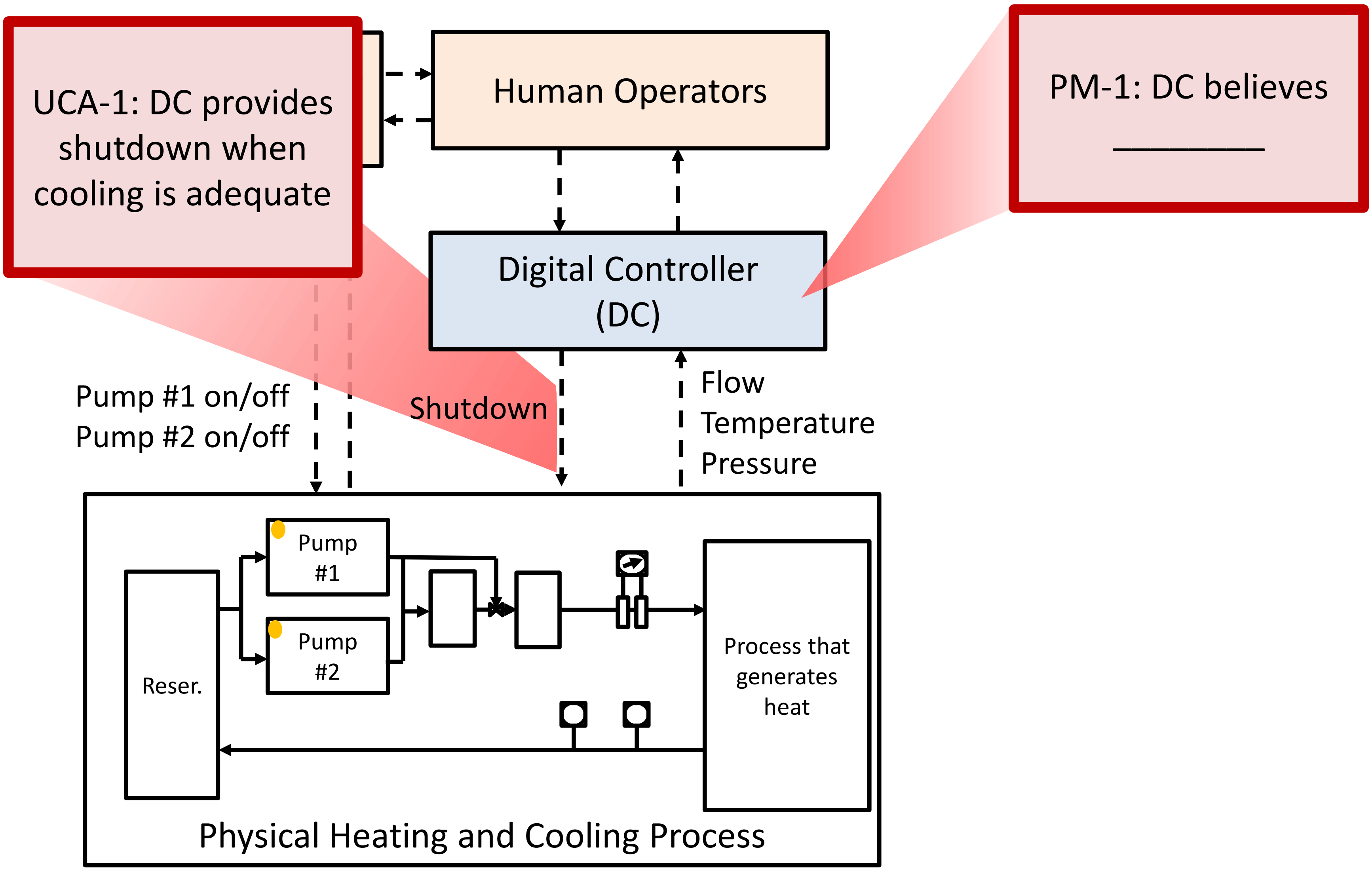
Unsafe Control Action		**Component Safety Requirement / Constraint**
Controller does not provide Shutdown Cmd when cooling is inadequate*	➡	Controller shall provide Shutdown Cmd when cooling is inadequate*
Controller provides Shutdown Cmd too late after equipment is damaged.	➡	Controller shall provide Shutdown Cmd within TBD s of TBD, before equipment is damaged
Controller stops providing Shutdown Cmd too soon before Shutdown can be completed/latched	➡	Controller shall continue providing Shutdown until confirmation of Shutdown Completed/Latched
Controller continues providing Shutdown Cmd too late after system & conditions are reset	➡	Controller shall stop providing Shutdown Cmd when system & conditions are reset

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



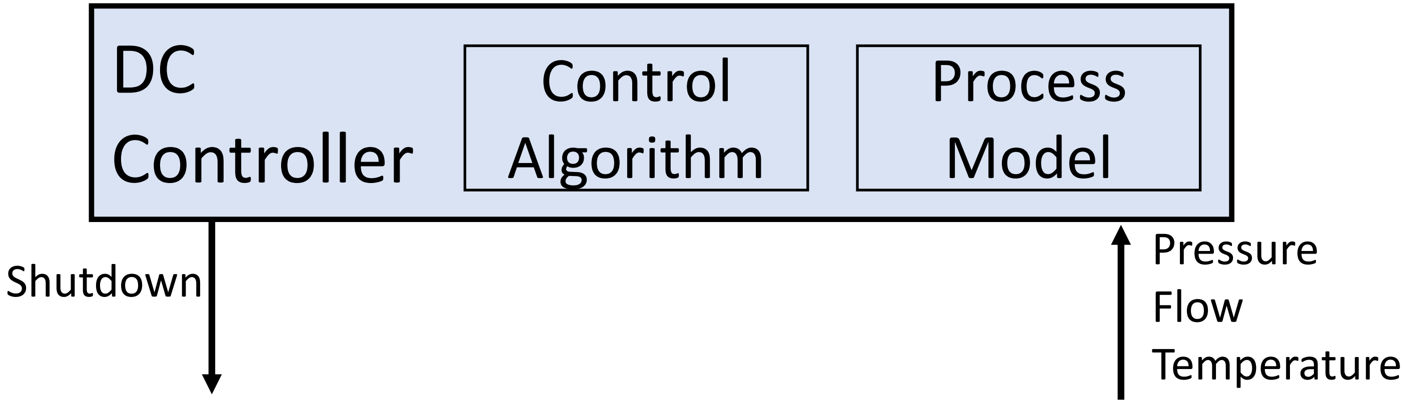
(Leveson and Thomas, 2018)

Building Loss Scenarios



John Thomas, 2020

Controller Analysis (Let's do this together!)



<u>DC output</u>

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

<u>DC process model</u>

PM-1: Controller believes _______

<u>DC input</u>

Flow inputs (observations by DC)
F-1: _______

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

Cooling System **2.0**

Purpose:

- Leadership has decided to commission a modification to improve reliability by eliminating single points of failure. The new system will include redundant input signal devices, redundant digital signal processors, and redundant output devices.

Cooling System 2.0 Concept of Operation:

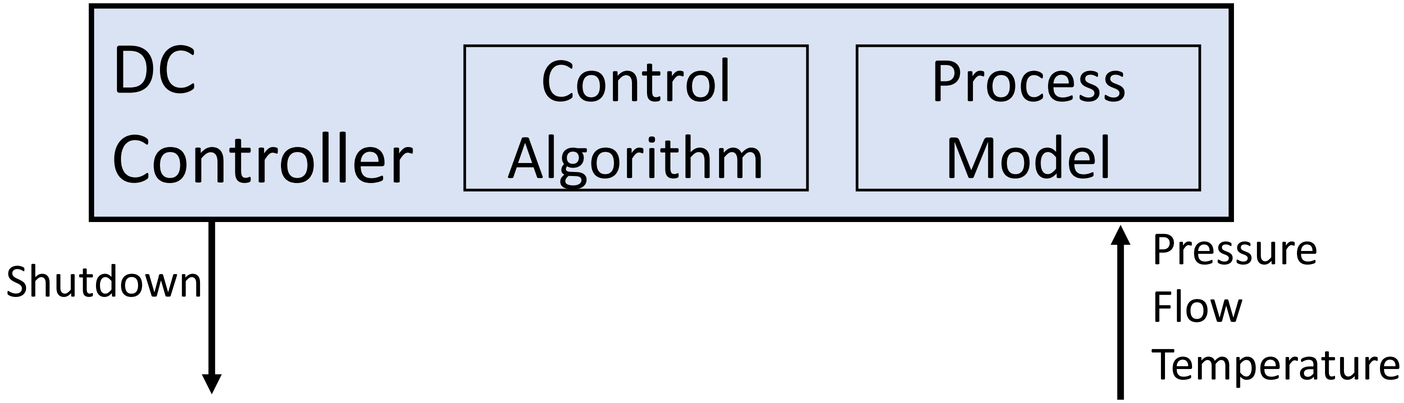
Same as 1.0

- System will provide automatic Shutdown on loss of cooling.
- Loss of cooling is measured by
  - Low cooling flow, OR
  - Low cooling pressure, OR
  - High cooling temperature

New in 2.0

- System will identify faulted instruments and will protect from inadvertent shutdown due to a faulted instrument.
  - If all 3 instruments for a channel are faulted, the system will send a shutdown command.

Controller Analysis (Let's do this together!)



DC output

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

DC process models

PM-1: Controller believes Pressure is too low

PM-2: Controller believes Temp is too high

PM-3: Controller believes Flow is too low

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

DC feedback

F-4: DC receives all flow sensor values out of range low (<3.8mA, 0 GPM)

F-5: DC receives all flow sensor values out of range high (>20.32mA, X GPM)

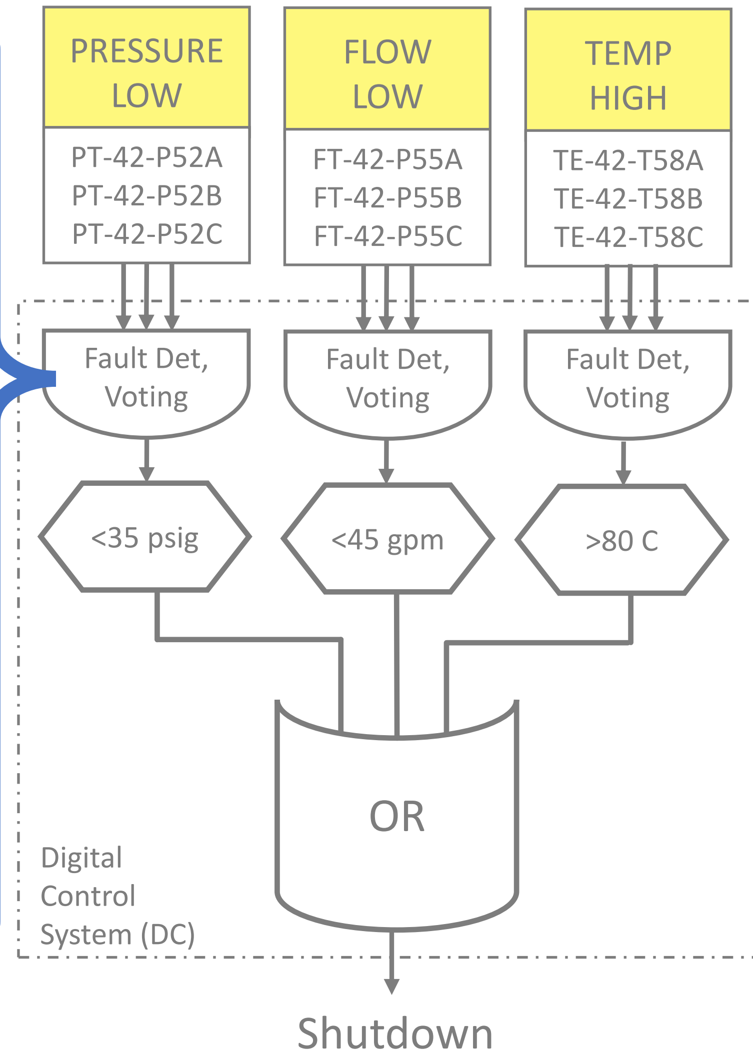
Note: This short example is incomplete, for demonstration only!

