Massachusetts Institute of Technology

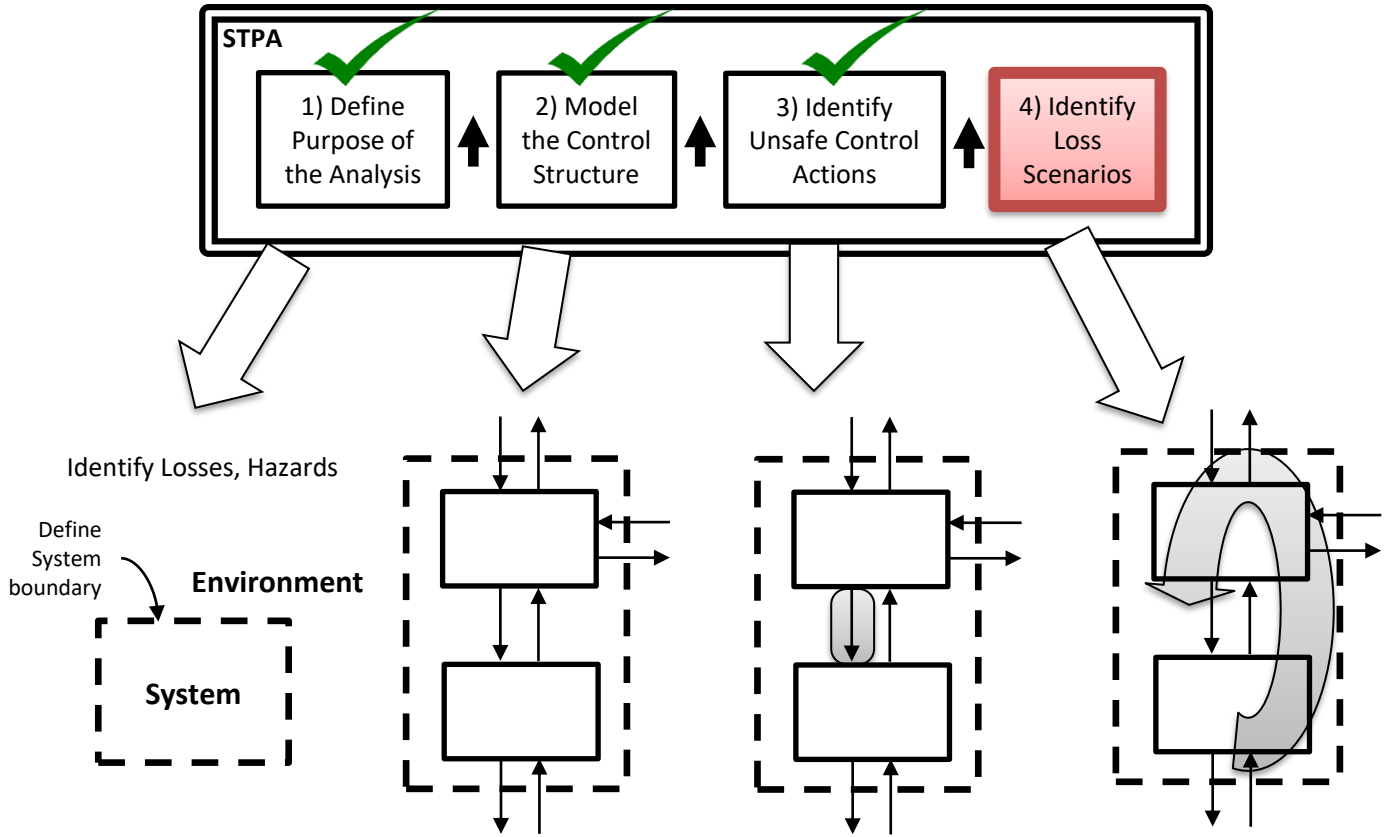
STPA Step 4
Building Formal Scenarios

A New Scenario Approach

John Thomas

Tutorial Objective

- These short tutorials are **not training classes**
- We cannot cover everything in these tutorial sessions.
- The objective is to introduce some of the core concepts so new attendees can follow the presentations this week.
- Training and practice with a qualified instructor are needed to apply these techniques and become proficient (as with most techniques). These short tutorials are subsets of larger training classes.



(Leveson and Thomas, 2018)

New STPA scenario approach has been tested for 8 years

Examples:

- (Nuclear) A New Process for Building STPA Causal Scenarios, John Thomas, 2016 MIT STAMP Workshop
- (Space) A Process for STPA: STAMP Accident Model of HITOMI and Expansion to Future Safety Culture, John Thomas and Nancy Leveson (MIT), Masa Katahira and Naoki Ishimama (**JAXA**), Nobuyuki Hoshino (JAMSS), 2017 MIT STAMP Workshop
- (Aircraft) Systems Theoretic Process Analysis Applied to **Air Force** Acquisition Technical Requirements Development, Sarah Summers, MIT Thesis, 2017
- (Aircraft) STPA Applied to Manned-Unmanned Teaming, Jeremiah Robertson, MIT Thesis, 2019
- (Auto) STPA Applied to Autonomous Vehicles, Jeff Stafford (**Renesas**), John Thomas (MIT), 2019 MIT STAMP Workshop
- (Software) STPA Applied to AV Software, Shaun Mooney (**Codethink**), John Thomas (MIT), 2019
- (Auto) Application of Hierarchy to STPA: A Human Factors Study on Vehicle Automation, Rachel Cabosky, 2020, MIT Thesis (collaboration with **GM**)
- (Military Aviation) Evaluation of STPA for Aircraft Safety Assessment, **US Army**, 2021
- (Aviation) Rotary-Wing Aircraft Development: Cybersecurity and Safety STPA Status Report, MIT & MIT-LL, 2021
- (Aviation) A Top-Down, Safety-Driven Approach to Architecture Development for Complex Systems, Justin Poh, MIT Thesis, 2022
- (Aviation) System-Theoretic Safety Analysis for Teams of Collaborative Controllers, Andrew N. Kopeikin, MIT Dissertation, 2024
- (Communications) Brittany Bishop, MIT Thesis, 2024
- (Software) **Qualcomm**, 2023-2024
- (Software) **Google**, 2023-2024

In all cases, the new approach has found loss scenarios and causes that had been previously overlooked

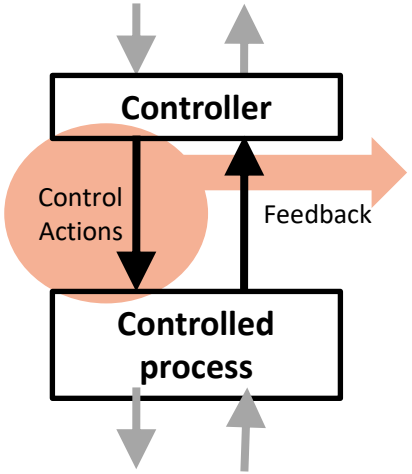
New Scenario Approach
Advantages and Disadvantages Observed

Disadvantages	**Advantages**
• More rules and structure • Takes longer to teach & learn • Unclear if it takes longer to perform (less time in some cases)	• The rules and structure provide more guidance • Enables a more directed search, less ad-hoc and informal • The rationale for the scenarios and how you found them is clearer. • So far, the new process has always captured additional cases that were previously overlooked • The top-down approach was more scalable to extremely complex systems compared to previous STPA attempts • Less repetition in the results (shorter documentation, higher information density) • Provides clear exit criteria to rigorously review and find gaps • Enables automation of some parts of Step 4 • The formal structure can enable mathematical proofs for properties like scenario coverage • Improved consistency and repeatability. Less dependence on who is doing the analysis.

Goals for new scenario approach

- Provide scenario guidance for new practitioners who may get stuck
- Provide a formal structure for scenarios (similar to UCA syntax)
- Provide a way to review scenario completeness and find gaps
- Handle more complexity: Implement a top-down strategy, not a backward search strategy.

STPA Step 3 Rigor: Unsafe Control Actions (UCA)



Example UCA:

"UCA-1: Computer provides Shift-to-Park cmd while vehicle is moving [H-1]"

Source Controller

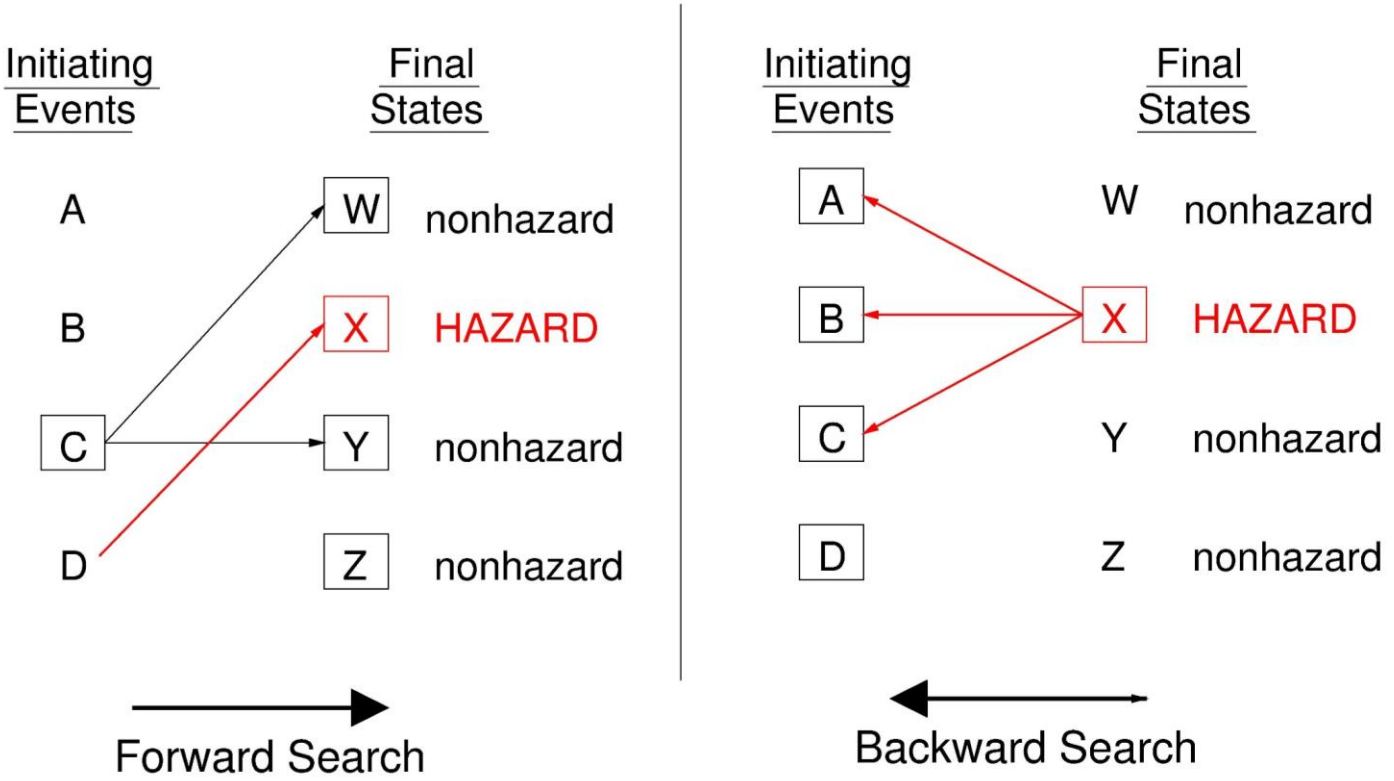
Type

Control Action

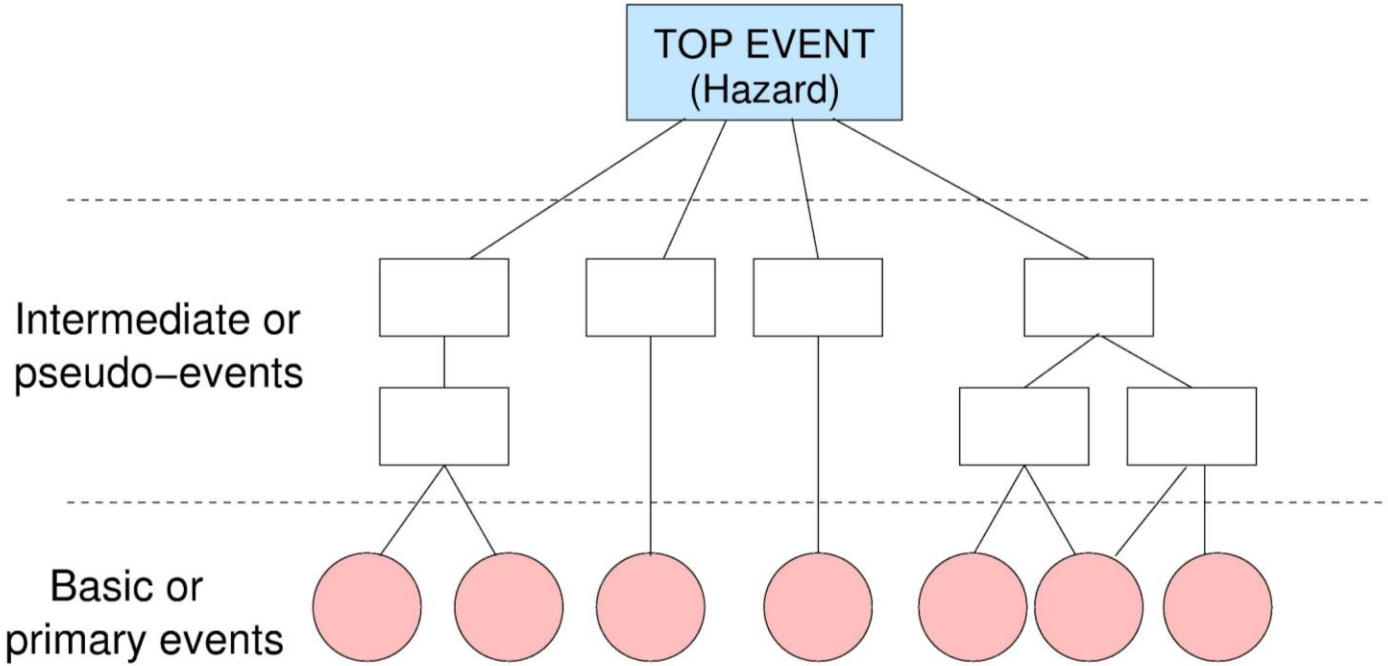
Context

Can we make STPA Step 4 more like this?

