STPA Tutorial Exercise
Aerial Refueling

John Thomas

Engineering Systems Lab

MIT

Please contact JThomas4@MIT.EDU with any questions!

Tutorial Objective

- These short tutorials are **not training classes**
- We cannot cover everything in these tutorial sessions. The objective is just to introduce some of the core concepts and help new attendees follow the workshop presentations.
- Like most techniques, training and practice with a qualified instructor are needed to become proficient.

Acknowledgements!

- Ben Luther
- Ryan Krogstad
- Martin Trae Span

Aerial Refueling Exercise

- Inspired by KC-10, KC-30, and others
- Not an analysis of one specific implementation
- We've made changes and simplifications due to time constraints!

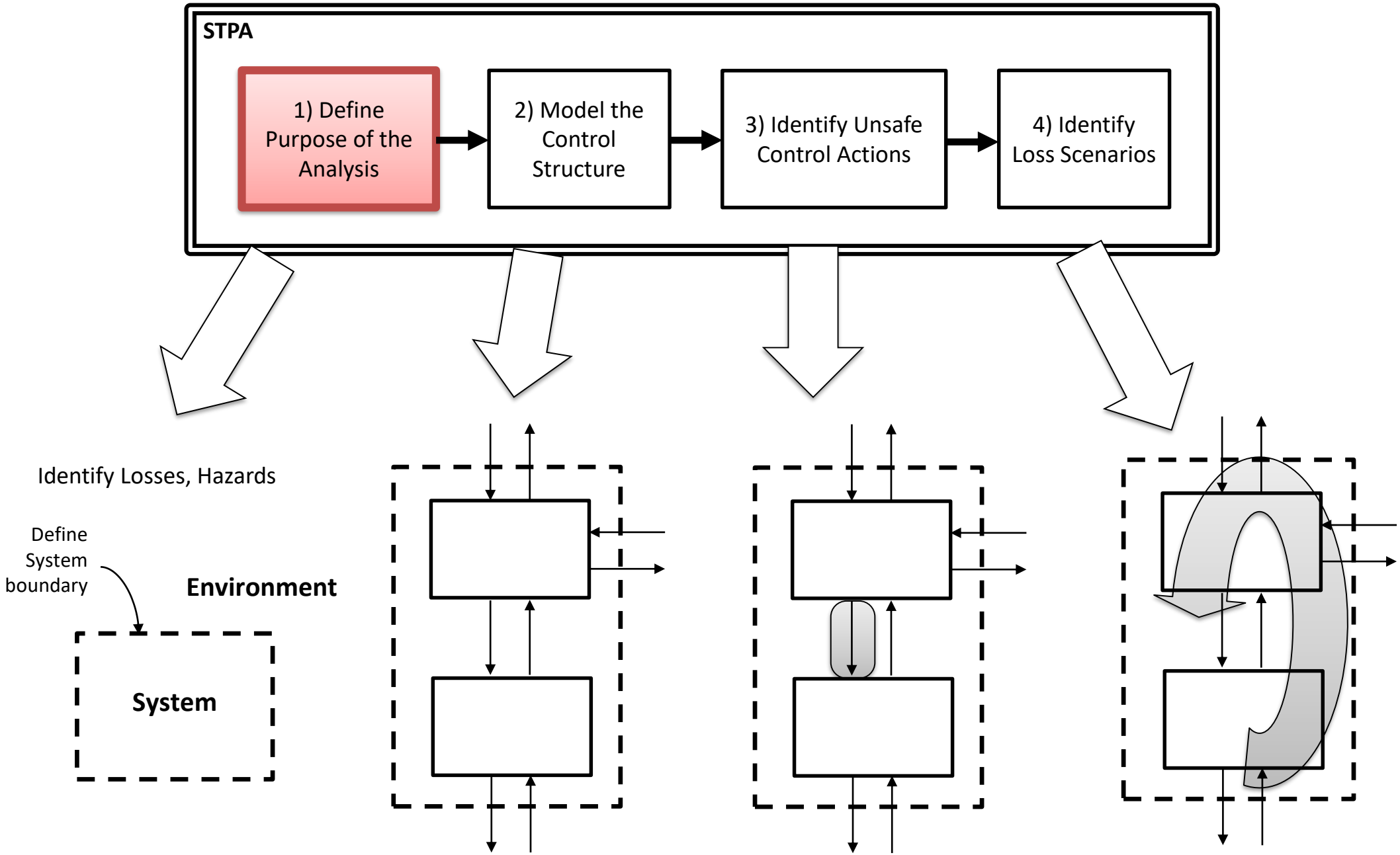
Based on the Airbus A330 airliner, a KC-30 refuels a F-16

Flying a boom is like flying a glider behind tanker.
You have full control authority: up, down, left, right, extend, retract.
Max extension to 23ft (7.6m), ~10° left/right, ~15° up/down

Boom designed to mechanically disconnect from receiver at 5 tons tension

Image: https://thaimilitaryandasianregion.wordpress.com/2016/02/

KC-30 refueling a B-1 Lancer



(Leveson and Thomas, 2018)

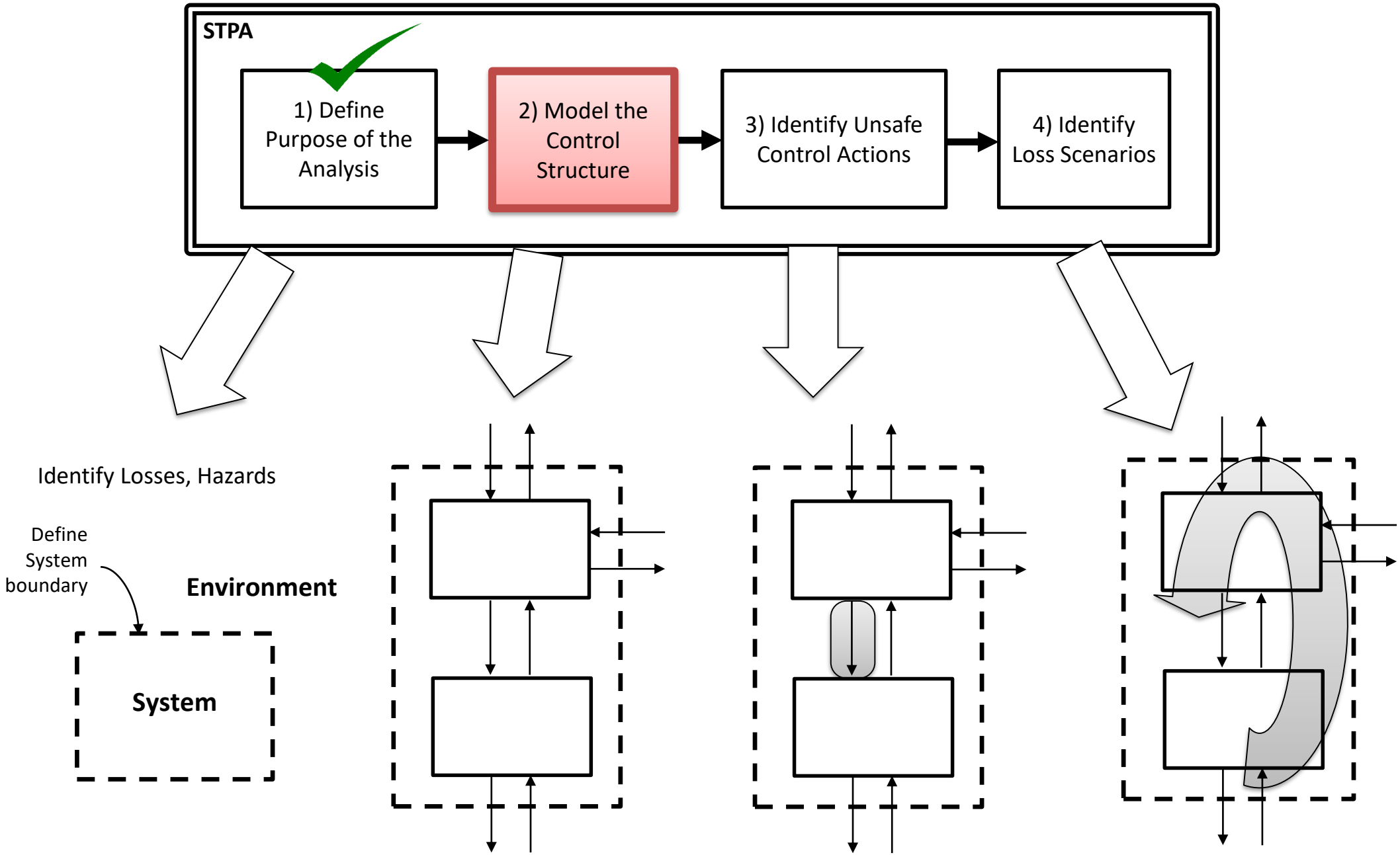
STPA Step 1: Define Purpose of the Analysis

- What are some Losses?
- What are some Aircraft-level Hazards?

Go to http://slido.com (event code is “STPA2”)

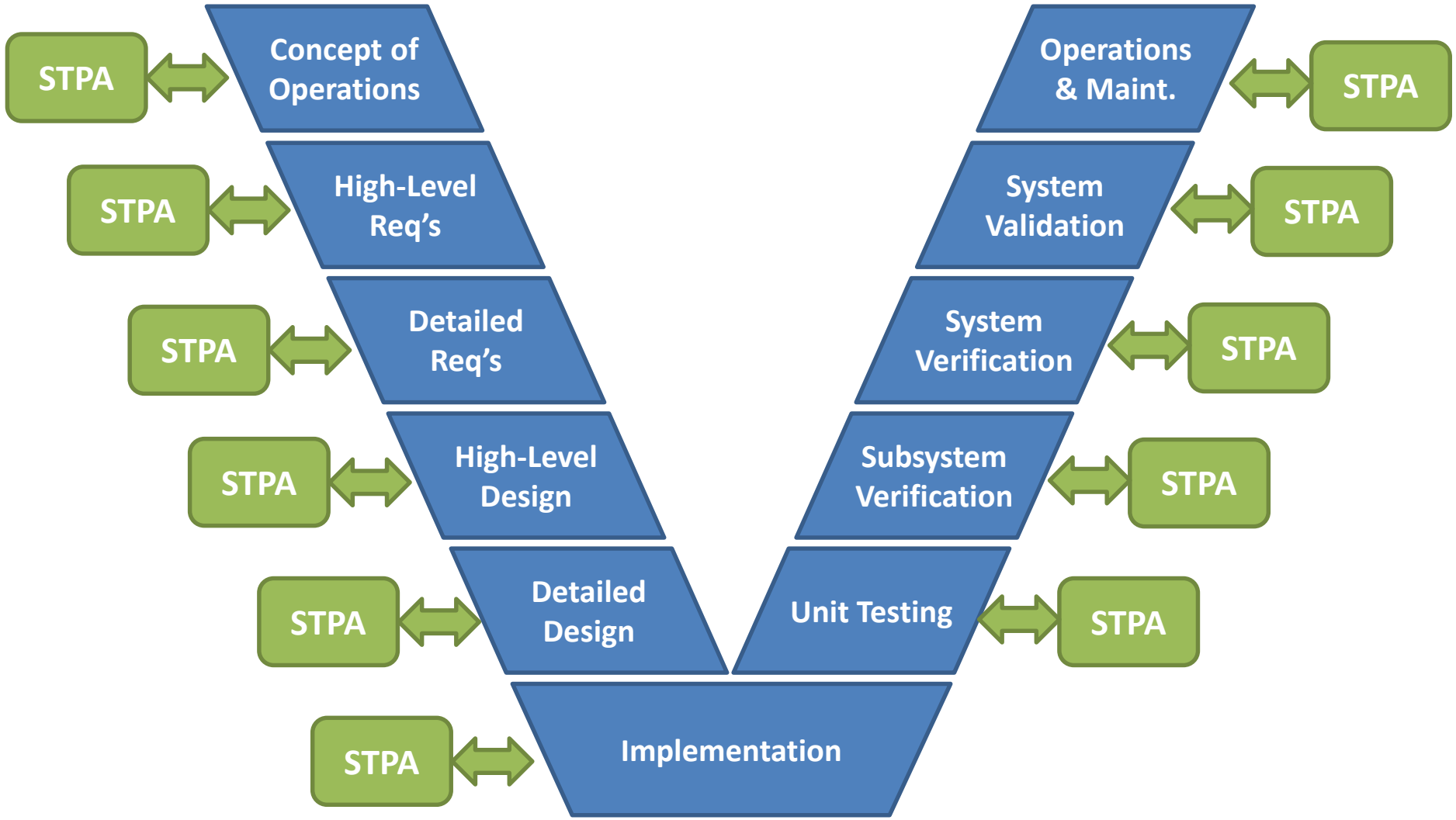
STPA Step 1: Define Purpose of the Analysis

- What are some Losses?
  - L1: Loss of life or injury
  - L2: Damage to aircraft
  - L3: Loss of refueling mission
- What are some Aircraft-level Hazards?
  - H1: **Aircraft** violate minimum separation for refueling [L1,2,3]
  - H2: **Aircraft** airframe integrity is degraded [L1,2,3]
  - […]



(Leveson and Thomas, 2018)

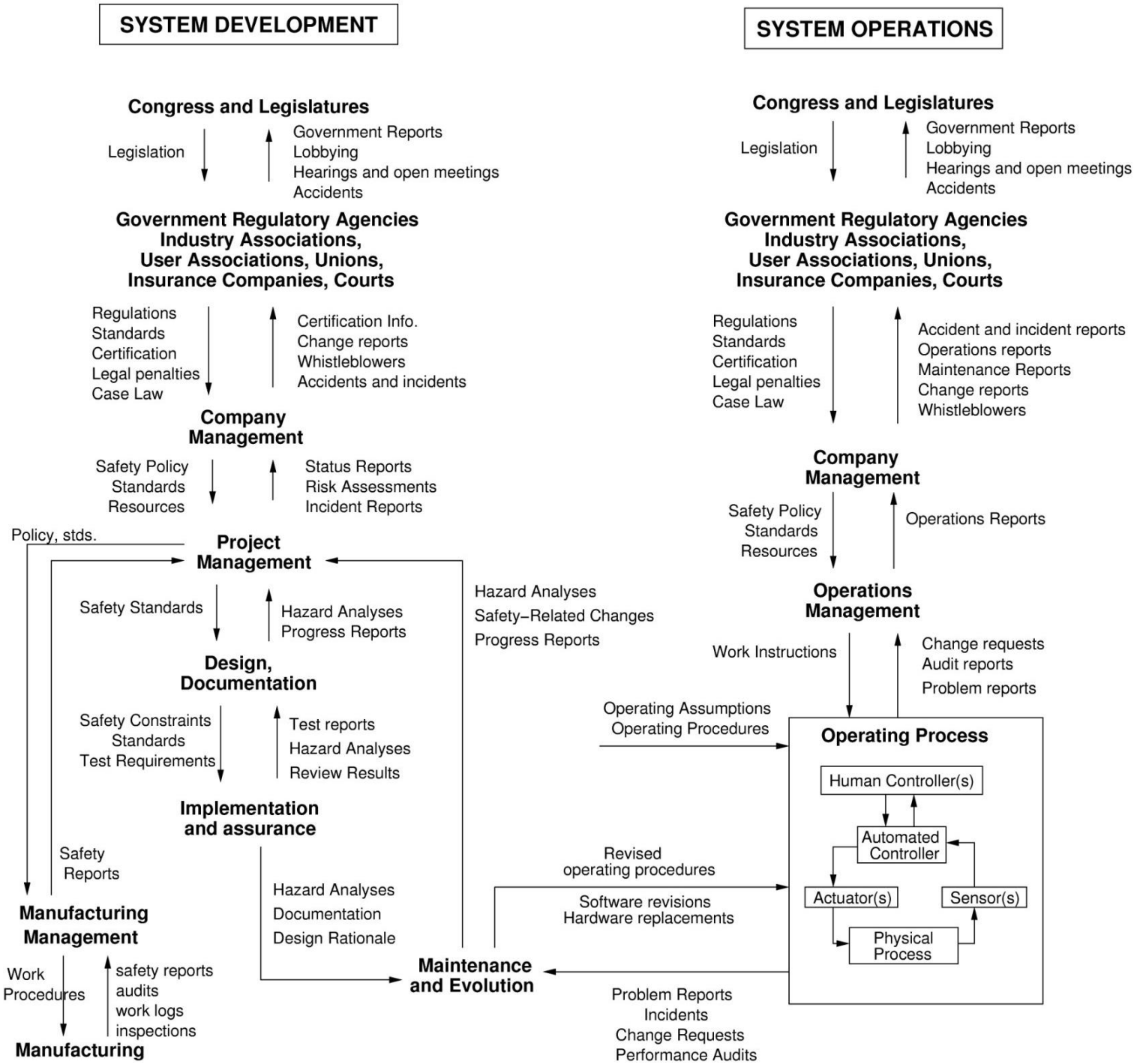
Famous Systems Engineering V-Model



STPA is iterated to support development!

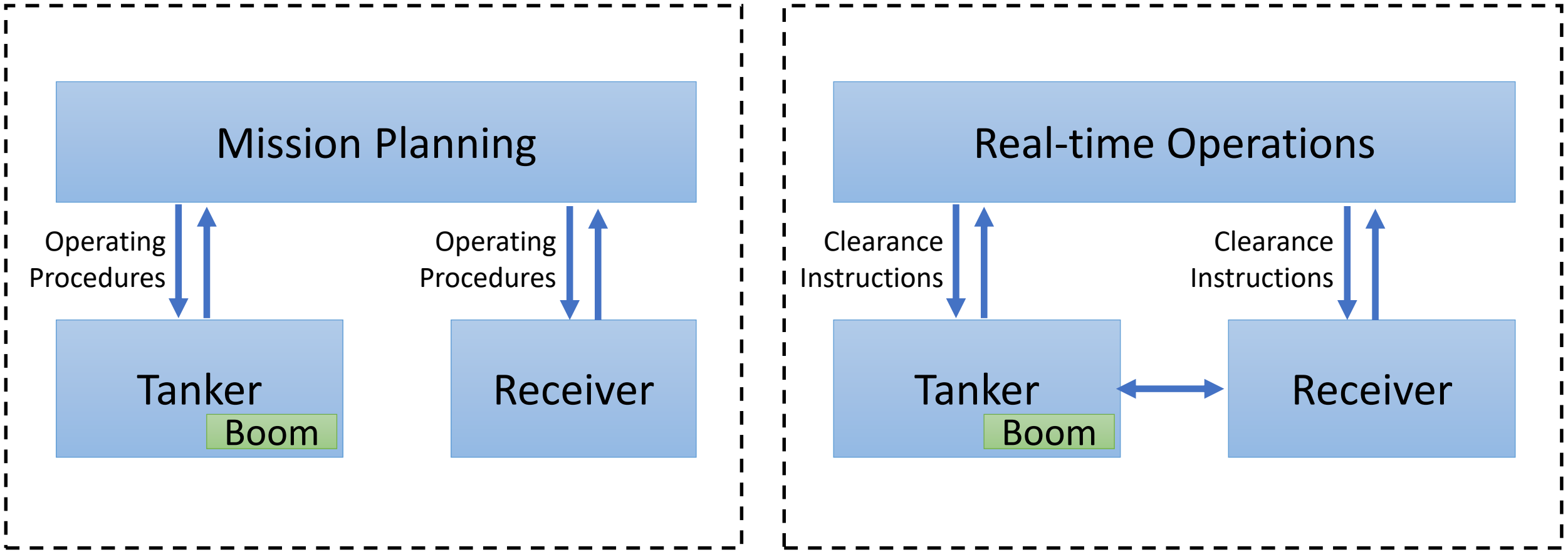
Please contact JThomas4@MIT.EDU with any questions!

Example Safety Control Structure



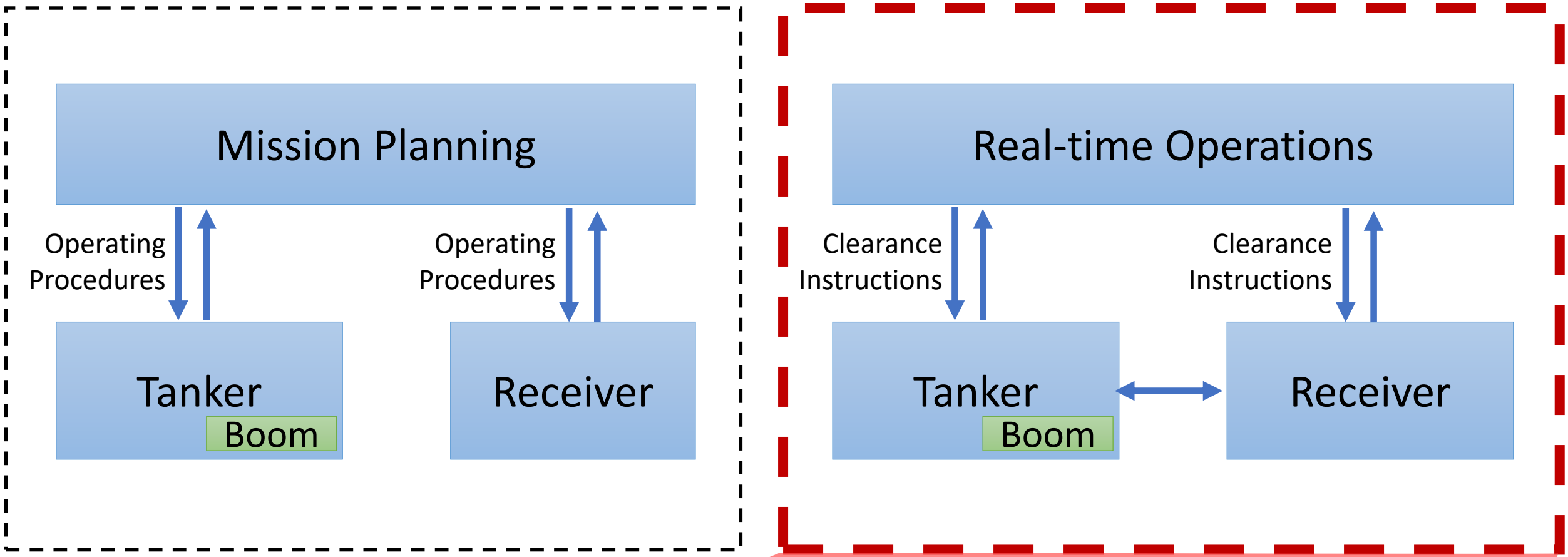
(Leveson, 2012)

Iterative Control Structure Development

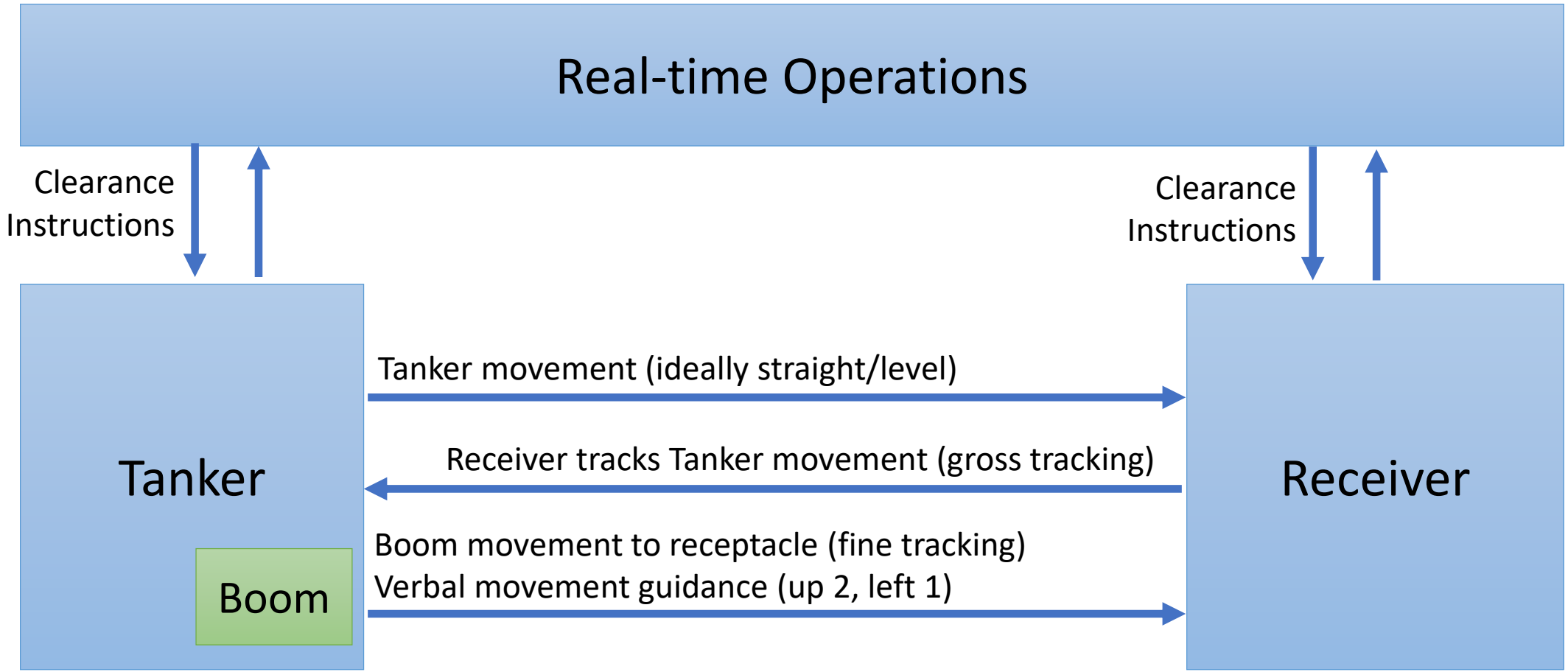


Please contact JThomas4@MIT.EDU with any questions!