Loss of Cooling detection:
New System 2.0

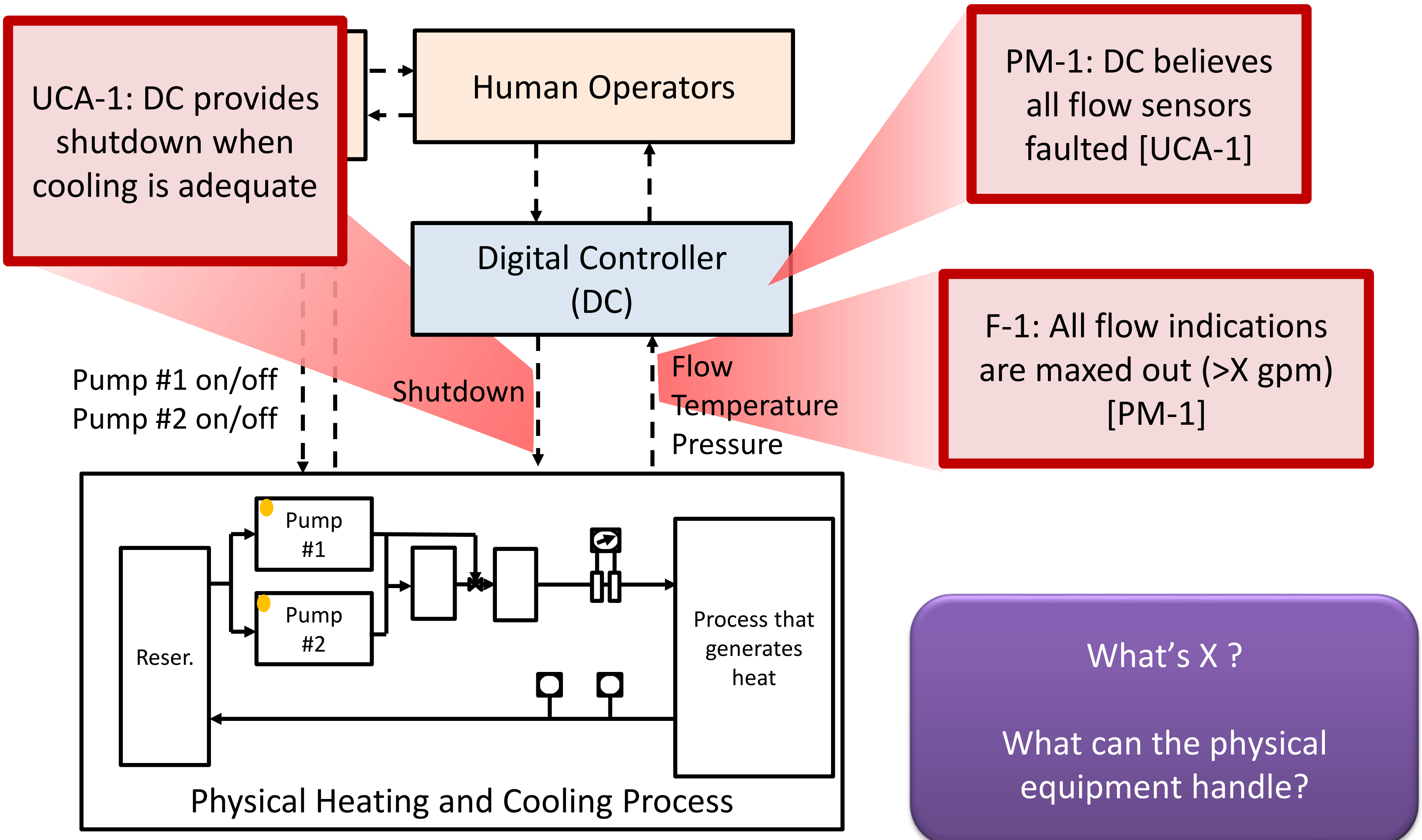
Fault detection and voting

- Voting:
  - Median select of non-faulted sensors
- 1oo3 logic on each channel:
  - One instrument faulted:
    Use the remaining two instruments
  - Two instruments faulted:
    Use the third valid instrument
  - All three instruments faulted:
    Send a shutdown signal
- Detecting faulted instruments:
  - Case A: It is outside the valid range (high or low). Setpoints for detection of faulted instrument are 3.8 mA (low) and 20.32 mA (high). OR
  - Case B: It's value differs from median select of non-faulted sensors

What value is out of bounds, indicating a faulted instrument?

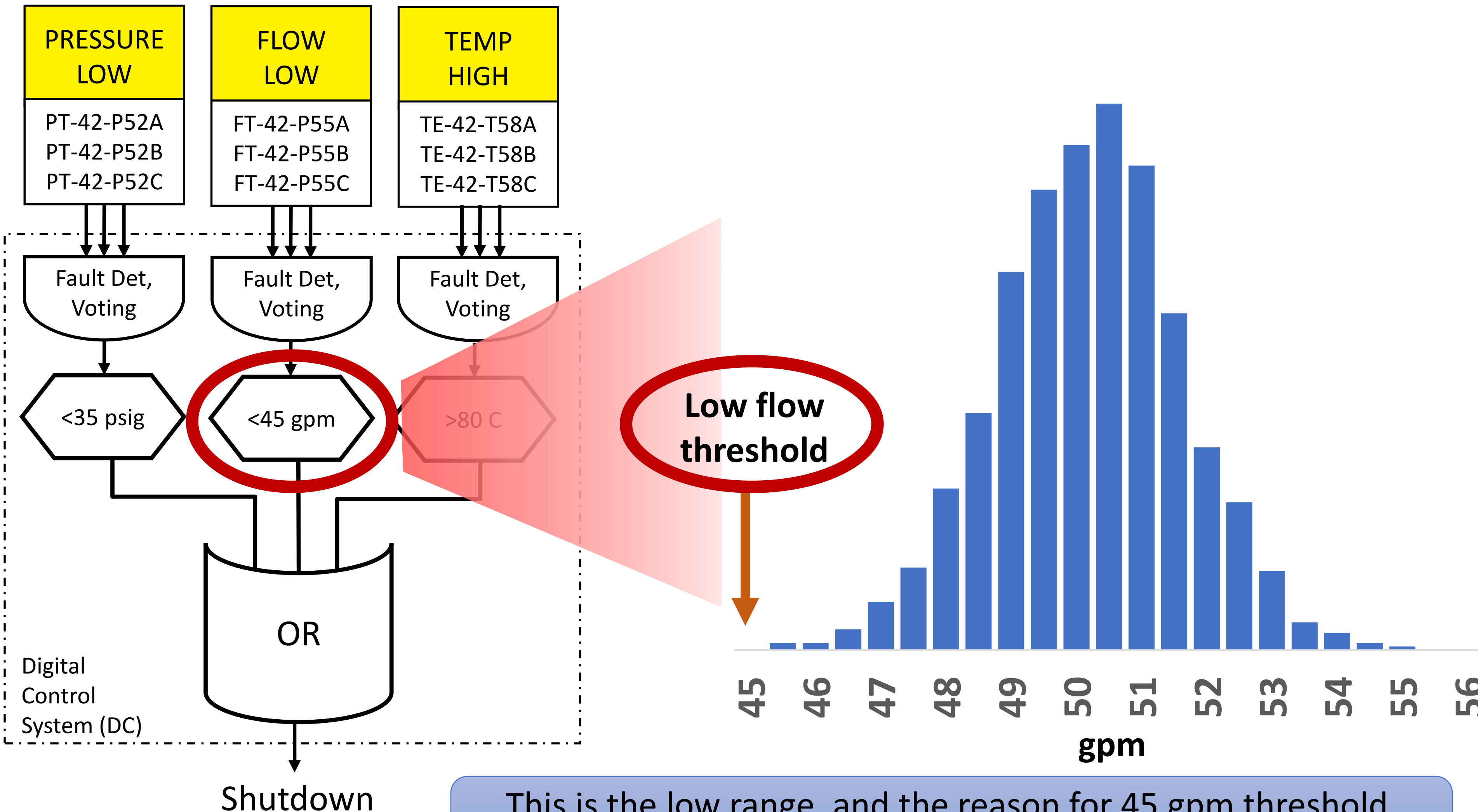


Building Loss Scenarios



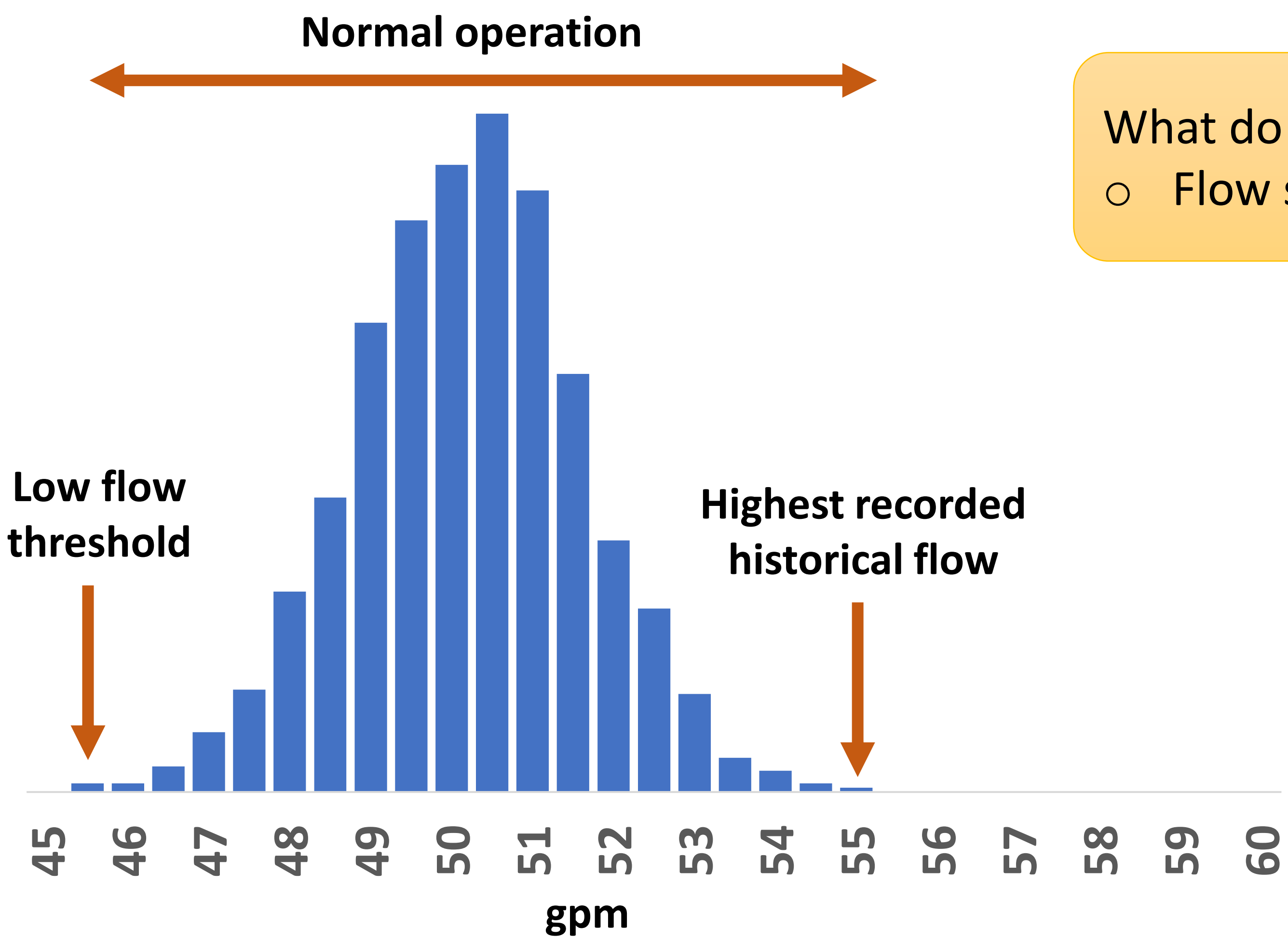
John Thomas, 2020

Historical flow data



This is the low range, and the reason for 45 gpm threshold.
What about too high? (sensor OORH)