Forward vs. Backward Search

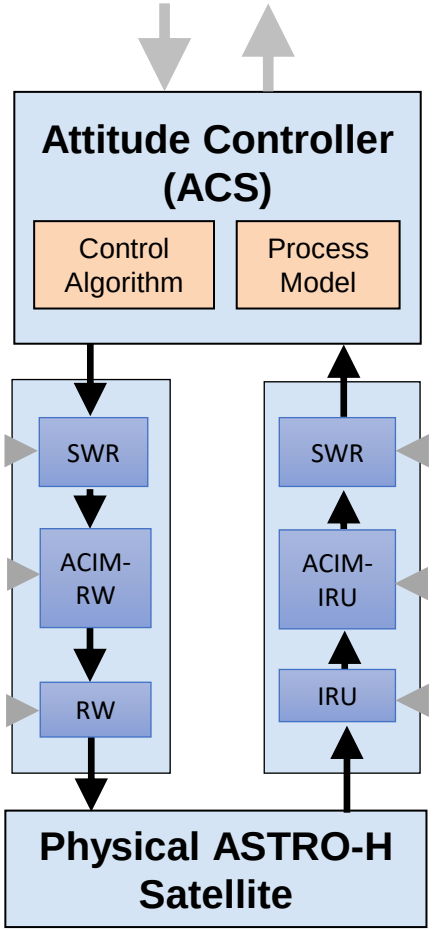


Top-Down Search

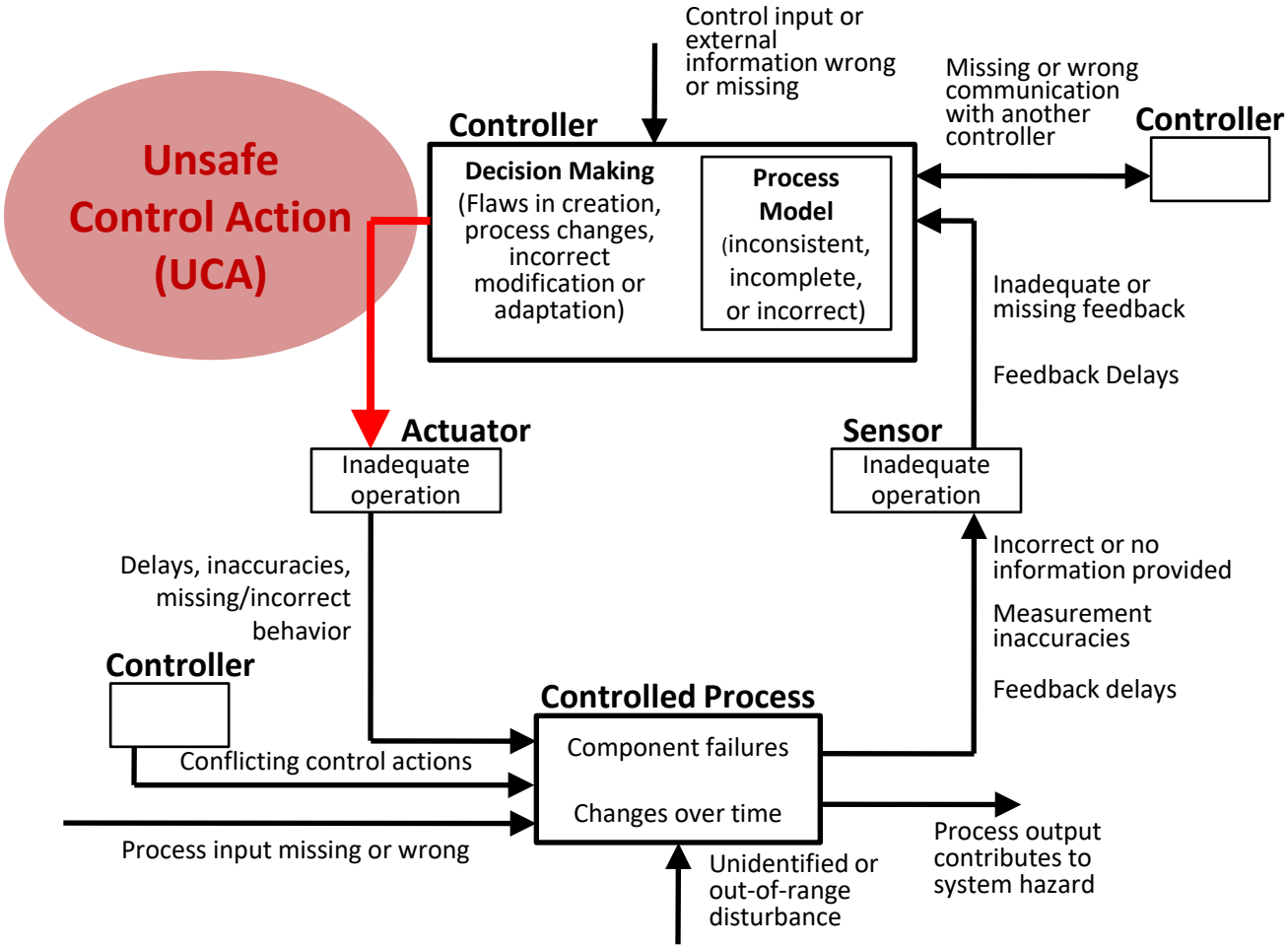


Building Scenarios

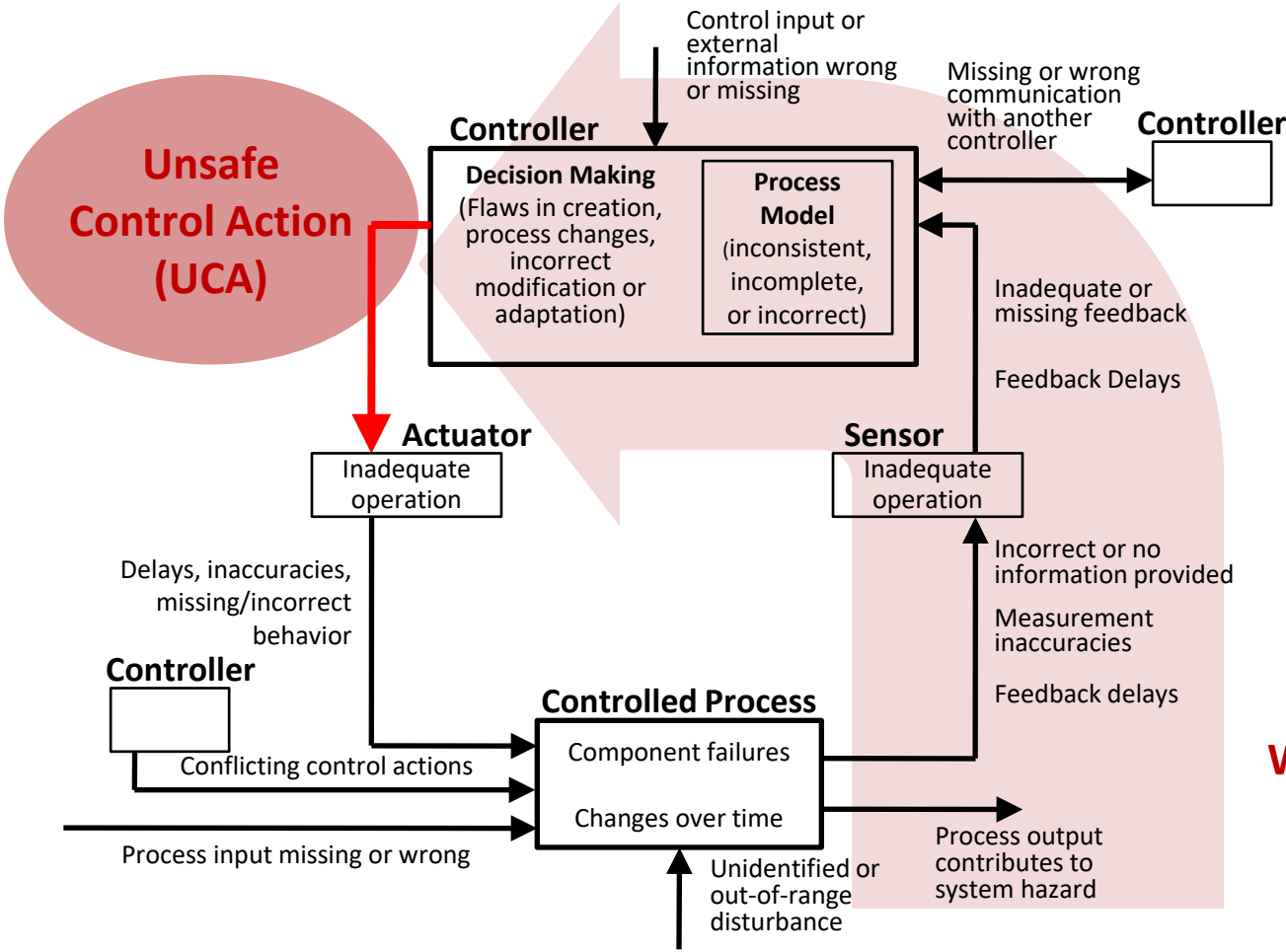
1. Define small number of high-level scenarios
   - Start with broad, abstract scenarios
   - Consider each class of scenario factors
   - Easy to review, show coverage, completeness, etc.
2. Identify potential solutions
   - Requirements
   - Modify control actions
   - Modify types of feedback
   - Modify responsibilities
   - Etc.
3. Refine into more detailed scenarios (if solutions not found)
   - Include more design detail
   - Can be done in parallel with development



STPA Step 4A: Identify scenarios that cause UCAs

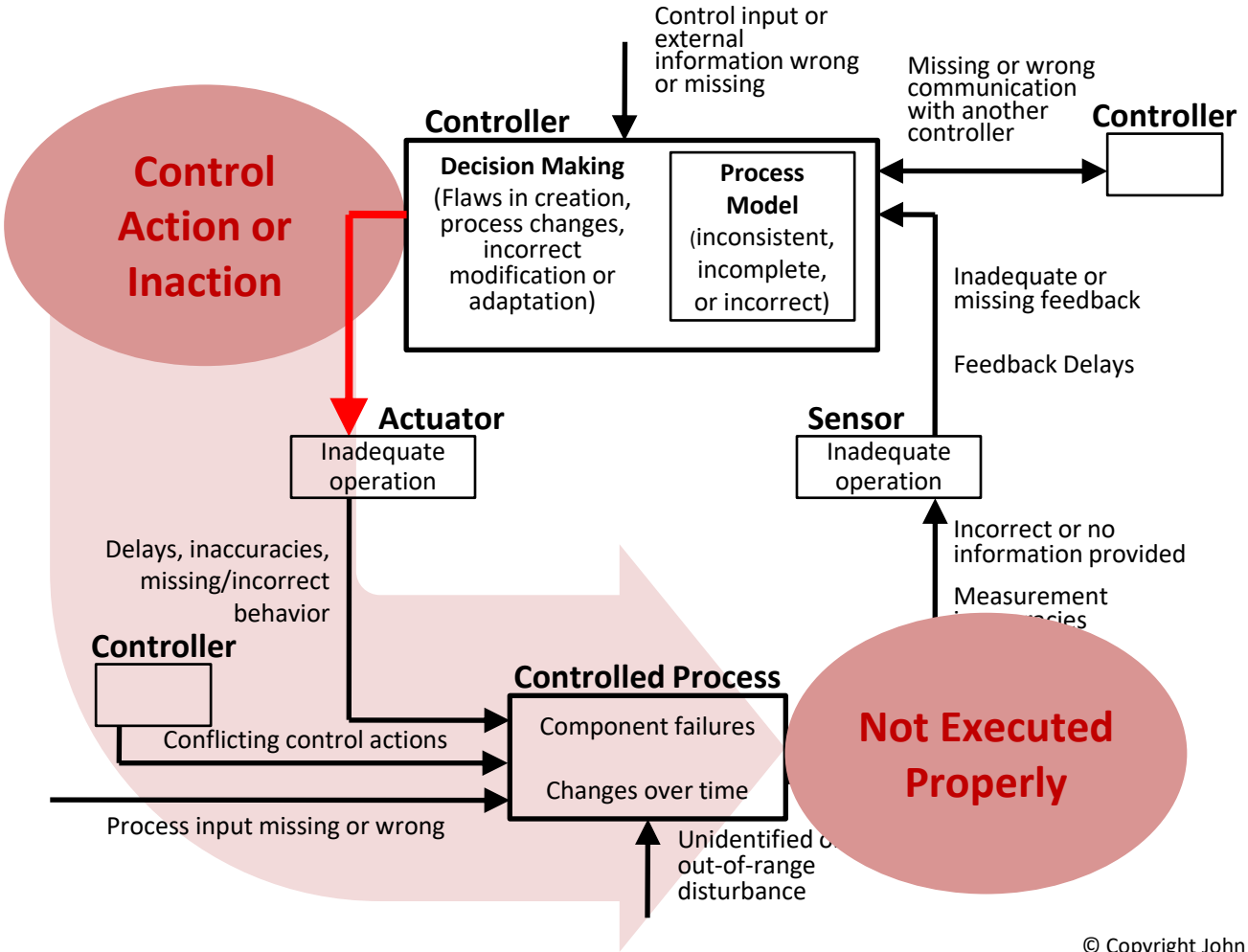


STPA Step 4A: Identify scenarios that cause UCAs

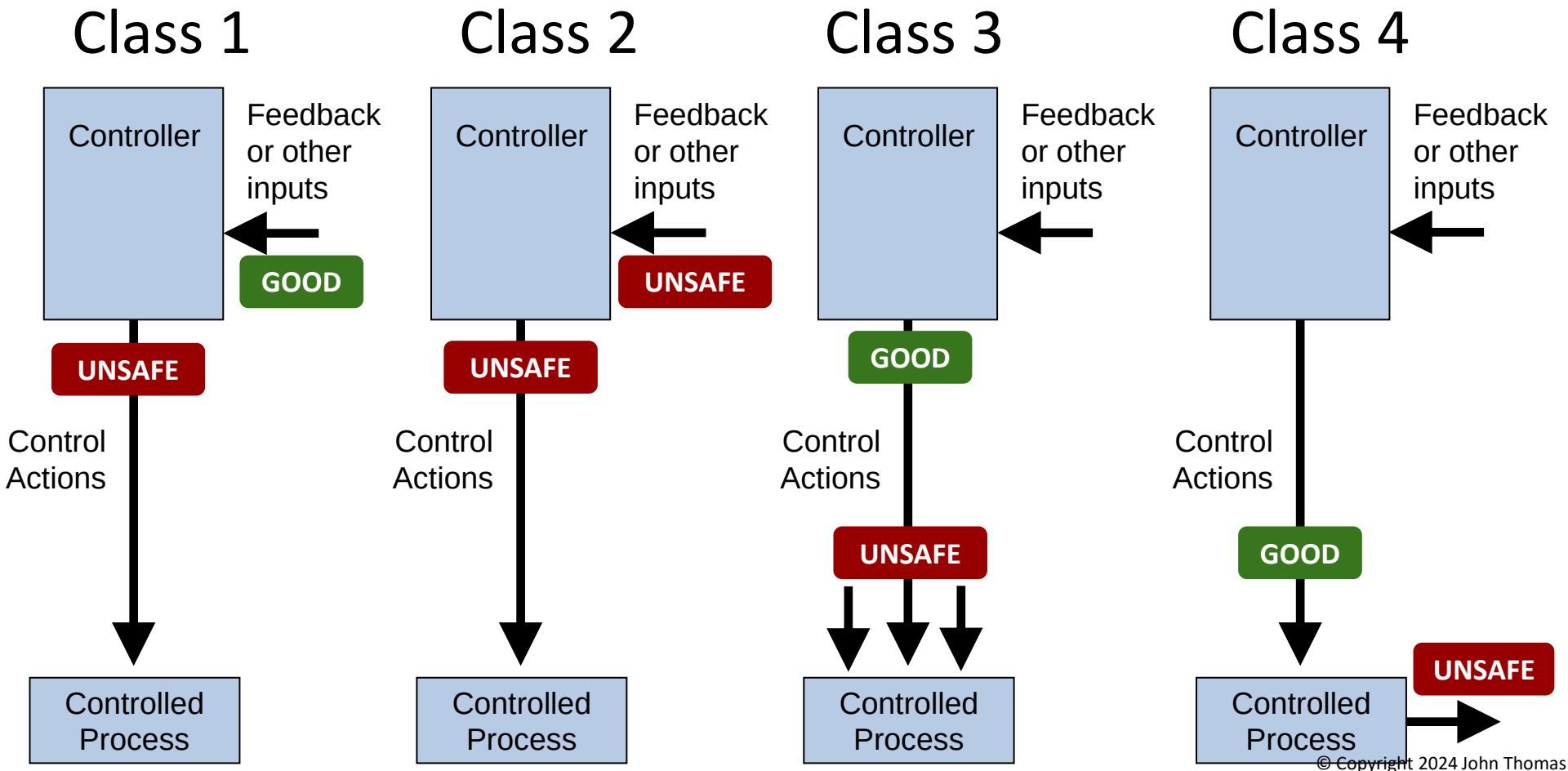


Why?

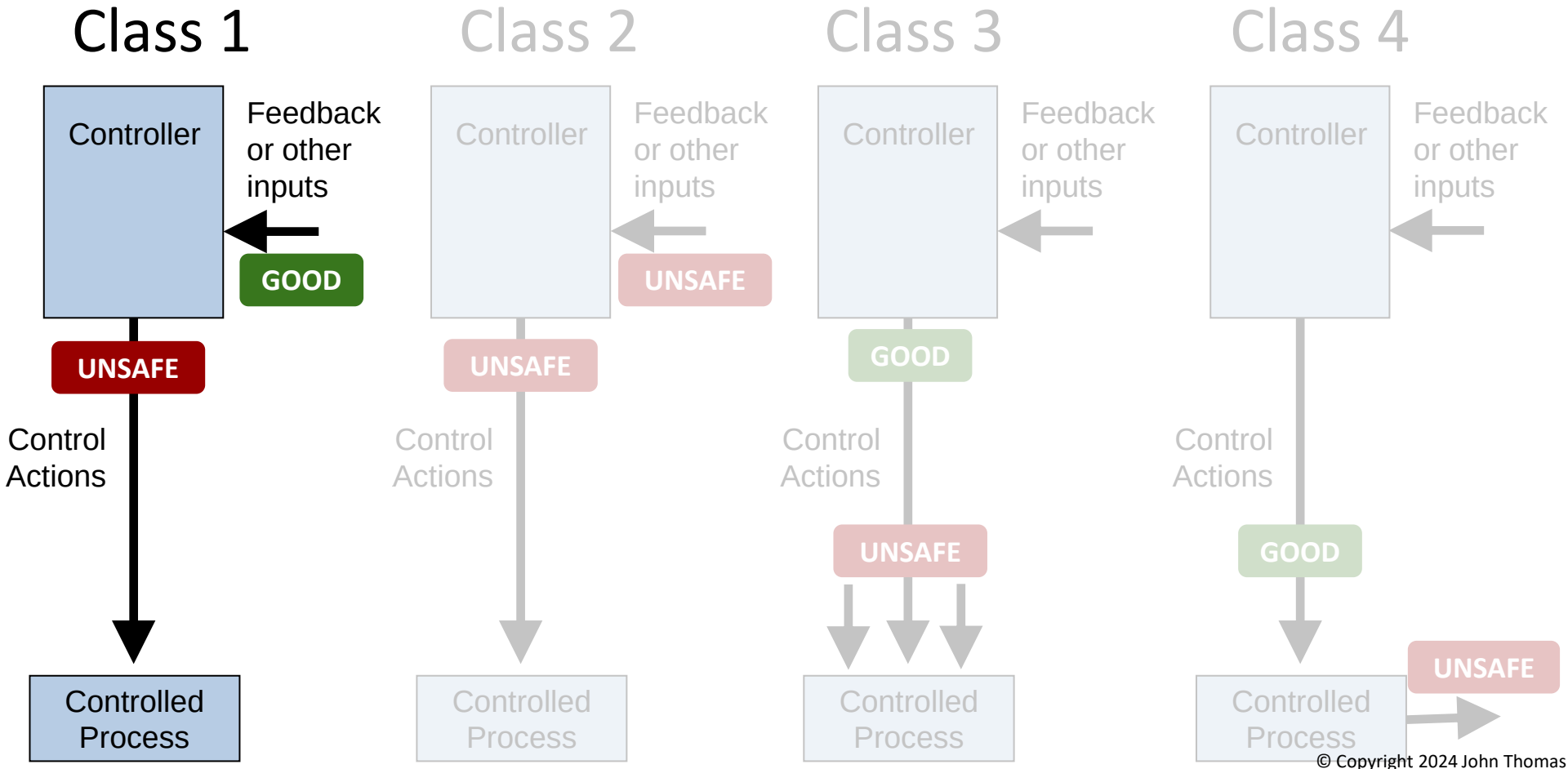
STPA Step 4B: Potential control actions not followed properly