Iterative Control Structure Development

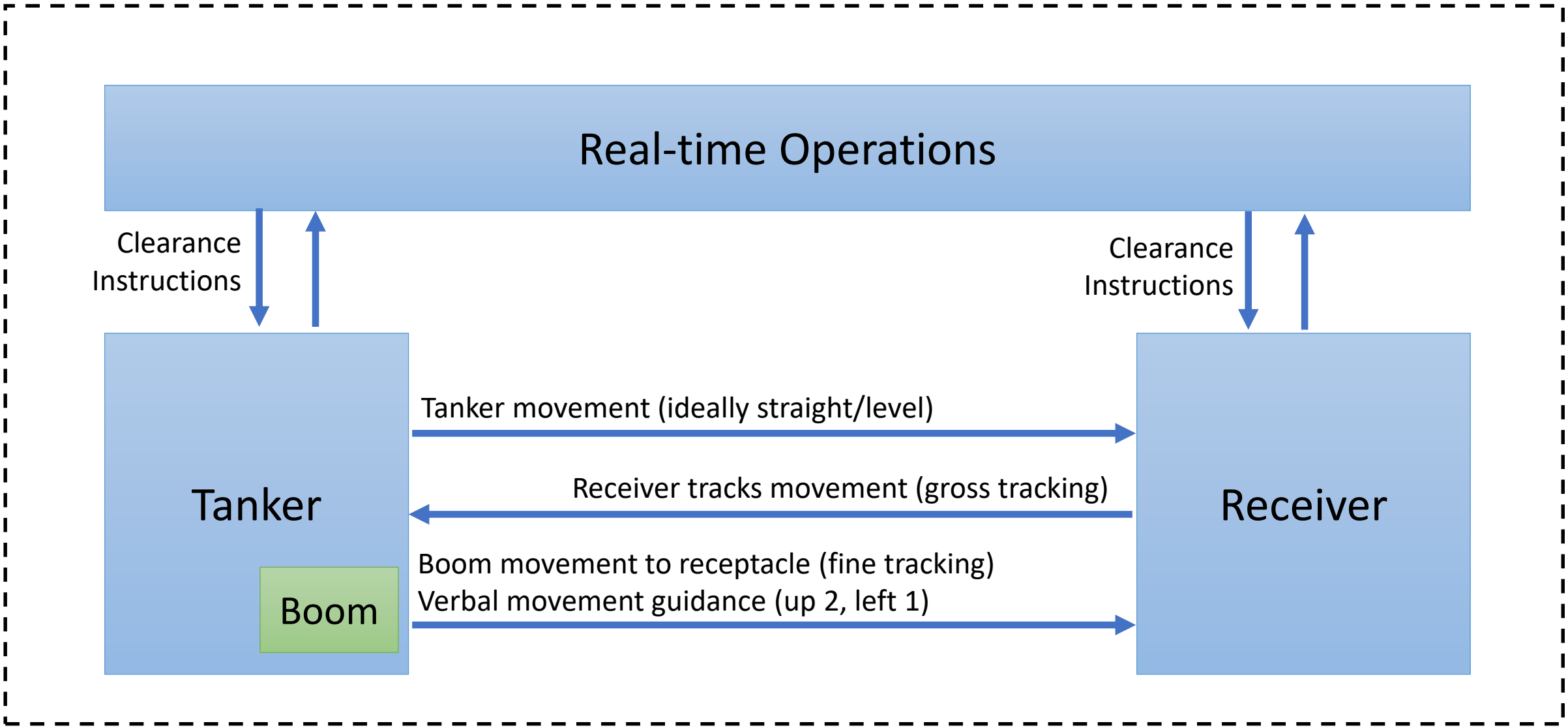


Iterative Control Structure Development



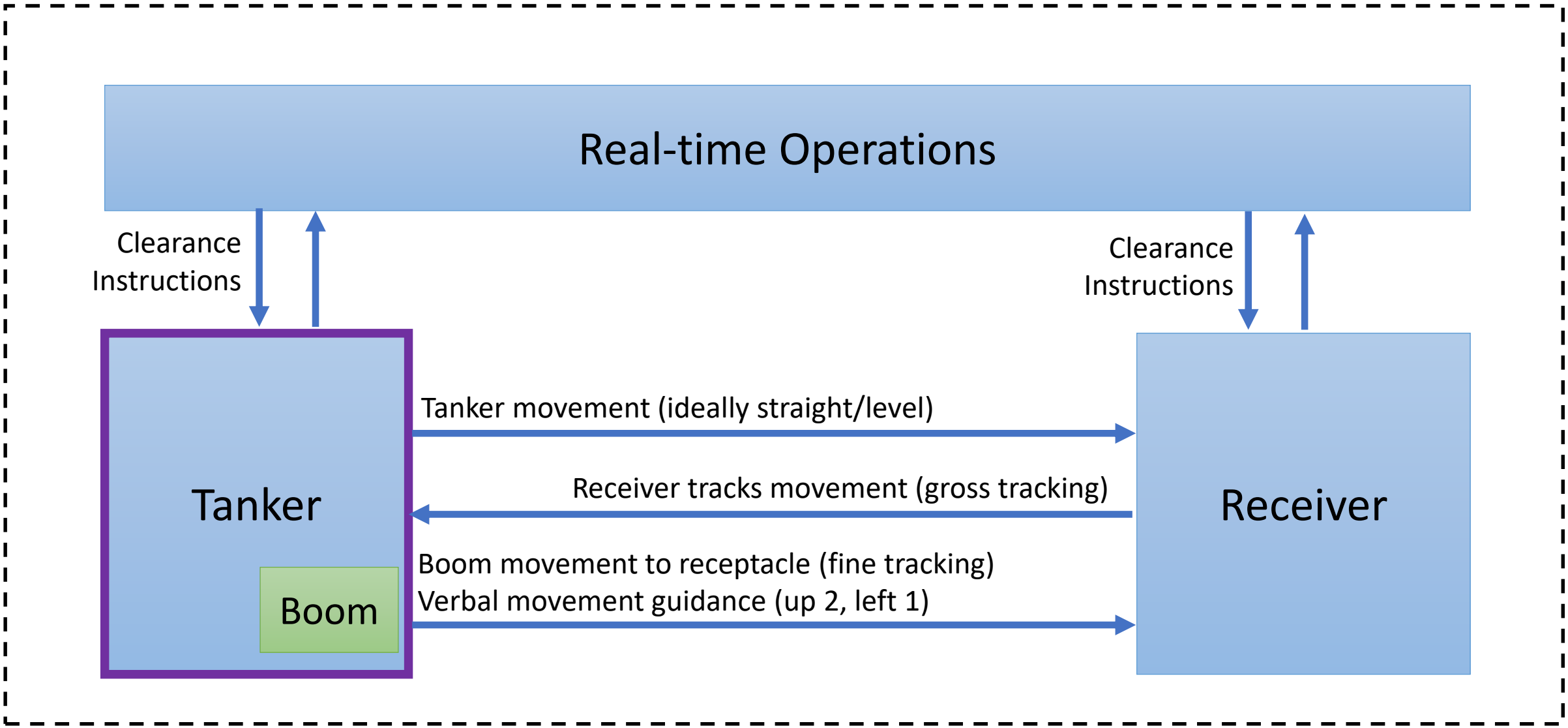
Please contact JThomas4@MIT.EDU with any questions!

Iterative Control Structure Development



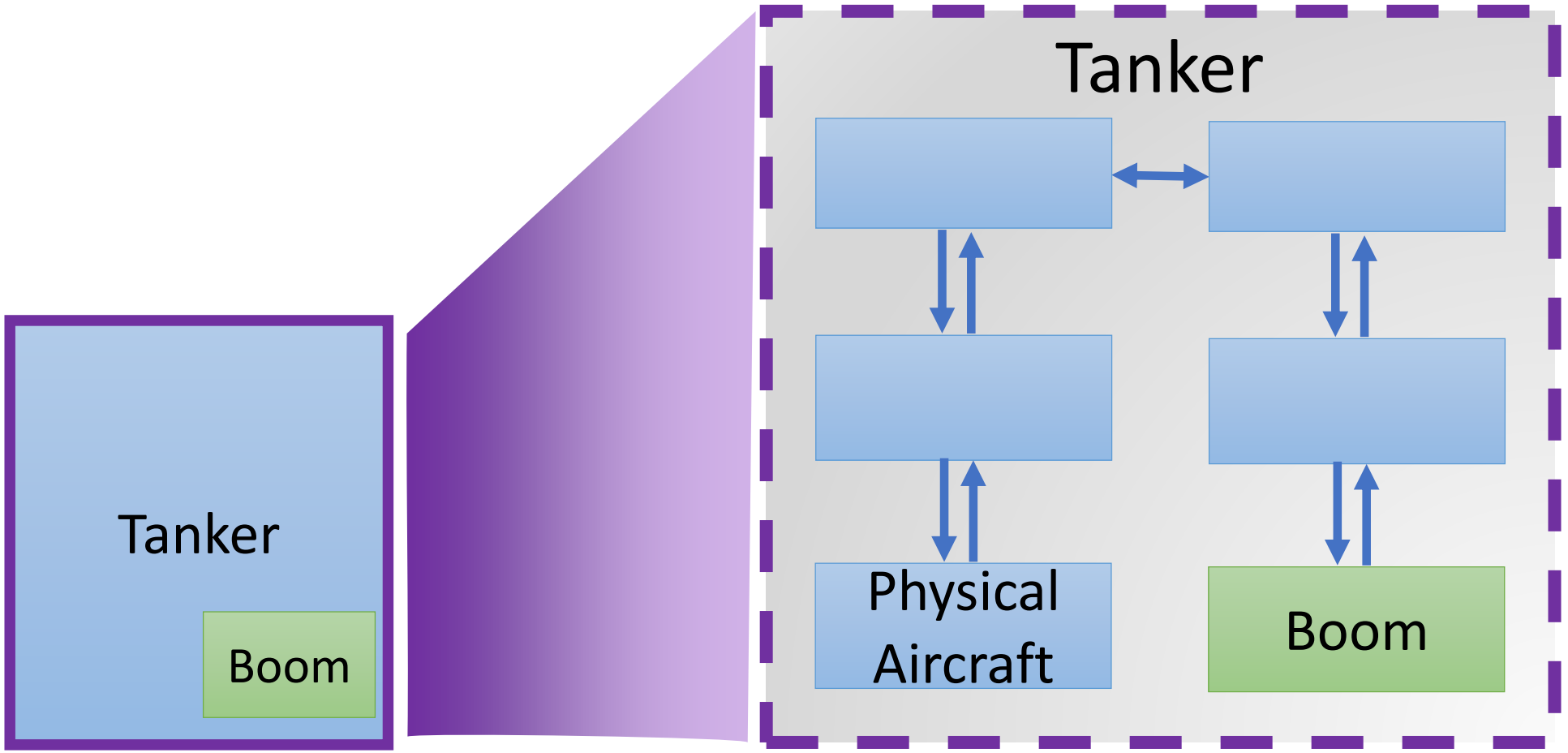
Please contact JThomas4@MIT.EDU with any questions!

Iterative Control Structure Development



Please contact JThomas4@MIT.EDU with any questions!

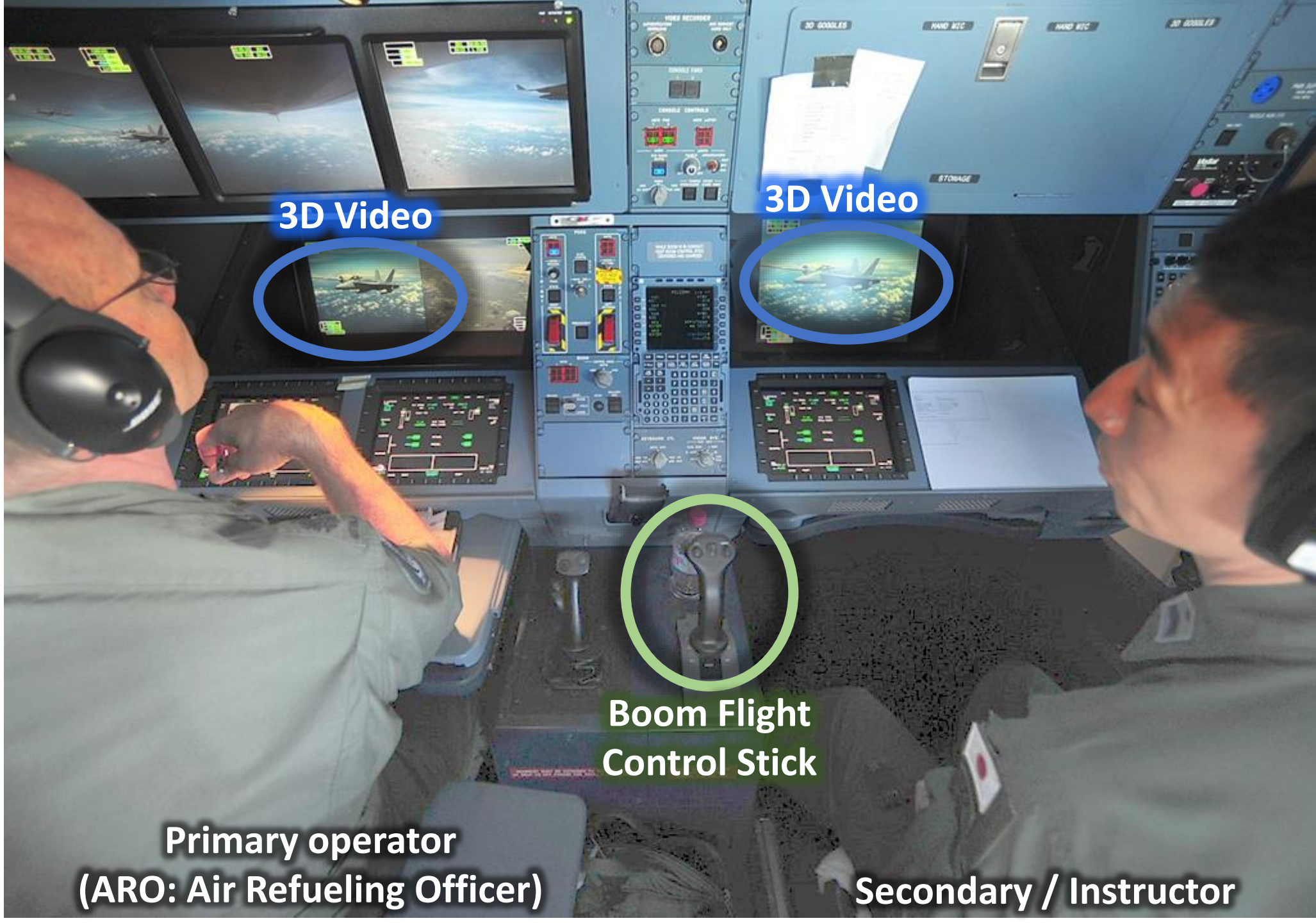
Iterative Control Structure Development



For the purpose of this exercise, let's focus on **Tanker Boom Operation**

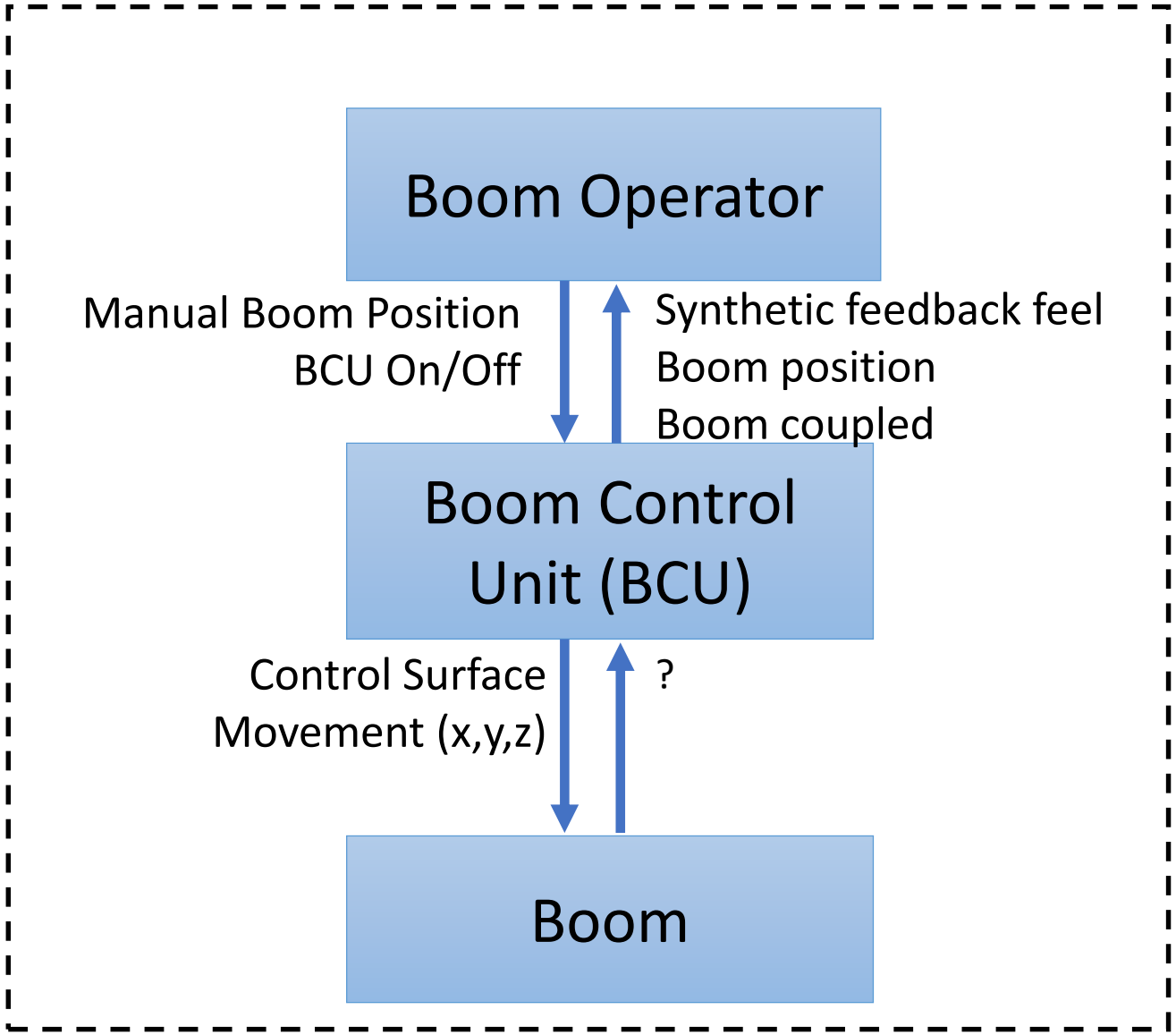
Please contact JThomas4@MIT.EDU with any questions!

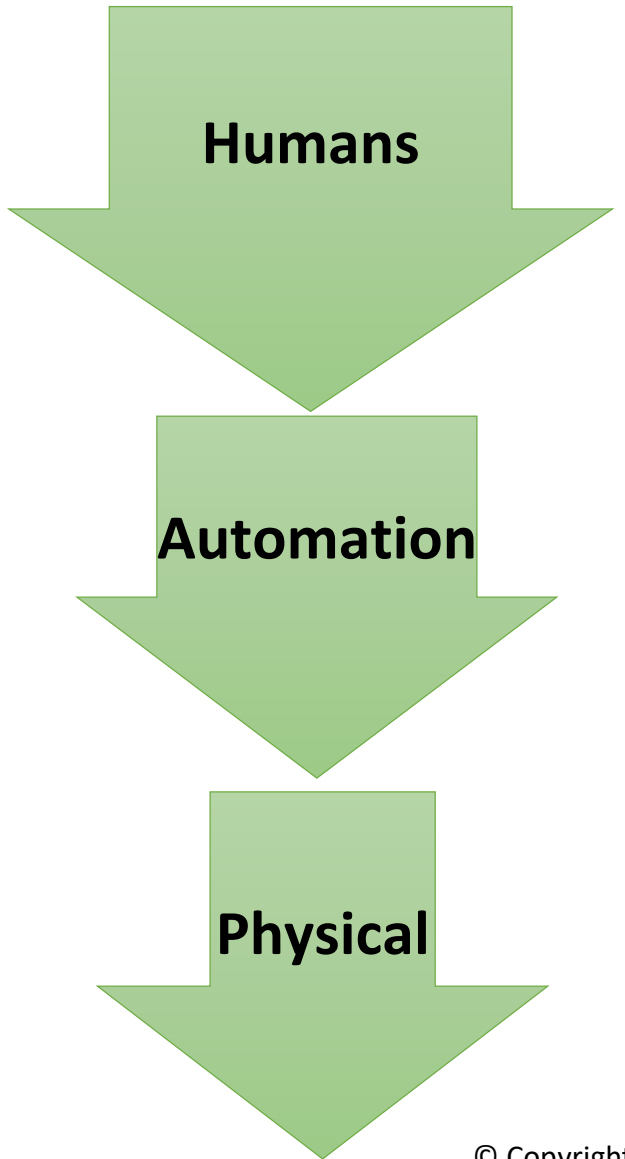
KC-30A Refueling Control Station



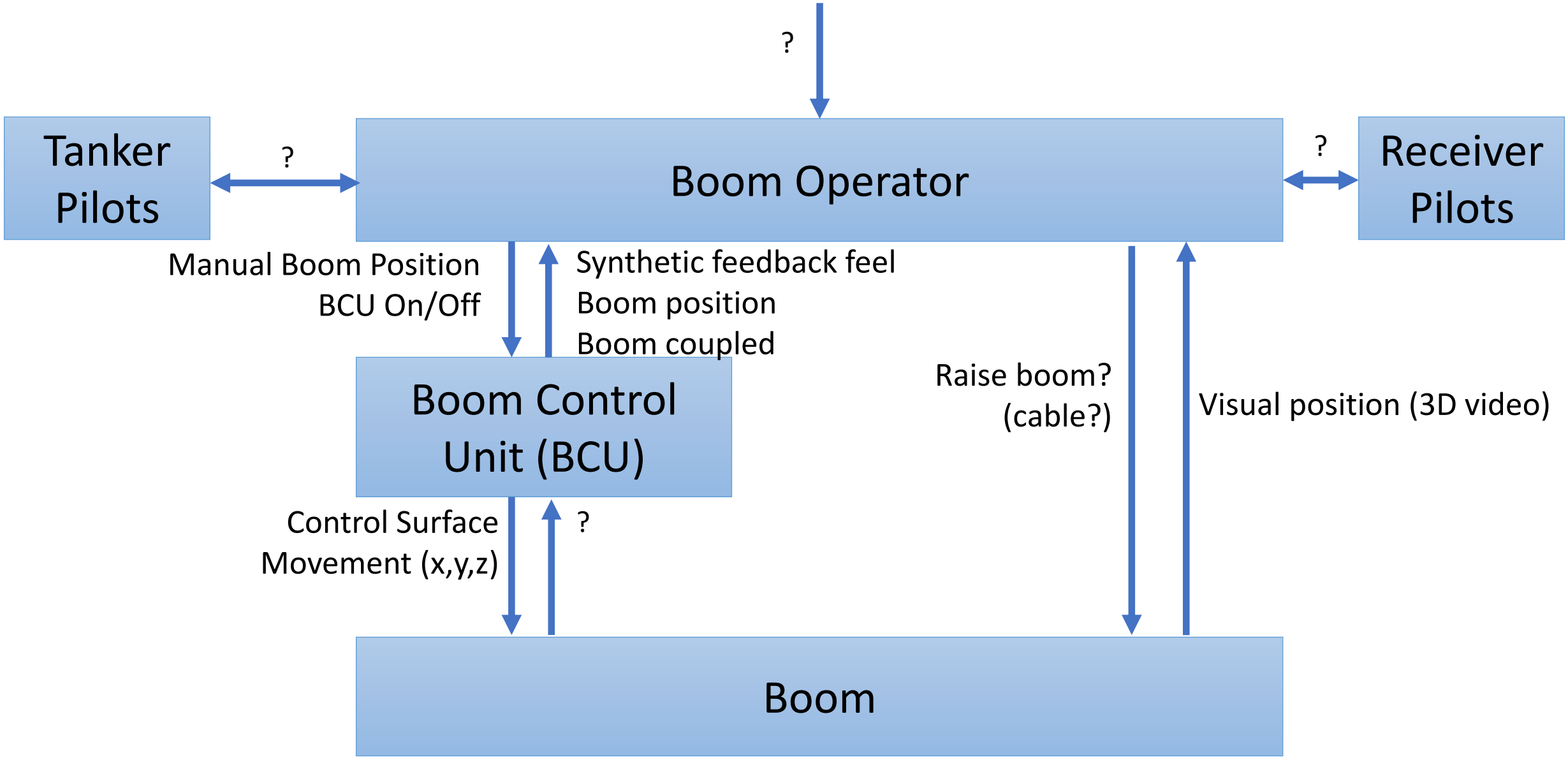
Let’s sketch the control structure for Boom Operation