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

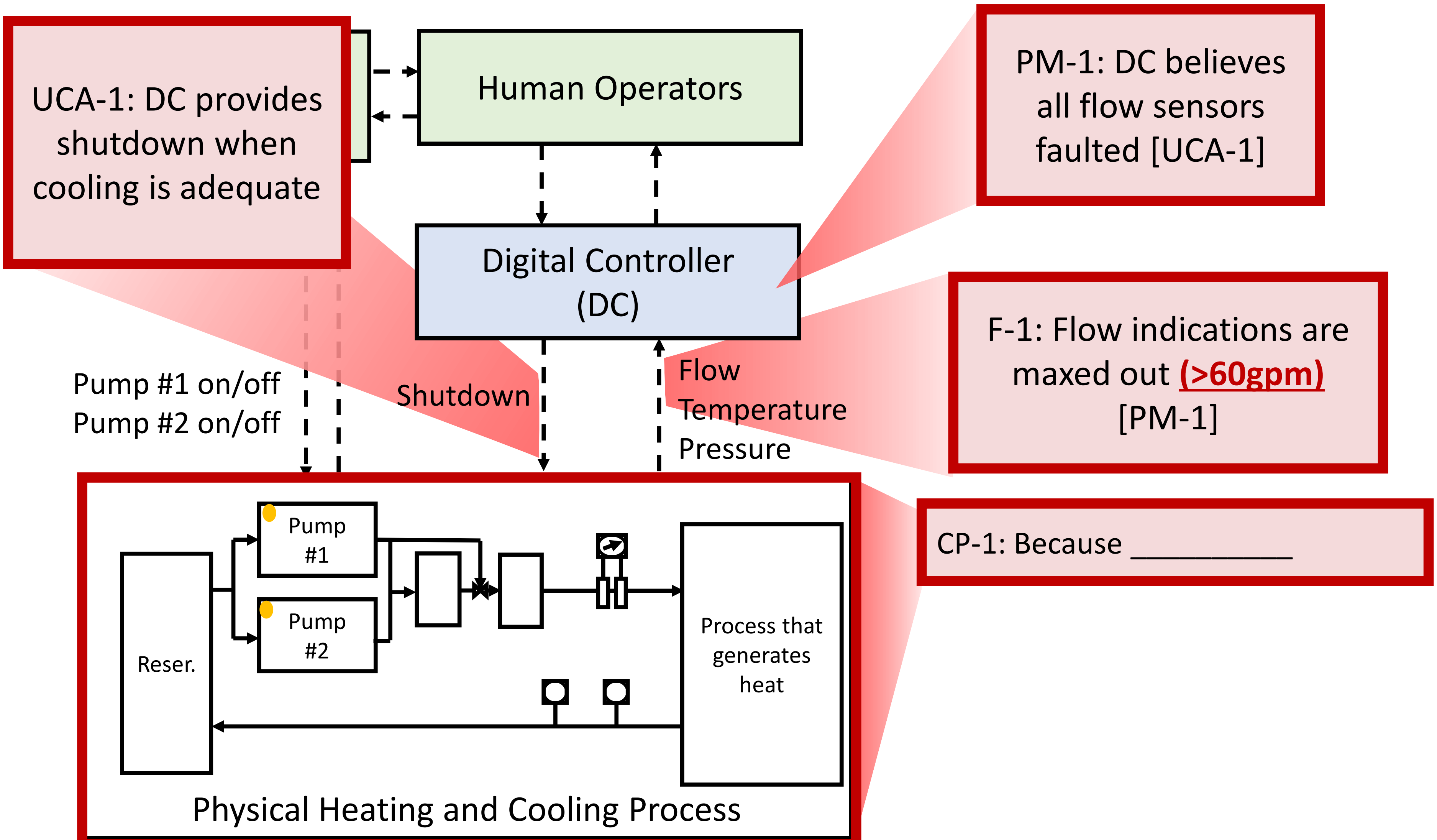


What do you think they chose?

- Flow sensor max: ? gpm

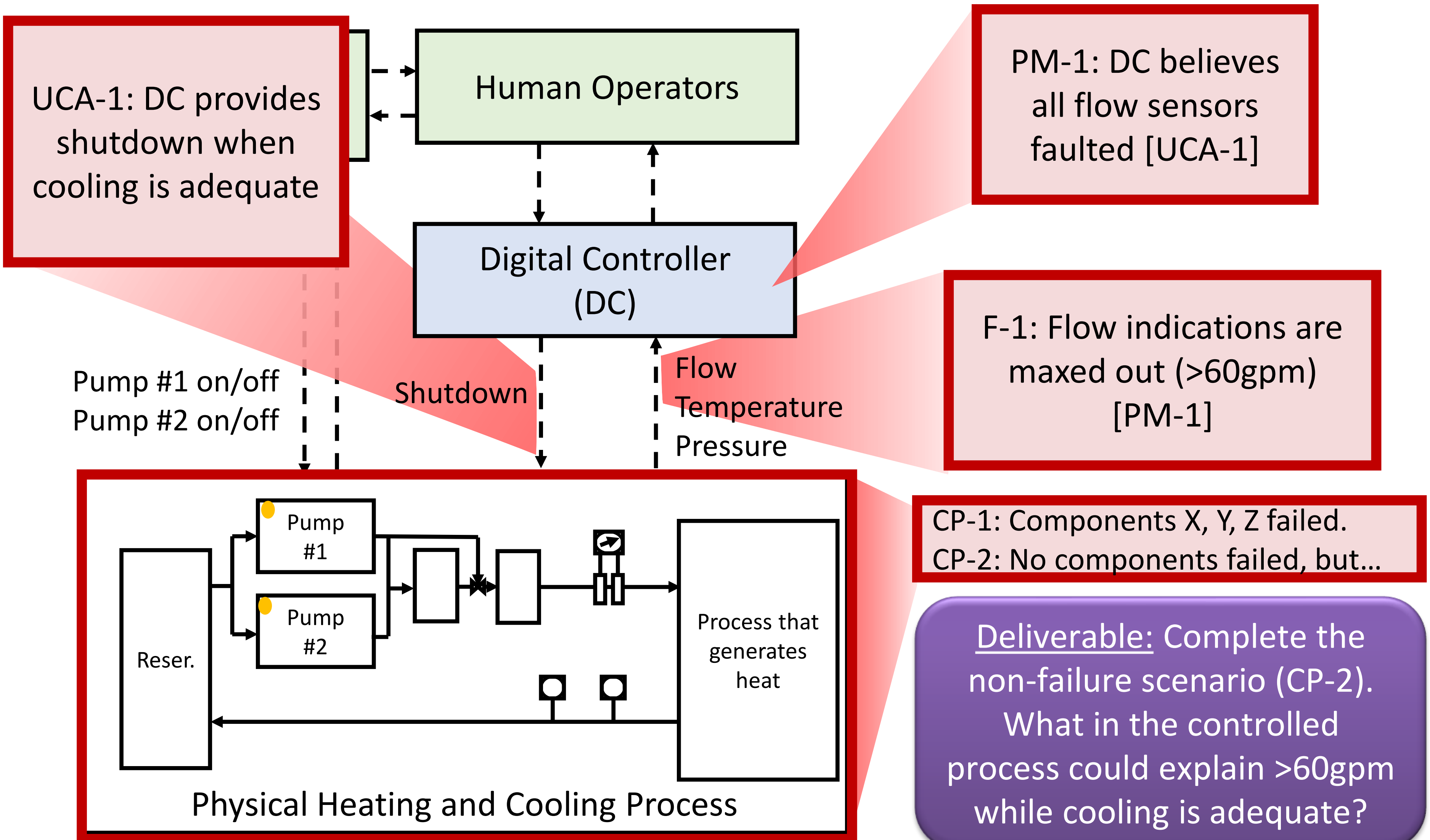
Historical flow data (sampled regularly over many years)