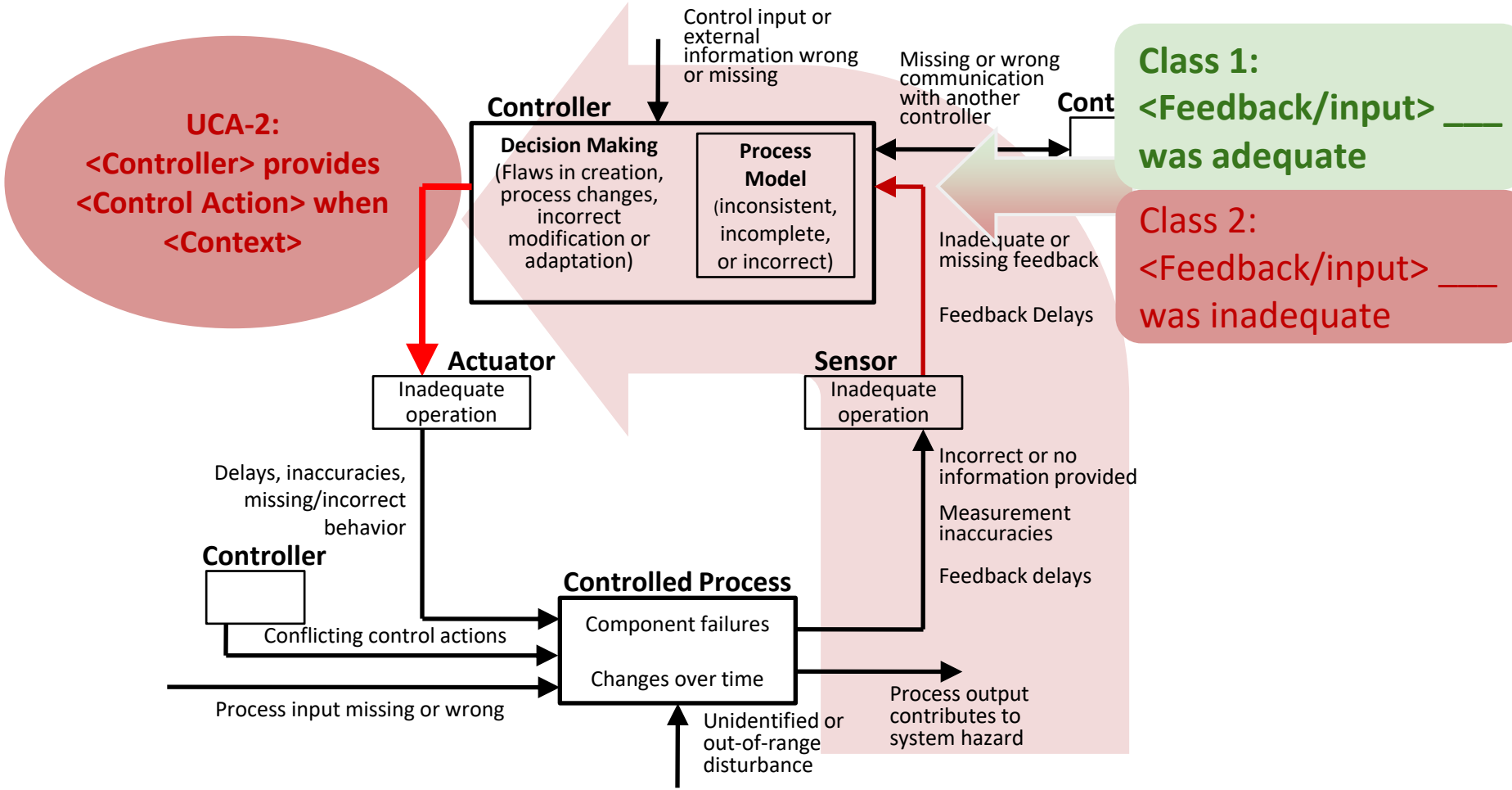
Four Classes of Formal Scenarios



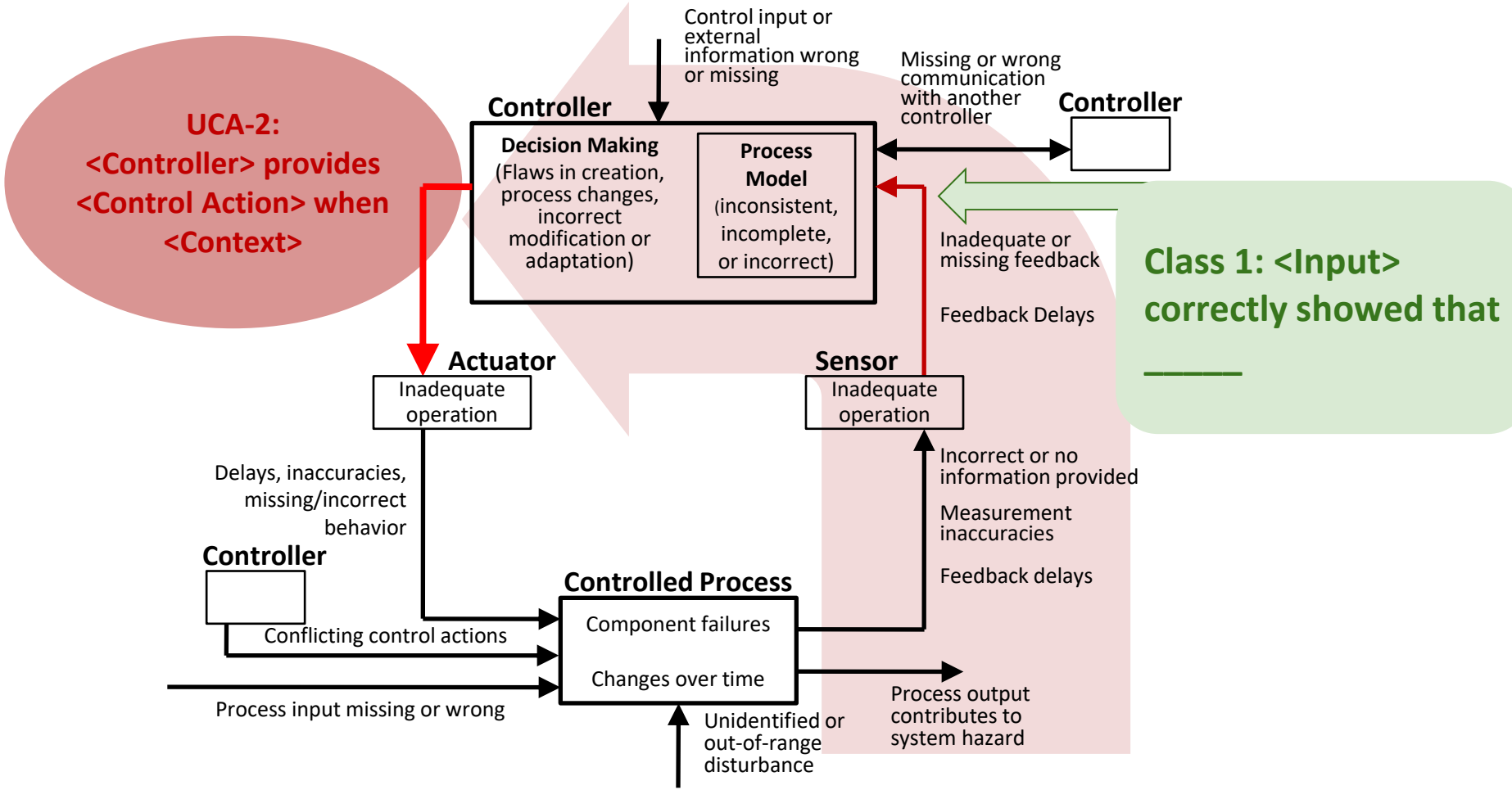
Four Classes of Formal Scenarios



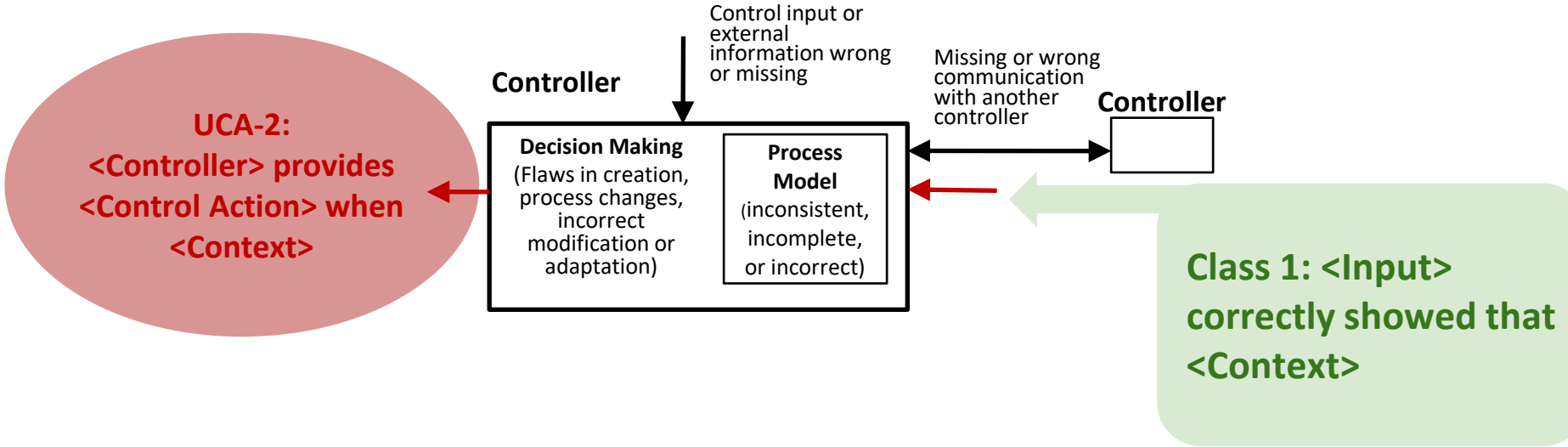
STPA Step 4A: Identify scenarios that cause UCAs



STPA Step 4A: Identify scenarios that cause UCAs



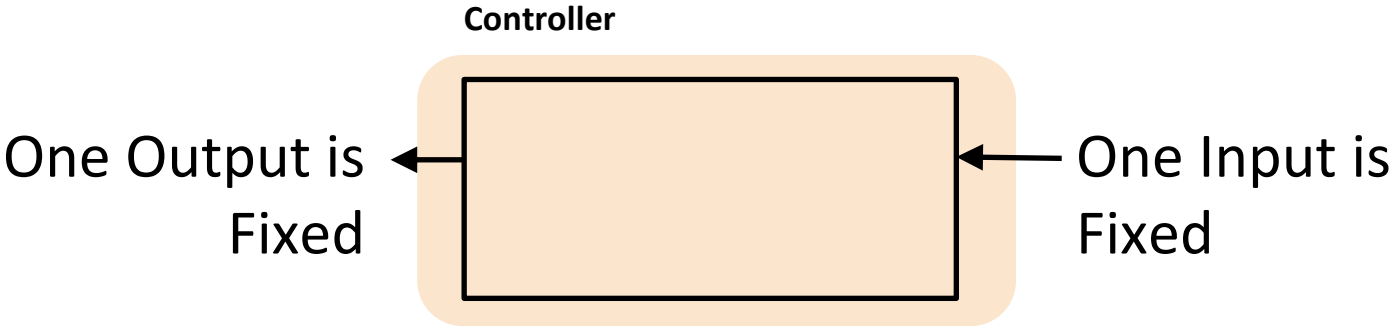
STPA Step 4A: Identify scenarios that cause UCAs



Class 1 Scenario Archetype:

- **Output**: UCA-1: <Controller> provides <Control Action> when <Context>
- **Input**: Class 1: <Input> correctly showed that <Context>

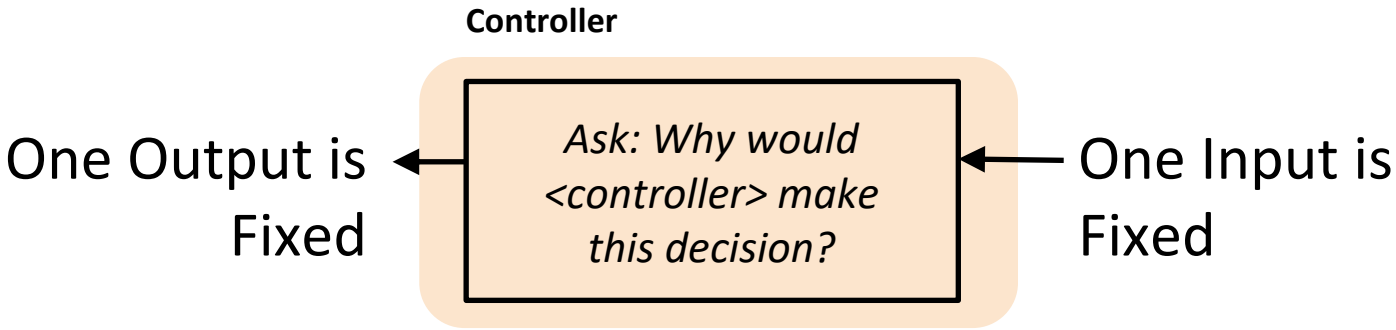
General Transfer Function Concept



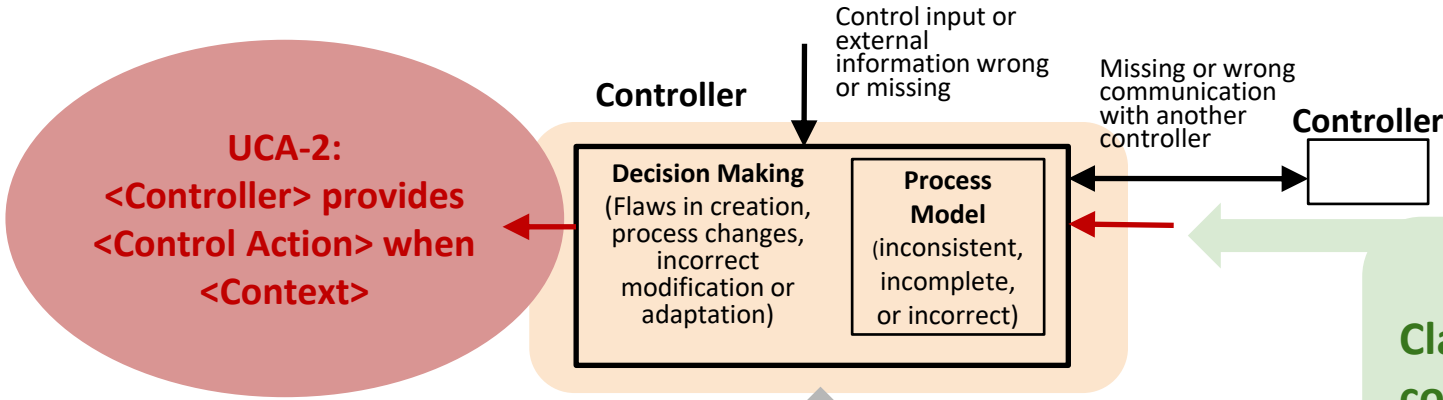
Class 1 Scenario Archetype:

- **Output**: UCA-1: <Controller> provides <Control Action> when <Context>
- **Input**: Class 1: <Input> correctly showed that <Context>

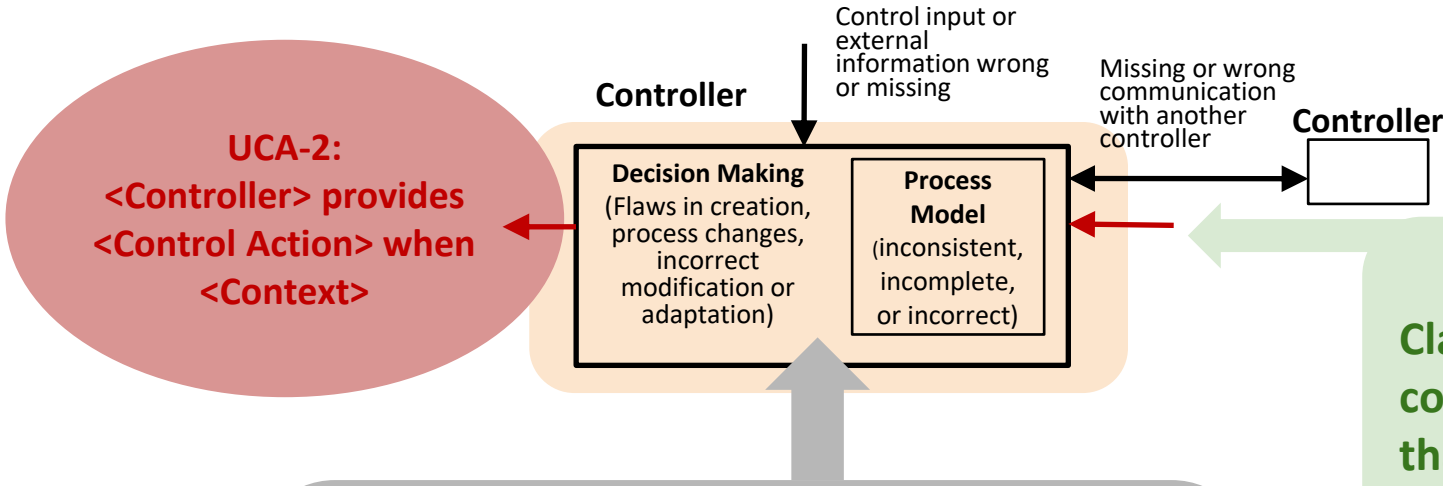
General Transfer Function Concept



STPA Step 4A: Identify scenarios that cause UCAs



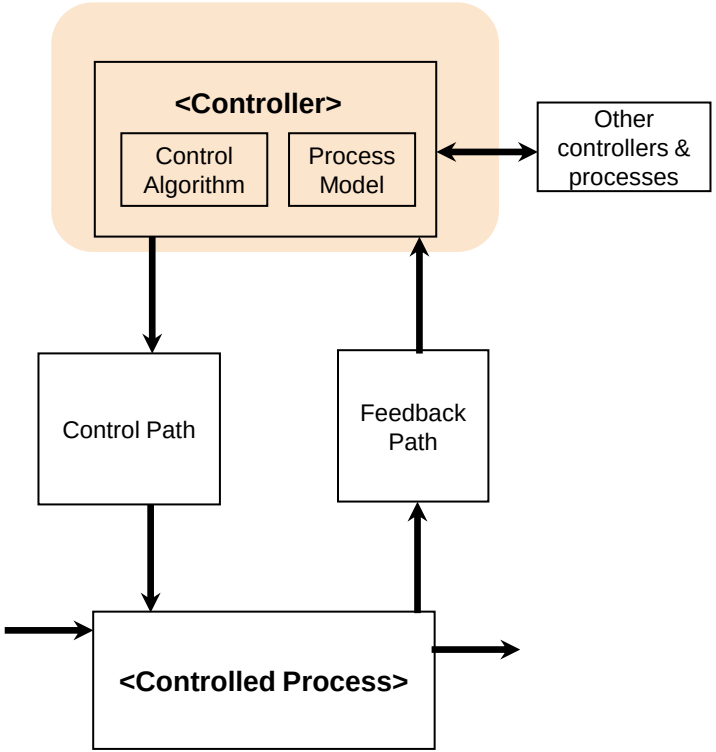
STPA Step 4A: Identify scenarios that cause UCAs



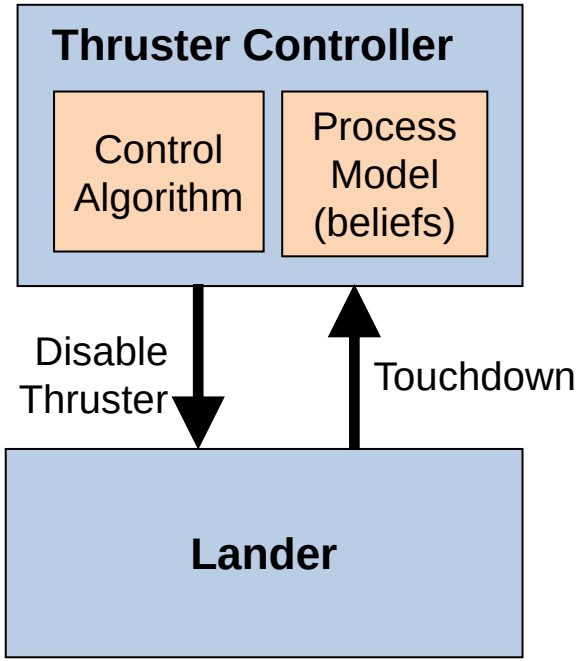
UCA-2:
<Controller> provides <Control Action> when <Context>

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____



Example: Mars Polar Lander



Mars Polar Lander

Process Model: Incorrectly believes spacecraft is on ground

Feedback: Touchdown indication received when in air

Unsafe Control Action (UCA): Computer provides Disable-Thruster cmd when spacecraft is in the air

Thruster Controller

Control Algorithm

Process Model (beliefs)

Disable Thruster

Touchdown

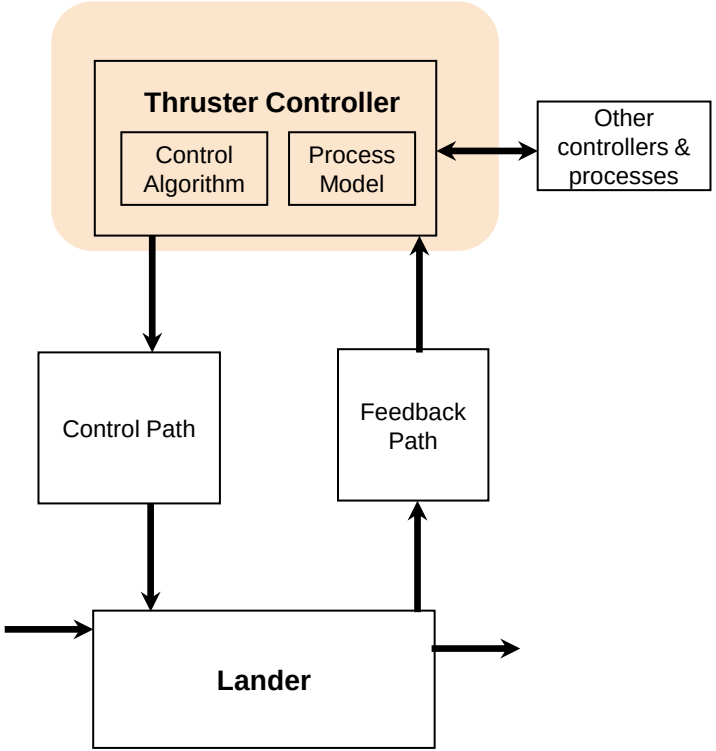
Lander

Physical Interaction: Simultaneous leg vibration during leg deployment

Scenario Archetypes

UCA-2:
Thruster Controller provides
Disable-Thruster Cmd
when spacecraft is in the air

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- UCA: <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

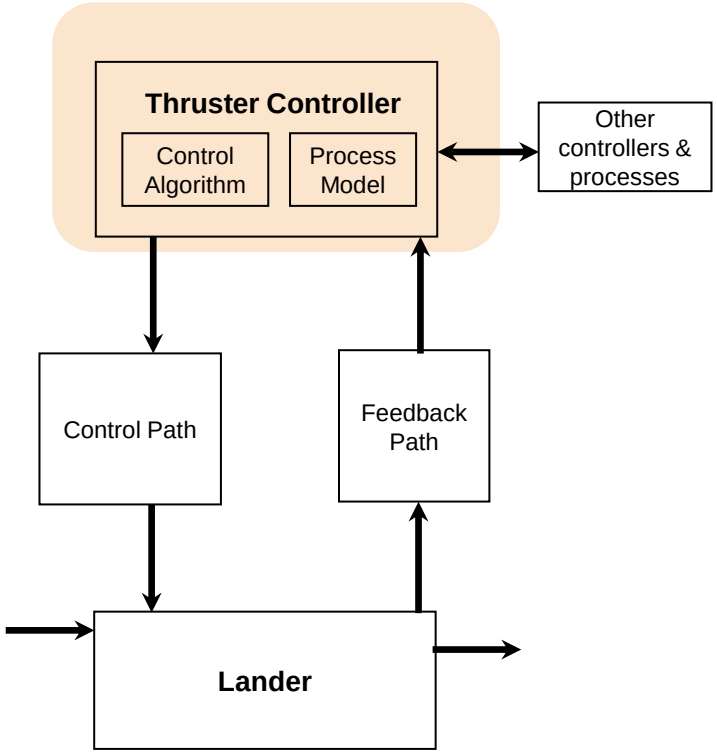


Scenario Archetypes

UCA-2:
Thruster Controller provides
Disable-Thruster Cmd
when spacecraft is in the air

Class 1 Scenario Archetype:
Inadequate Controller Behavior

- Controller provides Disable-Thruster Cmd when spacecraft is in the air
- <Input> to <Controller> correctly indicated _____

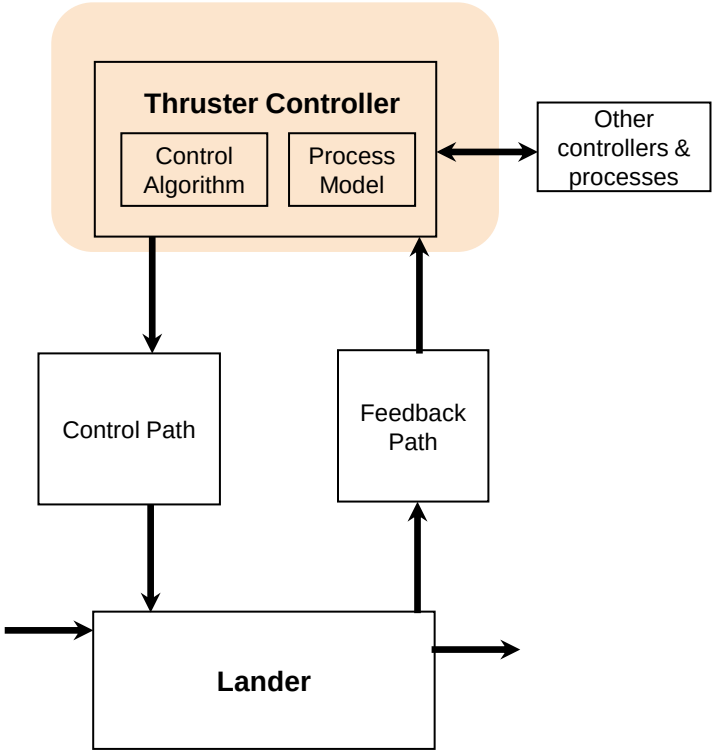


Scenario Archetypes

UCA-2:
Thruster Controller provides
Disable-Thruster Cmd
when spacecraft is in the air

Class 1 Scenario Archetype:
Inadequate Controller Behavior

- Controller provides Disable-Thruster Cmd when spacecraft is in the air
- Touchdown Input to Controller correctly indicated it's in the air



UCA-2:
<Controller> provides ____ when ____

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:

Class 3 Scenario Archetype:

Class 4 Scenario Archetype:

Refined Scenarios

Ask: Why would <Controller> make this decision?