Tanker Boom Operation

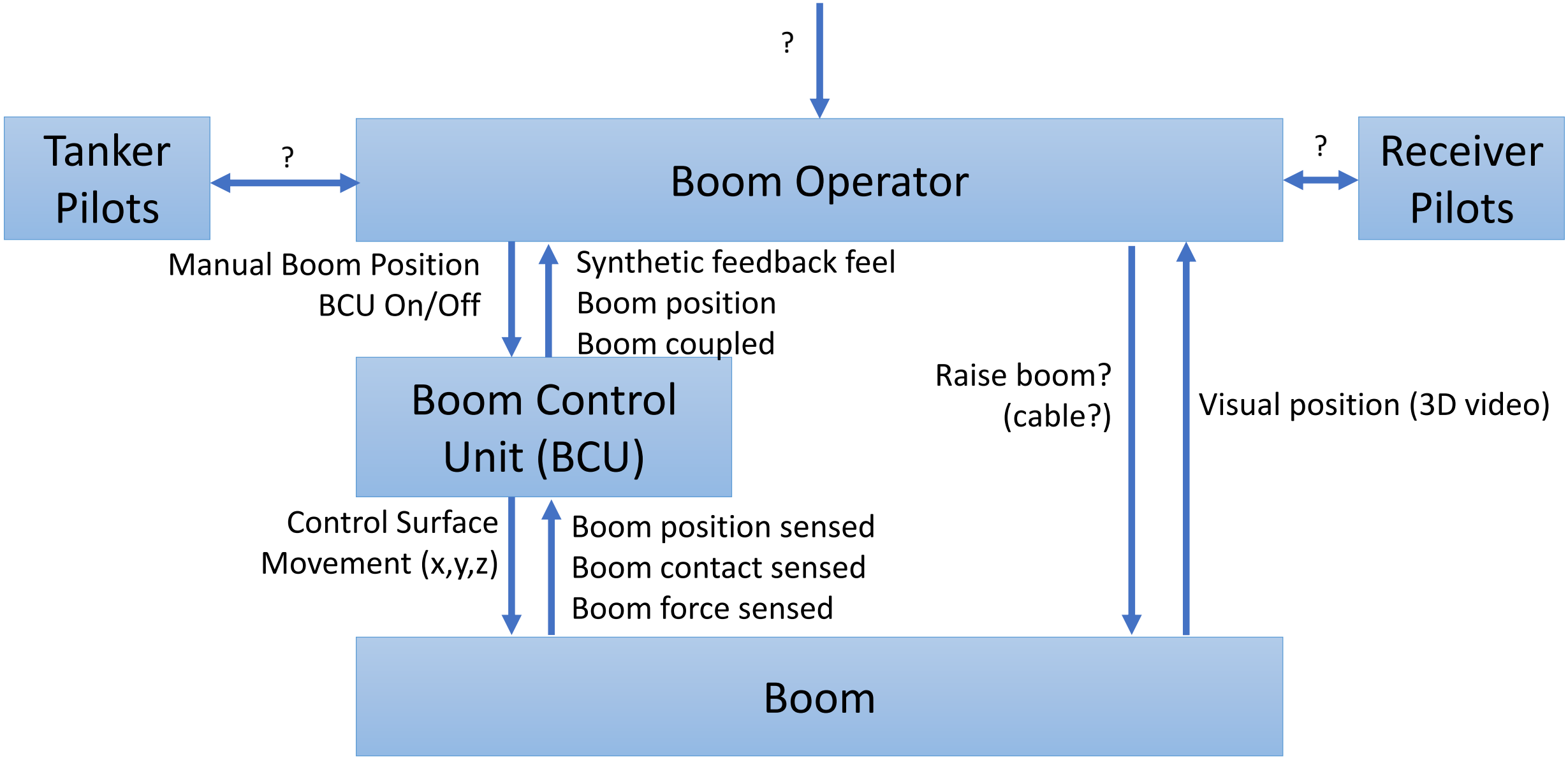




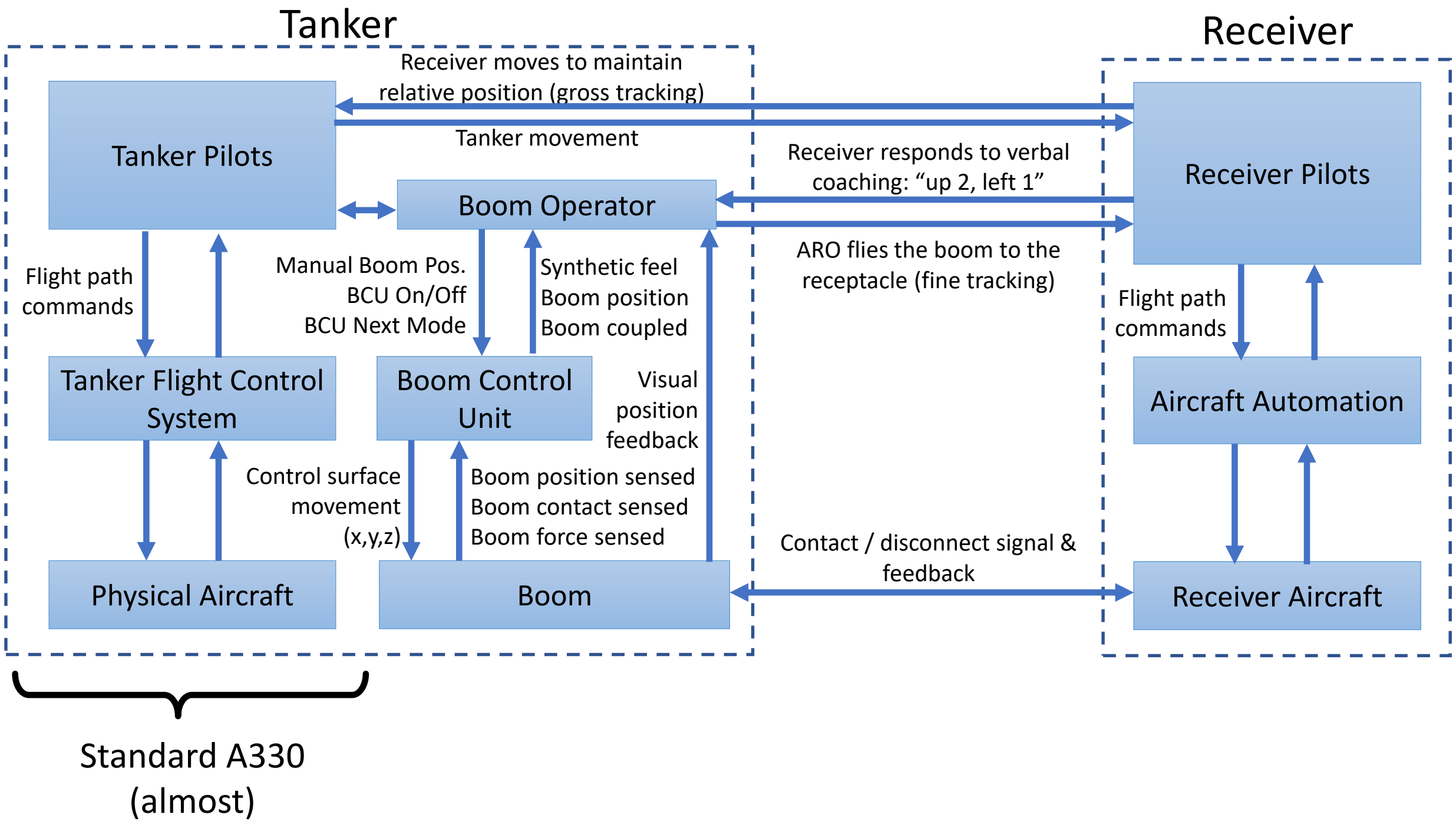
Please contact JThomas4@MIT.EDU with any questions!



Please contact JThomas4@MIT.EDU with any questions!



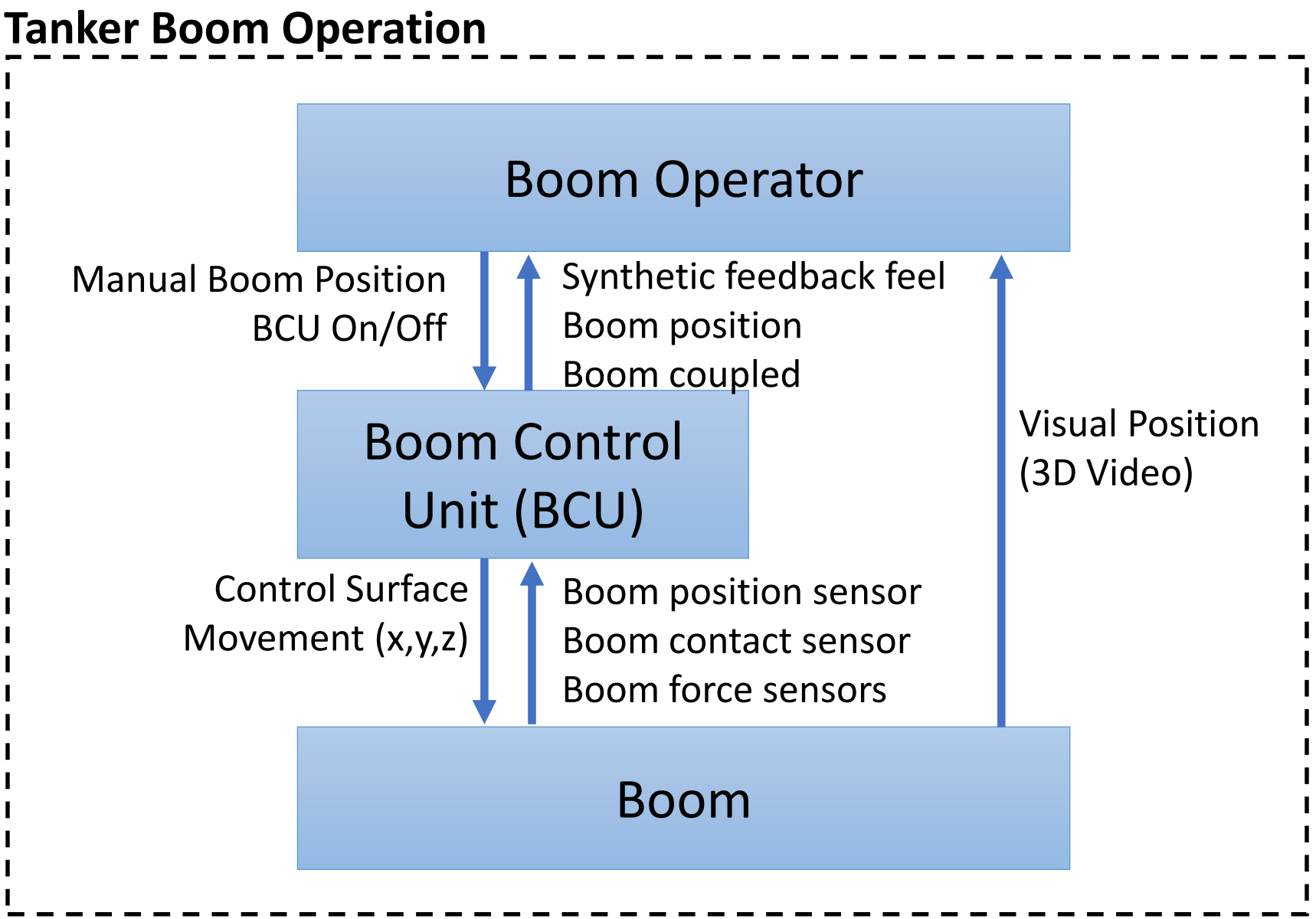
Please contact JThomas4@MIT.EDU with any questions!


Tanker
Receiver
Receiver moves to maintain relative position (gross tracking)
Tanker movement
Tanker Pilots
Boom Operator
Receiver responds to verbal coaching: “up 2, left 1”
Receiver Pilots
ARO flies the boom to the receptacle (fine tracking)
Flight path commands
Manual Boom Pos.
BCU On/Off
BCU Next Mode
Synthetic feel
Boom position
Boom coupled
Flight path commands
Tanker Flight Control System
Boom Control Unit
Visual position feedback
Aircraft Automation
Control surface movement (x,y,z)
Boom position sensed
Boom contact sensed
Boom force sensed
Contact / disconnect signal & feedback
Physical Aircraft
Boom
Receiver Aircraft
Standard A330 (almost)

Boom Operator Video

Image: https://www.kappa-optronics.com/en/cameras-for-aerospace-defense/cameras-for-aerospace/in-flight-refueling-cameras.cfm

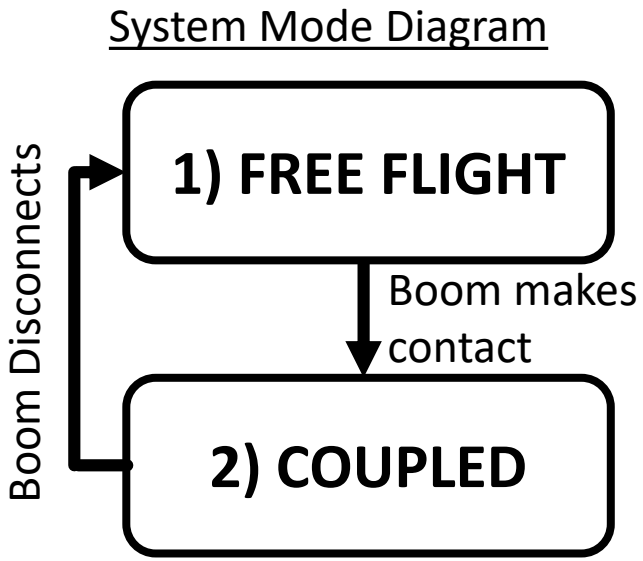
Our control structure



Please contact JThomas4@MIT.EDU with any questions!

A computer/digital upgrade!

Manual Boom Control (Old System)



1) FREE FLIGHT
   - Boom Operator moves boom into position
2) COUPLED
   - Boom Operator moves boom as needed to minimize contact loading

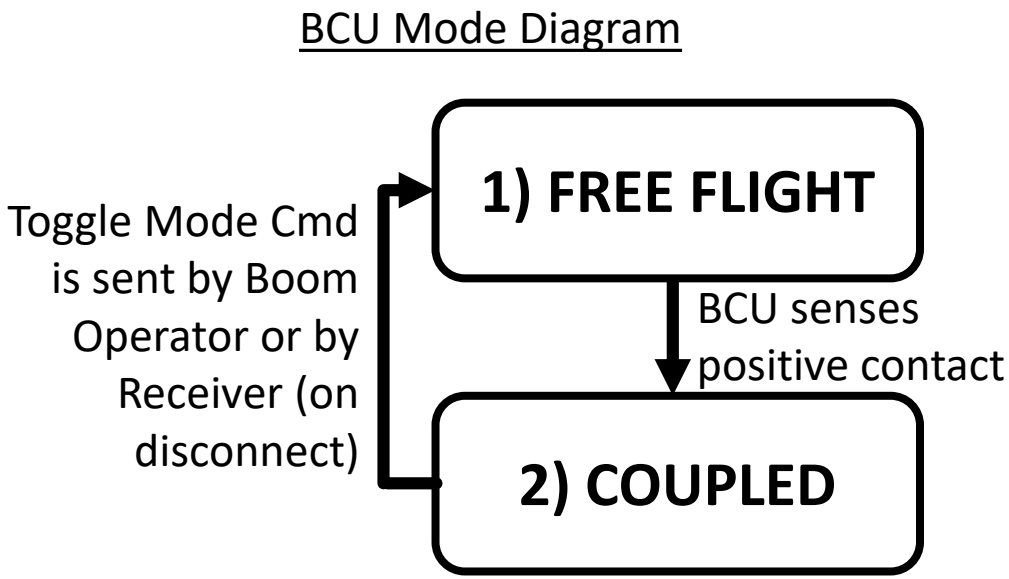
Please contact JThomas4@MIT.EDU with any questions!

Decision to Add Automation: Load Alleviation

- When boom is coupled, automatically fly boom
  - Use sensors to detect mechanical forces on boom tip
  - Boom Control Unit (BCU) automatically moves boom to minimize forces

Please contact JThomas4@MIT.EDU with any questions!

Partially Automated Boom Control

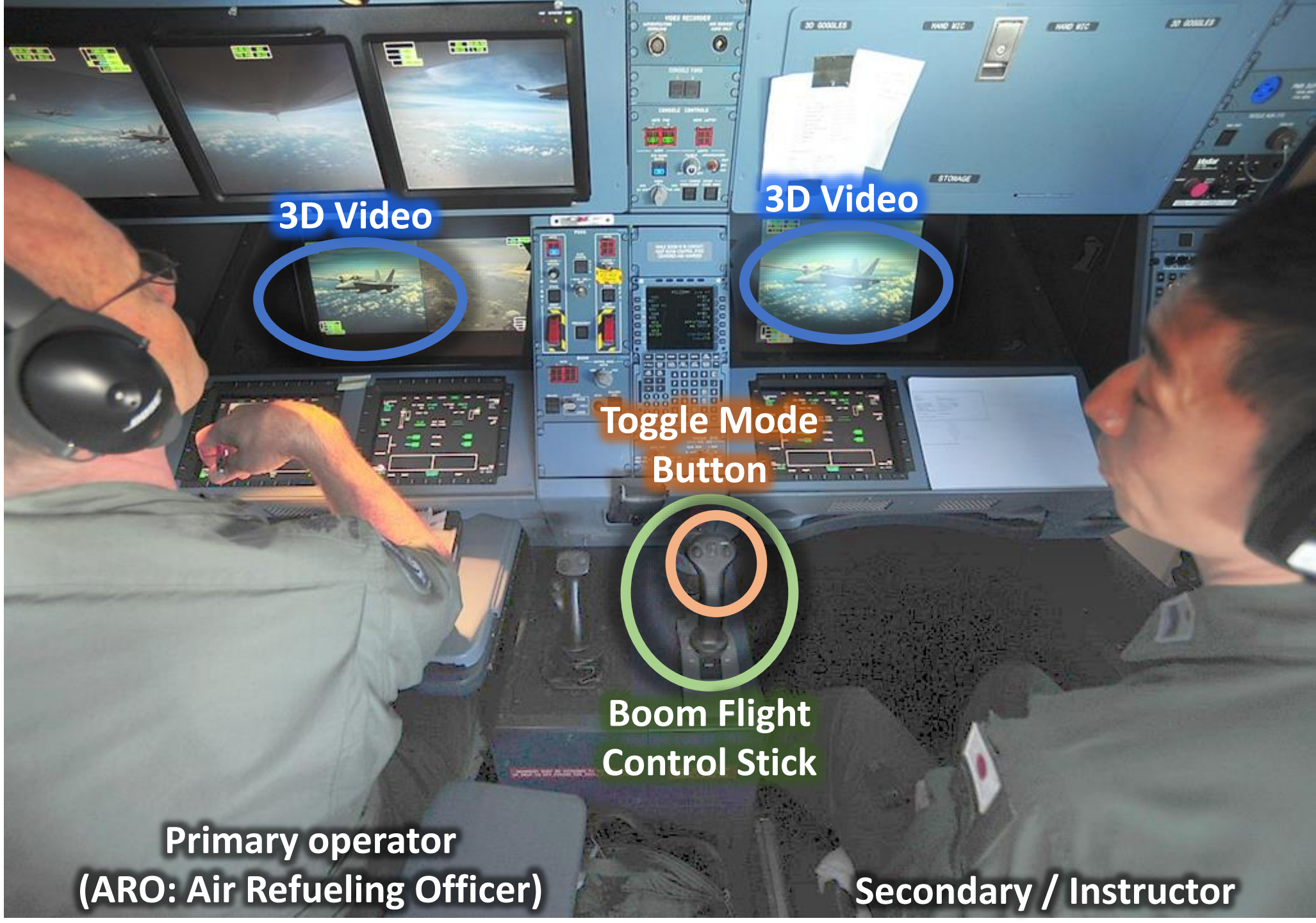


1) FREE FLIGHT
   - Boom Operator controls boom
   - Boom position matches current stick position
   - Boom Operator flies boom to insert probe into receptacle, making contact

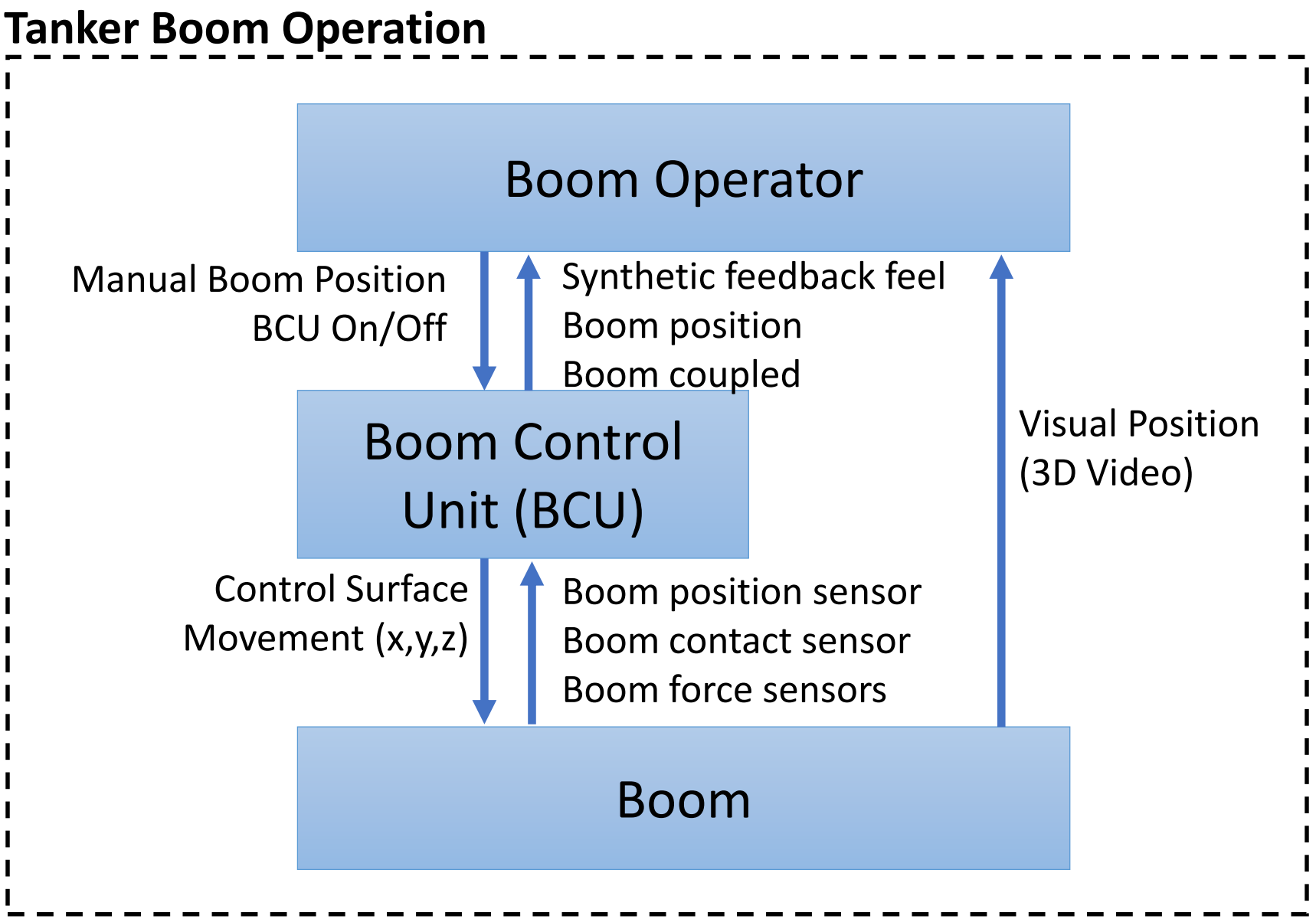
2) COUPLED
   - BCU automatically flies the boom
   - Boom Operator is not in control, stick ignored
   - The system senses tip loads and flies to null out that load

Please contact JThomas4@MIT.EDU with any questions!

KC-30A Refueling Control Station

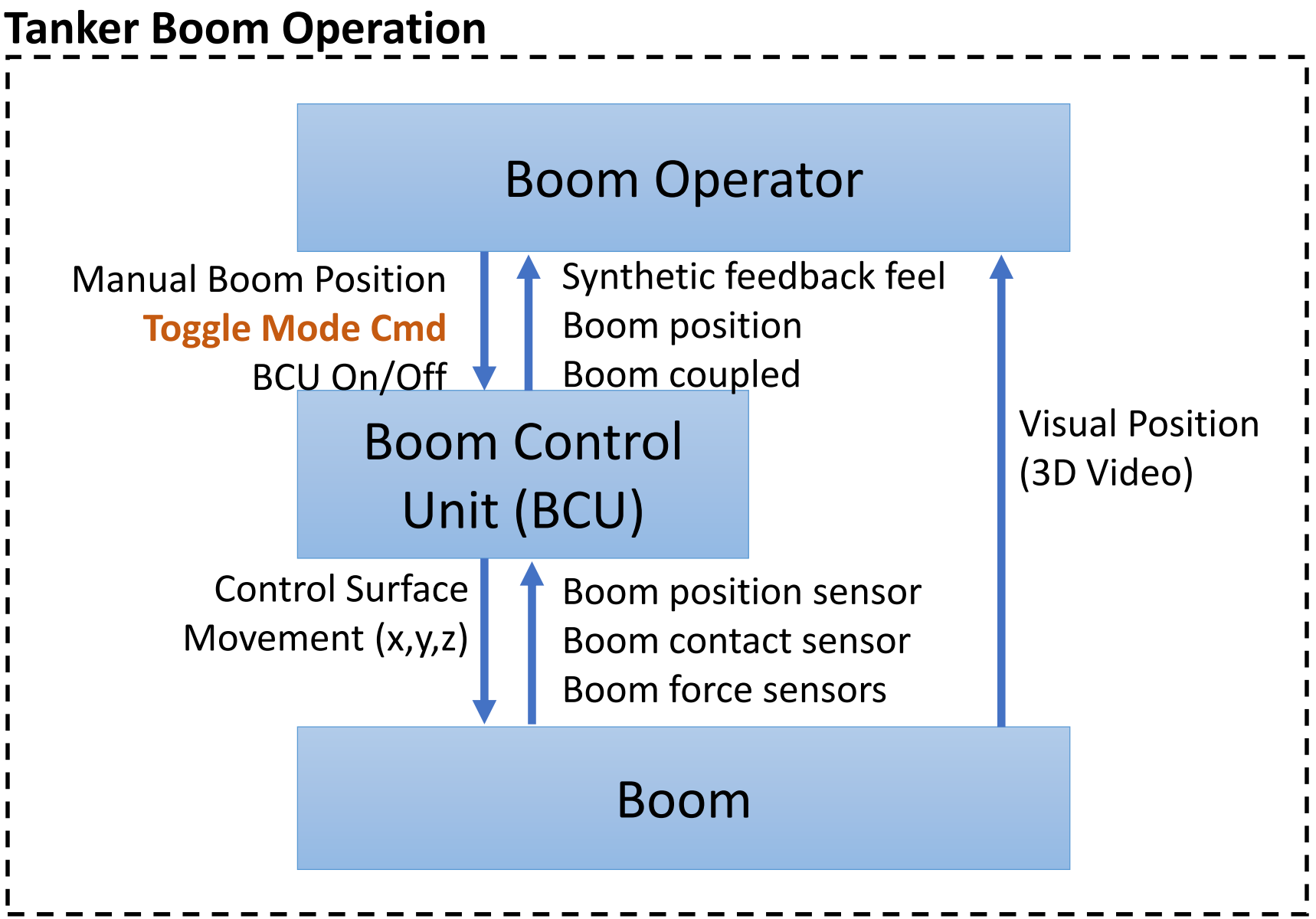


How does the control structure change?