Scenario Building

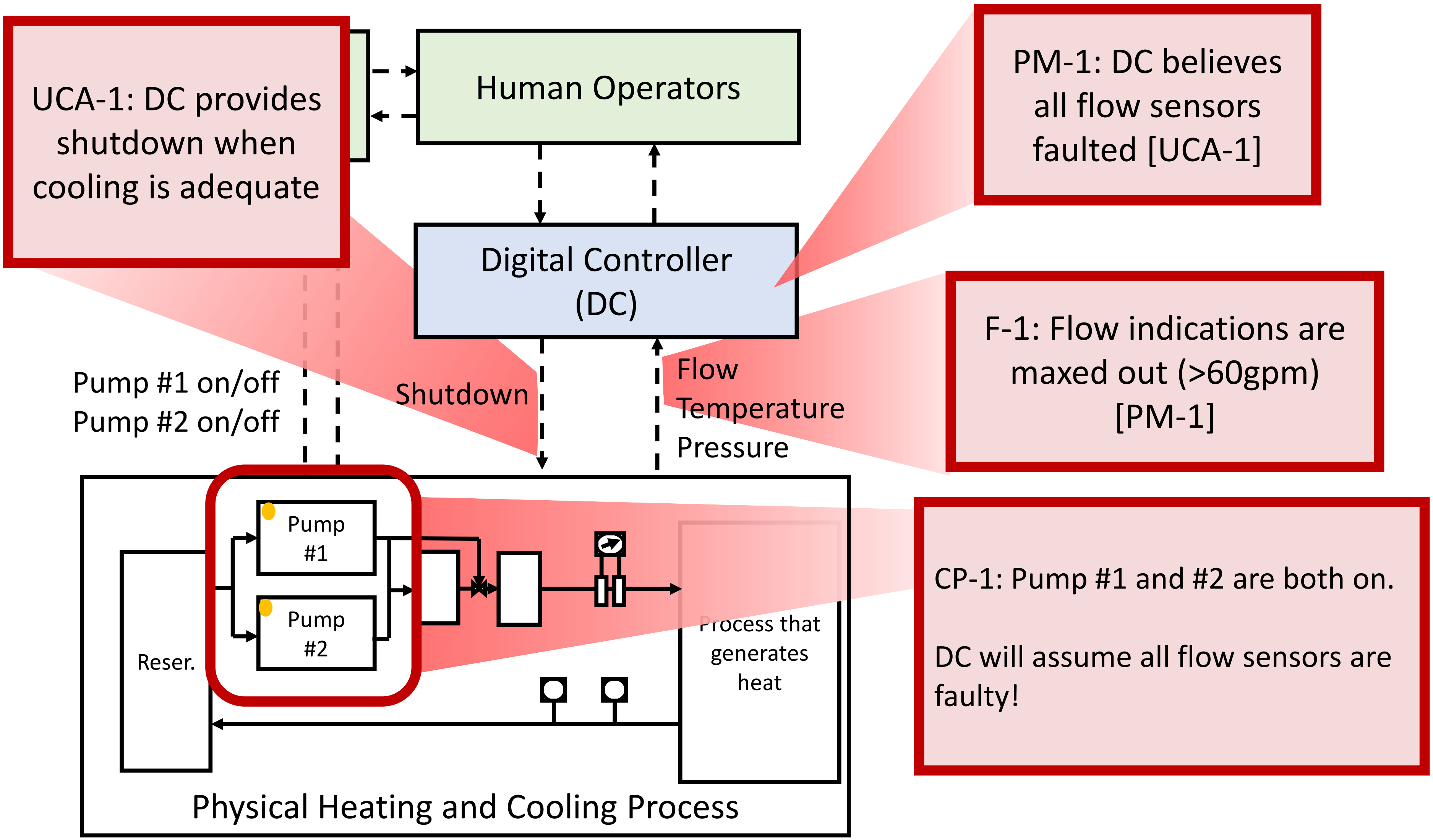


John Thomas, 2020

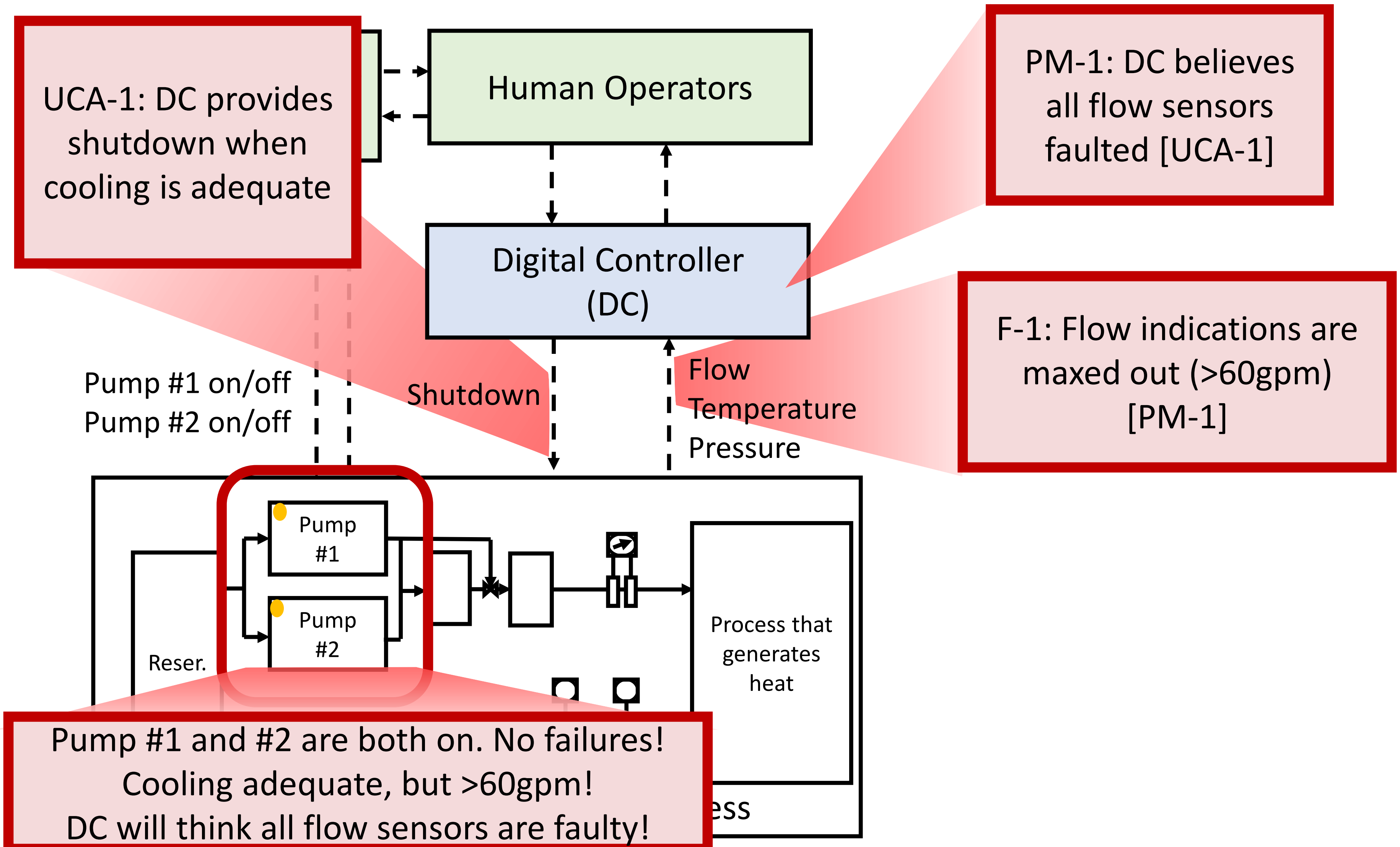
Scenario Building



Scenario Building



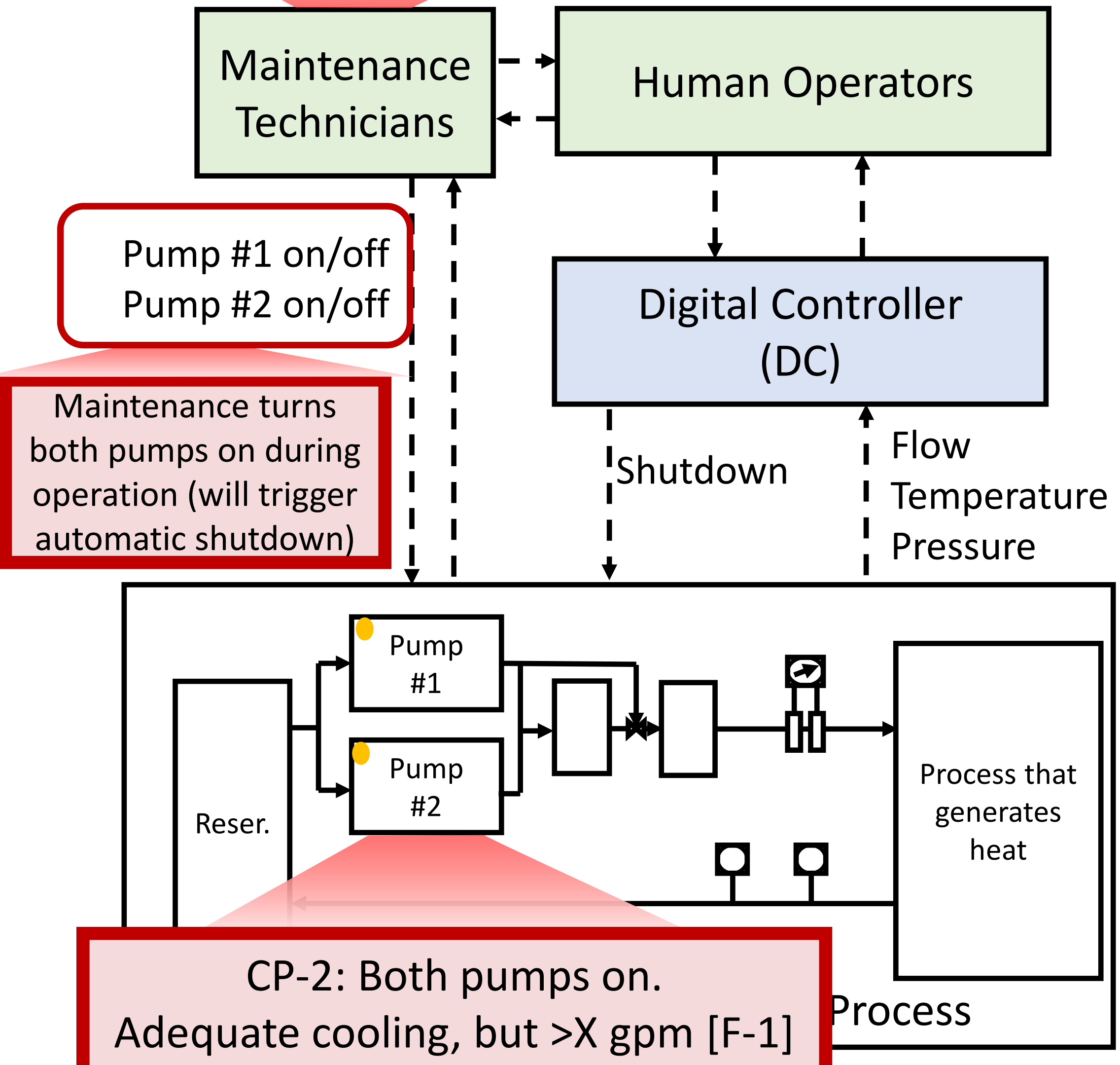
Scenario Building



John Thomas, 2020

?

nario Building



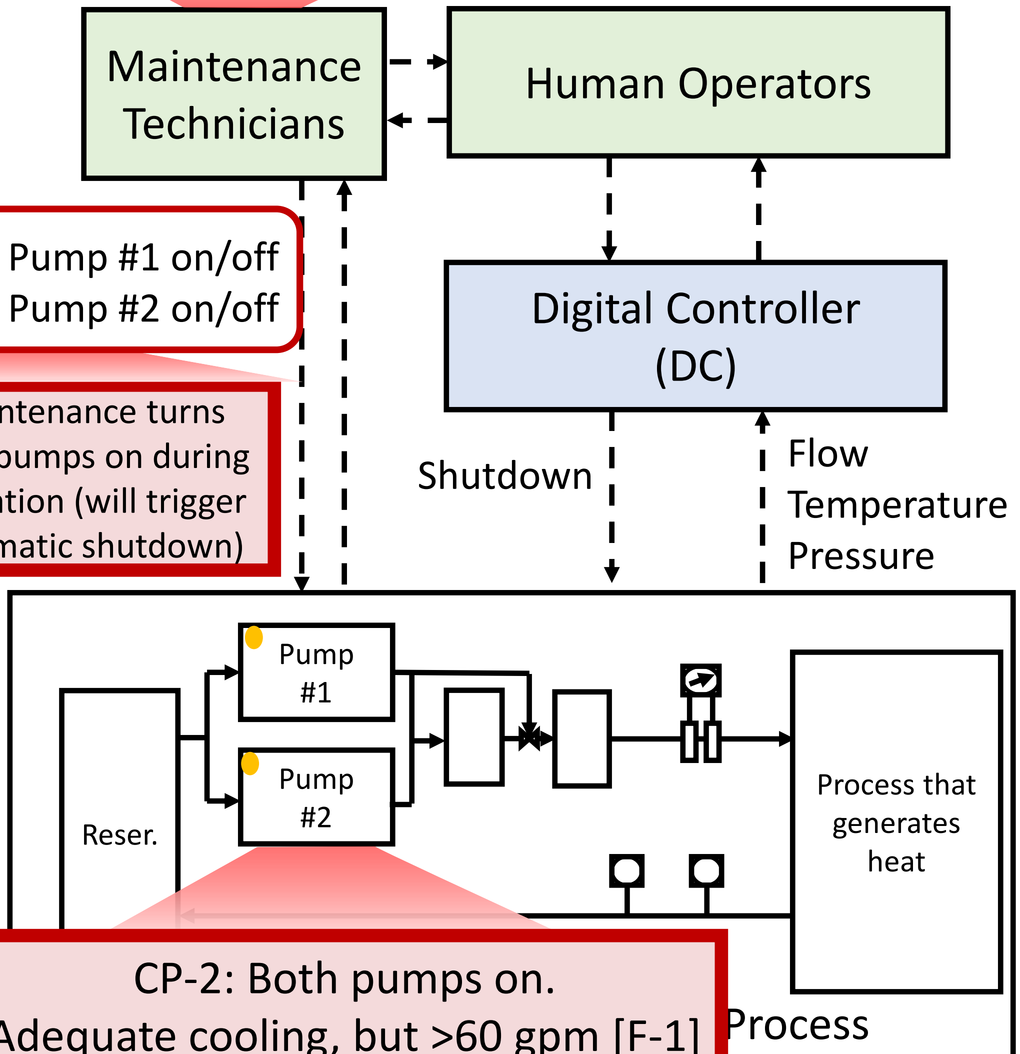
Scenario so far: If both pumps are on, flow is >60 gpm and DC will provide shutdown (will think all flow sensors are faulty).

Deliverable: What would cause both pumps to be on?

John Thomas, 2020

PM-1: Maintenance believes system can handle both pumps on
CA-1: Maintenance SOP (every X months):
- Turn on Pump #2
- Check X, Y, Z
- Turn off Pump #1

lding



Pump #1 on/off
Pump #2 on/off

Maintenance turns both pumps on during operation (will trigger automatic shutdown)

CP-2: Both pumps on.
Adequate cooling, but >60 gpm [F-1]

Aha! The overall system is flawed! All components (incl humans) 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!

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

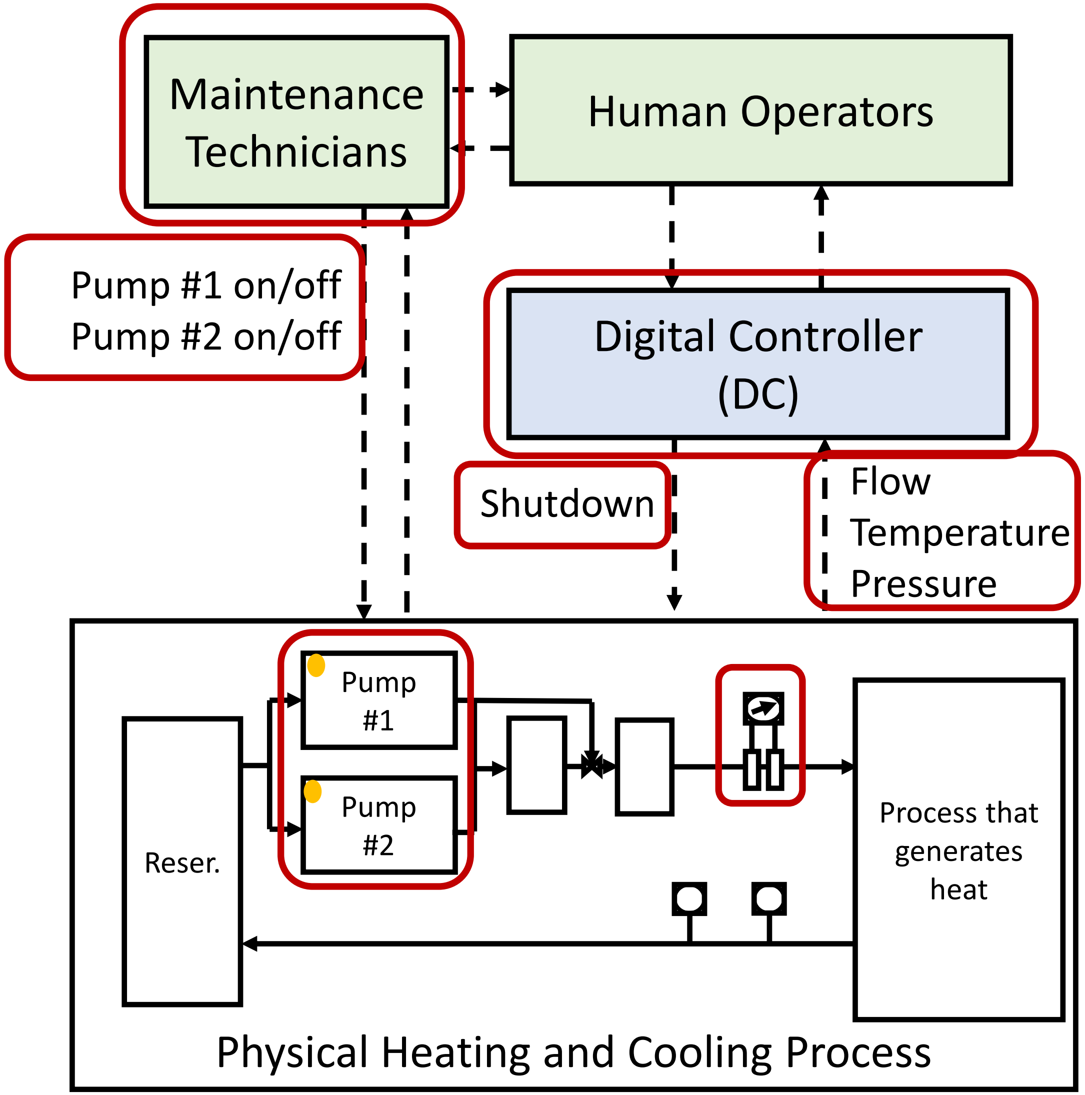
John Thomas, 2020

STPA is process for discovery, not just documentation.