UCA-2:
<Controller> provides ____ when ____

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:

Class 3 Scenario Archetype:

Class 4 Scenario Archetype:

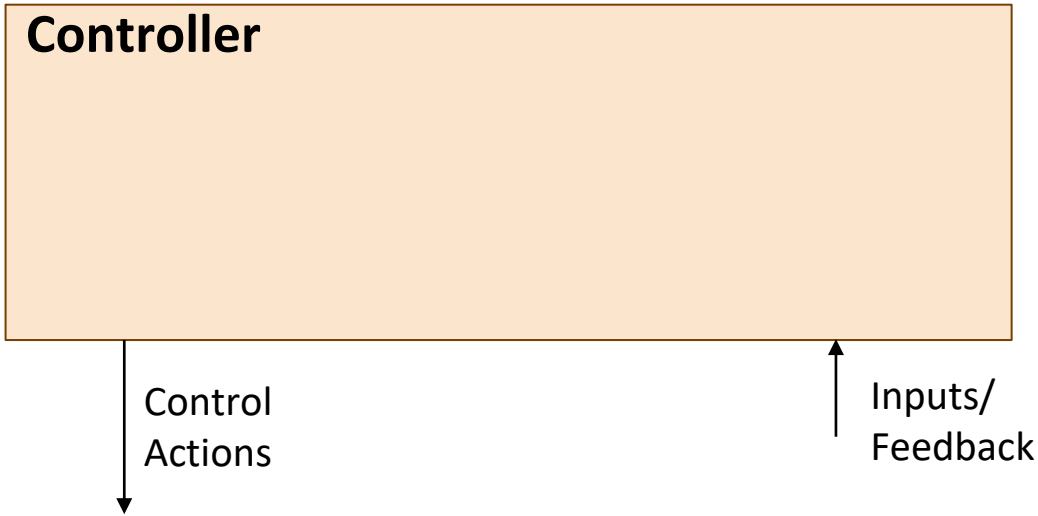
Refined Scenarios

Why would <Controller> make this decision?

- Because <Controller> is designed to default to ____ if _____ (will ignore ____ and ____)
- Because <Controller> also received ____, so it appeared reasonable to <Control Action>
- Because there is no other _____, so other control actions were not feasible
- Etc.

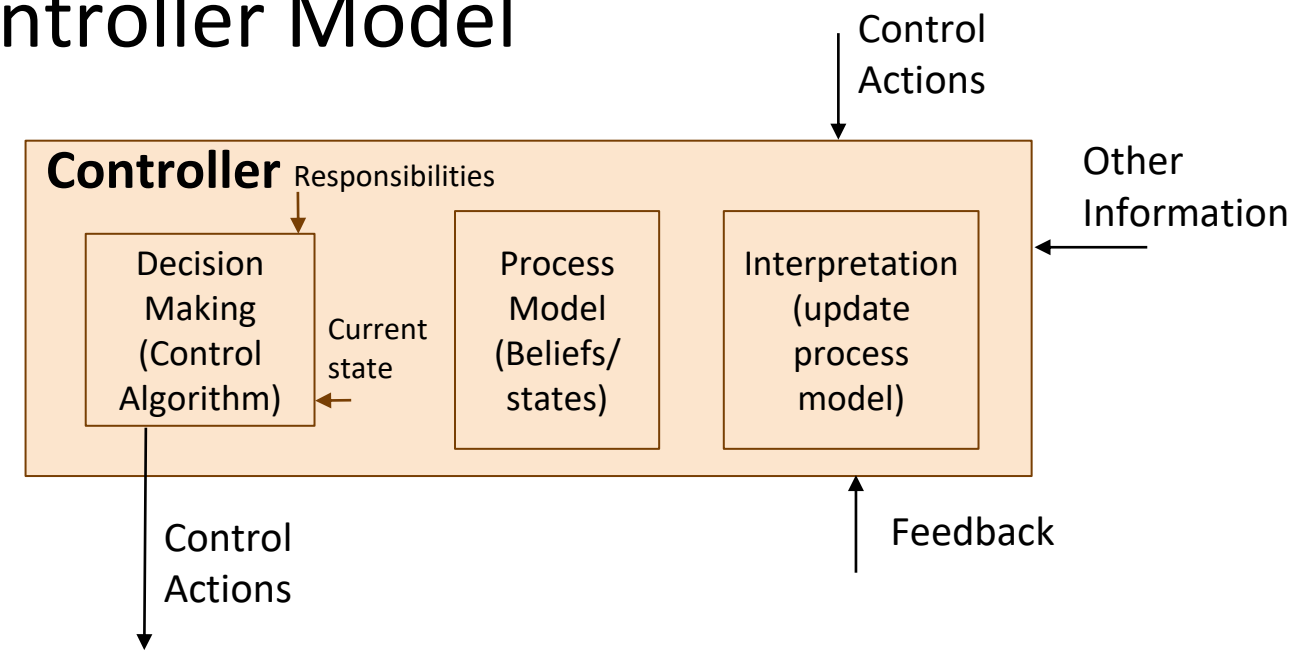
If you have trouble, a generic controller model can help you ask better questions & find actionable causes.

Generic Controller Model



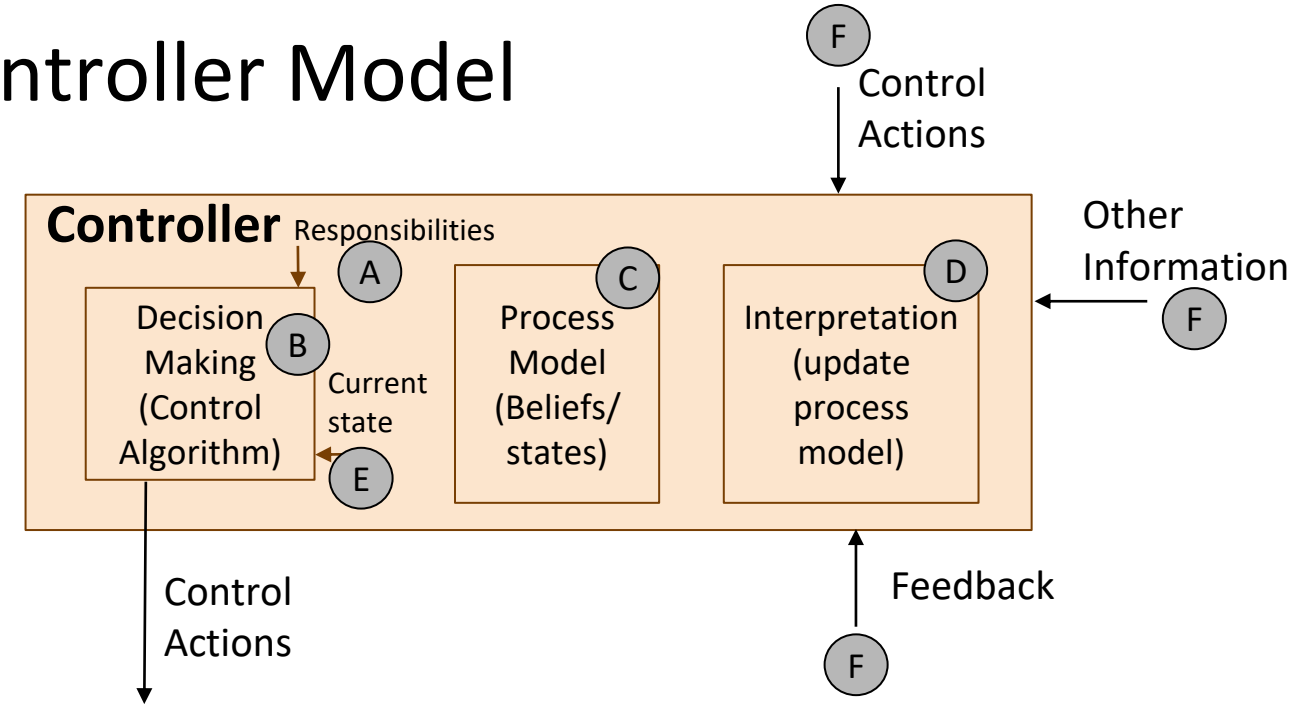
Class 1 Scenario Archetype: **Output**: UCA **Input**: Correctly indicates UCA context (but other inputs may override or conflict)

Generic Controller Model



Class 1 Scenario Archetype: **Output**: UCA **Input**: Correctly indicates UCA context (but other inputs may override or conflict)

Generic Controller Model



Class 1 Scenario Archetype: **Output**: UCA **Input**: Correctly indicates UCA context (but other inputs may override or conflict)

Why would <controller> make this decision? → A D B E C F

Refining Class 1 Scenario Archetype: Inadequate Controller Behavior

Common causes of Scenario Archetype 1:

A. Responsibilities (e.g., desired end states) that would produce this UCA

B. Control algorithms or decision-making rationale that would explain the UCA

C. Process models that would explain this UCA

D. Interpretation rules / process model updates that would explain the UCA

E. Internal controller states/modes that would explain the UCA (failure, lame duck mode, etc.)

F. Controller inputs (control actions, feedback, or other inputs) that would explain the UCA
   - E.g., Conflicting/contradictory inputs, inputs from another controller, etc.
   - If the input is another UCA, then make sure the new UCA is recorded in STPA Step 3. The new UCA will be analyzed using the same process.

G. Etc.

UCA-2:
<Controller> provides ____ when ____

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:

Class 3 Scenario Archetype:

Class 4 Scenario Archetype:

Refined Scenarios

A

Responsibilities
<Controller> by design is responsible for always assigning ____ to every ___ (even if _____.)

Discussion: Responsibilities can be:
- Fixed (hardcoded, embedded in design of algorithm)
- Dynamic (provided in real-time as a control action input into the controller)
- Adaptive (developed and changed by the controller as needed)

UCA-2:
<Controller> provides ____ when ____

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:

Class 3 Scenario Archetype:

Class 4 Scenario Archetype:

Refined Scenarios

B

Control Algorithms
<Controller> control algorithm is designed to fall back onto ____ strategy if _____

UCA-2:
<Controller> provides ____ when ____

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:

Class 3 Scenario Archetype:

Class 4 Scenario Archetype:

Refined Scenarios

C

Process Models

PM-1: <Controller> incorrectly believes _____

UCA-2:
<Controller> provides ____ when ____

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:

Class 3 Scenario Archetype:

Class 4 Scenario Archetype:

Refined Scenarios

D

<u>Interpretation of inputs</u>

In some situations, <Controller> will interpret ___ as an indicator of ___. This interpretation can underestimate ___, causing ___.

When <Feedback/input 1> conflicts with <feedback/input 2>, <Controller> may assume ____

When <feedback/input> is not available, <Controller> may assume ___

UCA-2:
<Controller> provides ____ when ____

Scenario Archetypes

Refined Scenarios

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:

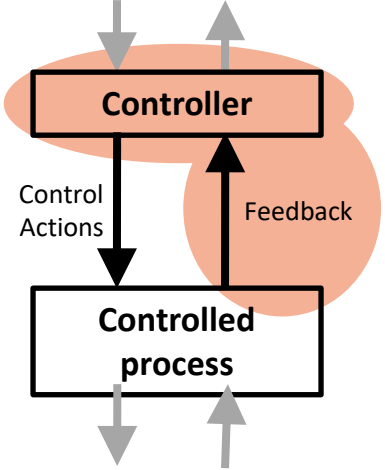
Class 3 Scenario Archetype:

Class 4 Scenario Archetype:

D

Update Process Model

Unsafe PM Update	**Unsafe Feedback** or Inputs
PM-1 is not updated when _ PM-1 is the initial (default) belief before feedback/input ___ received	Feedback/input ___ is (or is not) provided when ___
PM-1 is updated incorrectly due to feedback/input ___ that indicates ___	Feedback/input ___ is provided when ___
PM-1 is updated too late (or early) due to ___	Feedback/input ___ is delayed (or too early) when ___
PM-1 stops updating too soon before ____ PM-1 continues to be updated too long after ___	Feedback/input ___ is applied too long after (stopped too soon before) _____



Refined Scenarios

Not Provided Causes Hazard

Provided Causes Hazard

Too early / too late

Stopped too soon / Applied too long

Update Process Model

Unsafe PM Update	**Unsafe Feedback** or Inputs
PM-1 is not updated when _ PM-1 is the initial (default) belief before feedback/input ___ received	Feedback/input ___ is (or is not) provided when ___
PM-1 is updated incorrectly due to feedback/input ___ that indicates ___	Feedback/input ___ is provided when ___
PM-1 is updated too late (or early) due to ___	Feedback/input ___ is delayed (or too early) when ___
PM-1 stops updating too soon before ____ PM-1 continues to be updated too long after ___	Feedback/input ___ is applied too long after (stopped too soon before) _____

UCA-2:
<Controller> provides ____ when ____

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:

Class 3 Scenario Archetype:

Class 4 Scenario Archetype:

Refined Scenarios

E

Controller States / Modes

- If <Controller> is in ____ mode, it will continue to <Control Action> using alternate input ____.

- If <Controller> ___ is disabled, then <Controller> can _____.

UCA-2:
<Controller> provides ____ when ____

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:

Class 3 Scenario Archetype:

Class 4 Scenario Archetype:

Refined Scenarios

F

Other Inputs

<Controller> does not prevent <Control Action> when alternate input ___ is received.

UCA-2:
<Controller> provides ____ when ____

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:

Class 3 Scenario Archetype:

Class 4 Scenario Archetype:

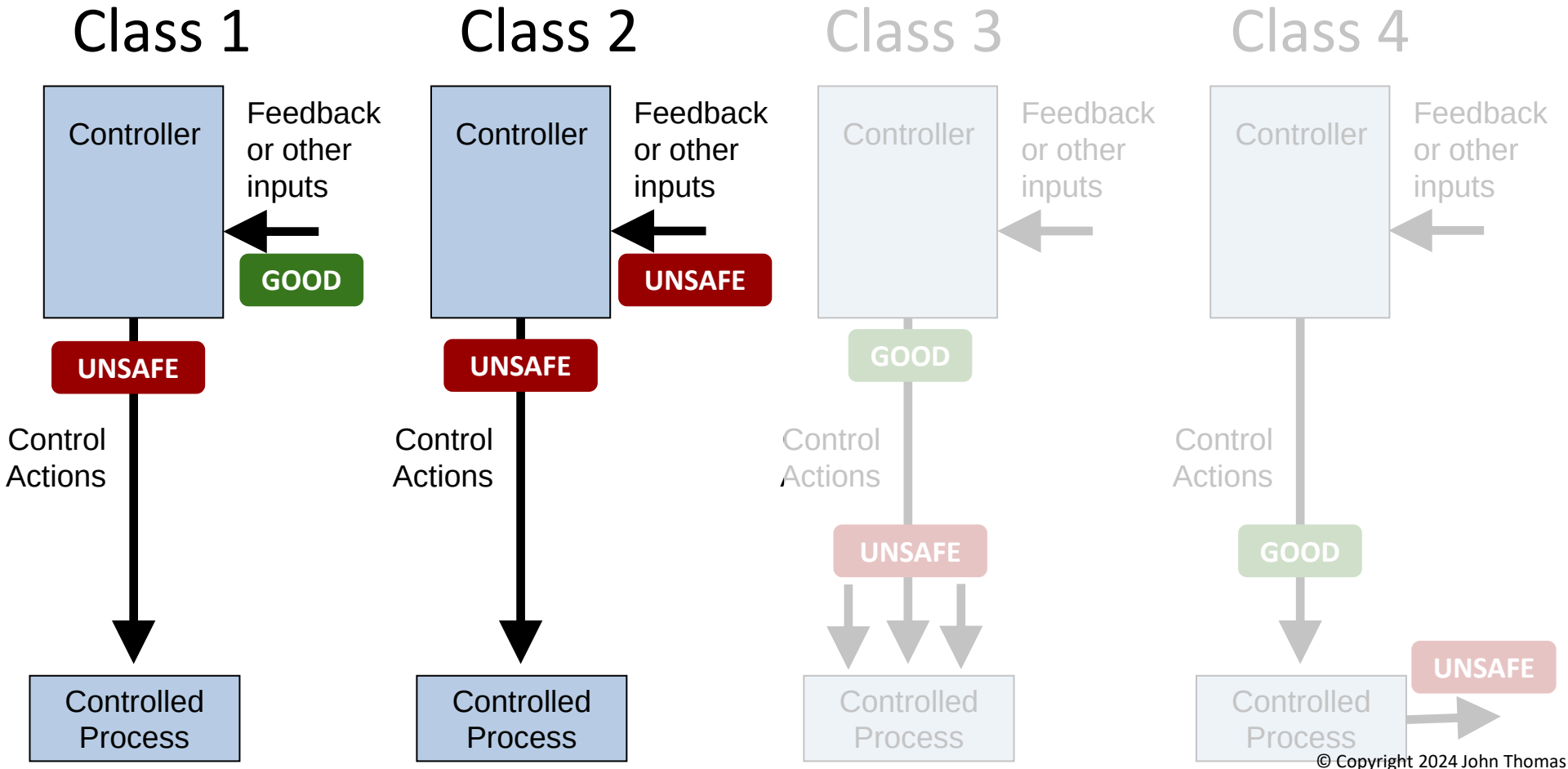
Refined Scenarios

F

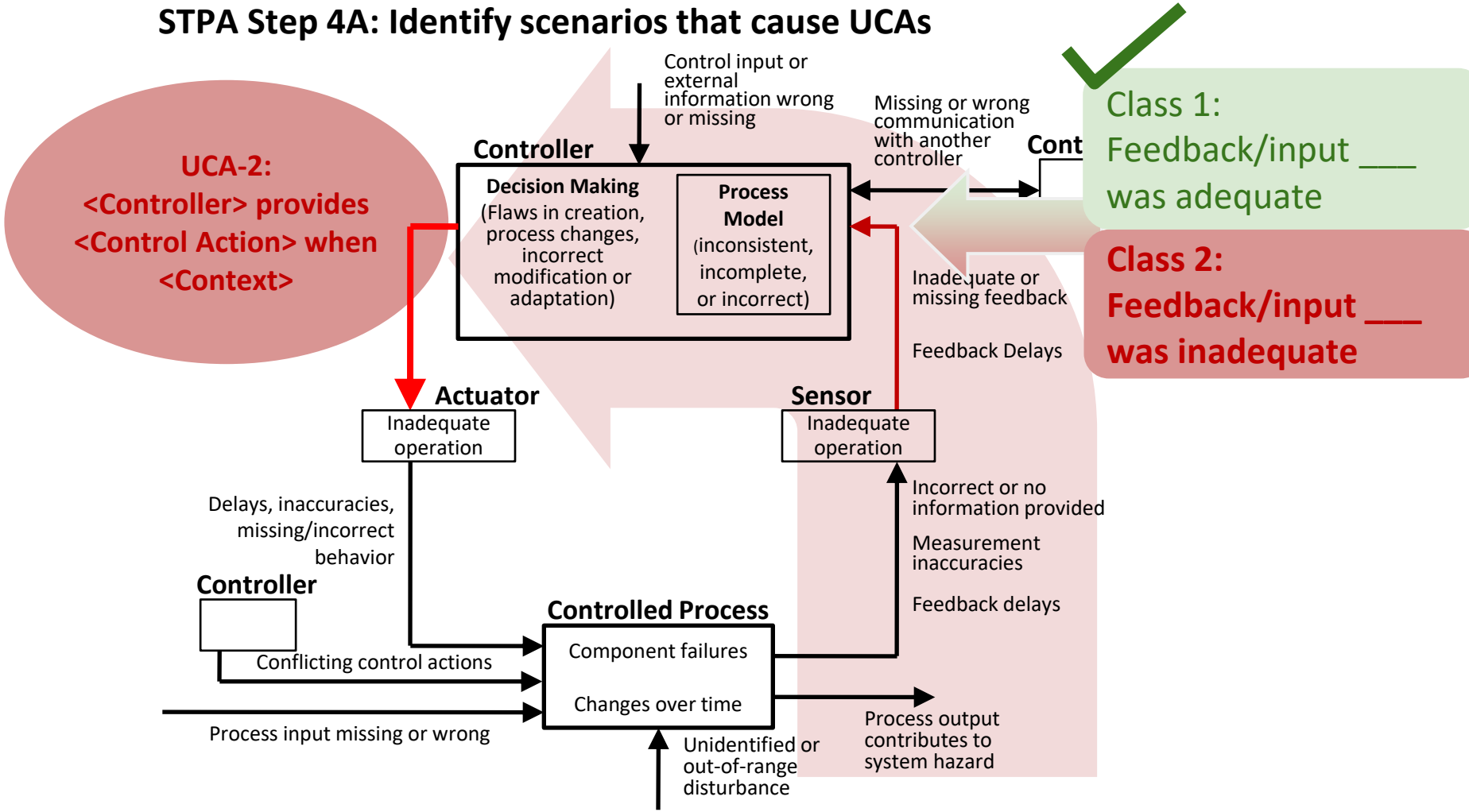
Other inputs

- Although <Input> is correct, the feedback from ___ may be incorrect and may cause <Controller> to ____.