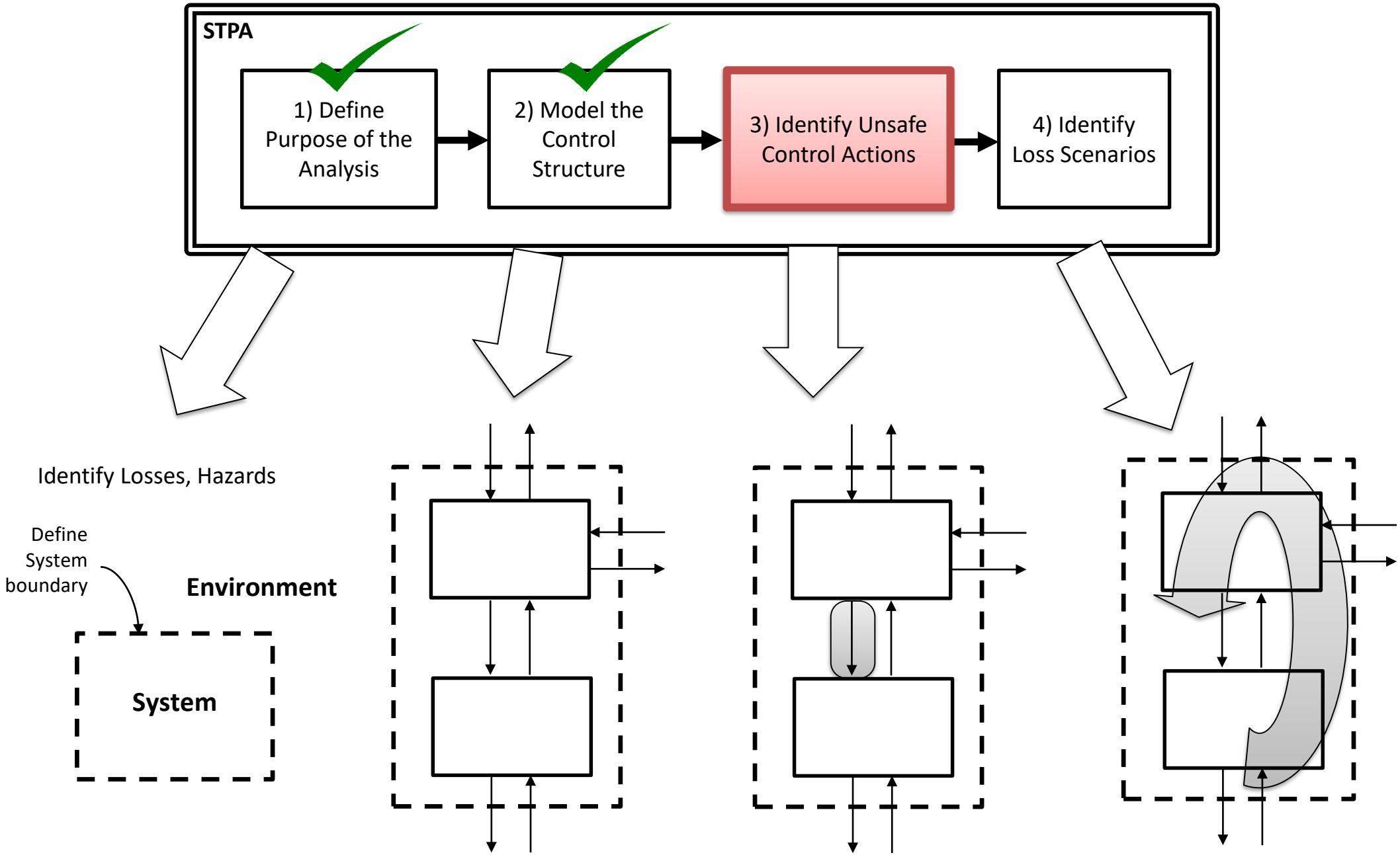


Please contact JThomas4@MIT.EDU with any questions!

How does the control structure change?

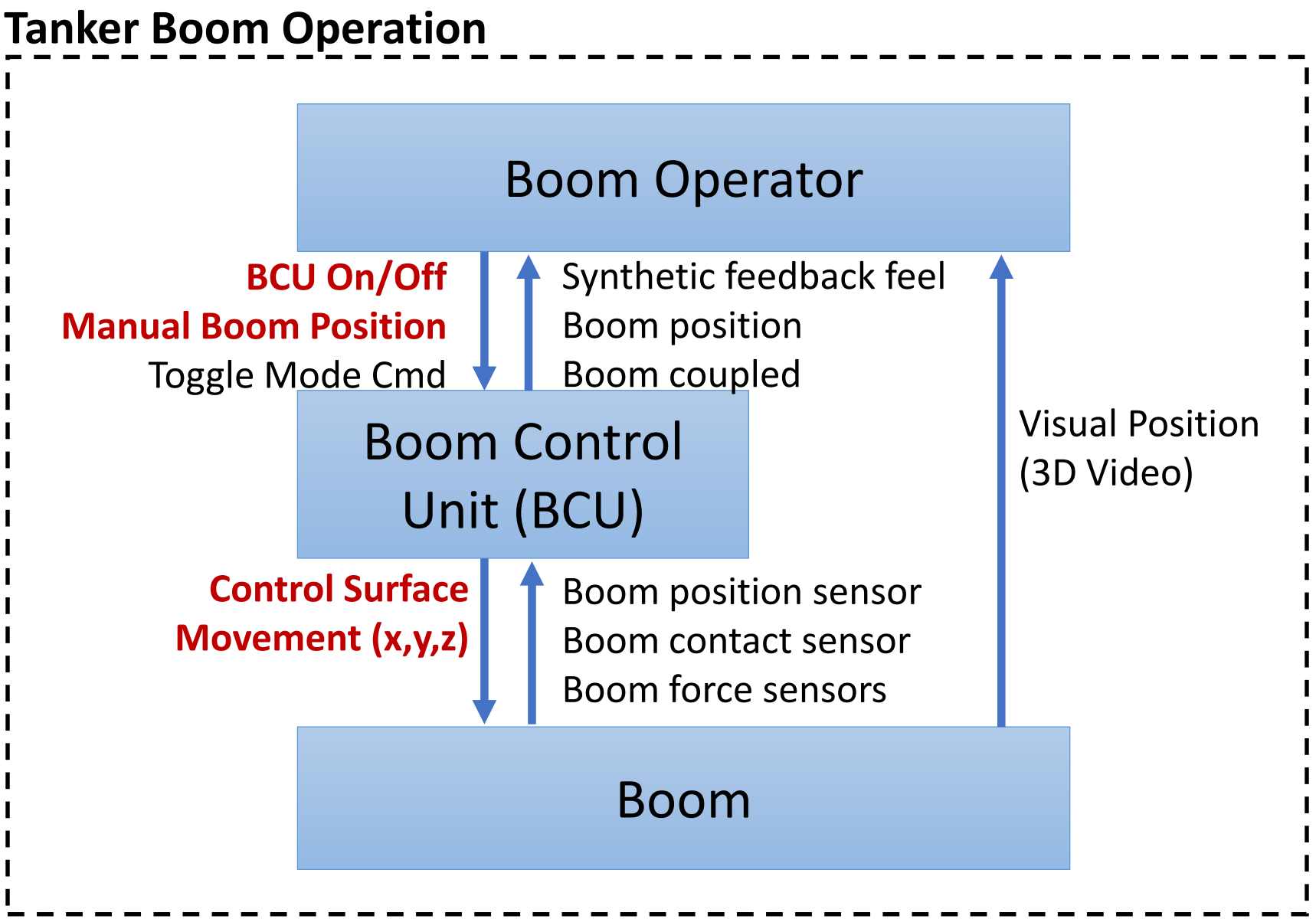


Please contact JThomas4@MIT.EDU with any questions!



(Leveson and Thomas, 2018)

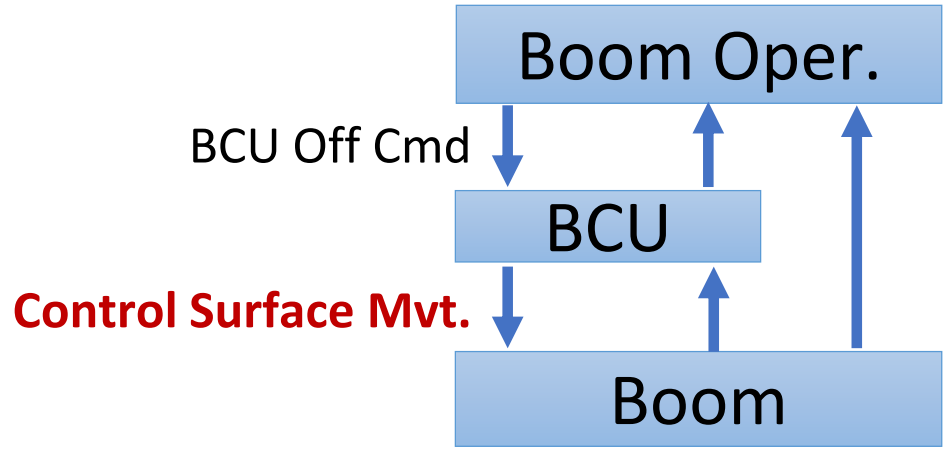
Analyze control actions



Please contact JThomas4@MIT.EDU with any questions!

Unsafe Control Actions

Control Structure:

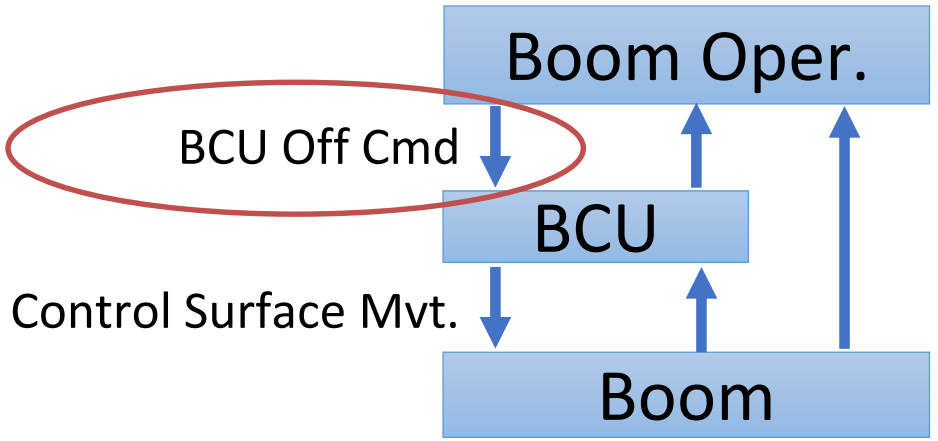


	?	?	?	?
BCU Off Cmd				

Please contact JThomas4@MIT.EDU with any questions!

Unsafe Control Actions

Control Structure:



Source Controller **Type** **Control Action** **Context**

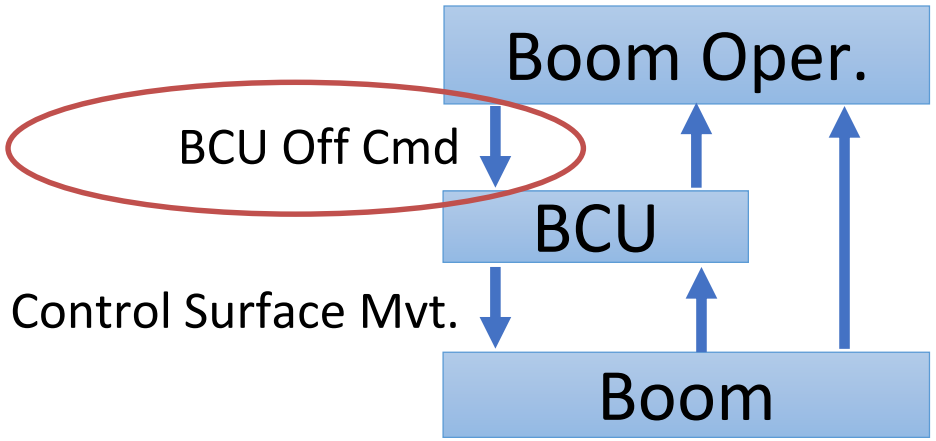
"Boom Operator provides BCU Off Cmd when BCU Operating Normally (Boom Coupled)"

	Not providing causes hazard	**Providing causes hazard** *[in wrong situation, excessive, insufficient, repetitive, wrong direction, etc.]*	**Too Early, Too Late, Order**	**Stopped Too Soon / Applied too long**
BCU Off Cmd	?	?	?	?

Please contact JThomas4@MIT.EDU with any questions!

Unsafe Control Actions

Control Structure:



Source Controller **Type** **Control Action** **Context**

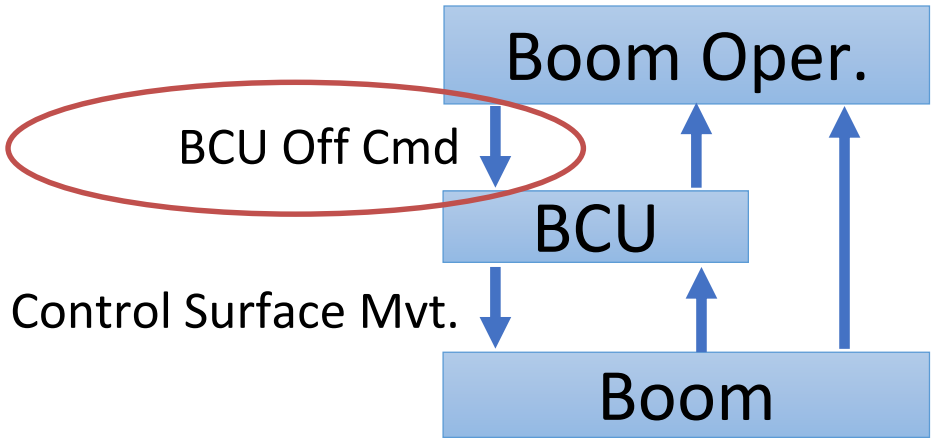
"Boom Operator provides BCU Off Cmd when BCU Operating Normally (Boom Coupled)

	Not providing causes hazard	**Providing causes hazard** *[in wrong situation, excessive, insufficient, repetitive, wrong direction, etc.]*	**Too Early, Too Late, Order**	**Stopped Too Soon / Applied too long**
BCU Off Cmd	[…]	**Boom Operator provides BCU Off Cmd when _____**	[…]	[…]

Please contact JThomas4@MIT.EDU with any questions!

Unsafe Control Actions

Control Structure:



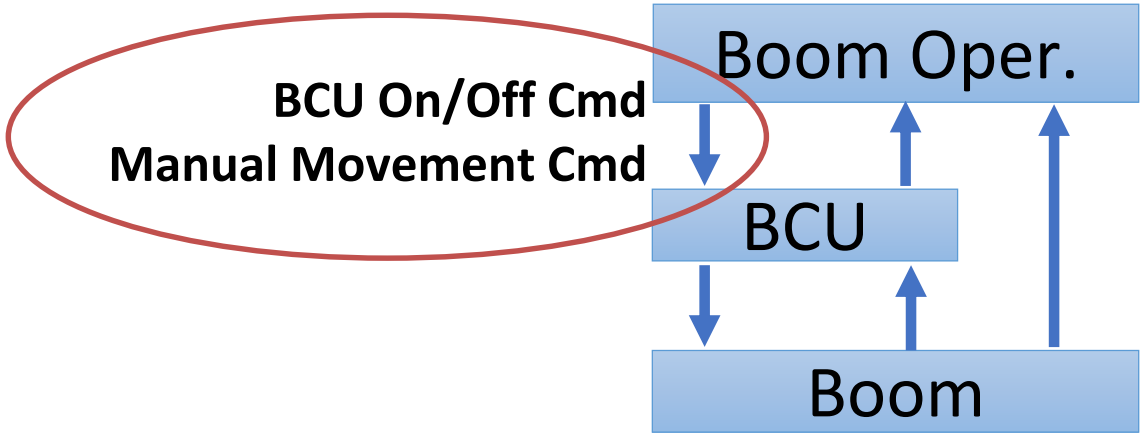
Source Controller **Type** **Control Action** **Context**

"Boom Operator provides BCU Off Cmd when BCU Operating Normally (Boom Coupled)"

	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
BCU Off Cmd	**Boom Operator does not provide BCU Off Cmd when _____**	[...]	[...]	[...]

Please contact JThomas4@MIT.EDU with any questions!

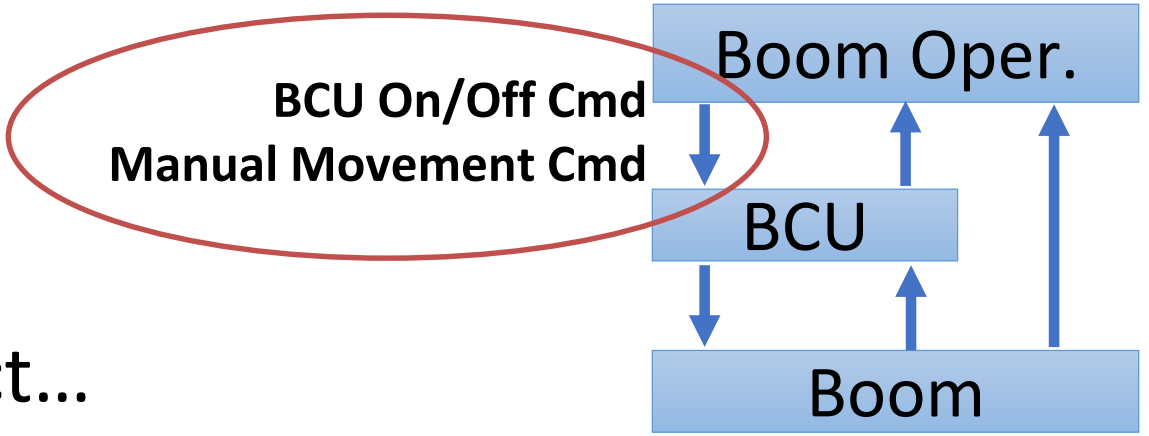
Operator UCAs



	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
BCU Off Cmd	**Boom Operator does not provide BCU Off Cmd when BCU is providing movement commands that exceed Boom structural limits** […]	Boom operator provides BCU Off Cmd when BCU Operating Normally (BCU is load alleviating, Boom Coupled) […]	Boom Operator provides BCU Off Cmd too late after _____ Boom Operator provides BCU Off Cmd too early before _____	[…]

Please contact JThomas4@MIT.EDU with any questions!

Operator UCAs



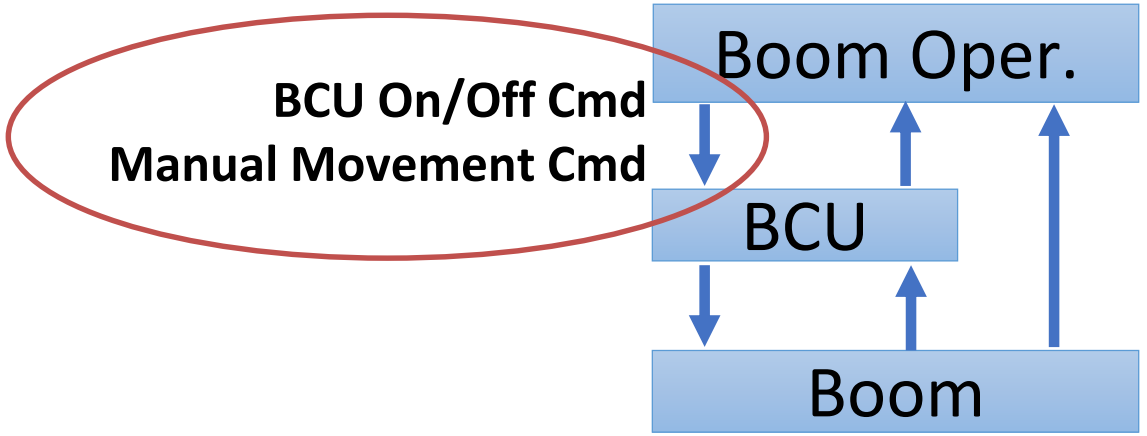
Case 1: Suppose Boom is In Contact…

Case 2: Suppose Boom is not In Contact…

	Not providing causes hazard	**Providing causes hazard** *[in wrong situation, excessive, insufficient, repetitive, wrong direction, etc.]*	**Too Early, Too Late, Order**	**Stopped Too Soon / Applied too long**
Manual Movement Cmd	Boom Operator does not provide Manual Movement Cmd when _____	**Boom Operator provides Manual Movement Cmd when _____**	Boom Operator provides Manual Movement Cmd too late after _____ Boom Operator provides Manual Movement Cmd too early before _____	Boom Operator stops providing Movement Cmd too soon before _____ Boom Operator continues providing Movement Cmd too long after _____

Please contact JThomas4@MIT.EDU with any questions!

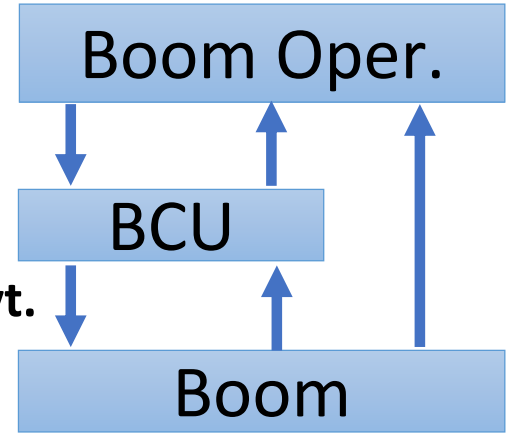
Operator UCAs



	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Manual Movement Cmd	Boom Operator does not provide Manual Movement Cmd when _____	**Boom Operator provides excessive Manual Movement Cmd (> TBD) when Boom is in contact (can break Boom)** Boom Operator provides Manual Movement Cmd when _____	Boom Operator provides Manual Movement Cmd too late after _____ Boom Operator provides Manual Movement Cmd too early before _____	Boom Operator stops providing Movement Cmd too soon before _____ Boom Operator continues providing Movement Cmd too long after _____

Please contact JThomas4@MIT.EDU with any questions!

Identify Unsafe Control Actions



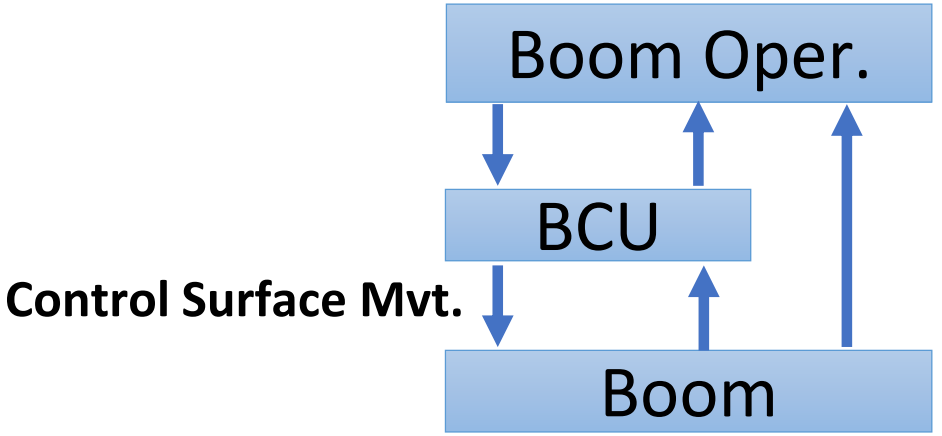
Case 1: Suppose the Boom is <u>In Contact</u>…

Case 2: Suppose the Boom is <u>Not In Contact</u>…

	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Control Surface Movement Cmd	BCU does not provide Movement Cmd when ____ […]	**BCU provides Movement Cmd when** _____ *[wrong situation, cmd insufficient, excessive, wrong direction, oscillatory, repetitive, etc.]*	BCU provides Movement Cmd too late after _____ BCU provides Movement Cmd too early before _____ […]	BCU continues providing Movement Cmd too long after _____ BCU continues providing Movement Cmd too long after _____ […]

Please contact JThomas4@MIT.EDU with any questions!