If you aren't generating these AHA! moments, something is wrong.

Diagnose and correct (see lessons learned).

STPA Step 4 Continued: Developing Solutions

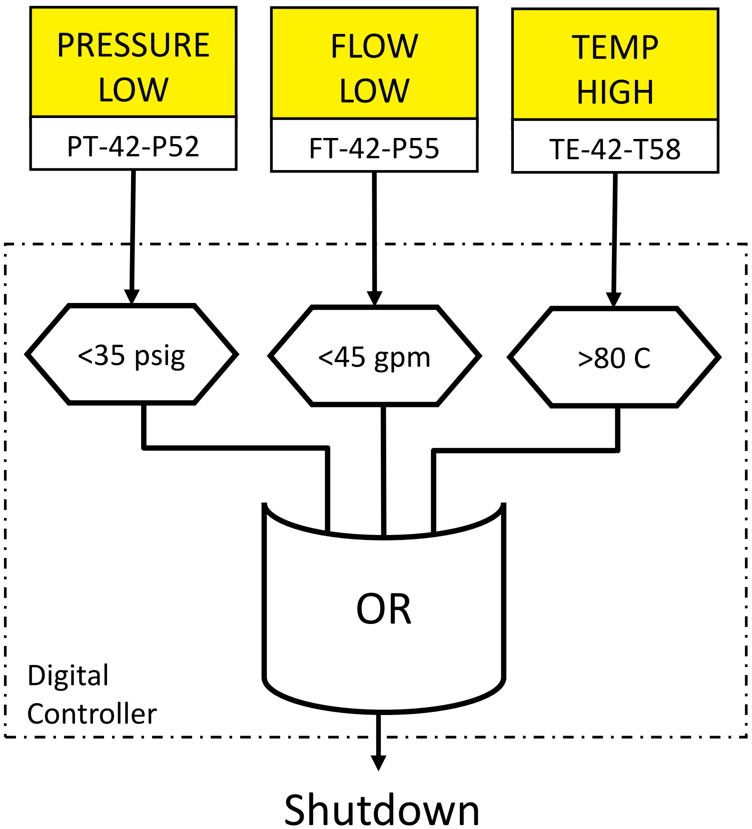


- Design solutions?
- New requirements?
- Alternative automation?
- Maintenance, operator procedures?

Deliverable: Identify multiple solutions for the scenario we just discussed

Compare to previous conclusions

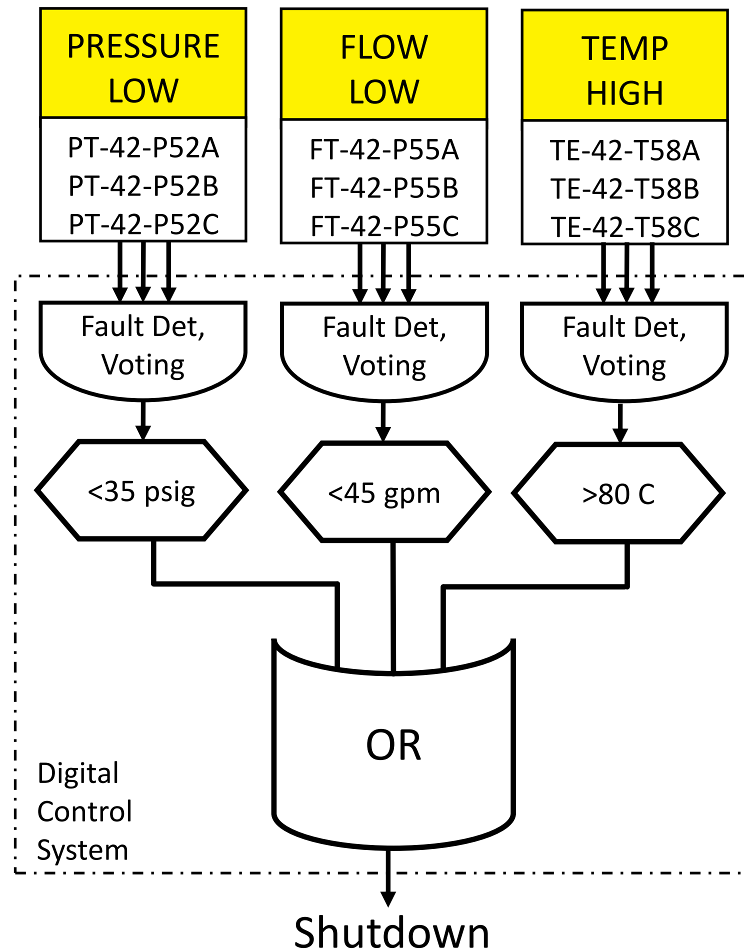
Old System



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

(~Once in 38 years)

New System



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

(~Once in 757 years)

IS = Inadvertent Shutdown

Different Results

Traditional Failure-based Recommendations

- **Independence Requirements**: Use independent pumps, power supplies, digital controllers, etc.
- **Probability**: The chance of an unknown common-cause error is 3.65E-5, which is negligible here.
- **Weakest link**: failure of redundant pumps.
  - Solution: more frequent preventative maintenance of the pumps.
- Conclusion: The new system with triple redundancy will be **~10x more reliable** than the old system with single points of failure.

Results from FMEA, FTA, HAZOP, FHA, Etc.

Recommendations from Systems Approach

- **We found the unknown error**: The specified GPM range is too low! We're using the wrong sensors!
- **We found the unknown assumption**: We'll have higher-than-specified flow rate when both pumps are turned on!
- **We found the procedure that violates** the assumption! Maintenance procedure needs to limit the time both pumps are turned on.
- **We found a missing digital/software requirement**! Needs to include a timer to ignore short high-flow situations. Potentially we should always ignore high-flow situations since the system can handle that.
- These sensors are **not independent**! The common cause is that they all share an assumption of maximum range.
- Conclusion: The **new system is worse**! You will cause $1m shutdown within 9 months if you don't fix these errors! Inadvertent shutdowns are ~4x worse than old system with single-point failures!

Results from STPA

Common pitfalls/mistakes in analysis

4. Incorrect understanding of system architecture → incorrect model of system failures and failure behaviors
5. **Paying more attention to crunching probabilities than to the physics of the problem.**
6. Analyst works alone; no independent validation/verification

Industry evaluations and adoption

NEI TECHNICAL REPORT

NEI 20-07, Rev D

Guidance for Addressing Common Cause Failure in High Safety-Significant Safety-Related Digital I&C Systems

Prepared by the Nuclear Energy Institute
September 2021

Using STPA in the front-end of the development process for an HSSSR [High Safety-Significant Safety-Related] system provides an effective means to establish requirements to prevent such systematic failures using systems theory principles. The process is repeated throughout the design process to reflect the available design detail considerations. This approach utilizes a multi-discipline team to analyze how the complete system interacts internally and externally and associates potential loss scenarios with these system interactions. By continuously analyzing the complex, digital HSSSR I&C system with a multi-discipline team, potential loss scenarios are considered and eliminated/mitigated throughout the design process through the application of control methods. Refer to Section 3.5 for application examples.

https://www.nrc.gov/docs/ML2127/ML21278A472.pdf

Nuclear Power: NuScale Experience

STPA has been used successfully by NuScale Power as a basis for their Digital Instrumentation and Control licensing with the US Nuclear Regulatory Commission (NRC).

From the public licensing application (FSAR):

- "The STPA methodology departs from the standard FMEA and fault-tree analysis by going beyond potential system failure caused by component failures. The STPA includes potential failures caused by interactions between system components, including human operators, which result in inadequate control actions, which can occur without component or logic faults.
- "By evaluating the control structures on a functional level, the analysis can be performed before any significant design work is completed and the design can be guided by the identified hazards and associated safety constraints.
- "The [STPA] hazard analysis identified causes such as operator error and procedural error as well as possible design deficiencies such as software and algorithm error. These differences support the use of the STPA methodology for analyzing complex systems such as the MPS (Module Protection System)."

Industry STPA Evaluation

	Functional Requirements	System Design Requirements	Design Solutions
Number of STPA Safety Constraints (SC) that were already well-enforced by requirements/design (10 or more relationships)	8	75	236
STPA Safety Constraints (SC) that were minimally addressed by requirements/design (5 or fewer relationships)	208	75	34
STPA Safety Constraints (SC) that were not covered by any existing requirements or solutions	82	20	15

Covered
These STPA results were addressed before STPA was applied.

Not Covered
These STPA results had NO existing mitigations or corrective measures. These were accidents waiting to happen.

Table: *Use of STPA in the Development of a Reactor Protection System*, Paul Butchart (NuScale), 2020

EPRI Blind Trials

EPRI has 10 years of experience studying STPA for I&C applications

Development and Validation Workshops

- Multiple Organizations
  - Site A
  - Site B
  - Site C
  - Site D
- Diverse practitioners using STPA
  - Digital I&C designers
  - PRA experts
  - Operators/supervisors
- Multiple applications studied
  - Turbine control system
  - Pressurizer control system
  - Turbine protection system
  - Main power system & protective relays
  - High Pressure Coolant Injection
  - Rod control system
  - Simple time-delay relay
- Applications contained hidden flaws
  - Real flaws that had been previously overlooked by utilities and regulators
  - Includes flaws that caused significant events at US facilities

Outcomes

- All teams successfully used STPA to identify the overlooked Digital I&C design errors, common cause errors/failures, unmitigated human errors, and requirements flaws
- All practitioners were blind: no awareness of the flaws without STPA
- The STPA results provided the necessary insights to improve design and prevent real events
- The DI&C errors and flaws were not identified in PRA.
- STPA results were used to update and fix the fault trees. Some STPA results are difficult to add to fault trees (e.g. beliefs, non-failures).
- STPA findings were consistent across multiple teams and applications
- The 2019 results are consistent with other STPA evaluations conducted by EPRI and others since 2011.