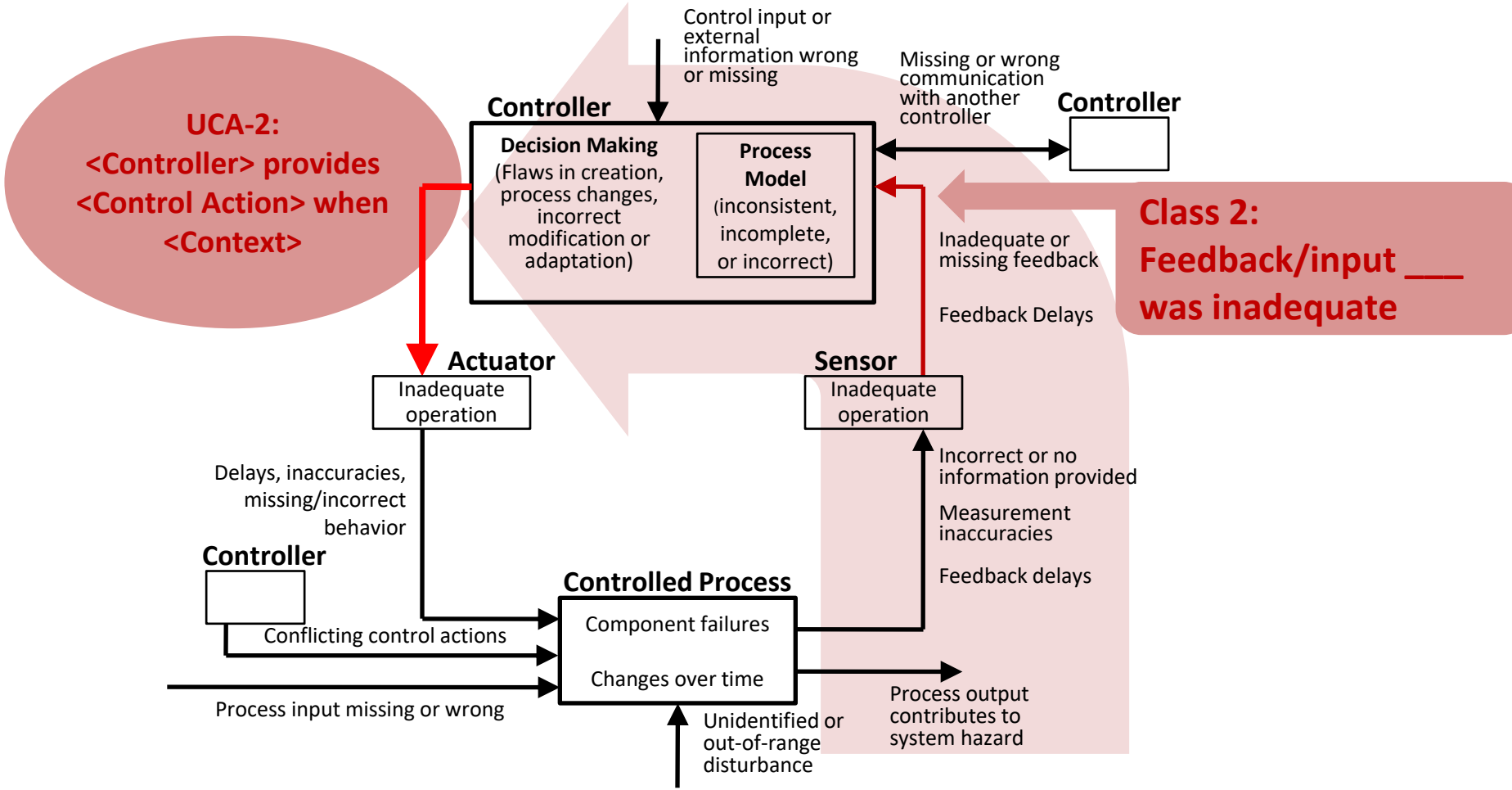
Four Classes of Formal Scenarios



STPA Step 4A: Identify scenarios that cause UCAs



STPA Step 4: Class 2 Scenario Archetype



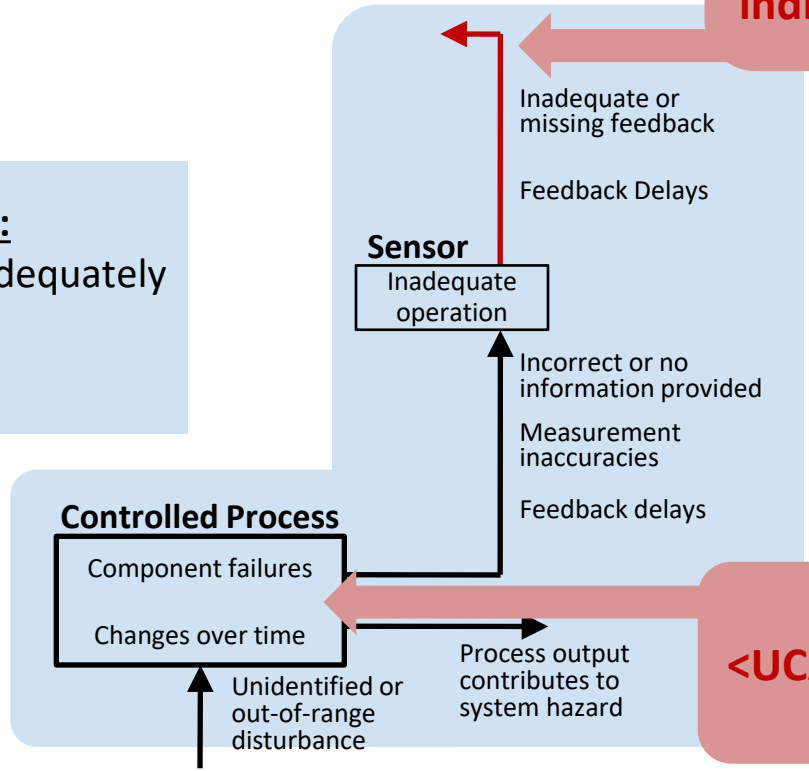
STPA Step 4: Class 2 Scenario Archetype

UCA-2:
<Controller> provides <Control Action> when <Context>

Class 2:
Feedback/Input did not adequately indicate ____

Class 2 Scenario Archetype:

- Feedback to <Controller> did not adequately indicate <Context>
- <Context> is true

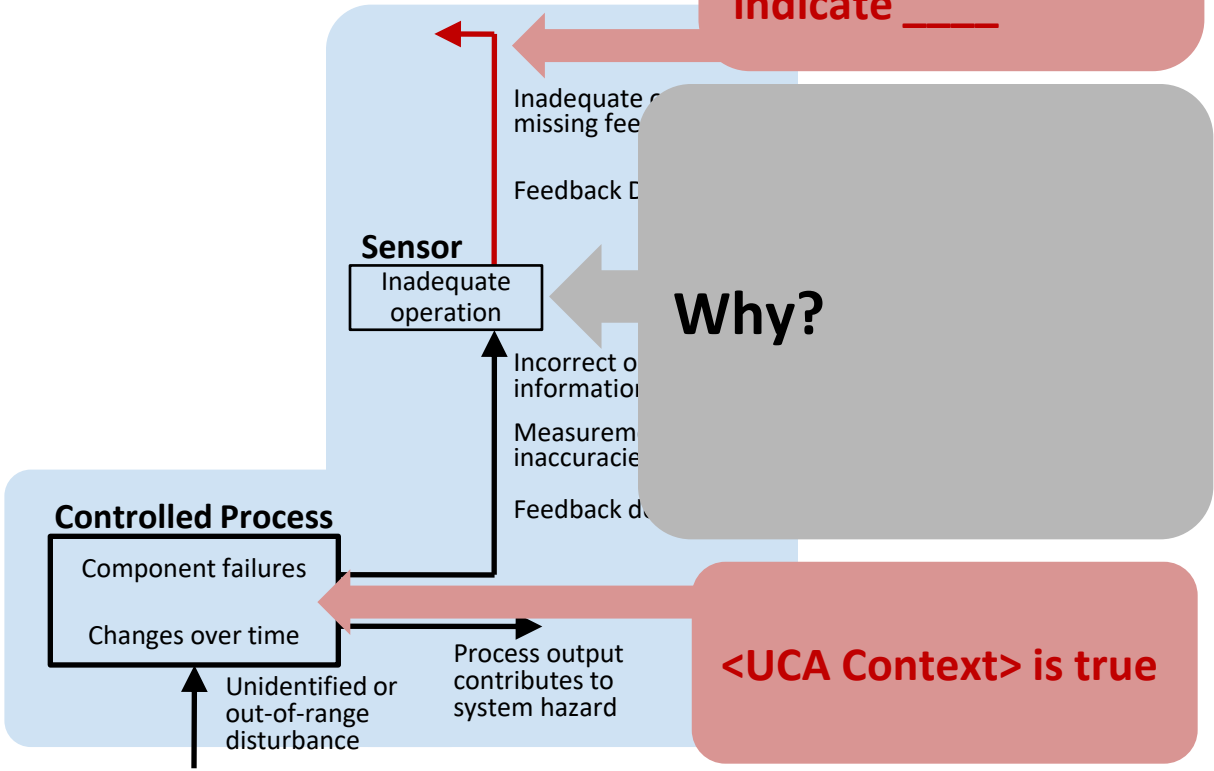


<UCA Context> is true

STPA Step 4: Class 2 Scenario Archetype

UCA-2:
<Controller> provides <Control Action> when <Context>

Class 2: Feedback/Input did not adequately indicate ____



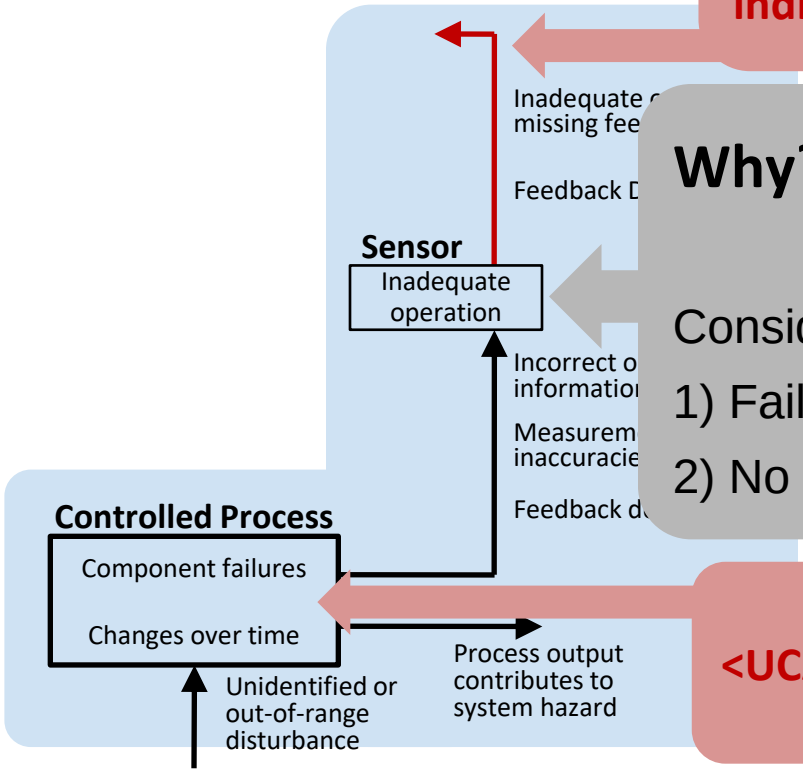
Why?

<UCA Context> is true

STPA Step 4: Class 2 Scenario Archetype

UCA-2:
<Controller> provides <Control Action> when <Context>

Class 2:
Feedback/Input did not adequately indicate ____



Why?

Consider:

1) Failure causes

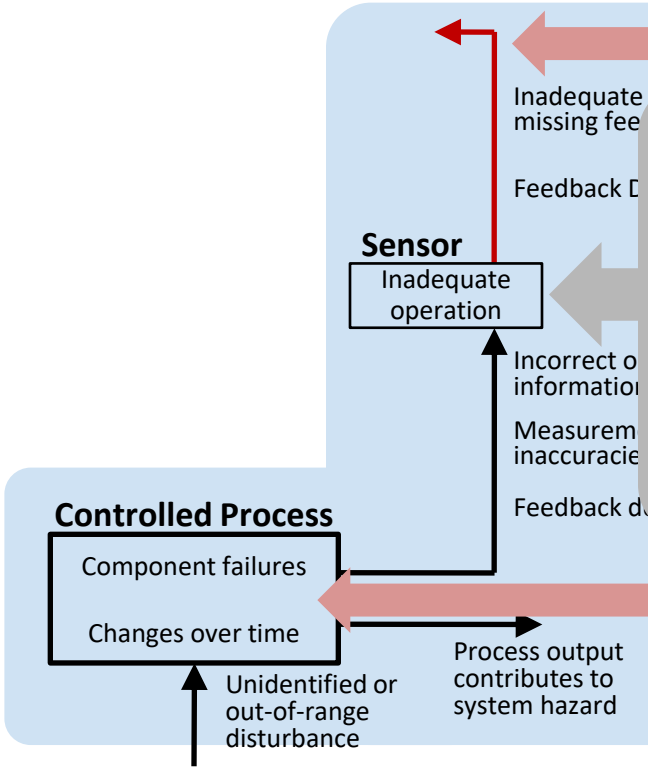
2) No failures

<UCA Context> is true

STPA Step 4: Class 2 Scenario Archetype

UCA-2:
<Controller> provides <Control Action> when <Context>

Class 2: Feedback/Input did not adequately indicate ____



Why? (non-failures)

- Because the ___metric is estimated from ___ that uses different ___
- Because the ___ feedback is outdated due to ___ second feedback delay
- Etc.

<UCA Context> is true

STPA Step 4: Class 2 Scenario Archetype

UCA-2:
<Controller> provides <Control Action> when <Context>

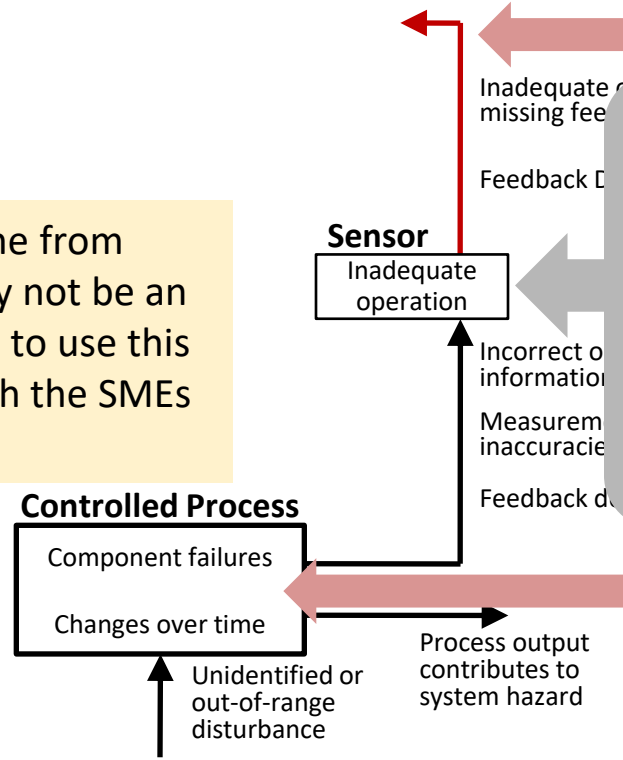
Class 2: Feedback/Input did not adequately indicate ____

Why? (non-failures)

- Because the ___metric is estimated from ___ that uses different ___
- Because the ___ feedback is outdated due to ___ second feedback delay
- Etc.

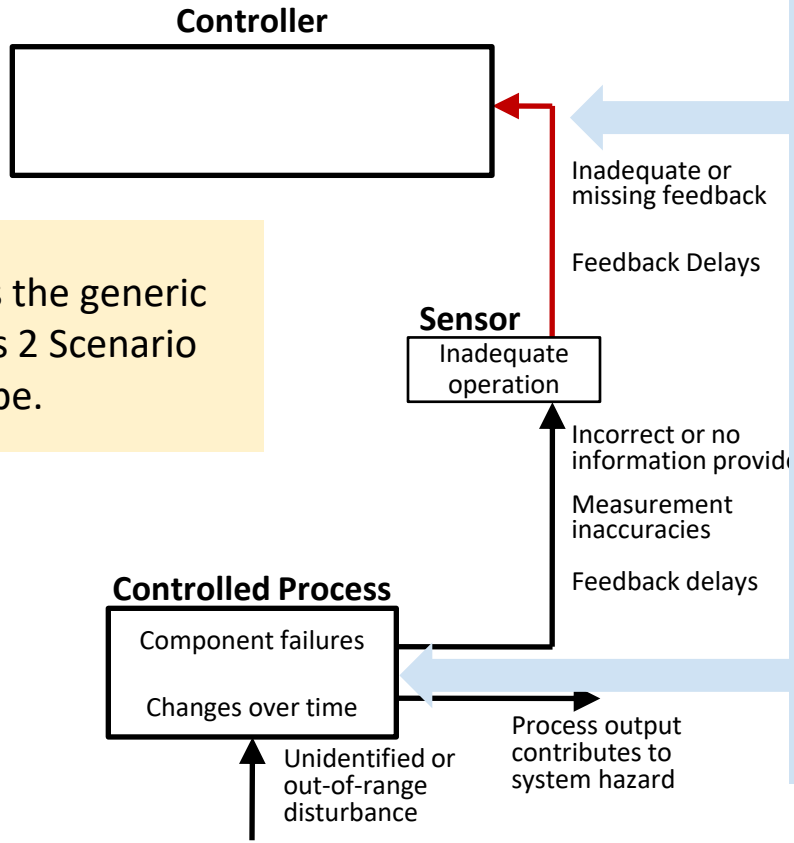
<UCA Context> is true

Discussion: The "Why" answers may come from SMEs, not the STPA practitioner. You may not be an expert in the system. The point is for you to use this framework to ask questions and approach the SMEs to find these answers.



STPA Step 4: Class 2 Scenario Archetype

UCA-2:
<Controller> provides <Control Action> when <Context>



Discussion: This is the generic form for the Class 2 Scenario Archetype.