Identify Unsafe Control Actions

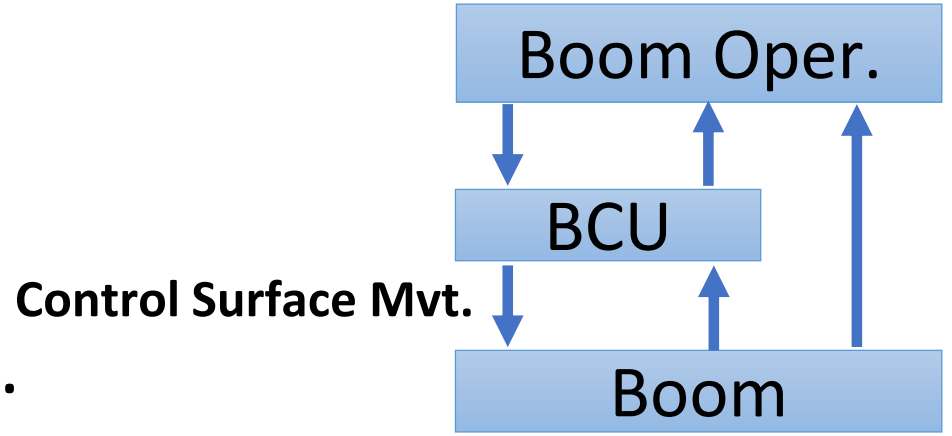


Case 1: Suppose the Boom is In Contact…

	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Control Surface Movement Cmd	BCU does not provide Movement Cmd when Load exceeds TBD […]	BCU provides Movement Cmd when Load does not exceed TBD **BCU provides excessive Movement Cmd (>TBD) when Boom is in contact (can break boom)** [insufficient, excessive, oscillatory, repetitive, etc.]	BCU provides Movement Cmd too late after Load exceeds TBD BCU provides Movement Cmd too early before Load exceeds TBD BCU provides Movement Cmd too early before Boom is Coupled BCU provides Movement Cmd too late after Boom is Disconnected […]	BCU continues providing Movement Cmd too long after Load drops below TBD BCU continues providing Movement Cmd too long after Load is increases beyond TBD BCU continues providing Movement Cmd too long after Boom Position exceeds TBD […]

Please contact JThomas4@MIT.EDU with any questions!

Identify Unsafe Control Actions

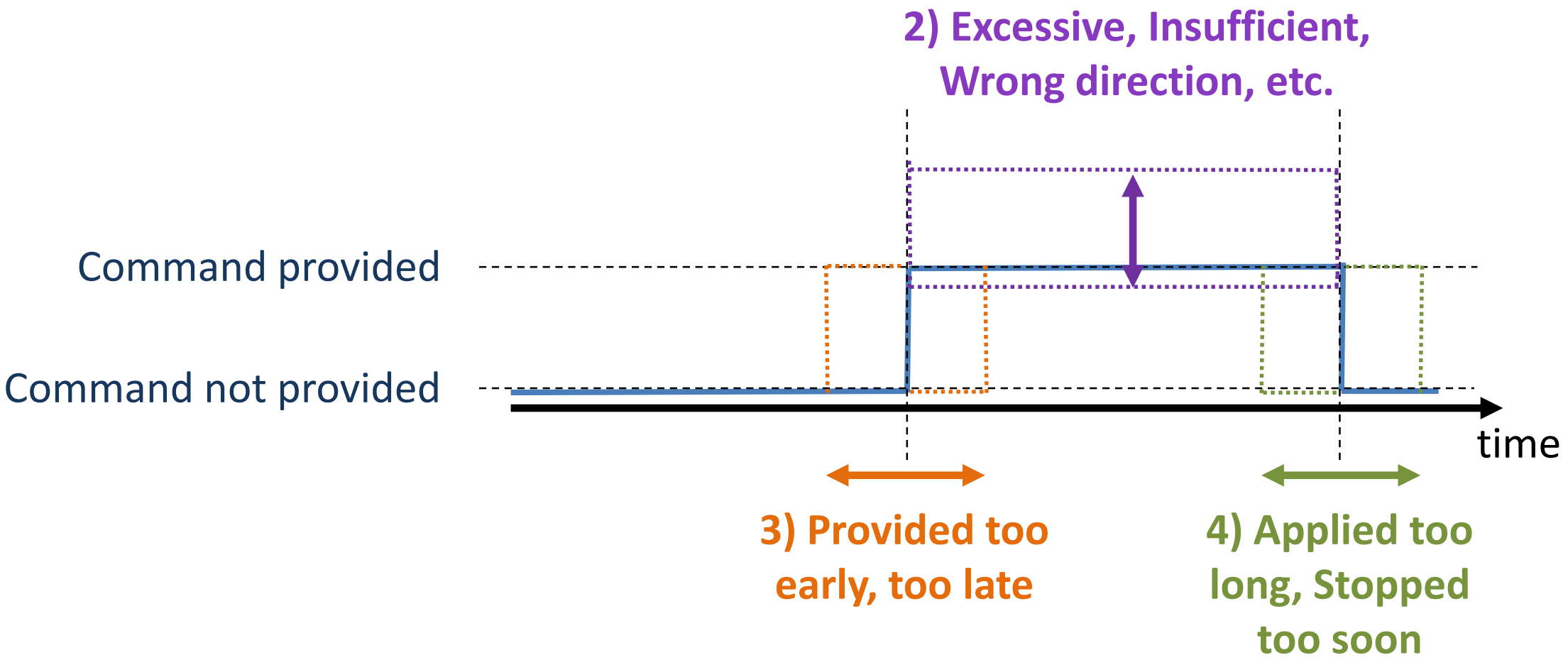


Case 2: Suppose the Boom is Not In Contact…

	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Control Surface Movement Cmd	BCU does not provide Movement Cmd when Boom Operator moves Stick […]	**BCU provides Movement Cmd when Boom Operator does not move Stick (Boom Not In Contact)** BCU provides Movement Cmd when Boom Operator has turned BCU Off BCU provides Movement Cmd in wrong direction (does not match Stick direction) **BCU provides excessive Movement Cmd beyond mechanical Boom limits** [insufficient, oscillatory, repetitive, etc.]	BCU provides Movement Cmd too late (more than TBD sec) after Boom Operator moves Stick Computer provides Movement Cmd too early (>0s) before Boom Operator moves Stick […]	BCU continues providing Movement Cmd too long after Boom reaches position commanded by Stick BCU continues providing Movement Cmd too long after Boom position exceeds TBD BCU stops providing Movement Cmd too soon before Boom reaches position commanded by Stick […]

Please contact JThomas4@MIT.EDU with any questions!

Timing Diagram: Different UCA Types



Please contact JThomas4@MIT.EDU with any questions!

Formal STPA

Source Controller	Control Action	Context			Unsafe to provide?
		Boom in Contact?	Strength of Cmded Movement	Stick movement?	
BCU	Movement Cmd	Boom in Contact	$Limit_H$ < Movement < $Limit_{HH}$	*	Yes
BCU	Movement Cmd	Boom not in Contact	$Limit_H$ < Movement < $Limit_{HH}$	Matches Cmded Movement	No
BCU	Movement Cmd	*	$Limit_{HH}$ < Movement	*	Yes
BCU	Movement Cmd	Boom not in Contact	*	No stick movement	Yes
[…]	[…]	[…]	[…]	[…]	[…]

$Limit_H$ = limit that leads to damage when coupled with receiver
$Limit_{HH}$ = limit that leads to damage when not coupled

Please contact JThomas4@MIT.EDU with any questions!

Formal STPA

Source Controller	Control Action	Context			Unsafe to provide?
		Boom in Contact?	Strength of Cmded Movement	Stick movement?	
BCU	Movement Cmd	Boom in Contact	$Limit_H$ < Movement < $Limit_{HH}$	*	Yes
BCU	Movement Cmd	Boom not in Contact	$Limit_H$ < Movement < $Limit_{HH}$	Matches Cmded Movement	No
BCU	Movement Cmd	*	$Limit_{HH}$ < Movement	*	Yes
BCU	Movement Cmd	Boom not in Contact	*	No stick movement	Yes
[…]	[…]	[…]	[…]	[…]	[…]

$Limit_H$ = limit that leads to damage when coupled with receiver
$Limit_{HH}$ = limit that leads to damage when not coupled

Please contact JThomas4@MIT.EDU with any questions!

Formal STPA

Source Controller	Control Action	Context			Unsafe to provide?
		Boom in Contact?	Strength of Cmded Movement	Stick movement?	
BCU	Movement Cmd	Boom in Contact	$Limit_H$ < Movement < $Limit_{HH}$	*	Yes
BCU	Movement Cmd	Boom not in Contact	$Limit_H$ < Movement < $Limit_{HH}$	Matches Cmded Movement	No
BCU	Movement Cmd	[illegible]	$Limit_{HH}$ < Movement	[illegible]	Yes
BCU	Movement Cmd	Boom not in Contact	*	No stick movement	Yes
[…]	[…]	[…]	[…]	[…]	[…]

$Limit_H$ = limit that leads to damage when coupled with receiver
$Limit_{HH}$ = limit that leads to damage when not coupled

Please contact JThomas4@MIT.EDU with any questions!

Formal STPA

Source Controller	Control Action	Context			Unsafe to provide?
		Boom in Contact?	Strength of Cmded Movement	Stick movement?	
BCU	Movement Cmd	Boom in Contact	$Limit_H$ < Movement < $Limit_{HH}$	*	Yes
BCU	Movement Cmd	Boom not in Contact	$Limit_H$ < Movement < $Limit_{HH}$	Matches Cmded Movement	No
BCU	Movement Cmd	*	$Limit_{HH}$ < Movement	*	Yes
BCU	Movement Cmd	Boom not in Contact	*	No stick movement	Yes
[…]	[…]	[…]	[…]	[…]	[…]

$Limit_H$ = limit that leads to damage when coupled with receiver
$Limit_{HH}$ = limit that leads to damage when not coupled

Please contact JThomas4@MIT.EDU with any questions!

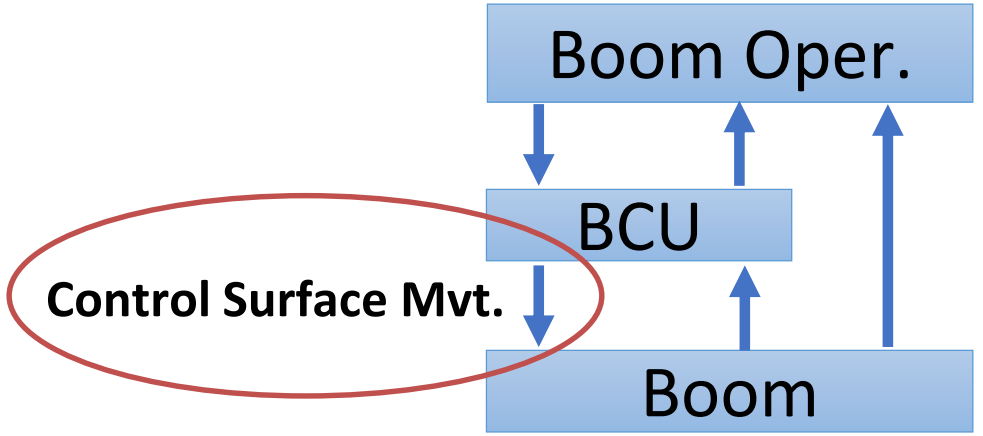
Formal STPA

Source Controller	Control Action	Context			Unsafe to provide?
		Boom in Contact?	Strength of Cmded Movement	Stick movement?	
BCU	Movement Cmd	Boom in Contact	$Limit_H$ < Movement < $Limit_{HH}$	*	Yes
BCU	Movement Cmd	Boom not in Contact	$Limit_H$ < Movement < $Limit_{HH}$	Matches Cmded Movement	No
BCU	Movement Cmd	*	$Limit_{HH}$ < Movement	*	Yes
BCU	Movement Cmd	Boom not in Contact	*	No stick movement	Yes
[…]	[…]	[…]	[…]	[…]	[…]

$Limit_H$ = limit that leads to damage when coupled with receiver
$Limit_{HH}$ = limit that leads to damage when not coupled

Please contact JThomas4@MIT.EDU with any questions!

Identify Unsafe Control Actions



Suppose the Boom is Not Coupled…

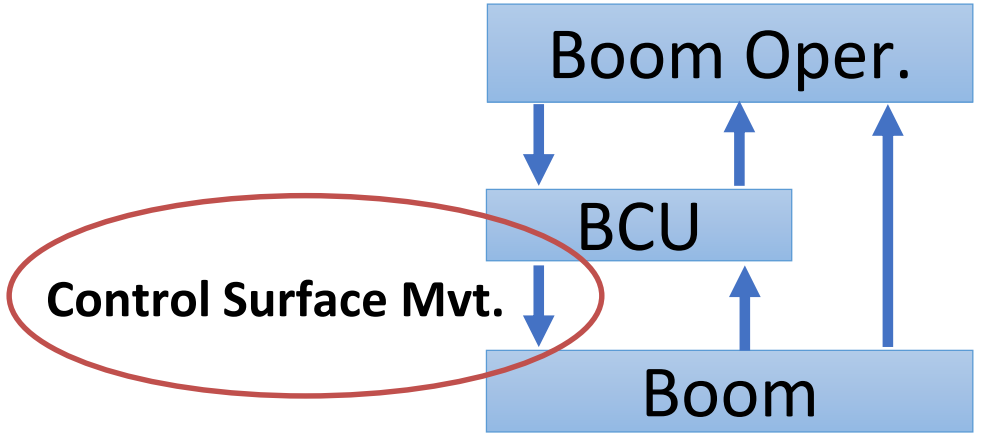
	Not providing	[illegible]ard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Surface Movement Cmd	Cmd when Boom Operator mov[illegible]	BCU provides Movement Cmd in wrong direction (does not match Stick direction)	Comput[illegible]rovides Movement Cmd too [illegible]	[illegible]
	[illegible]md when [illegible]ove Stick [illegible]d when [illegible] BCU Off		UCA-10: BCU provides Movement Cmd too late (more than TBD sec) after Boom Operator moves Stick [H-3]	BCU continues providing Movement Cmd too long after Boom reaches position commanded by Stick BCU continues providing Movement Cmd too long after Boom position exceeds TBD

R-1: BCU must provide Movement Cmd within TBD Sec after Boom Operator moves stick when Not Coupled [UCA-10]

TS-1:
Context: Boom is Coupled and Boom Operator moves stick
Verify: BCU does provides Movement Cmd within TBD sec [UCA-10]

Please contact JThomas4@MIT.EDU with any questions!

Identify Unsafe Control Actions



Suppose the Boom is Not Coupled…

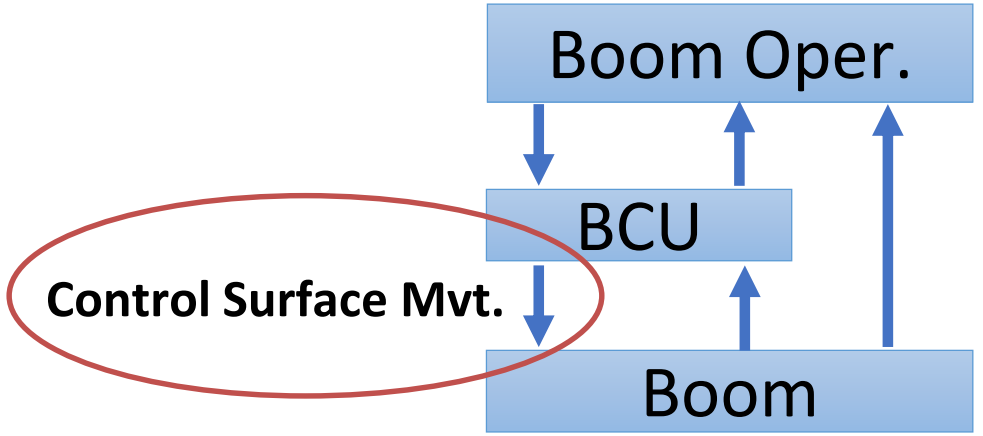
	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Control Surface Movement Cmd	BCU does not provide Movement Cmd when Boom Operator mov…	UCA-2: BCU provides Movement Cmd when Boom Operator does not move Stick [H-1] BCU provi… Movement Cmd when Boom Ope…tor has turned BCU Off BCU provide… Movement Cmd in wrong direction…does not match Stick	Mo… late… s… C… Computer provides Movement Cmd too…	…Boom position exceeds TBD … […]

R-2: BCU must not provide Movement Cmd when Boom is Coupled and Boom Operator has not moved stick [UCA-2]

TS-2:
Context: Boom is Coupled and Boom Operator has not moved stick
Verify: BCU does not provide Movement Cmd [UCA-2]

Please contact JThomas4@MIT.EDU with any questions!

Identify Unsafe Control Actions

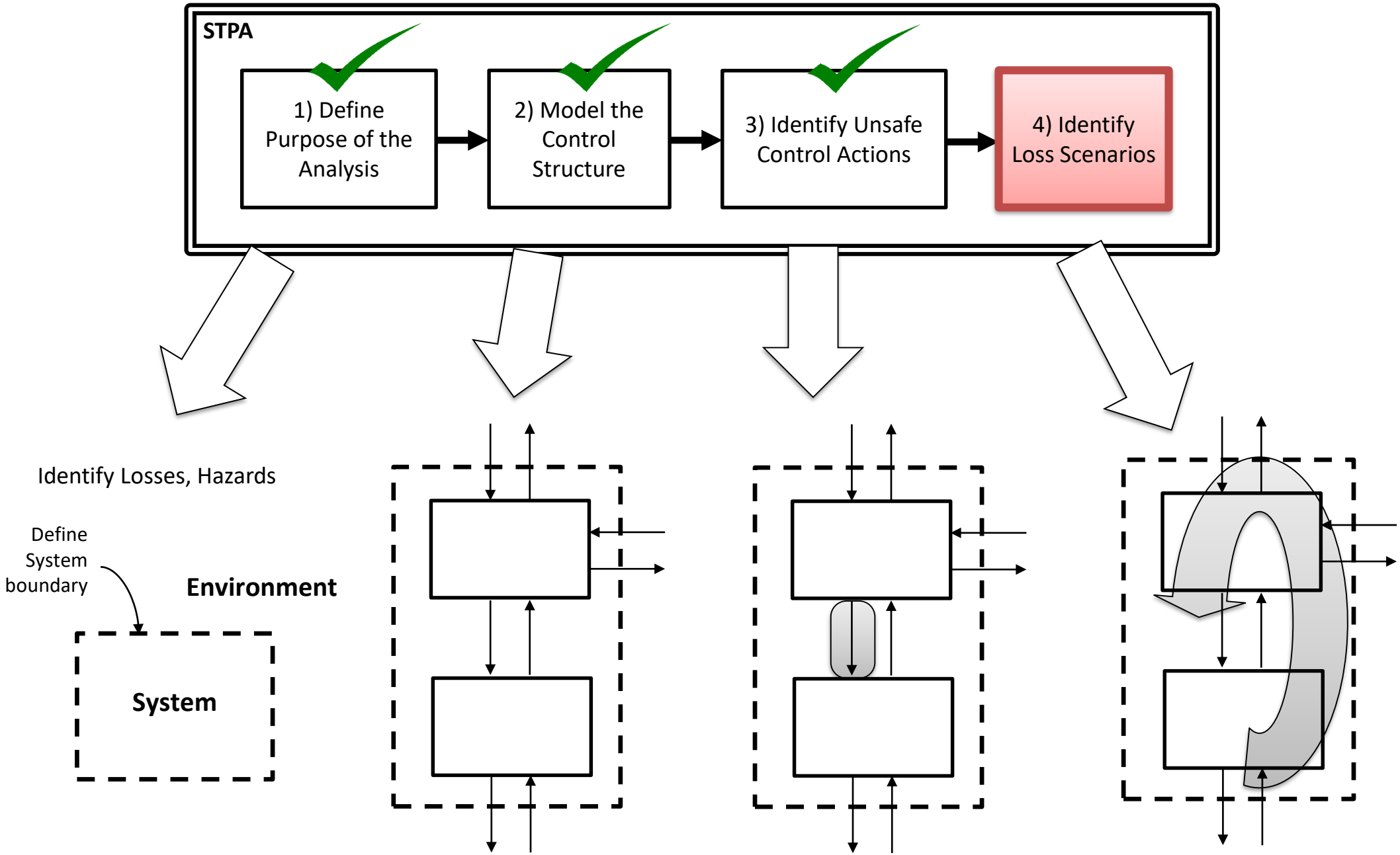


Suppose the Boom is Not Coupled…

	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Control Surface Movement Cmd	BCU does not provide Movement Cmd when Boom Operator moves Stick […]	BCU provides Movement Cmd when Boom Operator does not move Stick BCU provides Movement Cmd when Boom Operator has turned BCU Off BCU provides Movement Cmd in wrong direction (does not match Stick direction) BCU provides excessive Movement Cmd beyond amount of Stick movement [insufficient, oscillatory, repetitive, etc.]	BCU provides Movement Cmd too late (more than TBD sec) after Boom Operator moves Stick […]	BCU continues providing Movement Cmd too long after Boom reaches position commanded by Stick […]

Is this Safety or Security? Both!

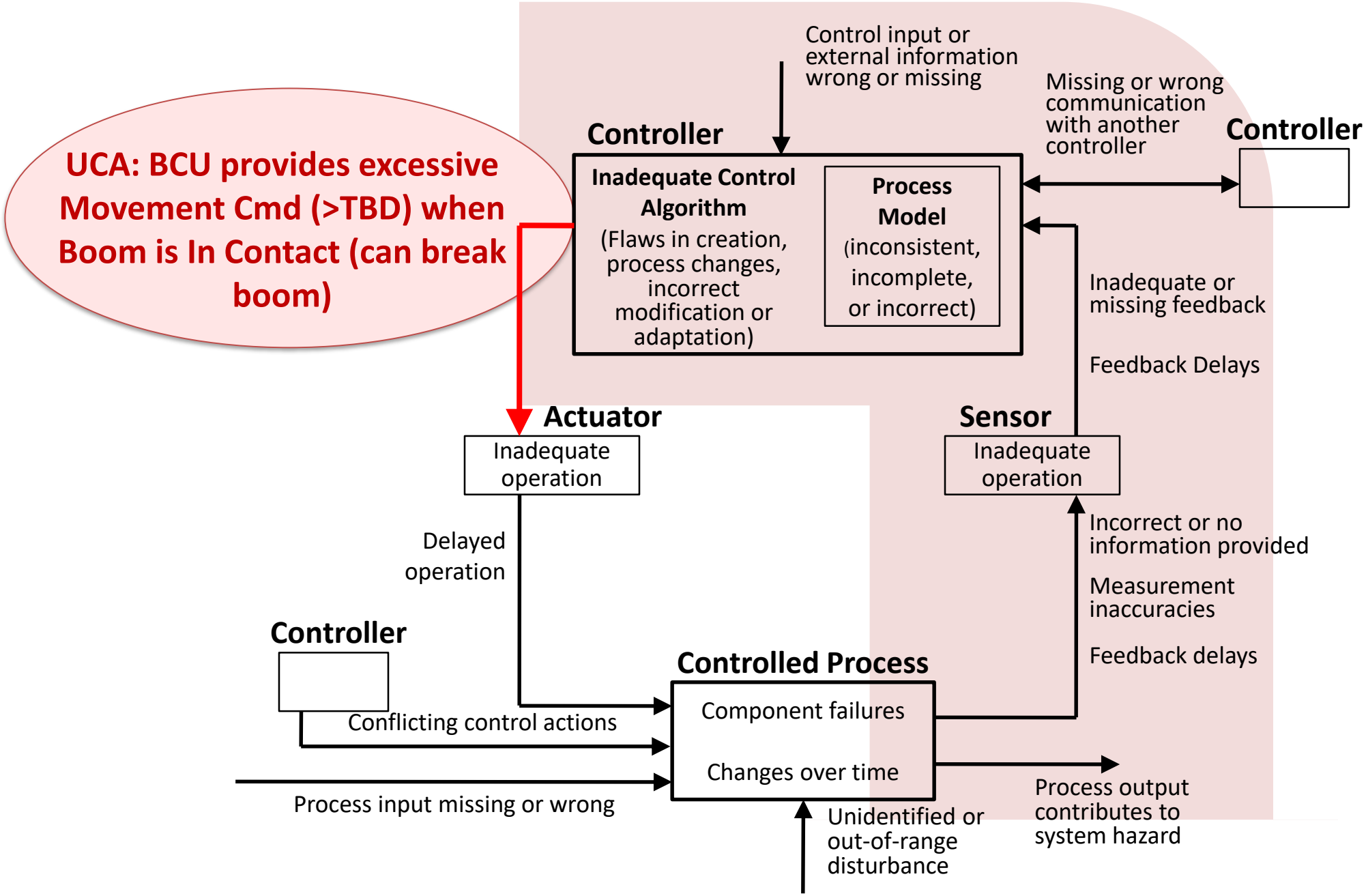
Please contact JThomas4@MIT.EDU with any questions!