STPA is proven to consistently identify design errors, mission requirements, human interactions, and other flaws that have been otherwise overlooked

Industry Trials to Evaluate STPA's Effectiveness and Practicality for Digital Control Systems (John Thomas and Matt Gibson)

Palo Verde Findings

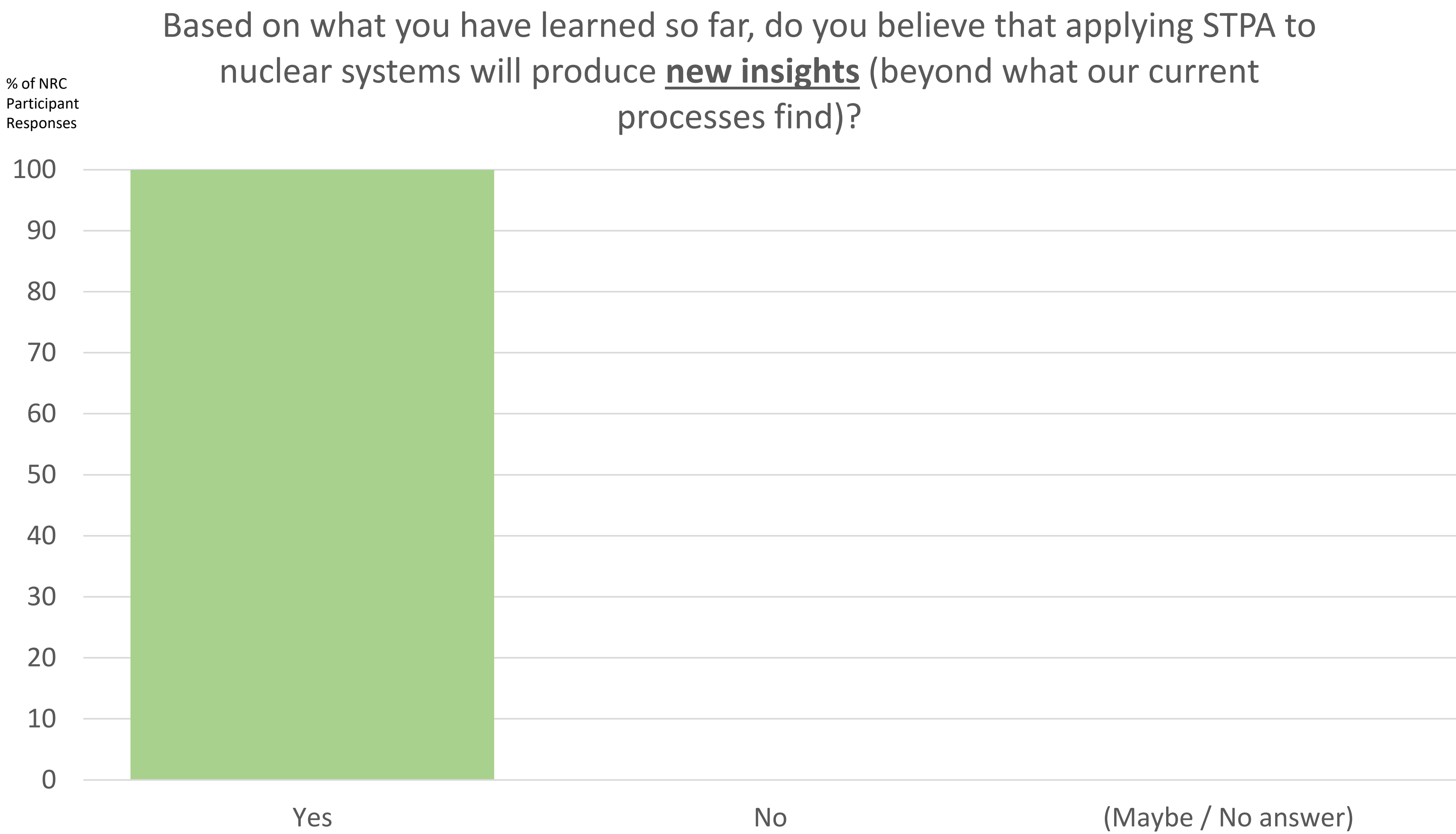
"… [STPA] found to provide more comprehensive coverage of potential vulnerabilities than traditional methods, with reductions in cost and schedule"

- *Hazard Analysis Demonstration – Generator Exciter Replacement: Lessons Learned,* EPRI 3002006956, 2015

NRC Staff Comments on STPA following STPA Workshops

- “PRA and STPA should be treated as complementary. STPA provides the "what can go wrong" from the perspective of systemic causes (hazardous interactions ... interdependencies). Thus, it **could serve as improving the "input" to PRA models**.”
- “I think that STPA could be an important & useful complement to PRA. Also, I think that **STPA is the only tool that could identify automation/operation control problems**.“
- “Because **STPA embeds traceability** to losses of concern, it seems to **provide appropriate regulatory review focus**. Unstructured descriptions of design details, especially when presented as components or subsystems, don't necessarily reveal the context necessary for safety conclusions.”
- STPA is already being used by licensees. **There is regulatory utility from accessing a licensees STPA** used to come to a safety determination.

US NRC Evaluations of STPA



US Nuclear Regulatory Commission (NRC) Evaluations of STPA

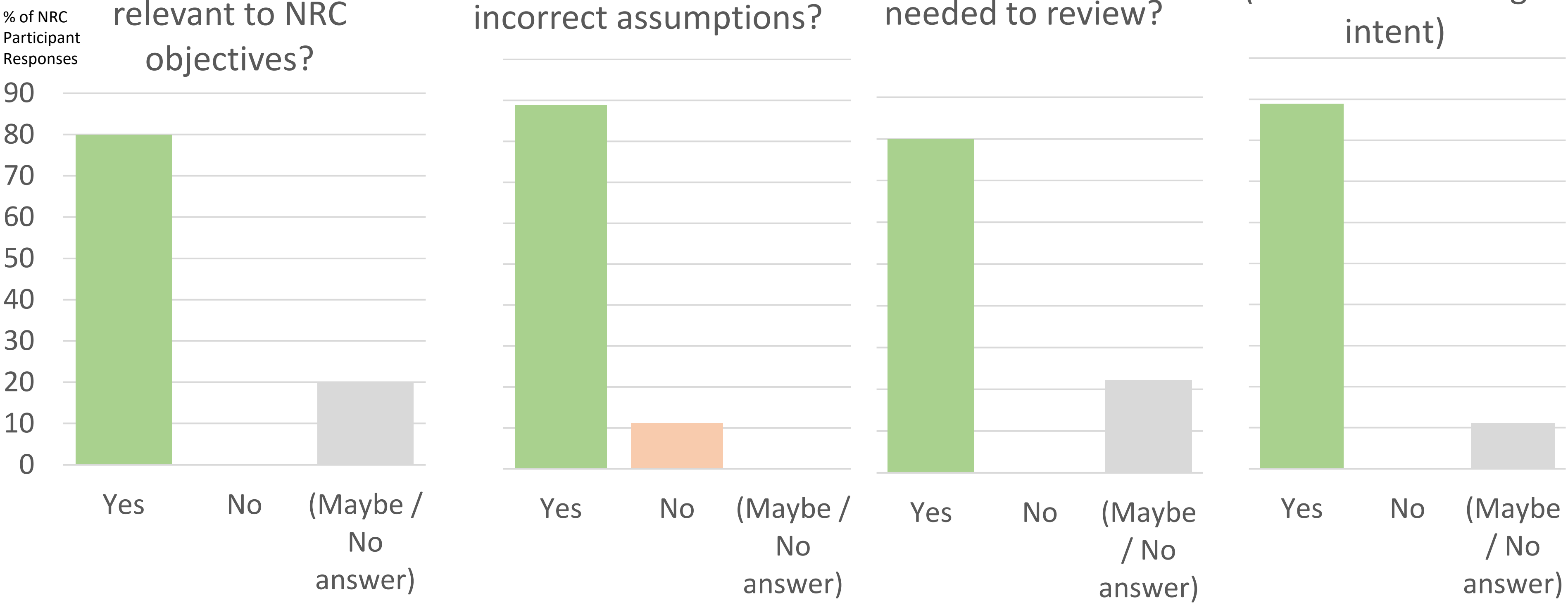
Exactly how would STPA help NRC achieve objectives?

Would STPA provide a way to identify unbounded or unanalyzed events relevant to NRC objectives?

Do you believe STPA can inform existing likelihood categorizations, such as likelihoods that may be incorrect or based on incorrect assumptions?

Do you believe STPA could provide a more efficient analysis in terms of effort needed to review?

Can STPA provide a more effective means of development assurance than what is currently done? (validation of design intent)



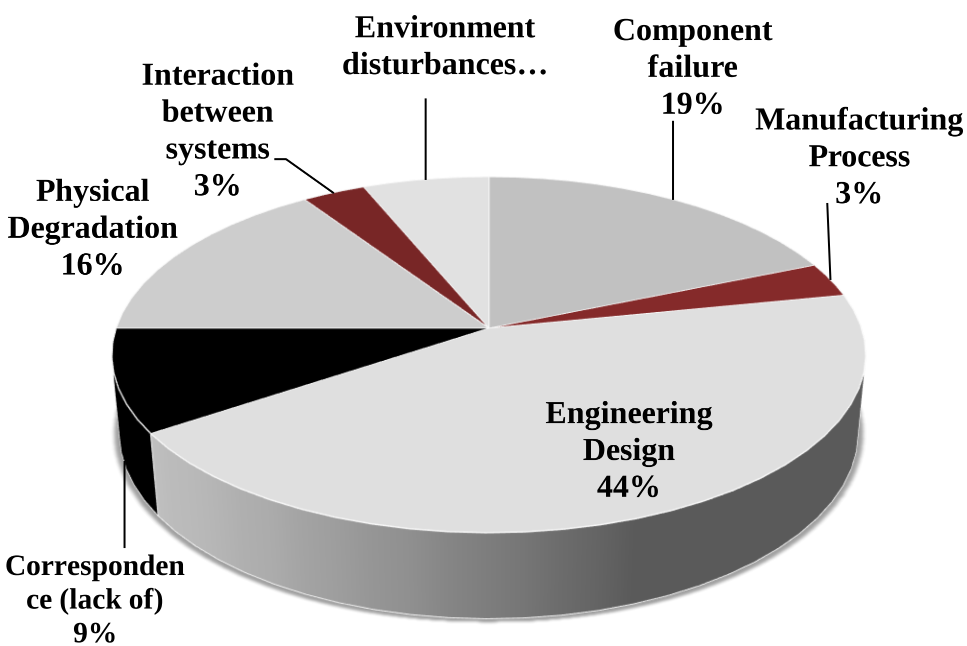
NRC staff identified four primary benefits of STPA

NRC Participant Feedback
What NRC groups would benefit from **STPA**?

- Any process can use this concept to identify situations where the planned thing occurs, but it is not the right thing. The fact that this catches incorrect/invalid/incomplete requirements is very valuable.
- Management
- Any risk or management group. Especially those who inform regulation.
- Cyber security
- Software
- I&C
- Licensing
- All areas that review
- Inspectors (regional; cyber)
- NSIR CSB
- Human factors engineering
- Division of Risk Analysis (DRA) in Research (RES)
- Anywhere significant automation or remote control is planned
- NSIR
- NRR
- RES
- NMSS

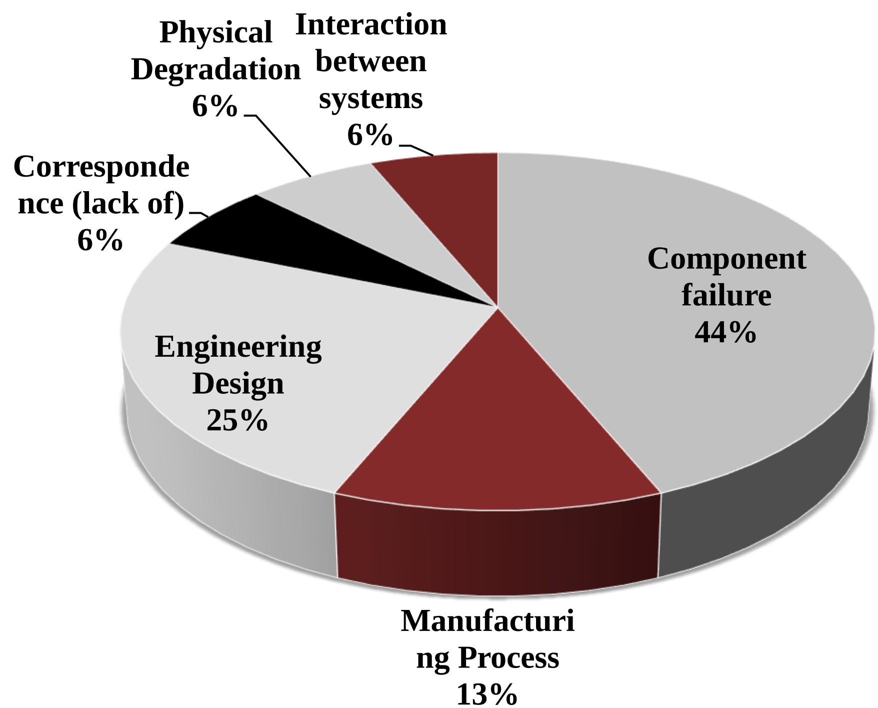
NRC Participants identified several NRC groups that would benefit from STPA