Class 2 Scenario Archetype
Inadequate Feedback

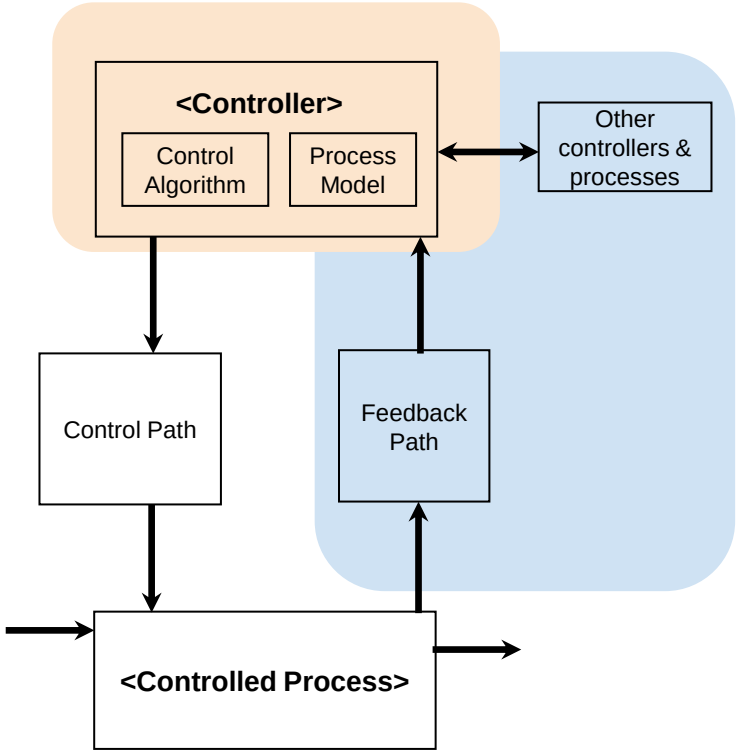
Output: <Feedback/Input> to <Controller> did not adequately indicate <Context>

Input: <Process> is actually <Context>

UCA-2:
<Controller> provides <Control Action>
when <Context>

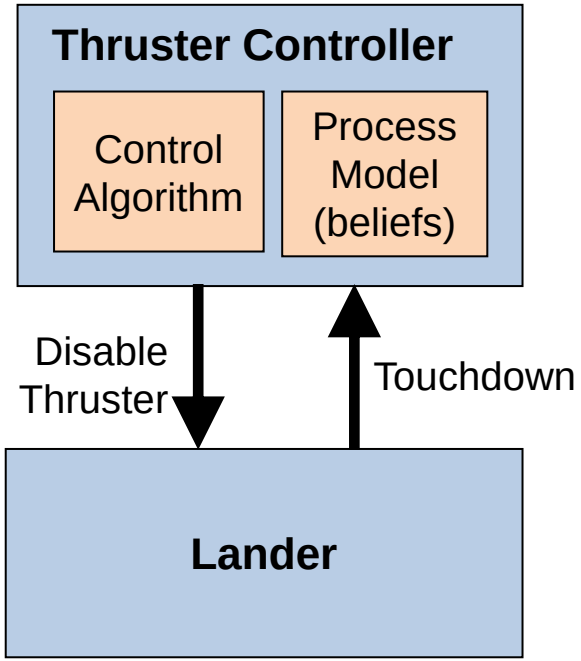
Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____



Class 2 Scenario Archetype:
Inadequate feedback/information
- <Feedback/Input> to <Controller> did not adequately indicate <Context>
- <Process> is actually <Context>

Example: Mars Polar Lander



Mars Polar Lander

Process Model: Incorrectly believes spacecraft is on ground

Feedback: Touchdown indication received when in air

Unsafe Control Action (UCA): Computer provides Disable-Thruster cmd when spacecraft is in the air

Thruster Controller

Control Algorithm

Process Model (beliefs)

Disable Thruster

Touchdown

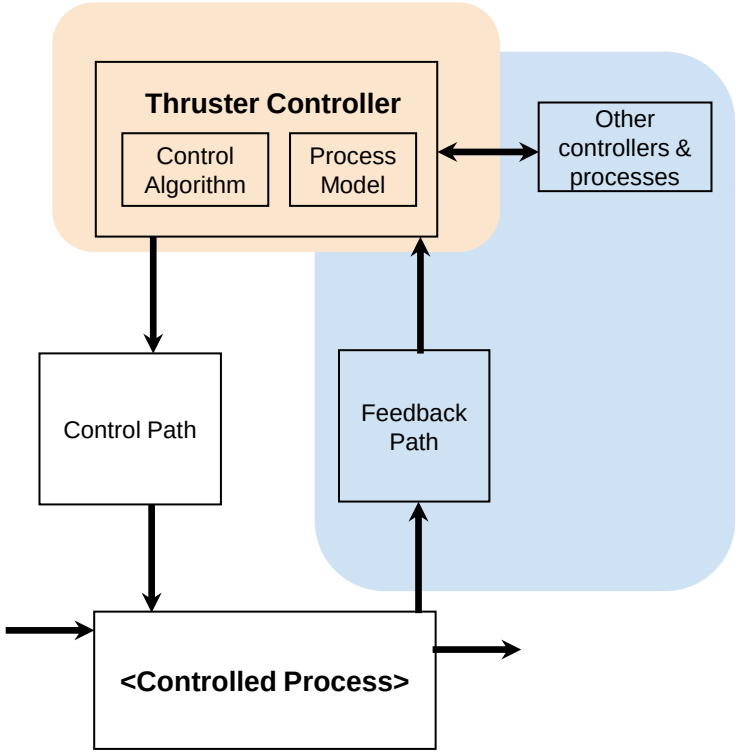
Lander

Physical Interaction: Simultaneous leg vibration during leg deployment

Example: Mars Polar Lander

UCA-2:
Thruster Controller provides Disable-Thruster Cmd when spacecraft is in the air

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- Controller provides Disable-Thruster Cmd when spacecraft is in the air
- Touchdown Input to Controller correctly indicated it's in the air

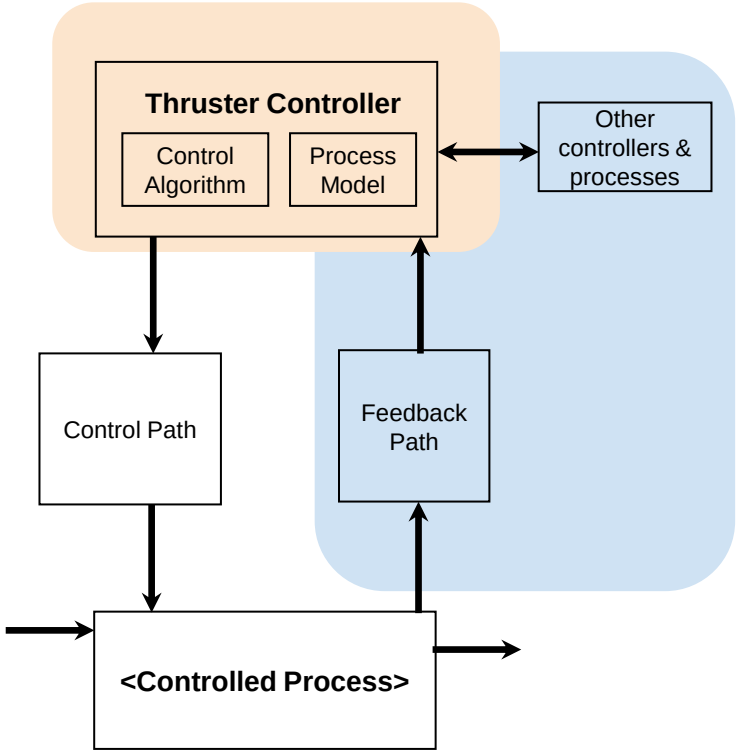


Class 2 Scenario Archetype:
Inadequate feedback/information
- <Feedback/Input> to <Controller> did not adequately indicate <Context>
- <Process> is actually <Context>

Example: Mars Polar Lander

UCA-2:
Thruster Controller provides Disable-Thruster Cmd when spacecraft is in the air

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- Controller provides Disable-Thruster Cmd when spacecraft is in the air
- Touchdown Input to Controller correctly indicated it's in the air

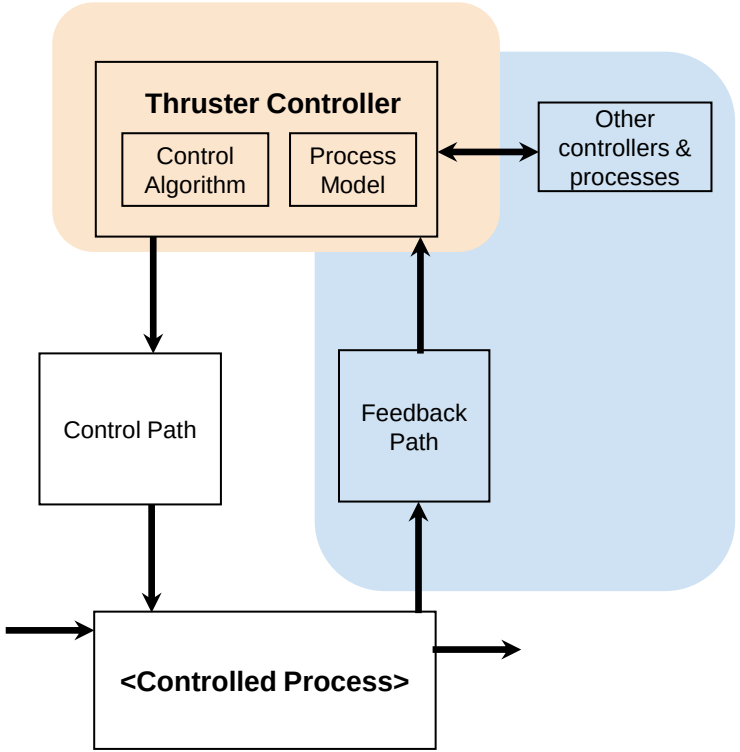


Class 2 Scenario Archetype:
Inadequate feedback/information
- Touchdown feedback does not indicate it's in air
- <Process> is actually <Context>

Example: Mars Polar Lander

UCA-2:
Thruster Controller provides Disable-Thruster Cmd when spacecraft is in the air

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- Controller provides Disable-Thruster Cmd when spacecraft is in the air
- Touchdown Input to Controller correctly indicated it's in the air



Class 2 Scenario Archetype:
Inadequate feedback/information
- Touchdown feedback does not indicate it's in air
- Lander is actually in the air

UCA-2:
<Controller> provides <Control Action> when <Context>

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:
Inadequate feedback/information
- <Feedback/Input> to <Controller> did not adequately indicate <Context>
- <Process> is actually <Context>

Class 3 Scenario Archetype:

Class 4 Scenario Archetype:

Refined Scenarios

Ask: What can cause this Scenario Archetype?

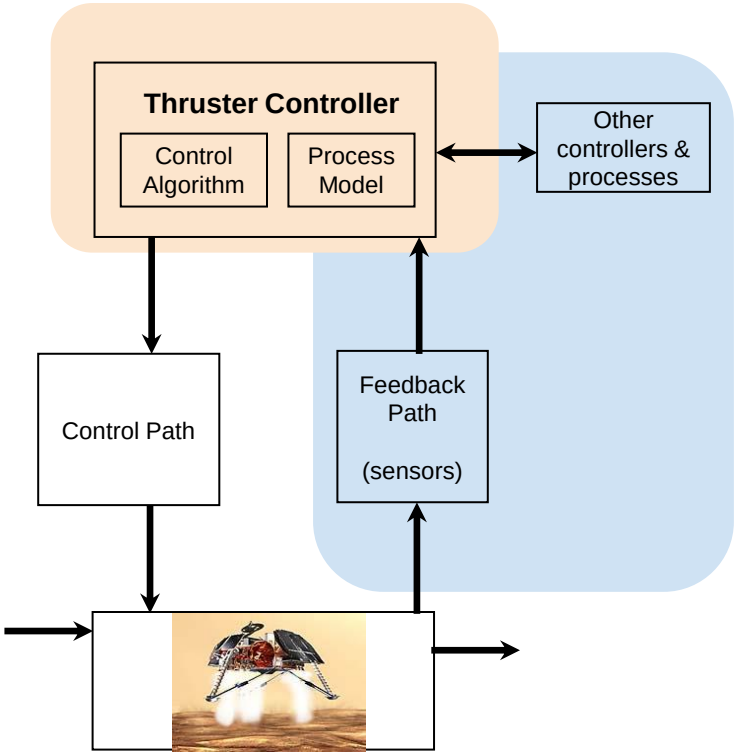
Consider:
1) Failure causes
2) No failures

UCA-2: Thruster Controller provides Disable-Thruster Cmd when spacecraft is in the air

Example: Mars Polar Lander

Refined Scenarios

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- Controller provides Disable-Thruster Cmd when spacecraft is in the air
- Touchdown Input to Controller correctly indicated it's in the air



Class 2 Scenario Archetype:
Inadequate feedback/information
- Touchdown feedback does not indicate it's in air
- Lander is in the air

What can cause this?

1) Failure causes

2) No failures

What does "no failure" mean?
- It means the sensors, etc., worked as specified

What does "touchdown sensor worked" mean?
- It means the sensor output was as specified for the sensor input

We know the sensor feedback was [NOT IN AIR]. What was the input?
- If output = [NOT IN AIR], then input = [VIBRATION > X]

UCA-2:
<Controller> provides <Control Action> when <Context>

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:
Inadequate feedback/information
- <Feedback/Input> to <Controller> did not adequately indicate <Context>
- <Process> is actually <Context>

Class 3 Scenario Archetype:

Class 4 Scenario Archetype:

Refined Scenarios

Why?
- Because the ___metric is estimated from ___ that uses different ___
- Because the ___ feedback is outdated due to ___ second feedback delay
- Etc.

Refining Class 2 Scenario Archetype: Inadequate Feedback/Information

Common causes of Scenario Archetype 2:

- Feedback/info missing from design/concept
- Feedback/info not provided
- Conflicting feedback/info
- Incorrect feedback/info provided
- Too early or too late (delayed) feedback/info
- Measurement inaccuracies
- Dropouts
- Corruption
- Content incomplete
- Feedback/info provided in a way the controller can't use
- Overloaded or too much feedback/info
- Etc.

UCA-2:
<Controller> provides <Control Action> when <Context>

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:
Inadequate feedback/information
- <Feedback/Input> to <Controller> did not adequately indicate <Context>
- <Process> is actually <Context>

Class 3 Scenario Archetype:

Class 4 Scenario Archetype:

Refined Scenarios

Too early or too late info
<Feedback> can be sent too early before ____ has occurred.

UCA-2:
<Controller> provides <Control Action> when <Context>

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:
Inadequate feedback/information
- <Feedback/Input> to <Controller> did not adequately indicate <Context>
- <Process> is actually <Context>

Class 3 Scenario Archetype:

Class 4 Scenario Archetype:

Refined Scenarios

No info provided

<Feedback> is not provided when ____ is initialized, reset, or on power up.

UCA-2:
<Controller> provides <Control Action> when <Context>

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:
Inadequate feedback/information
- <Feedback/Input> to <Controller> did not adequately indicate <Context>
- <Process> is actually <Context>

Class 3 Scenario Archetype:

Class 4 Scenario Archetype:

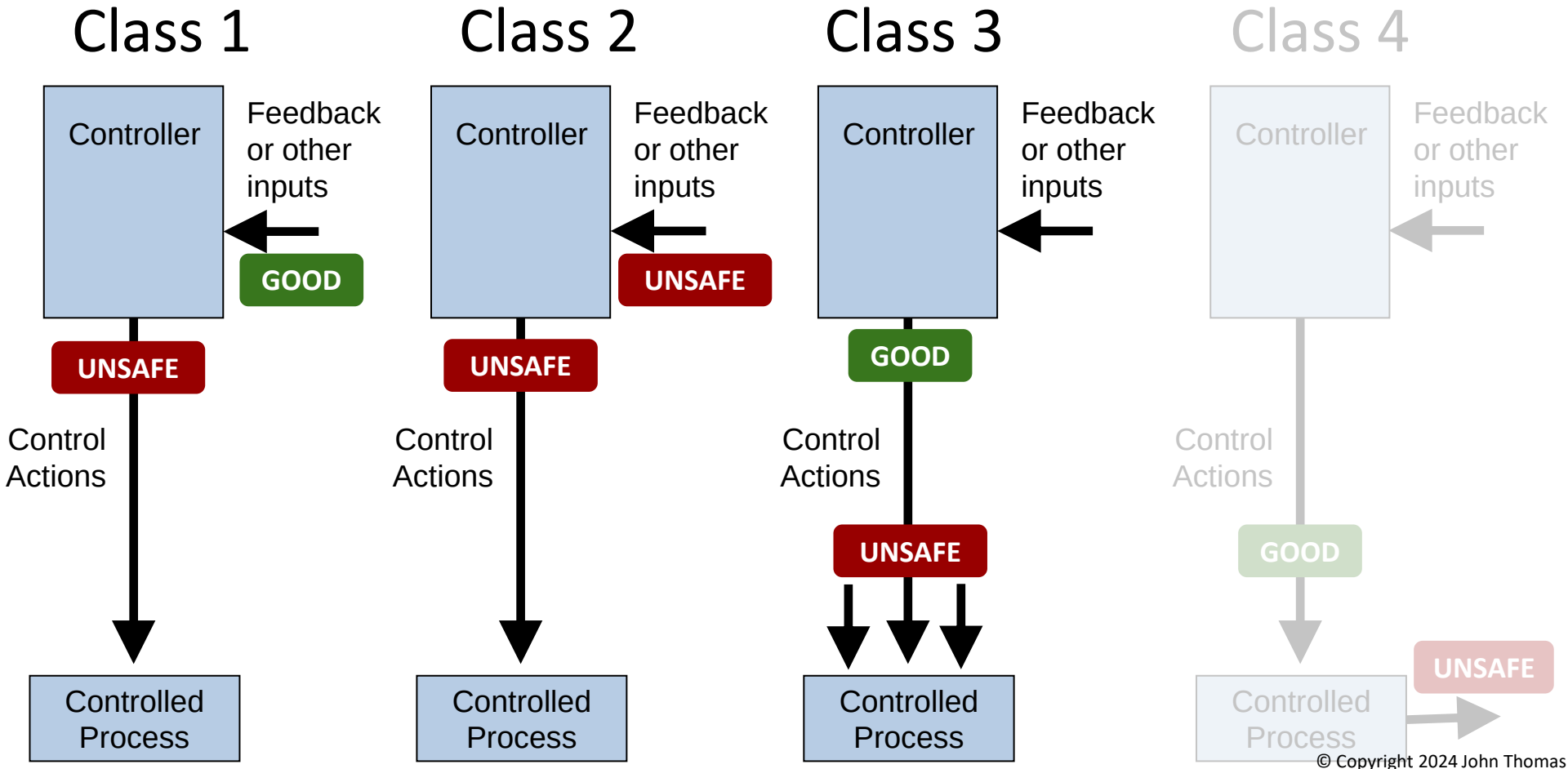
Refined Scenarios

Overloaded or too much info

If <Process> is overloaded, then there might not be any indication that <Context>

Discussion: These scenarios are used to help us think about mitigations. E.g., <Controller> currently has no feedback to indicate process overloading, so the design doesn't currently have any way to correct it.

Four Classes of Formal Scenarios



STPA Step 4: Class 3 Scenario Archetype

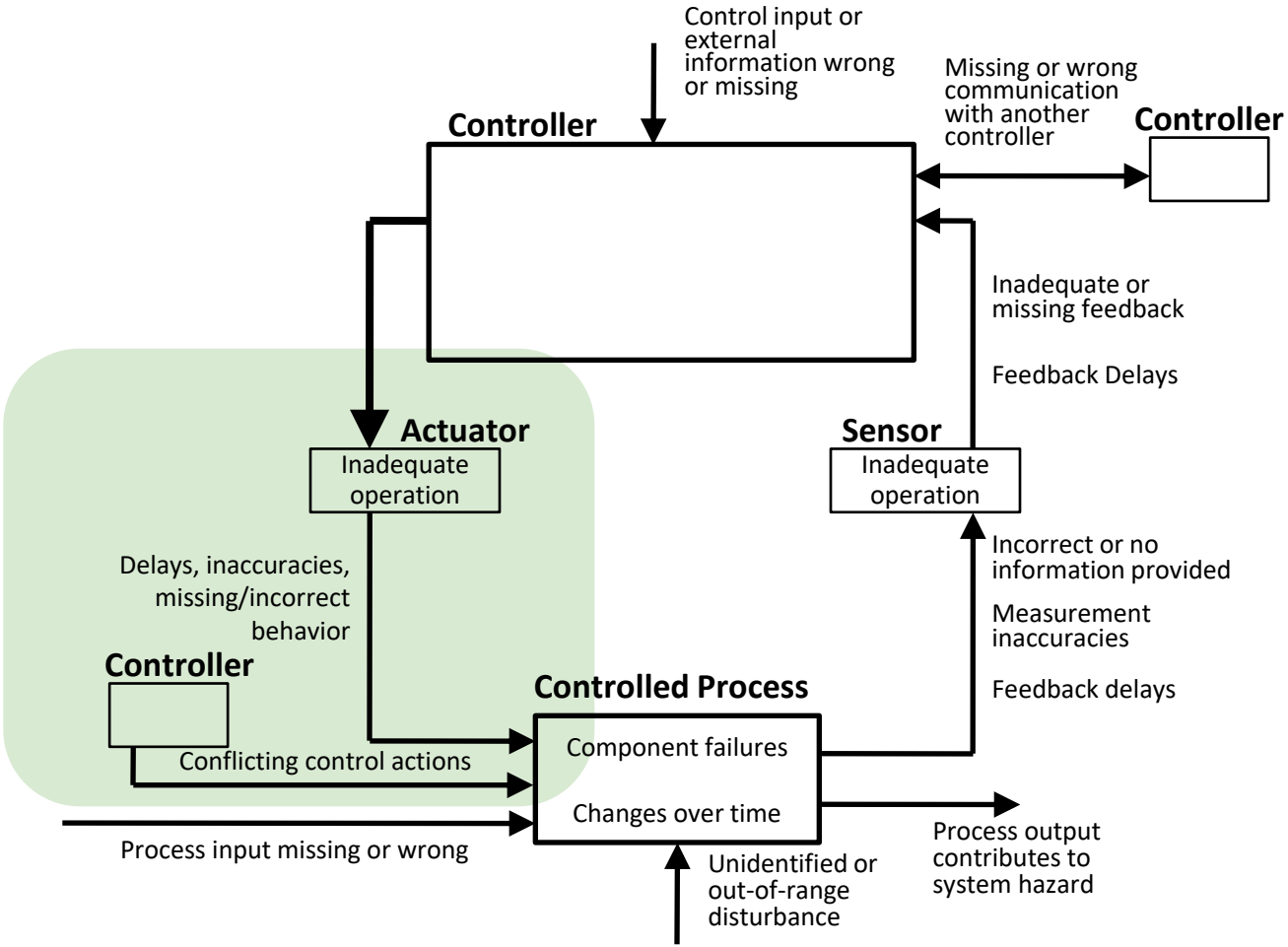
UCA-2:
<Controller> provides <Control Action> when <Context>

Class 3 Scenario Archetype: Inadequate Control Execution

We need to look at how the UCA can be emulated due to interactions in this region.