(Leveson and Thomas, 2018)

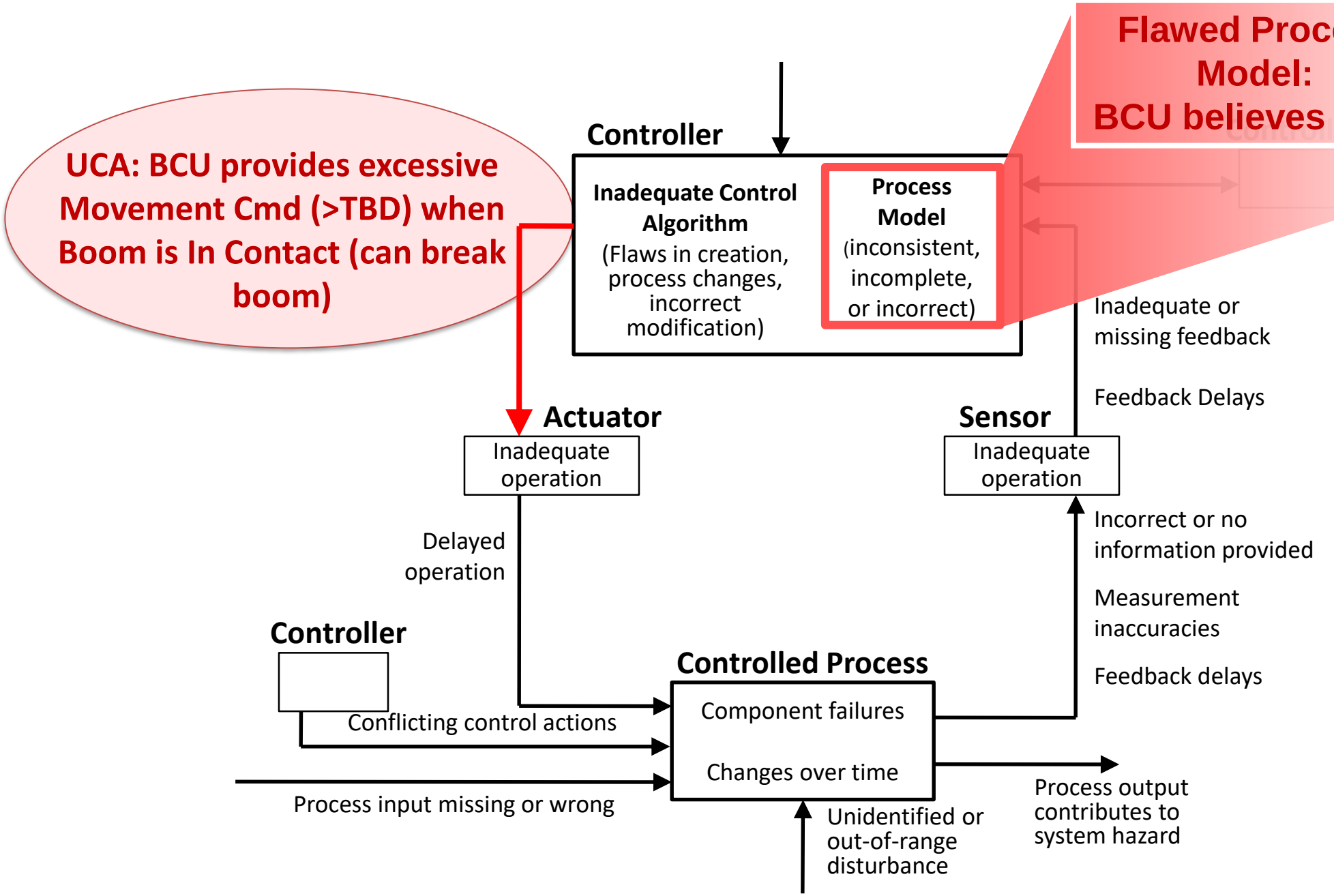
STPA Step 4. A: Potential causes of UCAs

Generic Control Loop



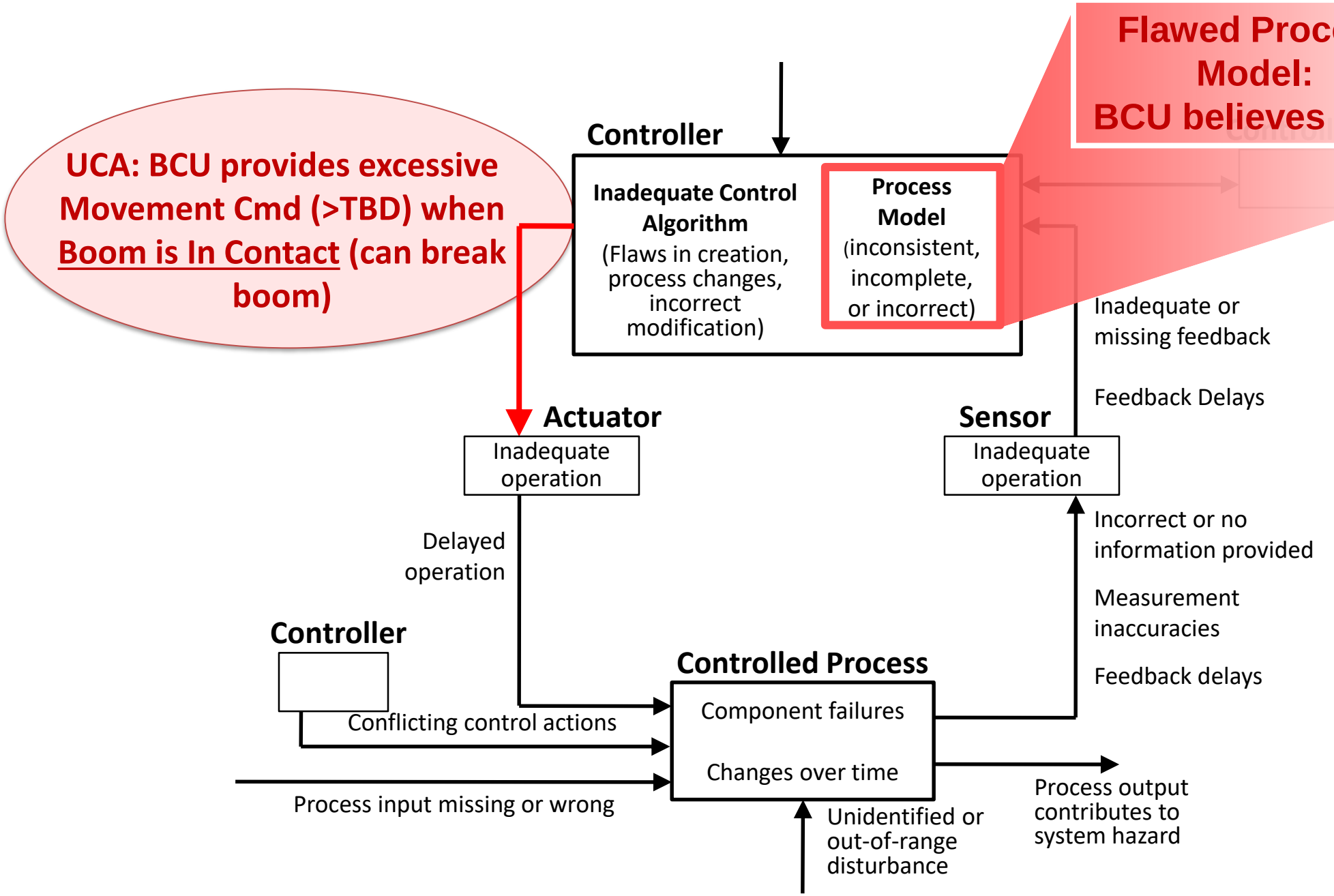
STPA Step 4. A: Potential causes of UCAs

Generic Control Loop



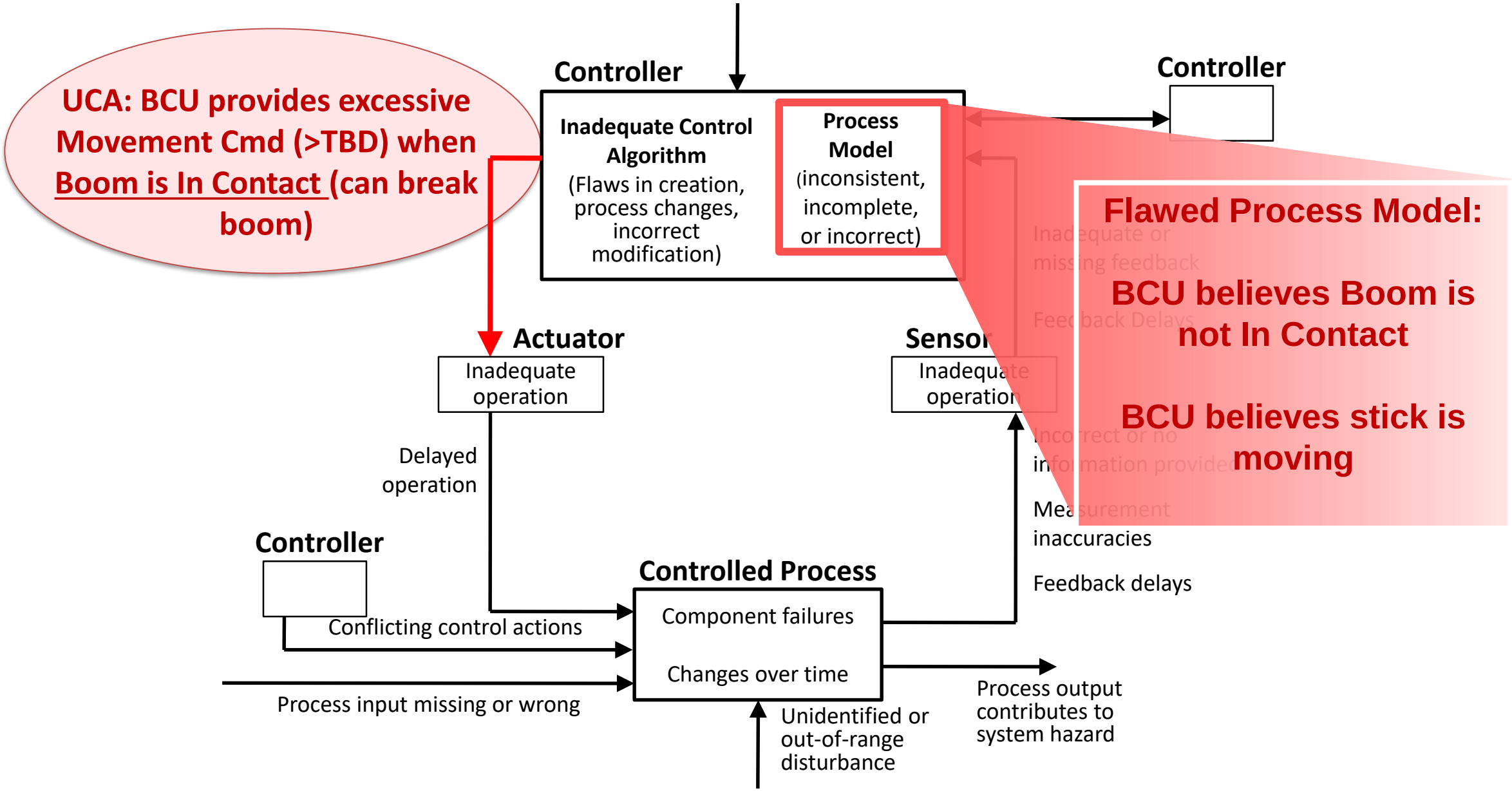
STPA Step 4. A: Potential causes of UCAs

Generic Control Loop



STPA Step 4. A: Potential causes of UCAs

Generic Control Loop

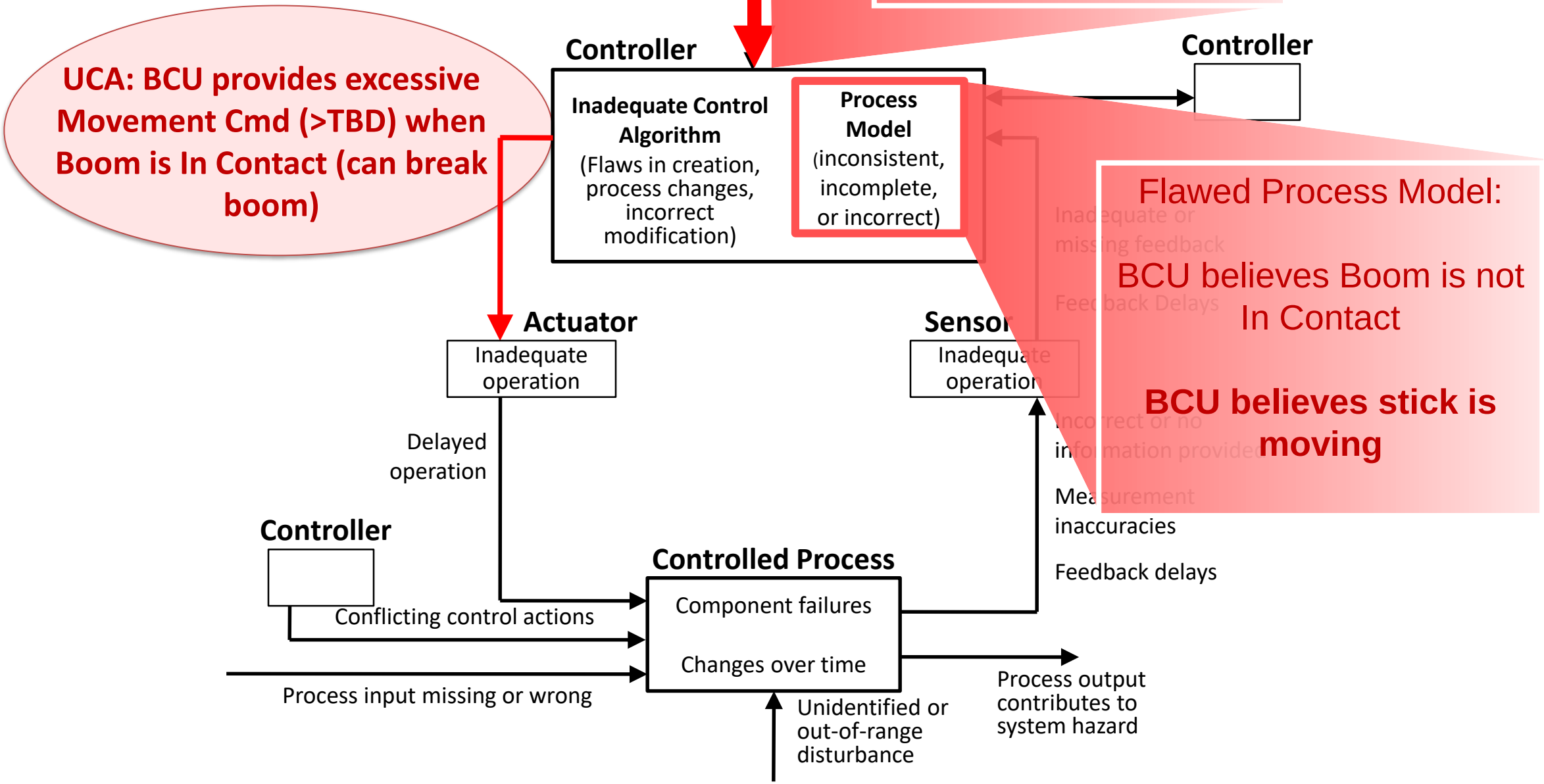


STPA Step 4. A: Potential causes of UCAs

Generic Control Loop

Operator sends manual movement command when Boom is In contact

UCA: BCU provides excessive Movement Cmd (>TBD) when Boom is In Contact (can break boom)



Flawed Process Model:

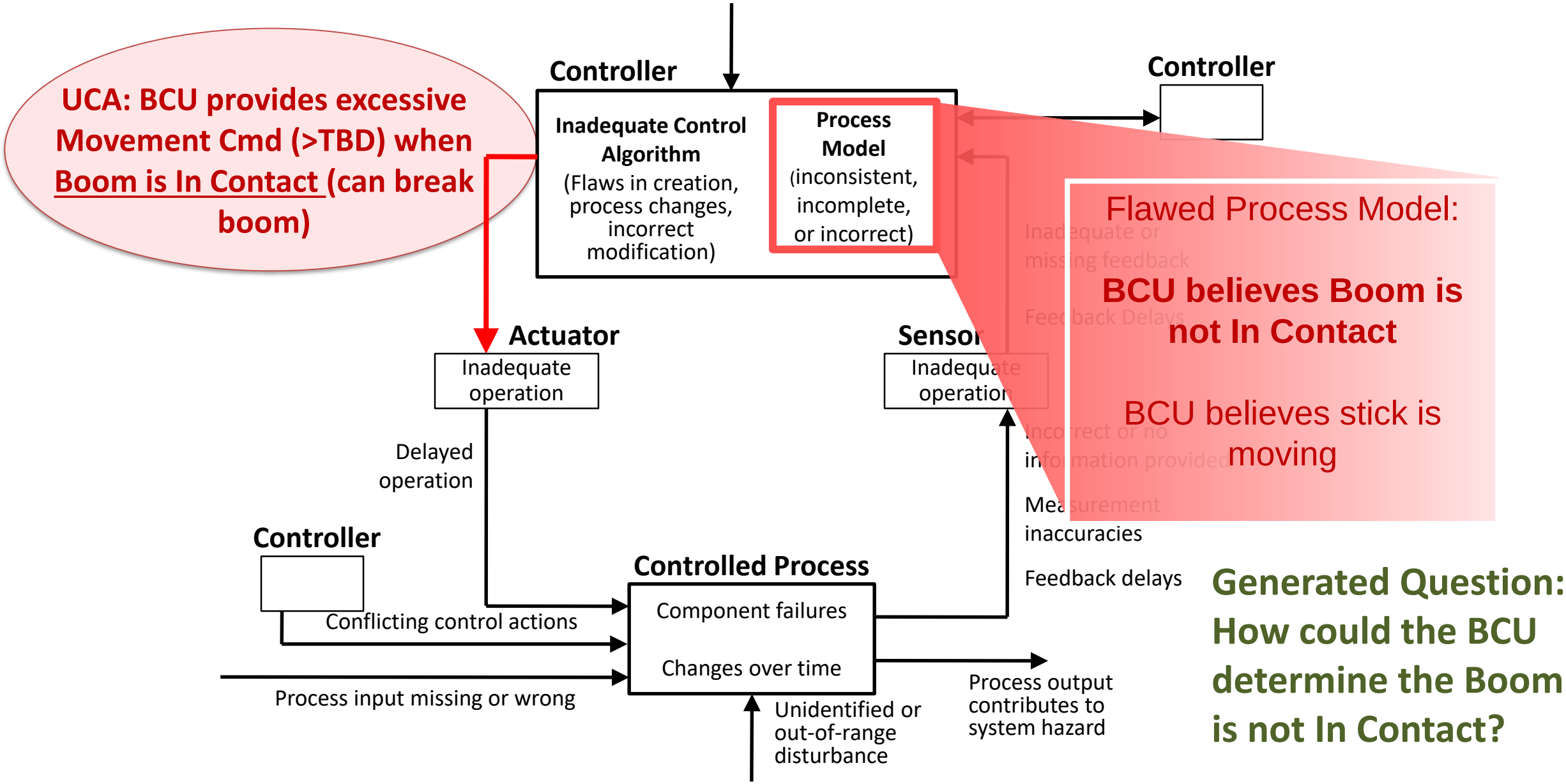
BCU believes Boom is not In Contact

BCU believes stick is moving

Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. A: Potential causes of UCAs

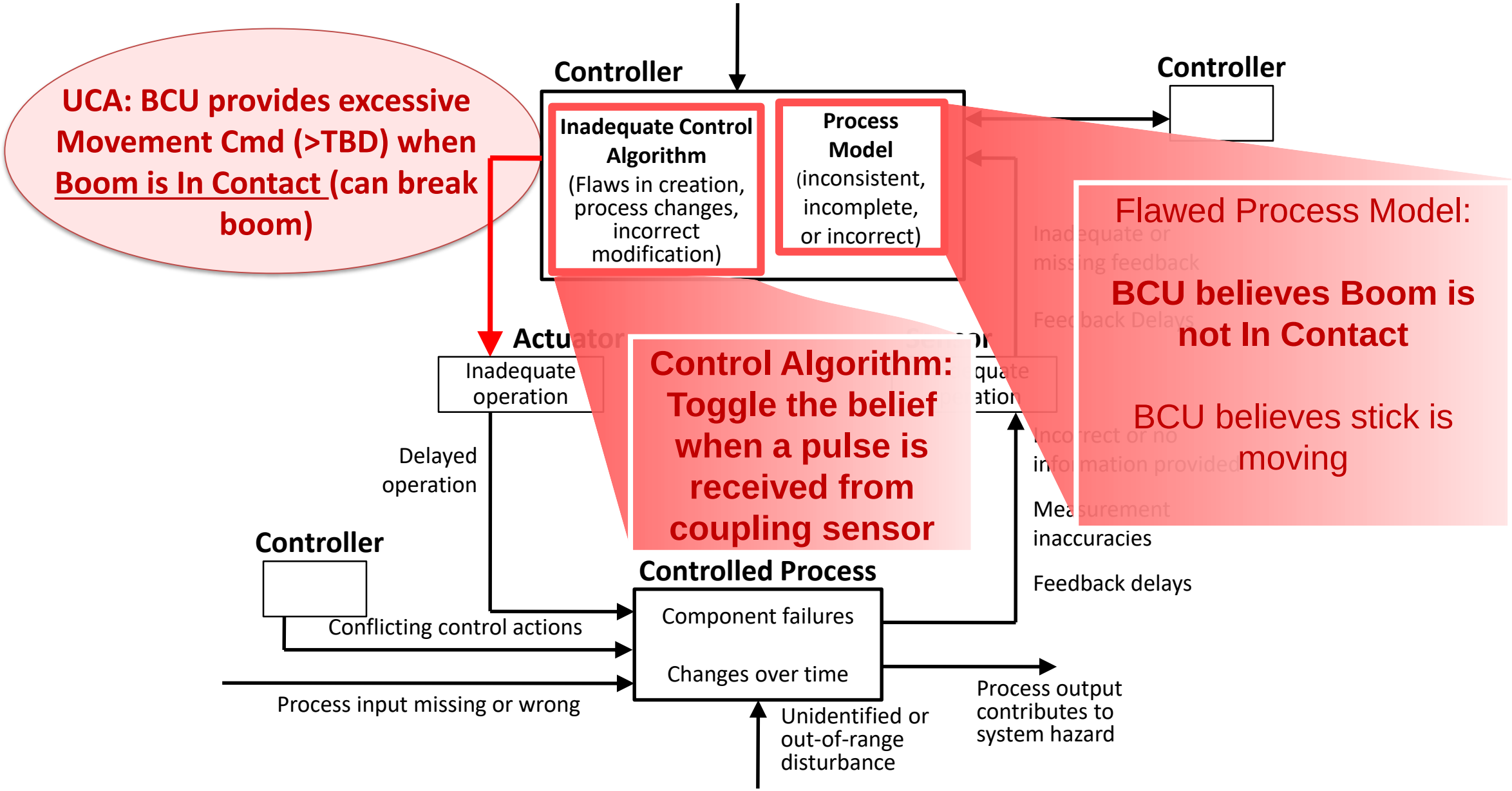
Generic Control Loop



Please contact JThomas4@MIT.EDU with any questions!