Types of accident causes found by STPA



STPA causes for UCA1

Types of accident causes found by FMECA

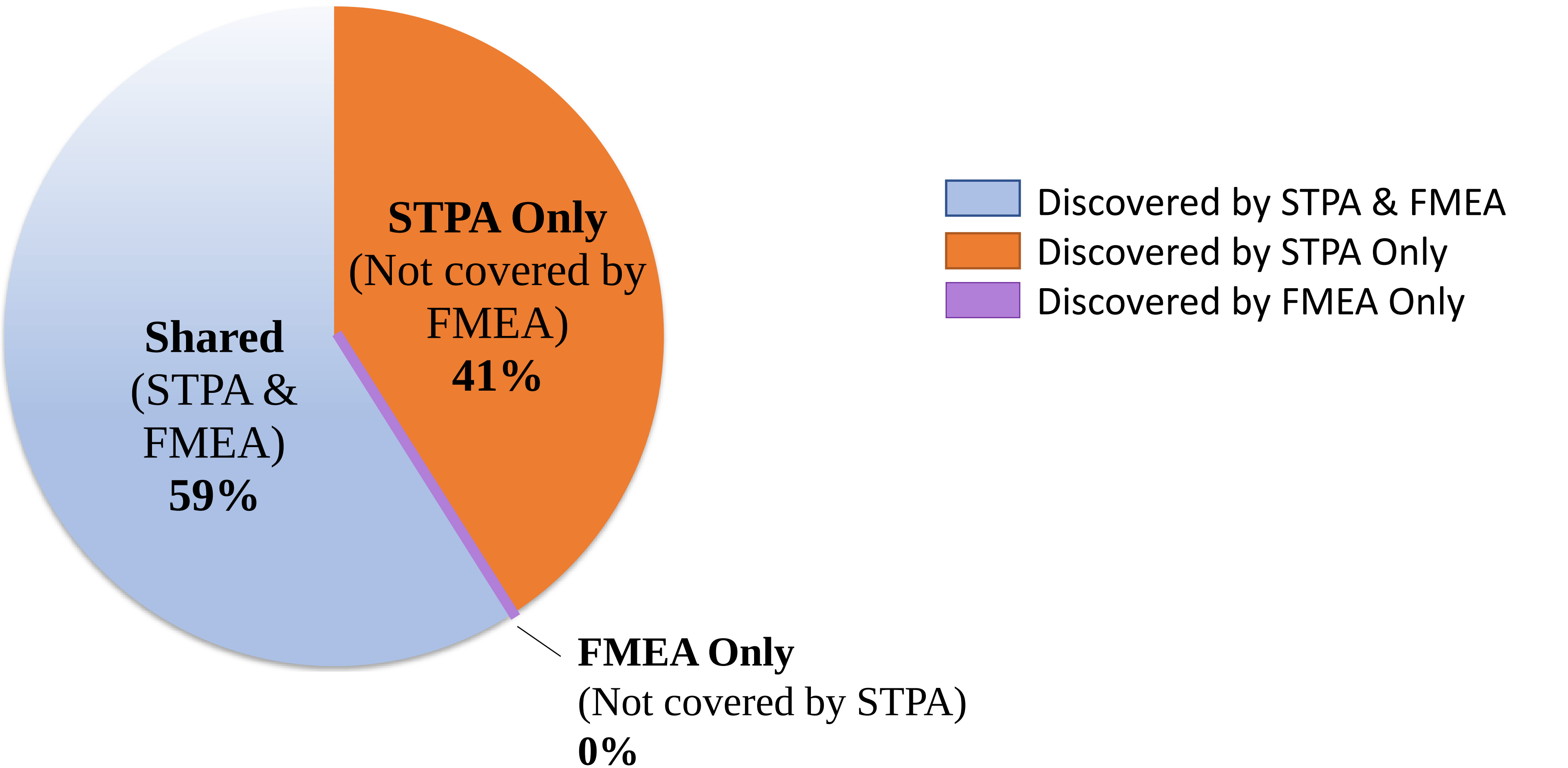


FMECA causes for FM1

A comparison of STPA and FMEA

Rodrigo Sotomayor

Application: Electric Power Steering System



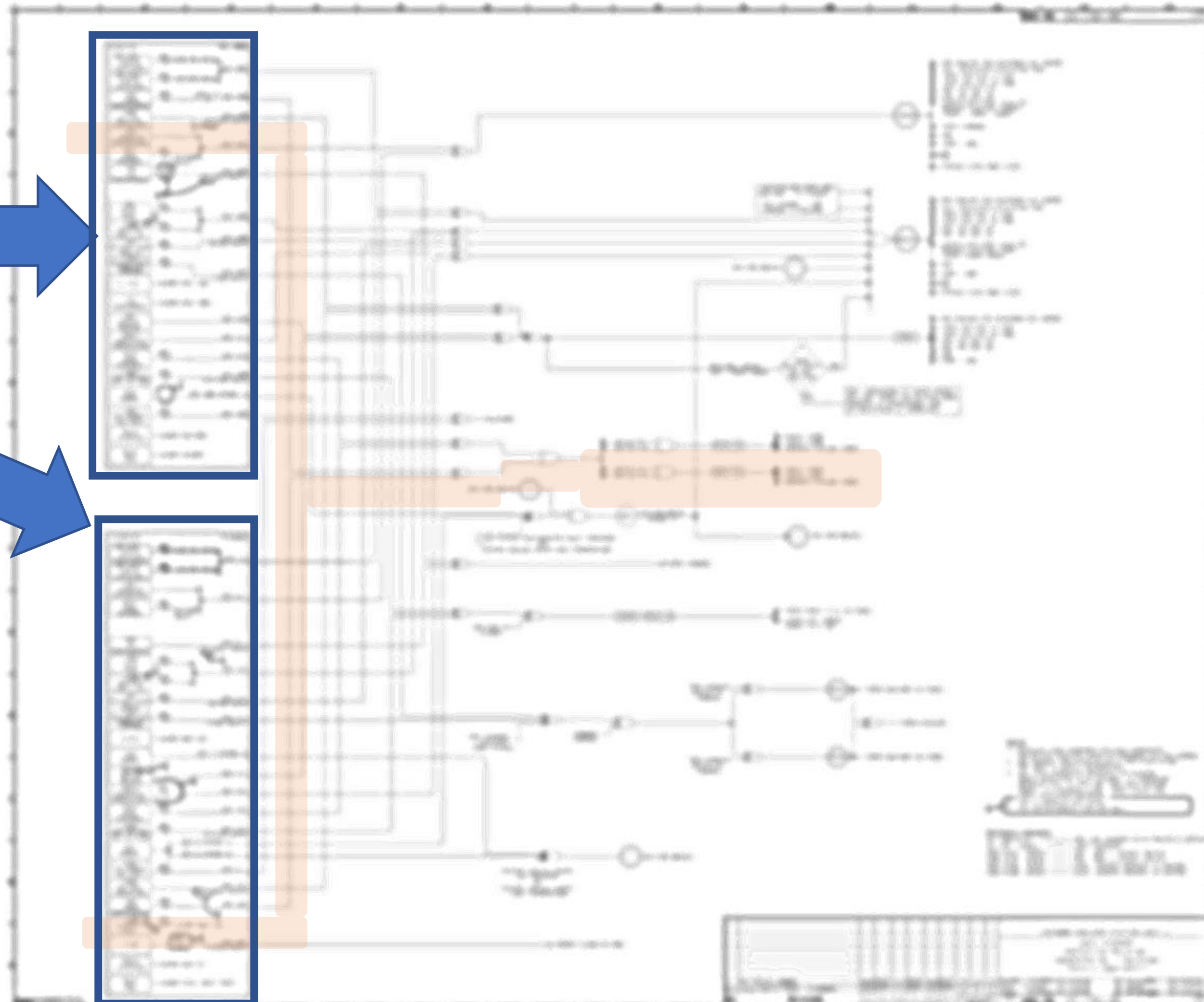
Rodrigo Sotomayor, 2015, "Comparing STPA and FMEA on an Automotive Electric Power Steering System"

*Using SAE J1739 (DFMEA and PFMEA)

Independence defeated by assumptions

Supplier 1
Digital Module

Supplier 2
Diverse Digital Module



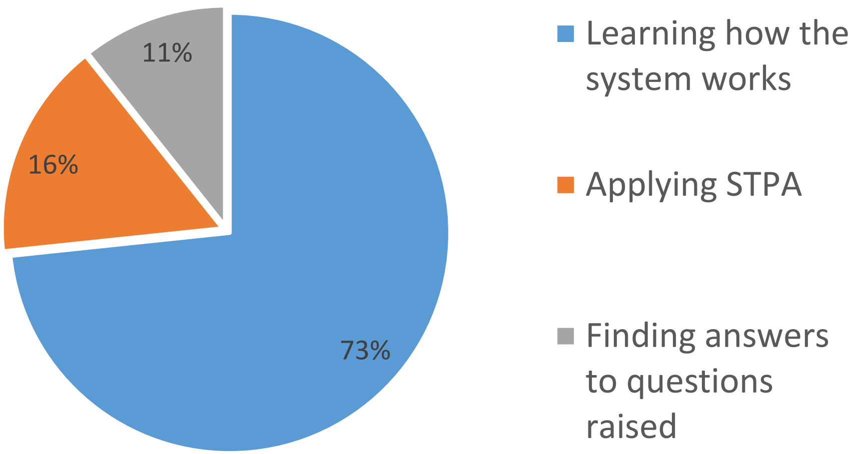
Both modules considered diverse. Both reviewed. Independent requirements, independent implementation. Installed, tested, put into operation.

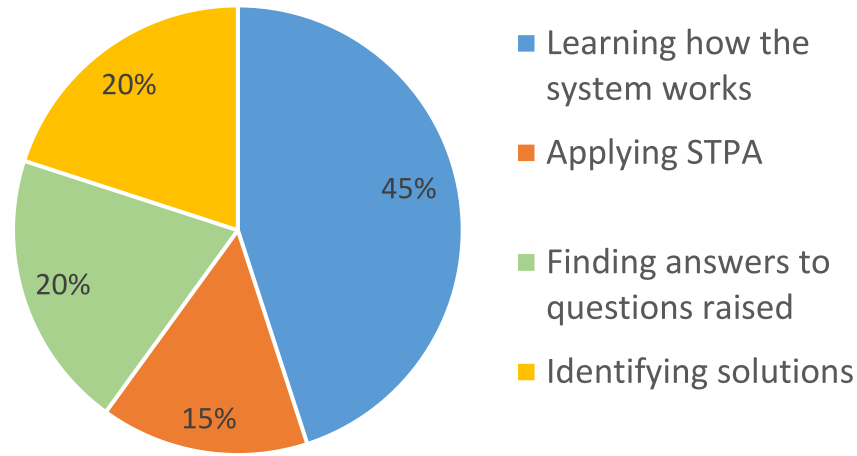
Months later during operation: New unforeseen interactions caused significant event. Both systems were based on similar incorrect assumptions. Overlooked by current (traditional) techniques.

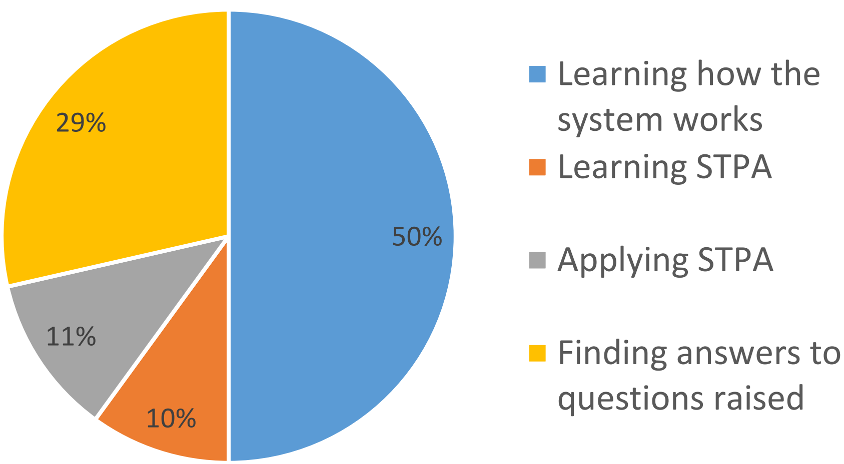
Event happened with no component "**failure**"!