Constructing Scenario Archetype 3:

- Suppose the UCA did not happen (invert the UCA). The controller provided a "safe" control action.
- BUT… something happened on the control path making it as if the UCA had occured



STPA Step 4: Class 3 Scenario Archetype

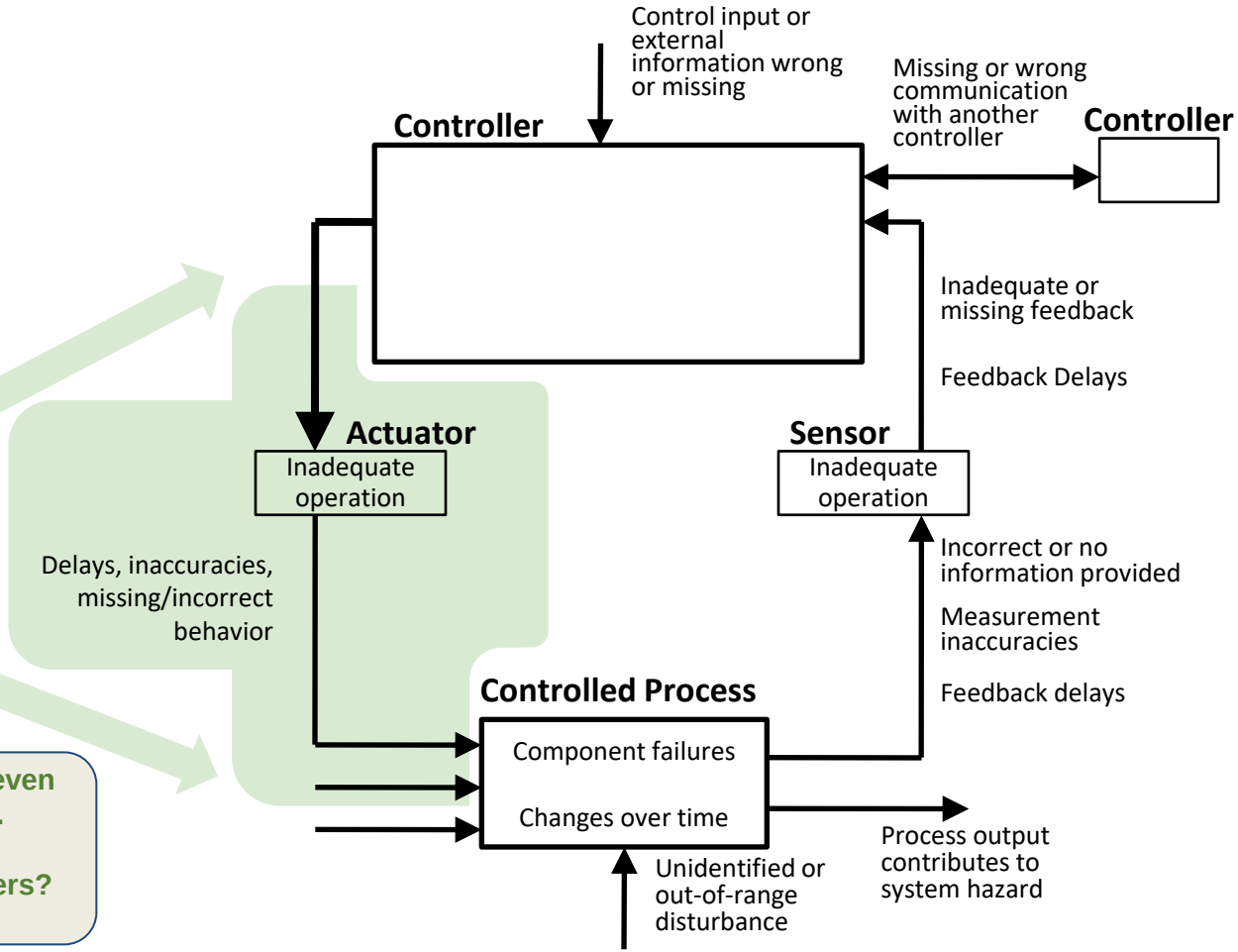
UCA-2:
<Controller> provides <Control Action> when <Context>

Class 3 Scenario Archetype:
Inadequate Control Execution

- <Controller> does not provide ____
- <Process> receives ____

This behavior would emulate the UCA, even if our controller does the right thing.

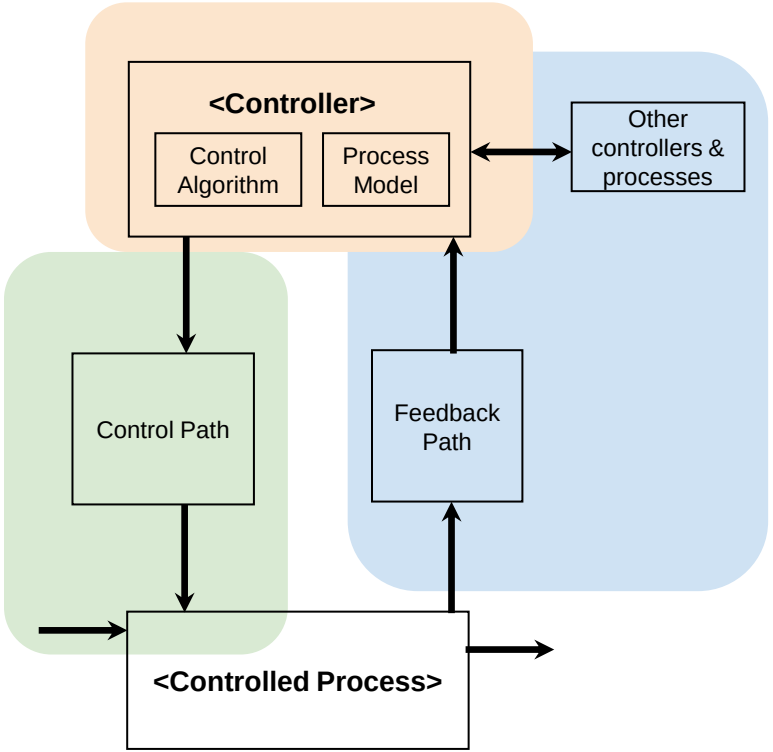
How could this happen? Other controllers? Spoofing? Other causes?



UCA-2:
<Controller> provides <Control Action>
when <Context>

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____



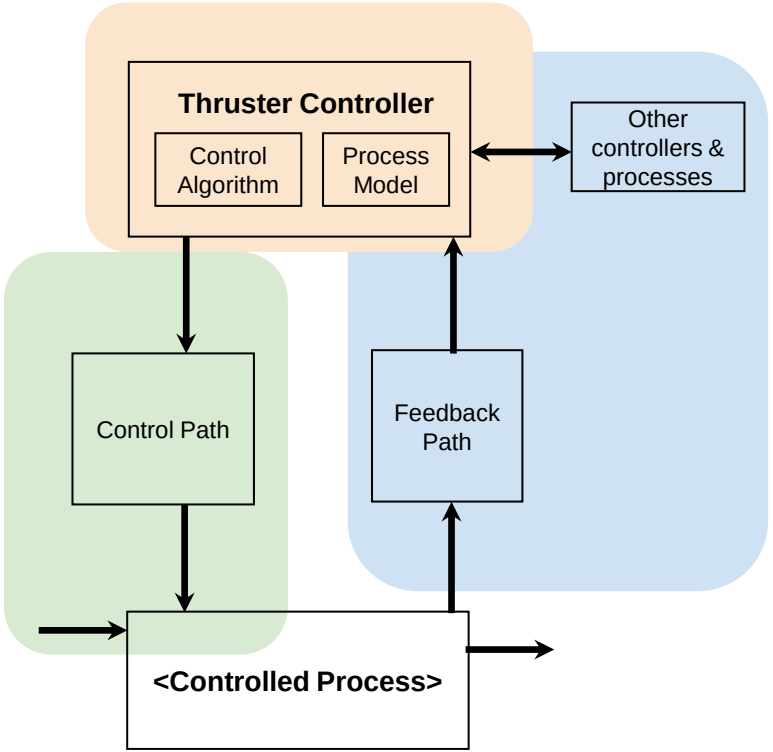
Class 2 Scenario Archetype:
Inadequate feedback/information
- <Feedback/Input> to <Controller> did not adequately indicate <Context>
- <Process> is actually <Context>

Class 3 Scenario Archetype:
Inadequate Control Execution
- <Controller> does not provide <Control Action> when <Context>
- <Process> receives a <Control Action> when <Context>

Example: Mars Polar Lander

UCA-2:
Thruster Controller
provides
Disable-Thruster Cmd
when spacecraft is in the air

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- Controller provides Disable-Thruster Cmd when spacecraft is in the air
- Touchdown Input to Controller correctly indicated it's in the air



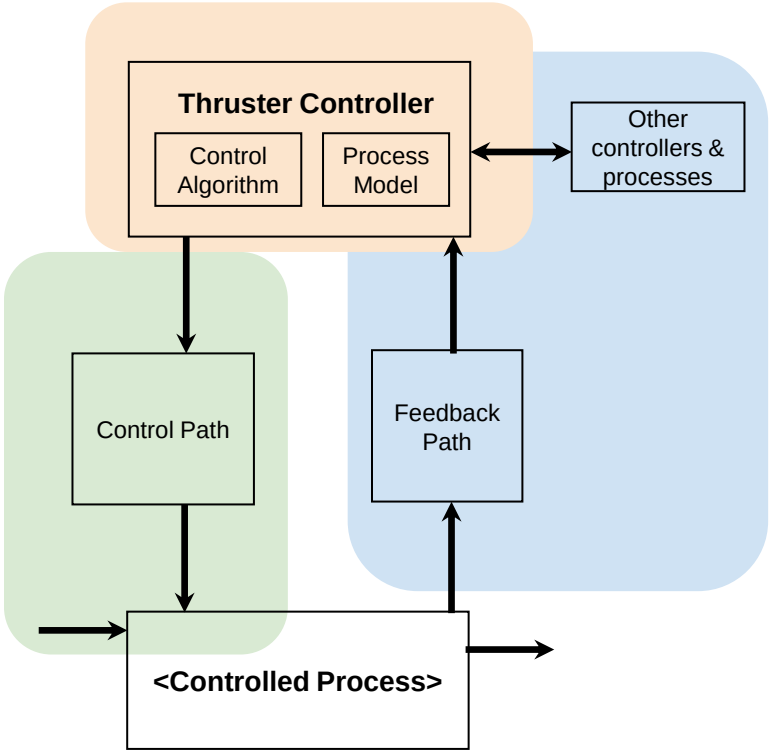
Class 2 Scenario Archetype:
Inadequate feedback/information
- Touchdown feedback does not indicate it's in air
- Lander is in the air

Class 3 Scenario Archetype:
Inadequate Control Execution
- <Controller> does not provide <Control Action> when <Context>
- <Process> receives a <Control Action> when <Context>

UCA-2:
Thruster Controller provides Disable-Thruster Cmd when spacecraft is in the air

Example: Mars Polar Lander

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- Controller provides Disable-Thruster Cmd when spacecraft is in the air
- Touchdown Input to Controller correctly indicated it's in the air



Class 2 Scenario Archetype:
Inadequate feedback/information
- Touchdown feedback does not indicate it's in air
- Lander is in the air

Class 3 Scenario Archetype:
Inadequate Control Execution
- Controller does not provide Disable-Thruster Cmd when spacecraft is in the air
- Lander receives Disable-Thruster Cmd when spacecraft is in the air

UCA-2:
<Controller> provides <Control Action> when <Context>

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:
Inadequate feedback/information
- <Feedback/Input> to <Controller> did not adequately indicate <Context>
- <Process> is actually <Context>

Class 3 Scenario Archetype:
Inadequate Control Execution
- <Controller> does not provide <Control Action> when <Context>
- <Process> receives a <Control Action> when <Context>

Class 4 Scenario Archetype:

Refined Scenarios

Ask: What can cause this Scenario Archetype?

UCA-2:
<Controller> provides <Control Action> when <Context>

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:
Inadequate feedback/information
- <Feedback/Input> to <Controller> did not adequately indicate <Context>
- <Process> is actually <Context>

Class 3 Scenario Archetype:
Inadequate Control Execution
- <Controller> does not provide <Control Action> when <Context>
- <Process> receives a <Control Action> when <Context>

Class 4 Scenario Archetype:

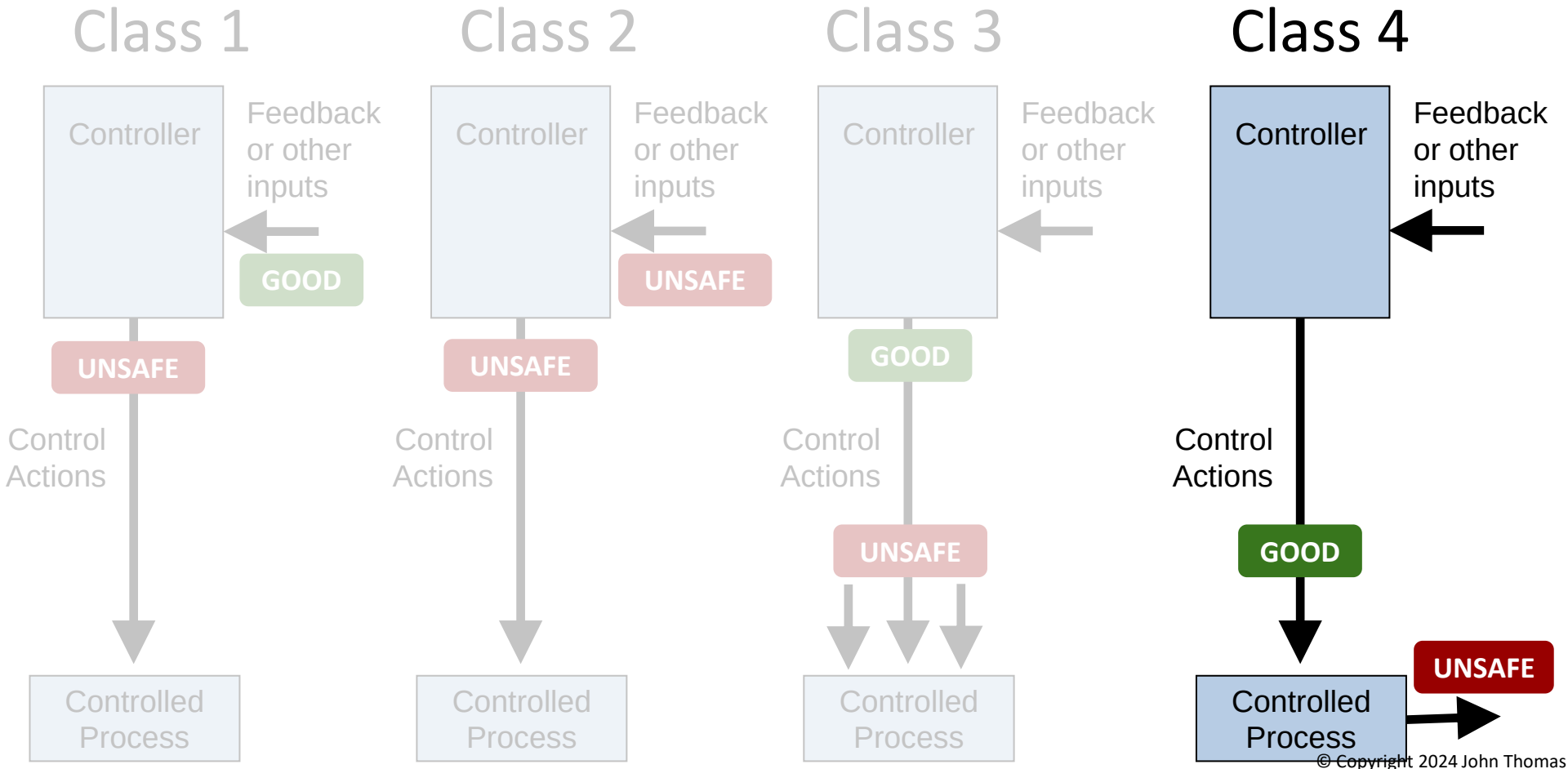
Refined Scenarios

Why?

- Some other <Controller> could generate <Control Action> and send it to ___
- <Controller> sends <Control Action> with Ignore bit set, but _____.
- Etc.

Discussion: How would <Controlled Process> know to ignore this? It might not know.