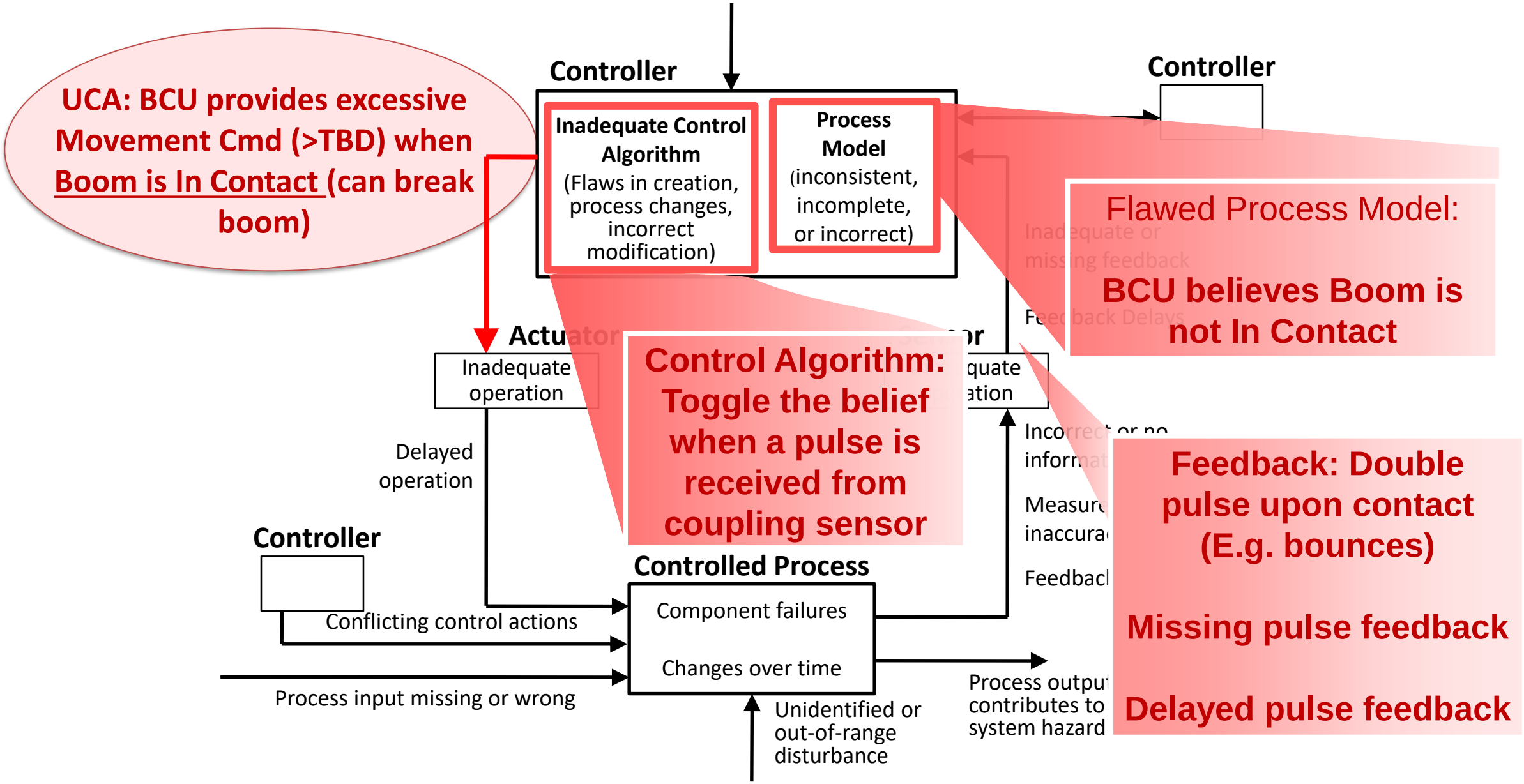
STPA Step 4. A: Potential causes of UCAs

Generic Control Loop



STPA Step 4. A: Potential causes of UCAs

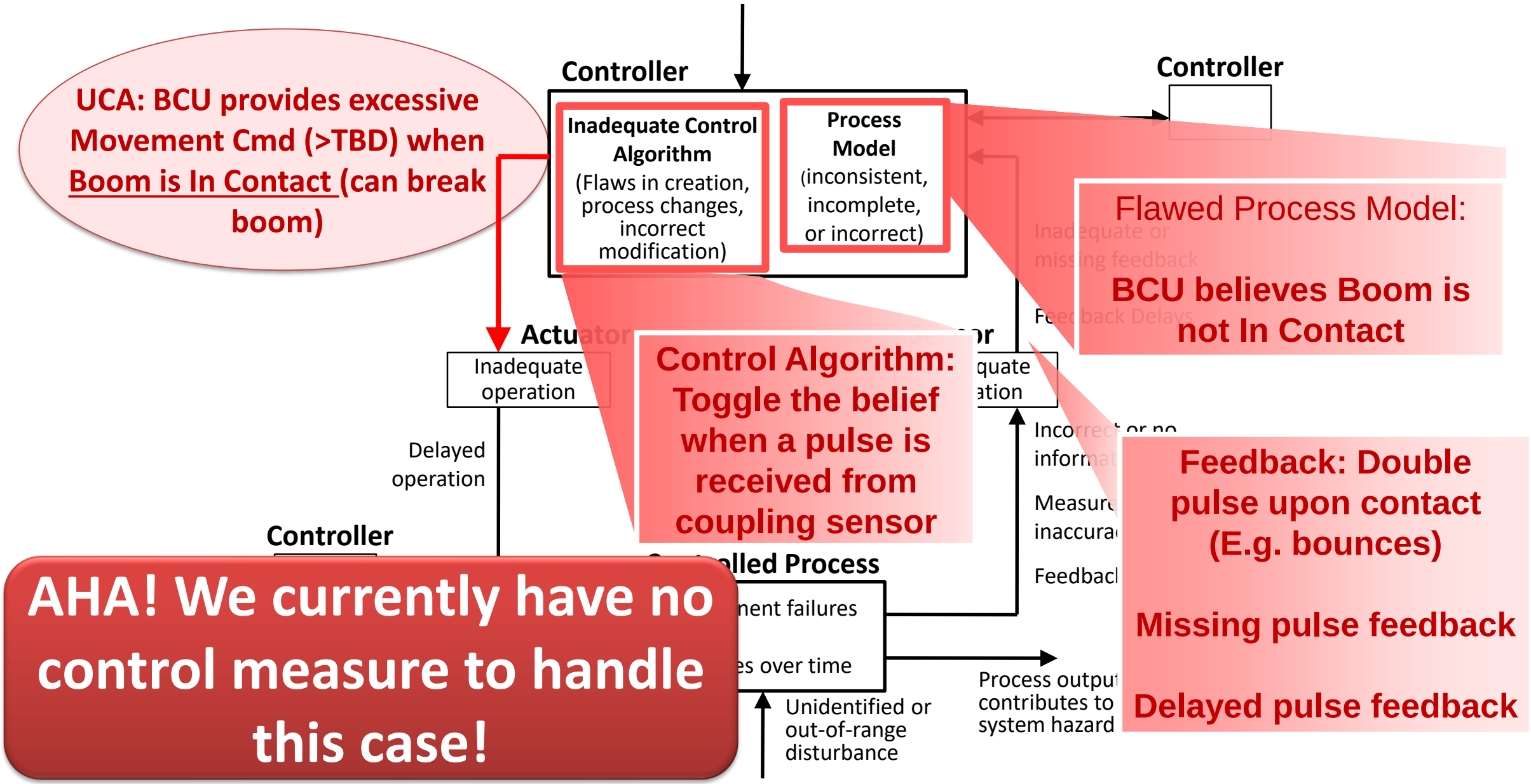
Generic Control Loop



Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. A: Potential causes of UCAs

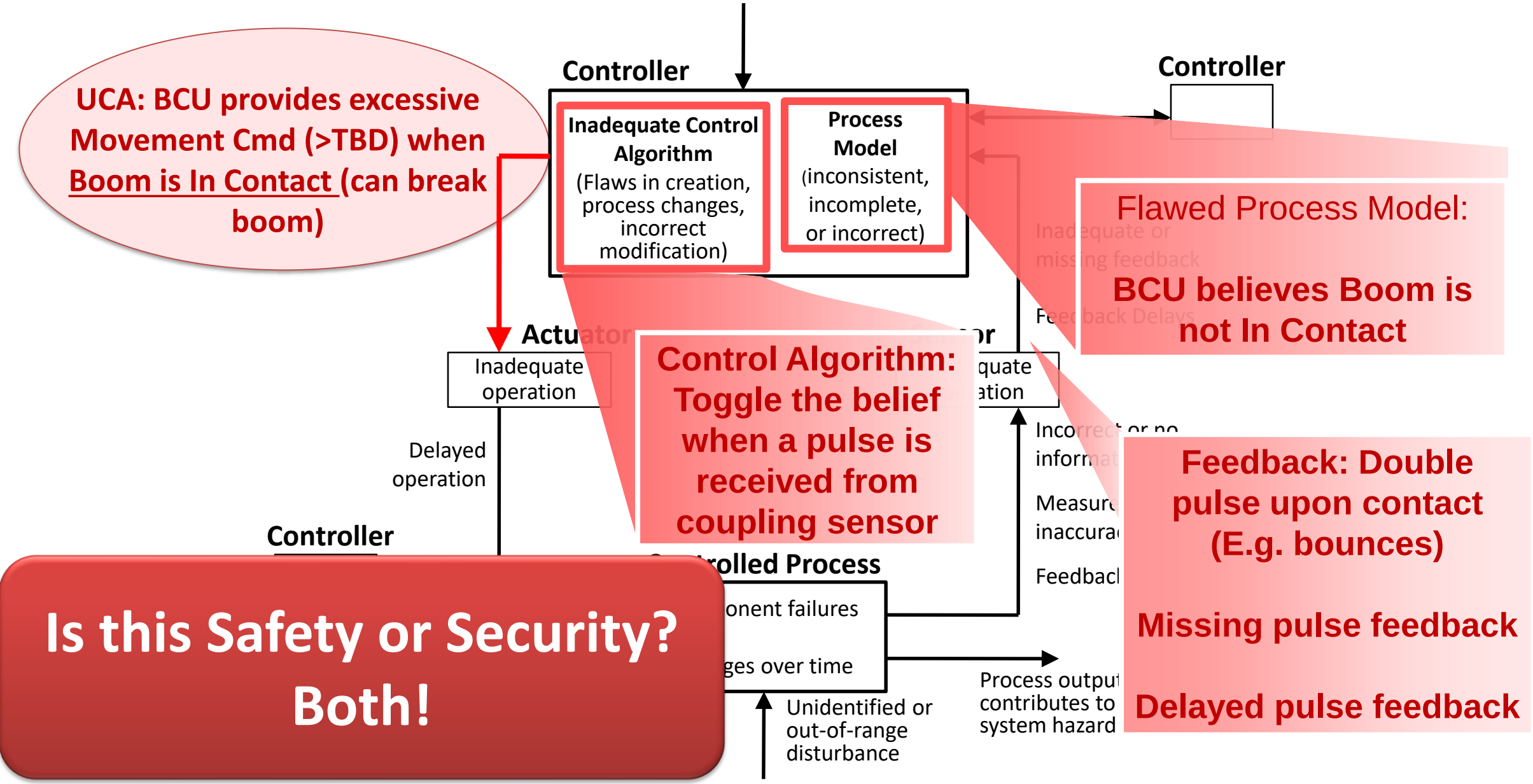
Generic Control Loop



Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. A: Potential causes of UCAs

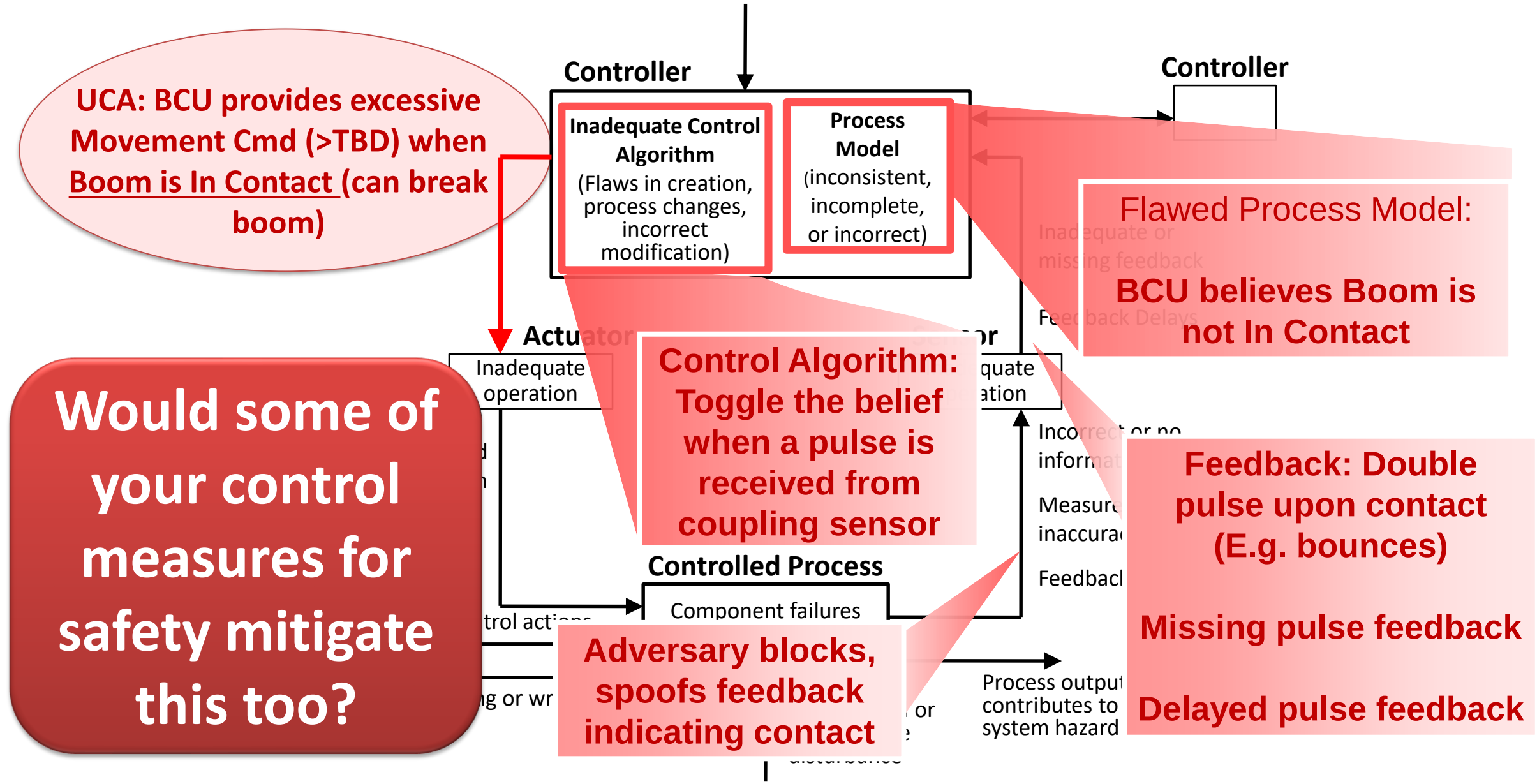
Generic Control Loop



Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. A: Potential causes of UCAs

Generic Control Loop

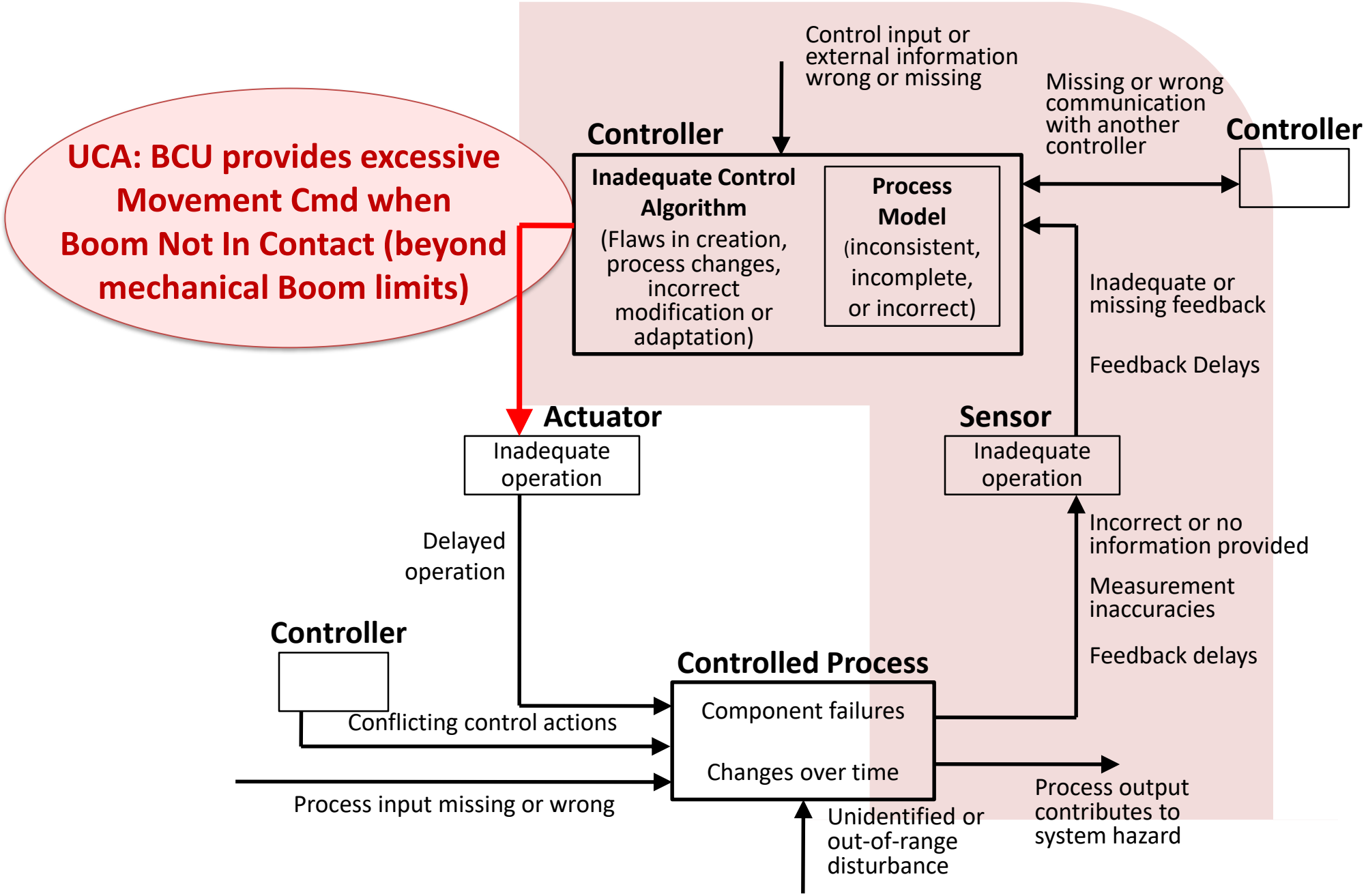


Please contact JThomas4@MIT.EDU with any questions!

Let’s try a different UCA

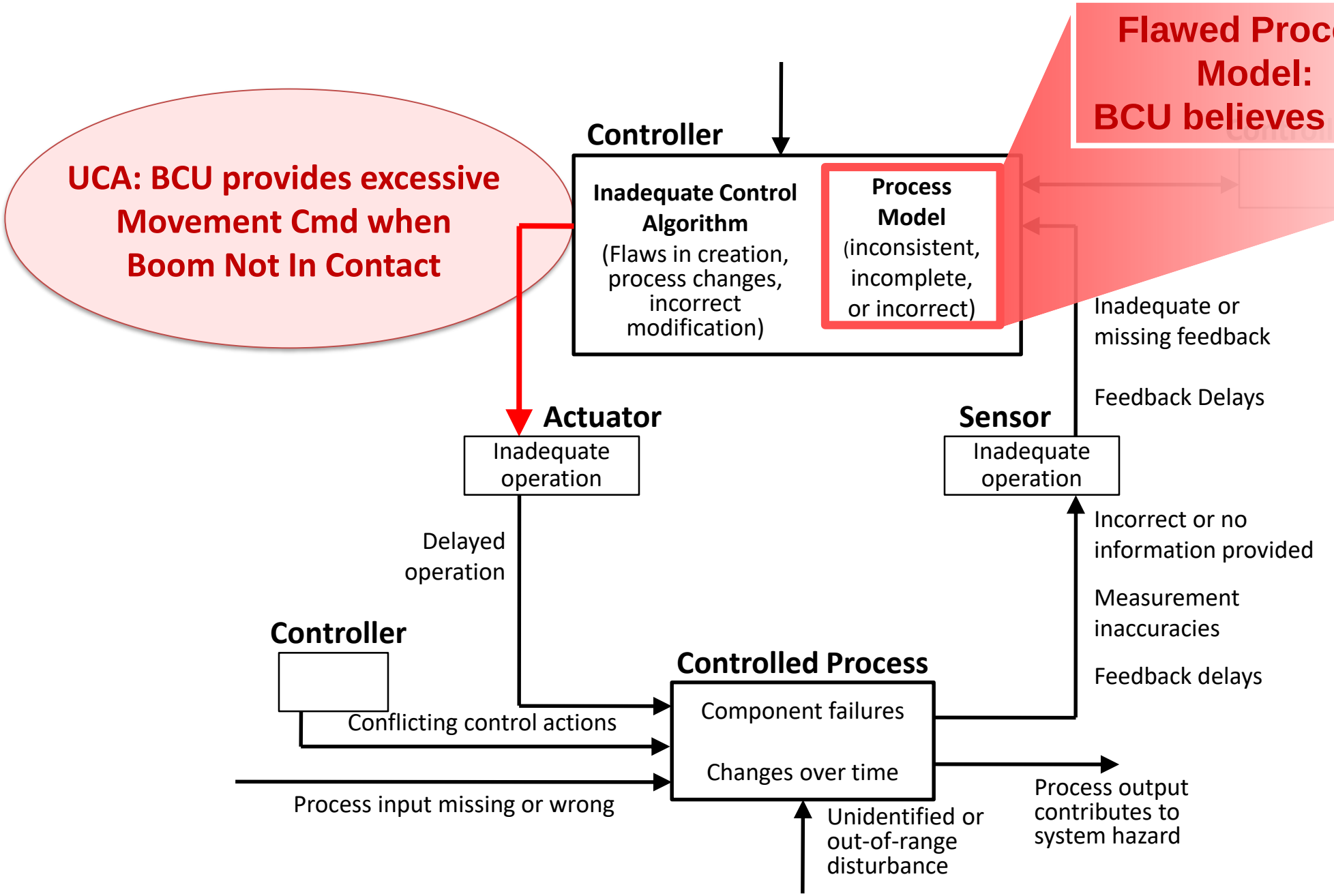
STPA Step 4. A: Potential causes of UCAs

Generic Control Loop



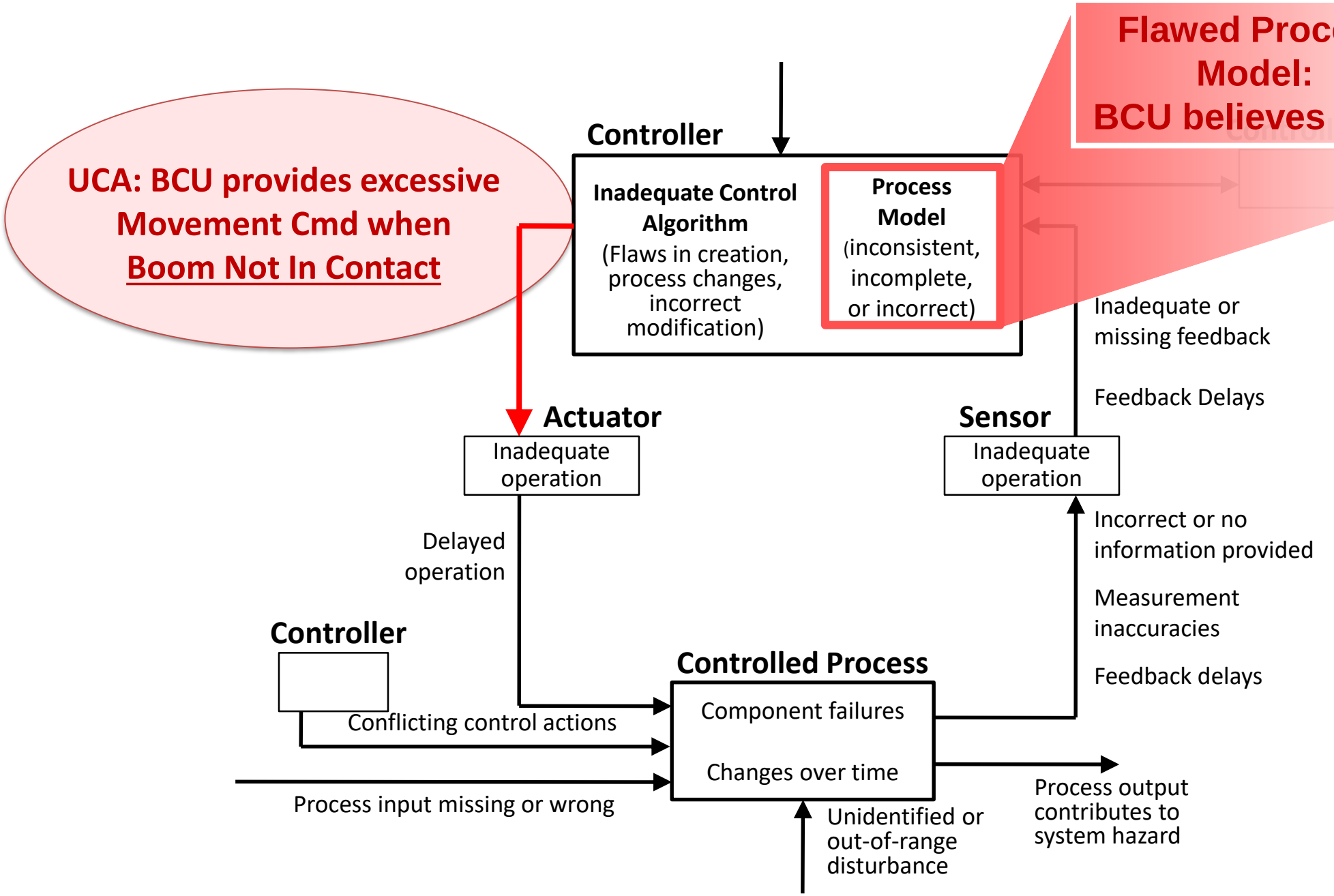
STPA Step 4. A: Potential causes of UCAs