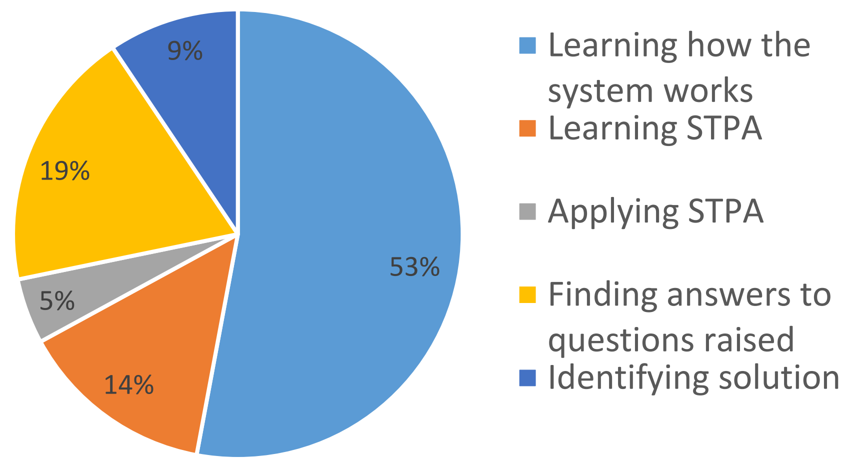
Massachusetts Institute of Technology

Time data from 4 STPA projects









Other organizations that have recently reported use of STPA for Nuclear Power

Government Orgs

U.S.NRC

CNEN Comissão Nacional de Energia Nuclear (Brazil)

Oak Ridge National Laboratory

Sandia National Laboratories

NASA SQA

Berkeley Lab Lawrence Berkeley National Laboratory

INL Idaho National Laboratory

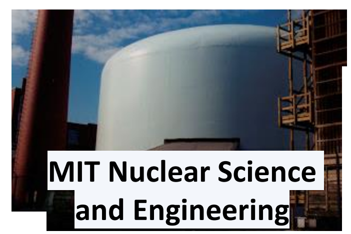
NPP Operators

Southern Nuclear

Dominion Energy®

Duke Energy®

Forsmark NPP (Sweden)


MIT Nuclear Science and Engineering

Dounreay Site Restoration (UK)

PaloVerde™ Generating Station

NPP Vendors

NuScale™ Power for all humankind

EPRI Electric Power Research Institute

Westinghouse Westinghouse Electric Company LLC

GE

Hitachi

Mitsubishi

Thales

Samsung Samsung Heavy Industries

50+ consulting orgs for the above are not shown

Additional known users have opted not to disclose publicly (not shown)

STPA in Industry Standards

- ISO/PAS 21448: SOTIF: Safety of the Intended Functionality
  - STPA used assess safety of automotive systems
- ASTM WK60748
  - “Standard Guide for Application of STPA to Aircraft”
- SAE AIR6913
  - “Using STPA during Development and Safety Assessment of Civil Aircraft”
- RTCA DO-356A
  - “Airworthiness Security Methods and Considerations”
  - STPA-sec used for cybersecurity of digital systems
- IEC 63187
  - “Functional safety - Framework for safety critical E/E/PE systems for defence industry applications”
- SAE J3187
  - “Recommended Practice for STPA in Automotive Safety Critical Systems”
- SAE J3187A
  - STPA Recommended Practice for Safety-Critical Evaluations in Any Industry”
- EPRI 3002016698 & 3002018387
  - STPA for digital I&C in nuclear power
- NIST SP800-160 Vol2
  - “Developing Cyber Resilient Systems: A Systems Security Engineering Approach”
  - “Attack scenarios can be represented as part of a model-based engineering effort […] based on identification of loss scenarios from System-Theoretic Process Analysis (STPA).
- IET 978-1-83953-318-1
  - “Code of Practice: Cyber Security and Safety”
  - Recommends use of STPA for Safety & Security
- NEI 20-07 Rev D
  - “Guidance for Addressing Common Cause Failure in High Safety-Significant Safety-Related Digital I&C Systems”
  - Outlines STPA process for digital technology at nuclear power stations
- UL 2800-1:2022: Standard for Medical Device Interoperability
  - Explicitly mentions STPA for performing system-level hazard analysis and control loop analysis

Who else is using STPA?

Full extent of STPA use is unknown, but…

From public conferences and other disclosures:

- **Known users across 80+ Countries**
- **Known users across 151+ Government & Regulatory Orgs**
- **Known users across 877+ Process Industry Groups**

130,000 STPA Handbook users (2021)

200,000 STPA Handbook users (2022)

A.C. & E. Srl
Abris Consulting Ltd
Accenture
Accident Research Institute (ARI)
Adama
adbForensics, Inc
Advisian
AEL Sistemas
Aeronautical Accident and Incident Investigations Commission
Aeronautics Institute of Technology – ITA
Aerospace Corp
Aerospace Medical Association
Aerospace Systems
Ahsanullah... of Science a... Technology
Air Hong Ko...
Airbus DS
AISIN
Akamai Tec...
Alaka'i Tec...
Alekto Met...
Allied Pilots Association
Alstom
Amazon
ANAC Brazi... National Ci... Aviation Ag...
ANG
ANSYS med...
Applus IDIA...
Aptiv
ARC
Arcanum In... Security
Argo AI
Armed For... Biomedical Institute
ARRIVAL
Arriver
Arriver Ron...
ASI
ASI Mining
Australian Departmen... Defence
Austrian Ai...
Austrian Ci... Aviation Authority
Austro Control GmbH
Autonomous Solutions, Inc.
Avatar Aircraft
AVIAGE SYSTEMS
AWS
Azbil Corporation
BAE Systems Inc
Baker Hughes
Bangladesh University of Engineerig and Technology
Bangladesh University of Engineering and Technology (BUET)
Bastion Technologies
BC Hydro
Beihang University
Beijing Jiaotong University
Ben Gurion

University, Israel
Ben-Gurion University, Israel
Binghamton University
Boeing
Boeing Defence Australia
Boeing Defense, Space & Security
Boeing Satellite Design Center
Boston Cybernetics Institute
Brane
Brazilian Air Force
Brazilian Department
...
Continental AG
Continental Automotive
CQU university
Critical Systems Labs Inc.
Cruise
CTU in Prague
CTU PRAGUE
CUGB
Cummins
Customroute Ltd
CVUT
CVUT FD
Cyber Risk Quant
Czech Technical University
Czech Technical University in Prague
Daimler Trucks AG
Dassault Systemes KK
Delta Airlines
DeltaV Aerospace (Pty) Ltd

Democritus University of Thrace (DUTH)
DENSO AUTOMOTIVE Deutschland GmbH
Department of Defence
DNV
DNV Business Assurance Japan K.K.
Dominion Energy
Draper Laboratory
DSO National Laboratories
DSTA
Dutch Safety Board
DUTh
...
GE Aviation Systems
Genentech
General Dynamics
General Electric Aviation
General Motors Company
Ghana CAA
Gibson Applied Technology & Engineering (GATE)
GKN
Global Maritime
GM
Google
Google Loon
Gulfstream Aerospace
Hancom Intelligence
Harvard Business School
Harvard Medical School
Healthcare Safety

Investigation Branch
Hemraj Consultants Ltd
Hensoldt Optronics
Herriot-Watt University
HFEx Ltd
Higher Engineering School TEHNIKUM – Belgrade
HIMA Australia
Hitachi Industry & Control Solutions, Ltd.
HKALPA
Honda Motor Co.,Ltd
Honeywell
...
Instituto Tecnologico de Aeronautica (ITA)
Intel Corp
ION energy
Irish Aviation Authority
Iron Mountain Solutions
ISAE-SUPAERO
Islamic Azad University, Iran
Istanbul Medeniyet University
ITA – Instituto Tecnológico de Aeronáutica Brazil
Japan Aerospace Exploration Agency (JAXA)
Japan Manned Space Systems Corporation (JAMSS)
Jilin University
John Deere

Jotai Solutions Safety Consulting
Karlsruhe Institute of Technology
Konkuk University
Korea Atomic Energy Research Institute
KTH Royal Institute of Technology
KU Leuven
kVA by UL
Kyushu University (Japan)
L3Harris
Lawrence Berkeley National Laboratory
Lendlease
...
Systems Research Center (SSRC)
MIT System Design and Management (SDM)
MITRE Corporation
Mitsubishi Chemical Corporation
Mitsubishi Electric Corporation
Mitsubishi Heavy Industries, Ltd.
Motional
Motional AD
Movares
MTI Co., Ltd.
MTSI
Murata manufacturing Co., Ltd.
Nagoya Institute of Technology
NASA
NASA Exploration

Ground Systems
NASA Glenn Research Center
NASA Goddard Space Flight Center (GSFC)
National Institute of Informatics
National Institute of Technology
National Maritime Research Institute
National Yunlin University of Science and Technology
Network Rail
Nexter Systems
Nihon Unisys Ltd.
...
Reykjavik University
Rheinmetall AG
Rigshospitalet
RISE Research Institutes of Sweden
Rivian
Rivian Automotive
Roche
Roche
Rolls-Royce
RWTH Aachen
SAE
Safeguard Engineering Ltd
Safety Associates
Safety Limited
Safety Management
SAIC, Inc.
Samsung
Sandia National Laboratories
Sapienza University of Rome
SBB

SBWORKDESIGN Ltd
SecIntel GmbH
Sendai College
Sensible4 oy
SGS Japan
Shabin Mahadevan
Shell
Shell TechWorks
Siemens Industrial Software Inc
Siemens Mobility GmbH
Sirris
Skai
Skai.co
Smith & Nephew Inc
SolutionLink
...
Corporation
The Affiliated Institute of ETRI
The Boeing Company
The Human Factor Hub
Therapeutic Goods Administration
Tier4
Tokyo Metropolitan Industrial Technology Research Institute
Tokyo University of Technology
TomTom NV
Toyota Motor North America
Transport for London (TfL)
Trinity College Dublin
TU Berlin
TU Graz
Tusimple
U.K. National Air

Traffic Services (NATS)
U.S. Air Force
U.S. Air Force 309th Software Engineering Group
U.S. Air Force 87 EWS
U.S. Air Force Air Combat Command (ACC)
U.S. Air Force Materiel Command (AFMC)
U.S. Air Force Operational Test and Evaluation Center (AFOTEC)
...
(UNIFESP)
Universitat Politècnica de Catalunya
Universiti Putra Malaysia
University of Alabama at Birmingham
University of Belgrade
University of Bundeswehr
University of Connecticut
University of Dayton
University of Democritus (Greece)
University of Derby
University of Genoa (Italy)
University of Glasgow
University of Michigan

University of Nagasaki
University of Ottawa
University of Oviedo
University of Parma
University of Pittsburgh
University of Queensland
University of Sao Paulo
University of São Paulo (USP)
University of Southampton
University of Strathclyde
University of Sydney
...
Finland Ltd
Warwick Manufacturing Group (WMG)
Water Association – Serbia
Waymo
Waymo Inc.
Whiteley Aerospace
WIBIH
Wisk Aero
Worldsteel
Worley
WSP
Xiamen University
ZF Friedrichshafen
ZIN Technologies
Zoox
Zoox Labs, Inc.
Zurich University of Applied Sciences (ZHAW)

Massachusetts Institute of Technology

STPA Common Mistakes

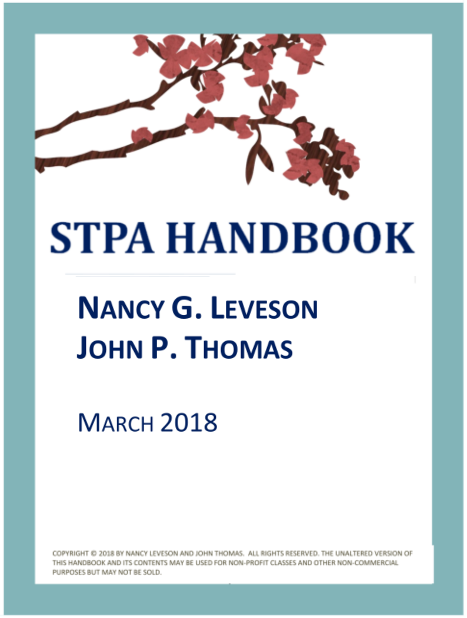
- Not adequately educated in STPA

- Implementing STPA without an expert STPA facilitator
  - Example mistake: We already have a facilitator with decades of experience facilitating fault tree analysis. Just give us a couple days to “bring him up to speed on the STPA methodology”.

- Limiting STPA to a simple system or simple problem with obvious answers

For more information

- Google: “STPA Handbook”
    - How-to guide for practitioners applying STPA
    - Free PDF
    - Same book used in our professional/industry STPA training classes
- Website: mit.edu/psas



Free PDF

- Email: jthomas4@mit.edu

LinkedIn

Search: “John Thomas MIT”