Four Classes of Formal Scenarios



STPA Step 4: Class 4 Scenario Archetype

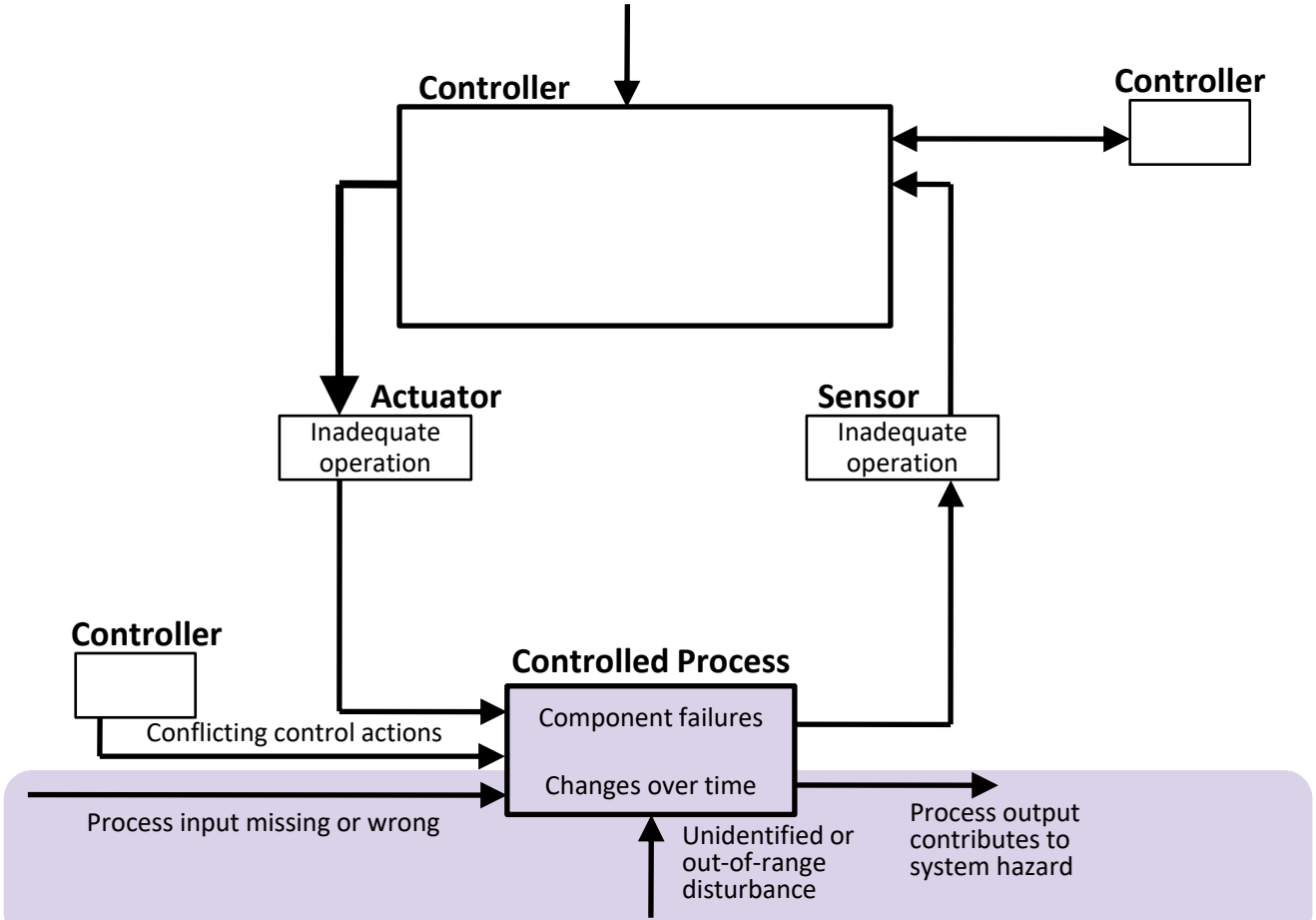
UCA-2:
<Controller> provides <Control Action> when <Context>

Class 4 Scenario Archetype: Inadequate Process Behavior

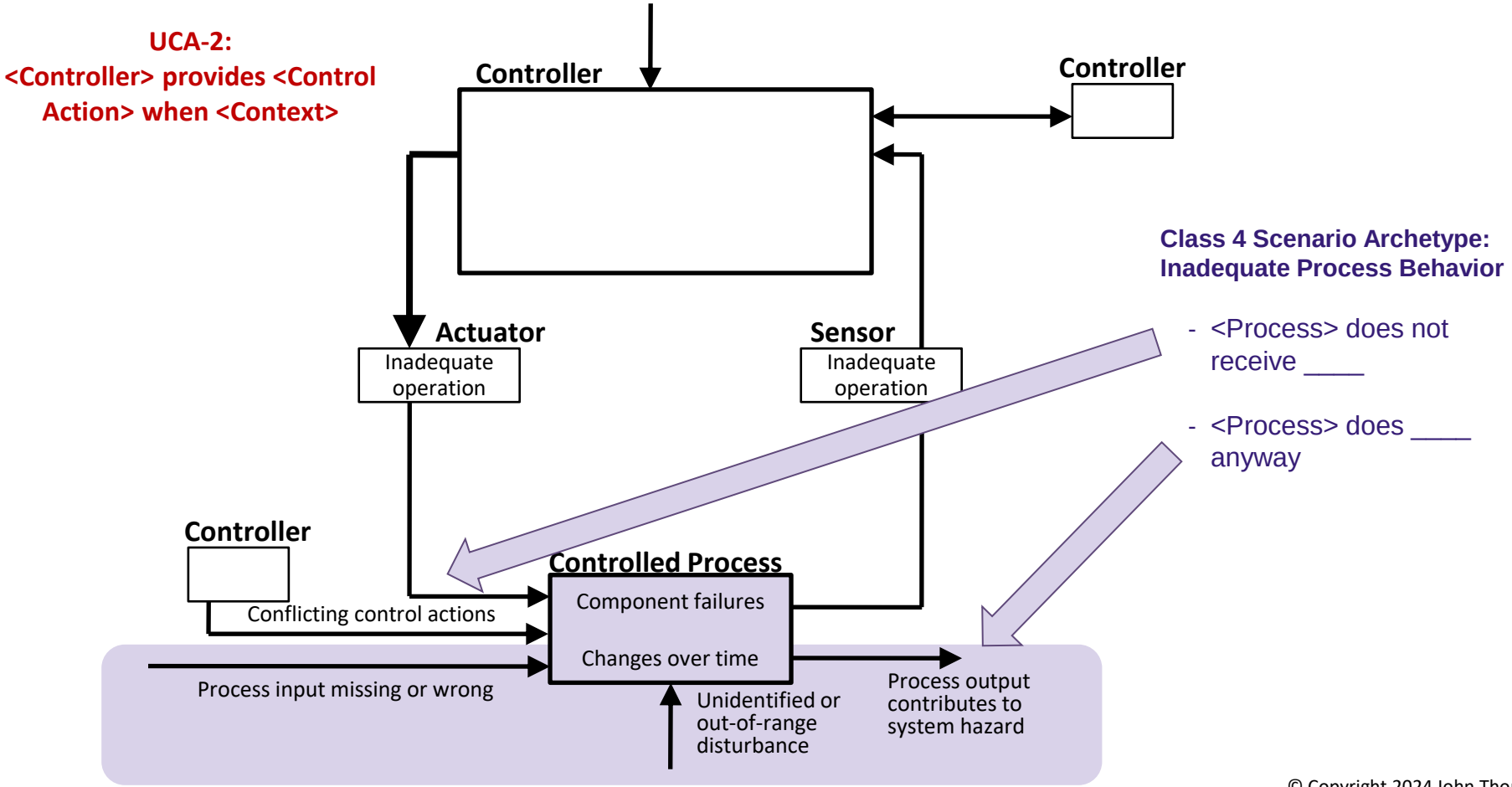
We need to look at how the UCA can be emulated due to interactions in this region.

Constructing Scenario Archetype 4:

- Suppose the UCA did not happen (invert the UCA), and was not received by the controlled process.
- BUT… something happened with the controlled process and its other interactions making it as if the UCA had been provided.



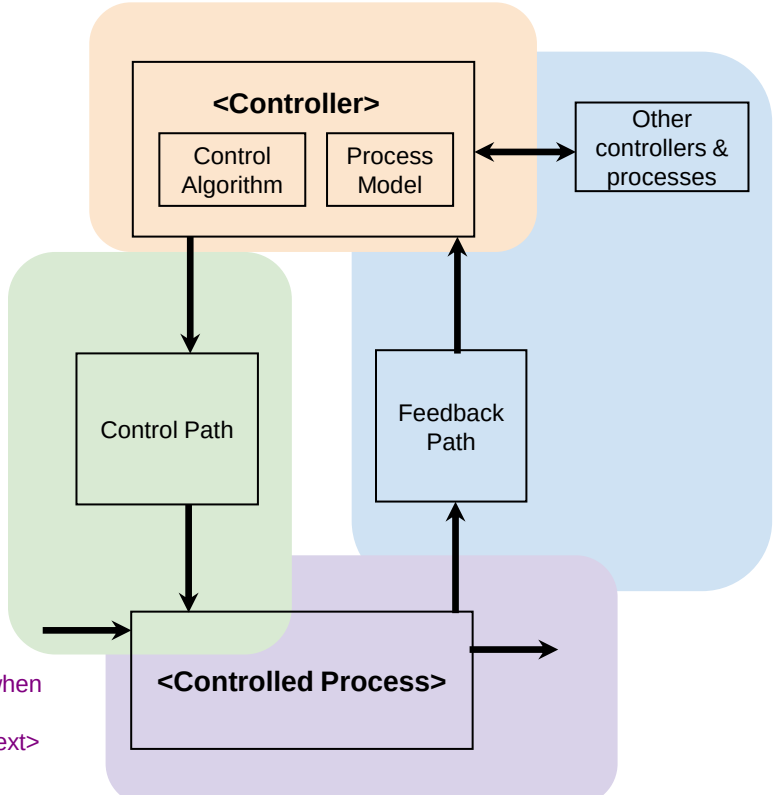
STPA Step 4: Class 4 Scenario Archetype



UCA-2:
<Controller> provides <Control Action>
when <Context>

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____



Class 2 Scenario Archetype:
Inadequate feedback/information
- <Feedback/Input> to <Controller> did not adequately indicate <Context>
- <Process> is actually <Context>

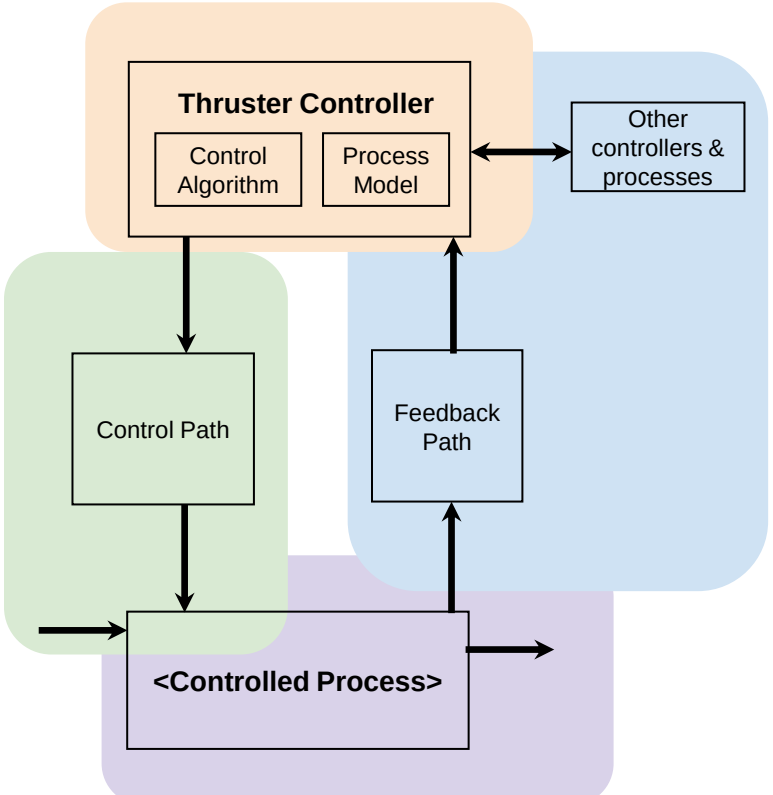
Class 3 Scenario Archetype:
Inadequate Control Execution
- <Controller> does not provide <Control Action> when <Context>
- <Process> receives a <Control Action> when <Context>

Class 4 Scenario Archetype:
Inadequate process behavior
- <Process> does not receive a <Control Action> when <Context>
- <Process> applies <Control Action> when <Context>

UCA-2:
Thruster Controller provides Disable-Thruster Cmd when spacecraft is in the air

Example: Mars Polar Lander

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- Controller provides Disable-Thruster Cmd when spacecraft is in the air
- Touchdown Input to Controller correctly indicated it's in the air



Class 2 Scenario Archetype:
Inadequate feedback/information
- Touchdown feedback does not indicate it's in air
- Lander is in the air

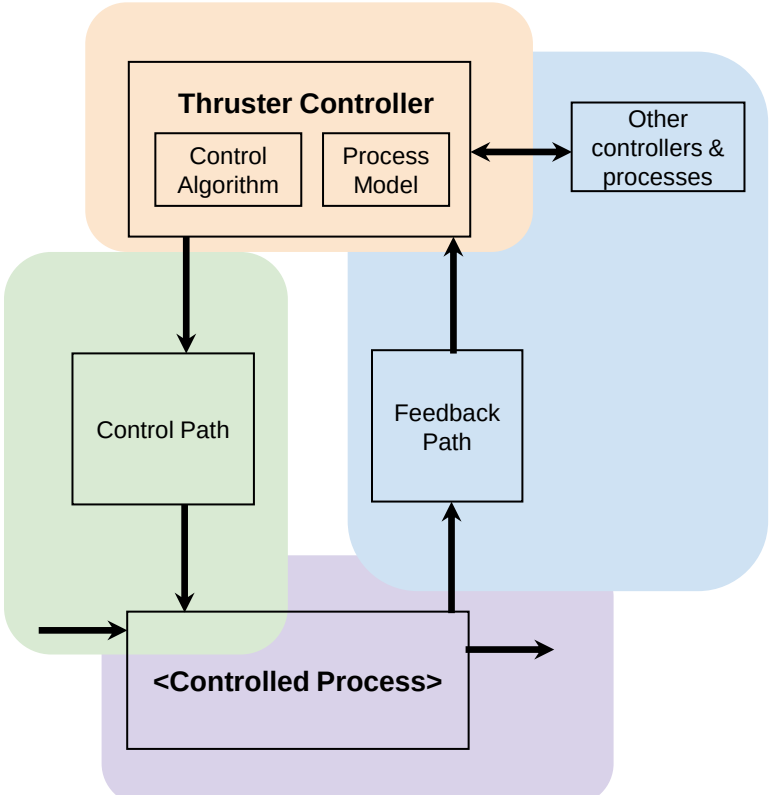
Class 3 Scenario Archetype:
Inadequate Control Execution
- Controller does not provide Disable-Thruster Cmd when spacecraft is in the air
- Lander receives Disable-Thruster Cmd when spacecraft is in the air

Class 4 Scenario Archetype:
Inadequate process behavior
- <Process> does not receive a <Control Action> when <Context>
- <Process> applies <Control Action> when <Context>

UCA-2:
Thruster Controller provides Disable-Thruster Cmd when spacecraft is in the air

Example: Mars Polar Lander

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- Controller provides Disable-Thruster Cmd when spacecraft is in the air
- Touchdown Input to Controller correctly indicated it's in the air



Class 2 Scenario Archetype:
Inadequate feedback/information
- Touchdown feedback does not indicate it's in air
- Lander is in the air

Class 3 Scenario Archetype:
Inadequate Control Execution
- Controller does not provide Disable-Thruster Cmd when spacecraft is in the air
- Lander receives Disable-Thruster Cmd when spacecraft is in the air

Class 4 Scenario Archetype:
Inadequate process behavior
- Thrusters do not receive Disable command (when spacecraft is in the air)
- Thrusters are disabled (when in the air)

UCA-2:
<Controller> provides <Control Action> when <Context>

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:
Inadequate feedback/information
- <Feedback/Input> to <Controller> did not adequately indicate <Context>
- <Process> is actually <Context>

Class 3 Scenario Archetype:
Inadequate Control Execution
- <Controller> does not provide <Control Action> when <Context>
- <Process> receives a <Control Action> when <Context>

Class 4 Scenario Archetype:
Inadequate process behavior
- <Process> does not receive a <Control Action> when <Context>
- <Process> applies <Control Action> when <Context>

Refined Scenarios

Ask: What can cause this Scenario Archetype?

UCA-2:
<Controller> provides <Control Action> when <Context>

Scenario Archetypes

Class 1 Scenario Archetype:
Inadequate Controller Behavior
- <Controller> provides _____ when _____
- <Input> to <Controller> correctly indicated _____

Class 2 Scenario Archetype:
Inadequate feedback/information
- <Feedback/Input> to <Controller> did not adequately indicate <Context>
- <Process> is actually <Context>

Class 3 Scenario Archetype:
Inadequate Control Execution
- <Controller> does not provide <Control Action> when <Context>
- <Process> receives a <Control Action> when <Context>

Class 4 Scenario Archetype:
Inadequate process behavior
- <Process> does not receive a <Control Action> when <Context>
- <Process> applies <Control Action> when <Context>

Refined Scenarios

Why?

- <Process> may mechanically ___
- <Process> may run out of ___
- <Process> may see that ___ is full, in which case <Process> will automatically ____, which results in ____.
- If <Process> is in ___ mode, then all ___ will be ignored.

Scenario Archetype Generation

	Not providing causes hazard	Providing causes hazard	Too early, too late, Order	Stopped Too Soon / Applied too long
Control Action	UCA-1	UCA-2	UCA-3	UCA-4

Scenario Archetype Table:

	UCA type 1: not providing causes hazard (UCA-#)	UCA type 2: providing causes hazard (UCA-#)	UCA type 3: too early, too late, out of order causes hazard (UCA-#)	UCA type 4: stopped too soon, applied too long causes hazard (UCA-#)
Scenario Class 1: Unsafe Controller Behavior	1)<controller> doesn't provide <cmd> 2)<controller> received feedback (or other inputs) that indicated <context>	1)<controller> provides <cmd> 2)<controller> received feedback (or other inputs) that indicated <context>	1)<controller> provides <cmd> too late/early/out of order 2)<controller> received feedback (or other inputs) that indicated <context> on time / in order	1)<controller> stops/continues providing <cmd> too soon/long 2)<controller> received feedback (or other inputs) that indicated <context> on time
Scenario Class 2: Unsafe Feedback Path	1)feedback (or other inputs) received by <controller> does not adequately indicate <context> 2)<context> is true	1)feedback (or other inputs) received by <controller> does not adequately indicate <context> 2)<context> is true	1)feedback (or other inputs) received by <controller> does not indicate <context> (too late/early/out of order) 2)<context> is true	1)feedback (or other inputs) received by <controller> does not indicate <context> (inappropriate duration) 2)<context> is true
Scenario Class 3: Unsafe Control Path	1)<controller> does provide <cmd> when <context> 2)<cmd> is not received by <controlled process> when <context>	1)<controller> does not provide <cmd> when <context> 2)<controlled process> receives <cmd> when <context>	1)<controller> does not provide <cmd> <context> (not too late/early/out of order) 2)<cmd> is received by <controlled process> <context> (too late/early/out of order)	1)<controller> provides <cmd> with appropriate duration 2)<cmd> is received by <controlled process> with <context> (inappropriate duration)
Scenario Class 4: Unsafe Controlled Process Behavior	1)<cmd> is received by <controlled process> when <context> 2)<controlled process> does not respond by <…>	1)<cmd> is not received by <controlled process> when <context> 2)<controlled process> responds by <…>	1)<cmd> is not received by <controlled process> <context> (not too late/early/out of order) 2)<controlled process> responds by <…> <context> (too late/early/out of order)	1)<cmd> is received by <controlled process> with appropriate duration 2)<controlled process> does not respond by <…> with <context> (inappropriate duration)

(Thomas, 2016), (Thomas, 2017), (Cabosky, 2020)

STPA Scenarios should cover:

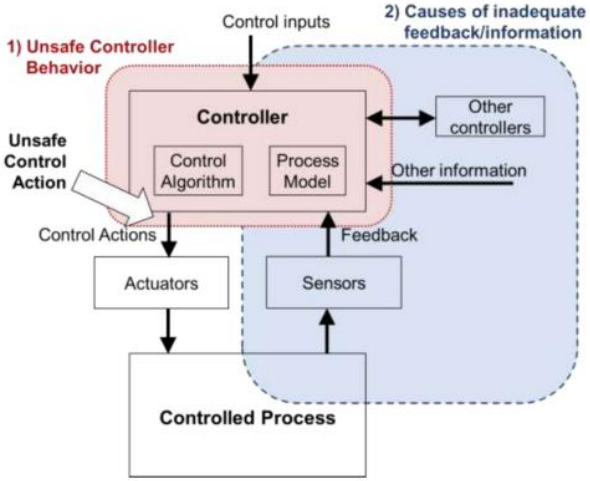


Figure 2.18: Unsafe Control Actions can be caused by (1) unsafe controller behavior and (2) inadequate feedback and other inputs

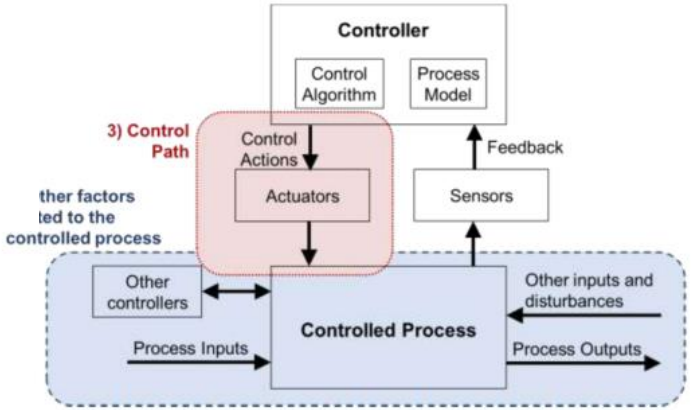
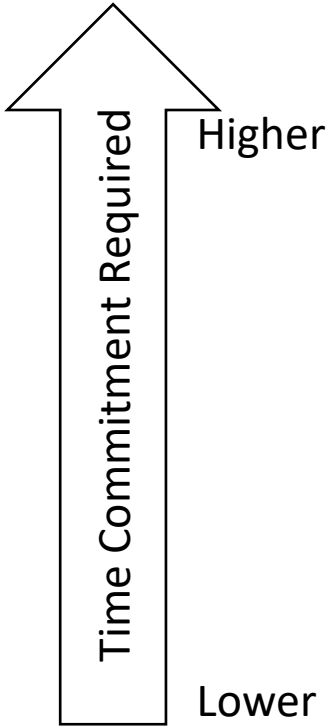


Figure 2.19: Generic control loop illustrating 1) the control path and 2) other factors that can affect the controlled process

How to run an STPA project

Let’s discuss who would do this and how they would coordinate with others

STPA Project Participants



STPA Core Team

STPA Practitioners

STPA Facilitator

STPA Practitioners
- Perform majority of STPA work
- Interdisciplinary team
- Should have STPA training and certification, but may not be experts

STPA Facilitator
- The STPA expert
- Provide STPA method guidance (and other responsibilities)

Other SMEs

- Provide specialized domain knowledge as needed by team
- May have little or no STPA familiarity
- May not be actively involved in STPA, but must be accessible by team