Generic Control Loop



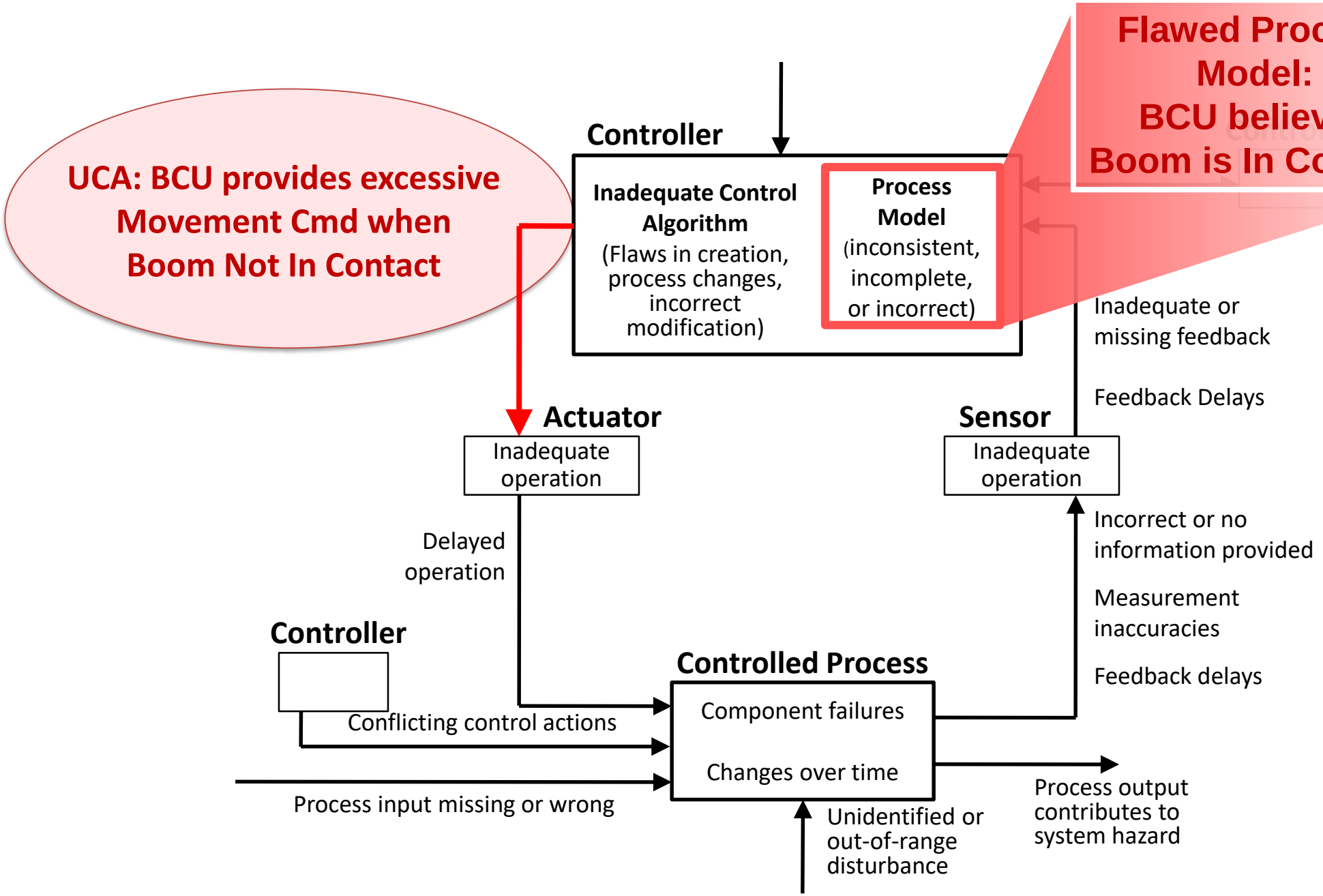
STPA Step 4. A: Potential causes of UCAs

Generic Control Loop



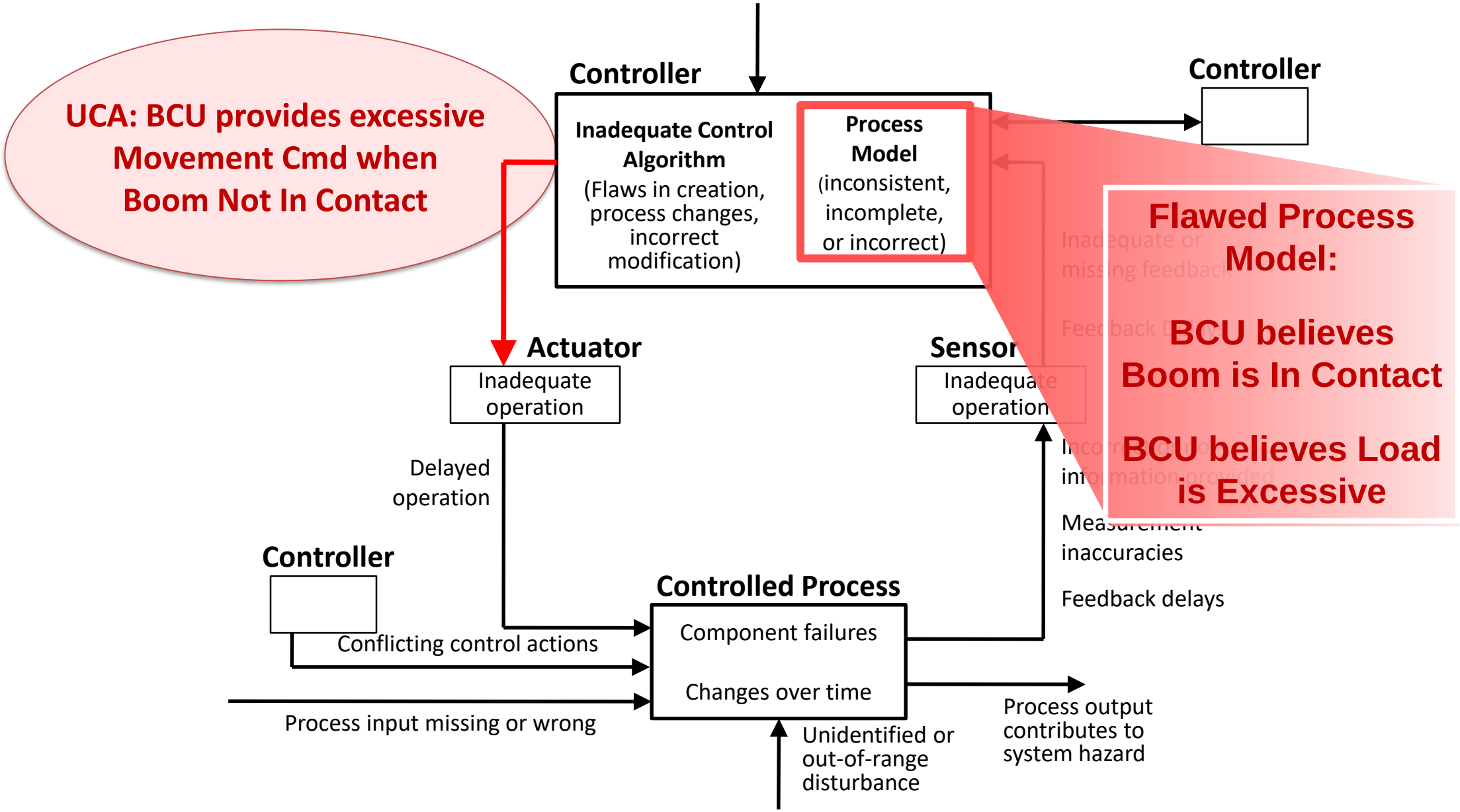
STPA Step 4. A: Potential causes of UCAs

Generic Control Loop



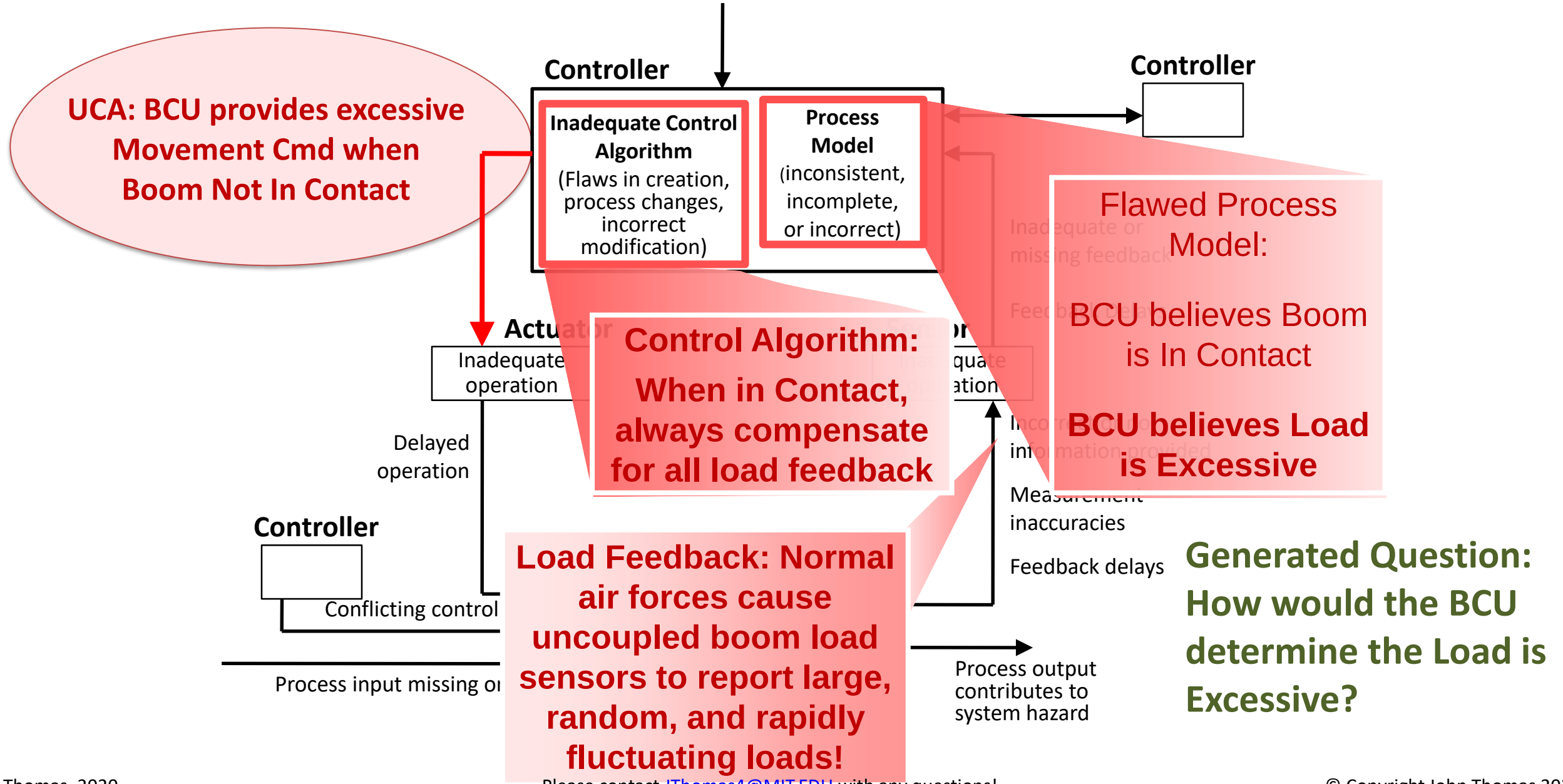
STPA Step 4. A: Potential causes of UCAs

Generic Control Loop



STPA Step 4. A: Potential causes of UCAs

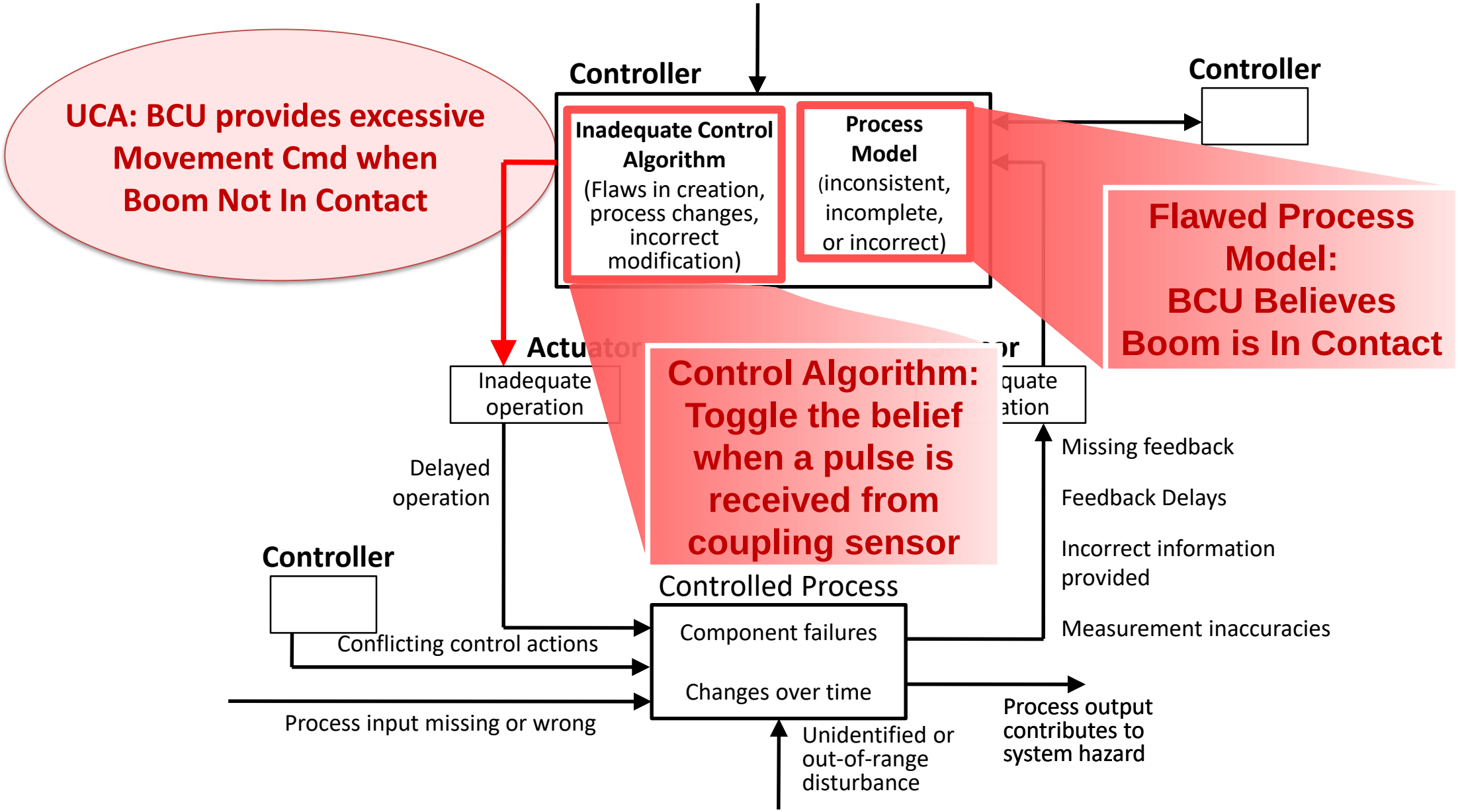
Generic Control Loop



Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. A: Potential causes of UCAs

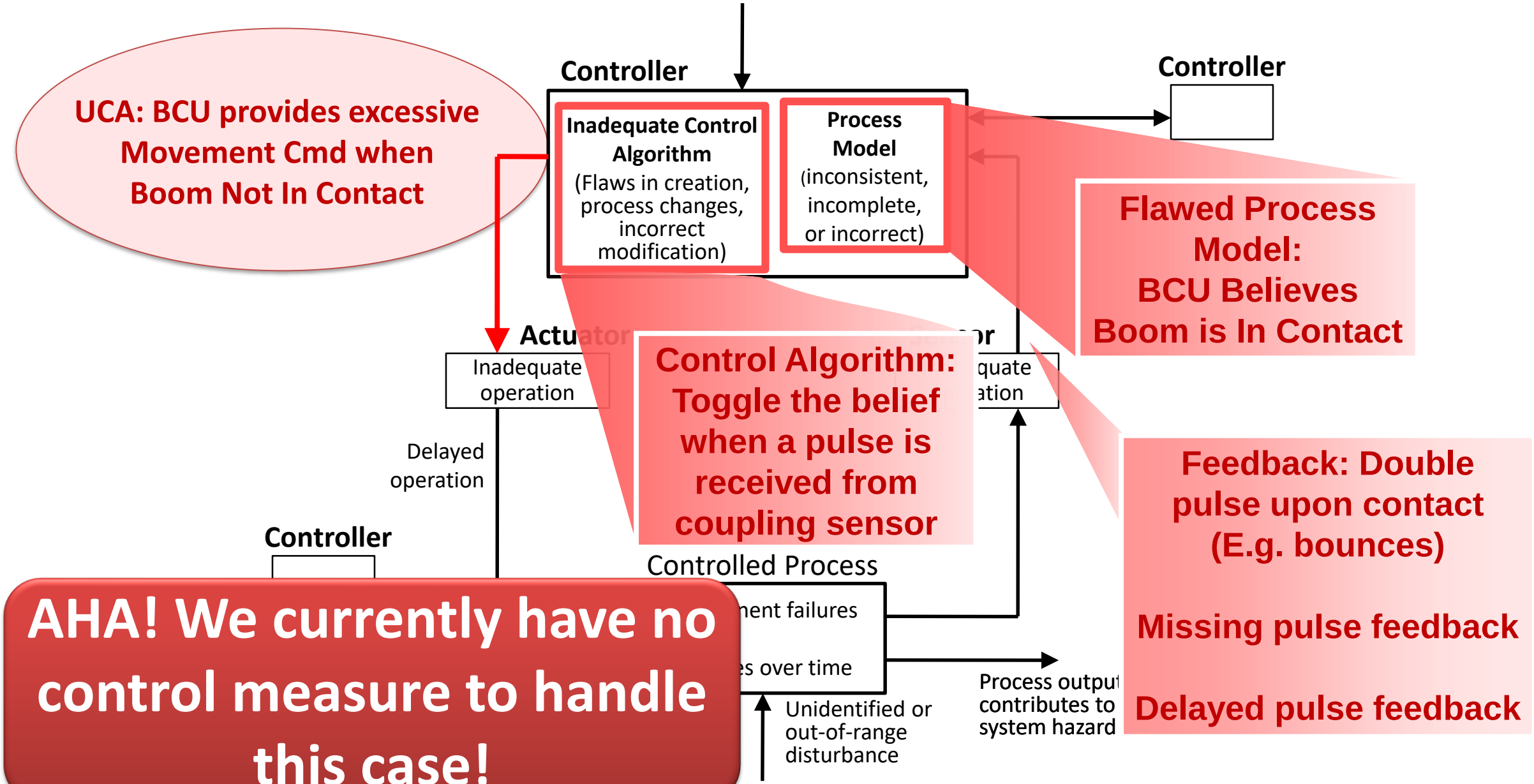
Generic Control Loop



Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. A: Potential causes of UCAs

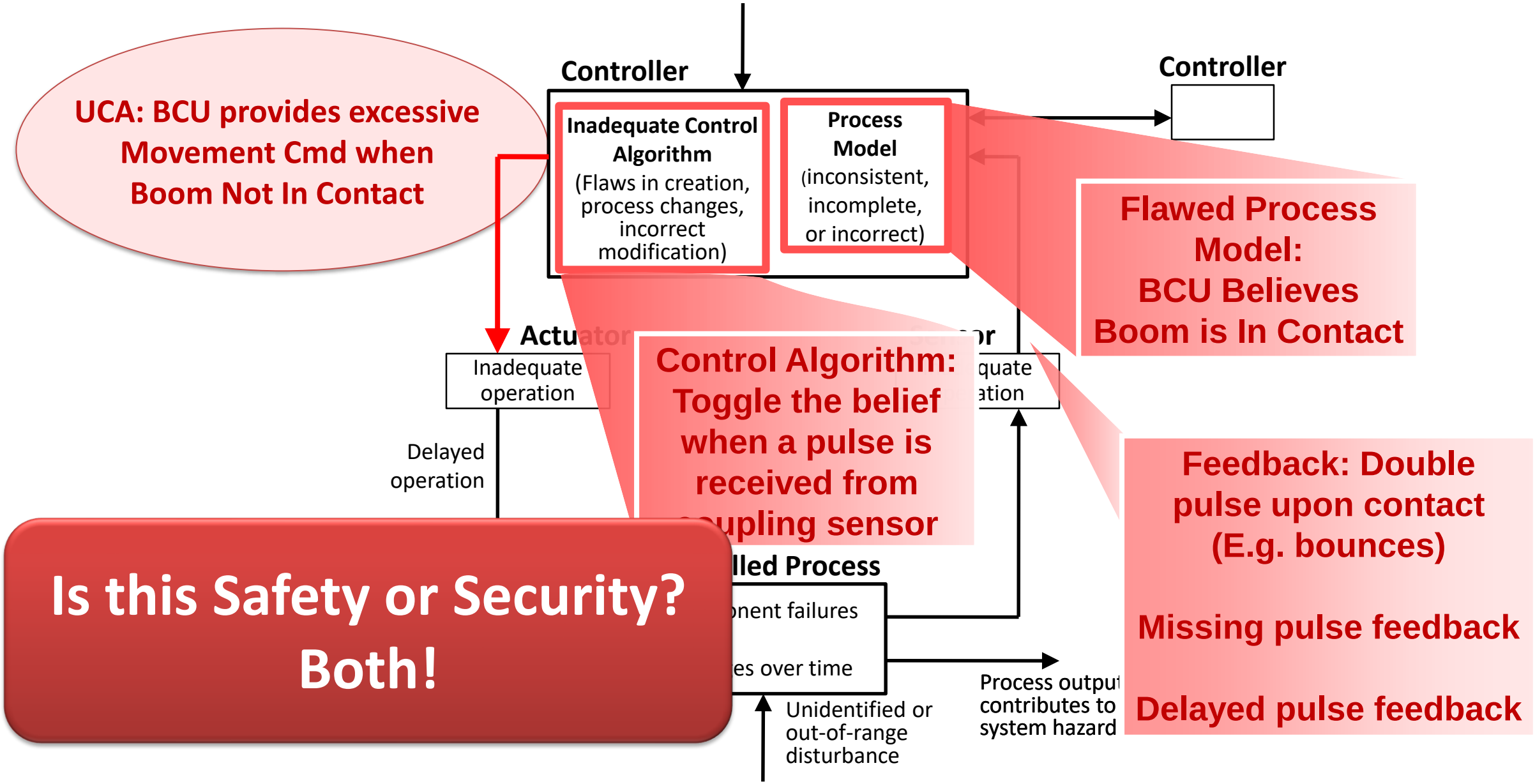
Generic Control Loop



Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. A: Potential causes of UCAs

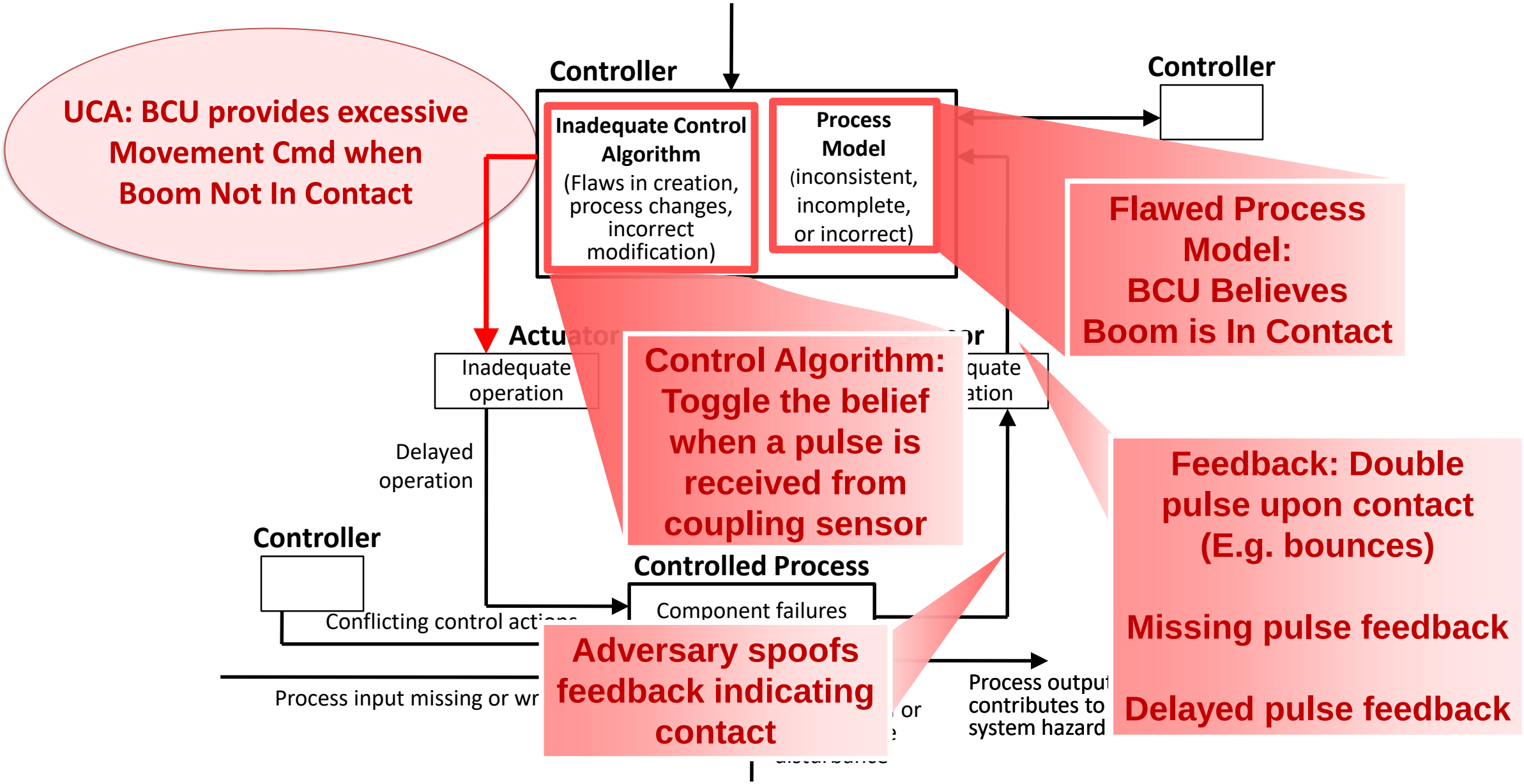
Generic Control Loop



Please contact JThomas4@MIT.EDU with any questions!

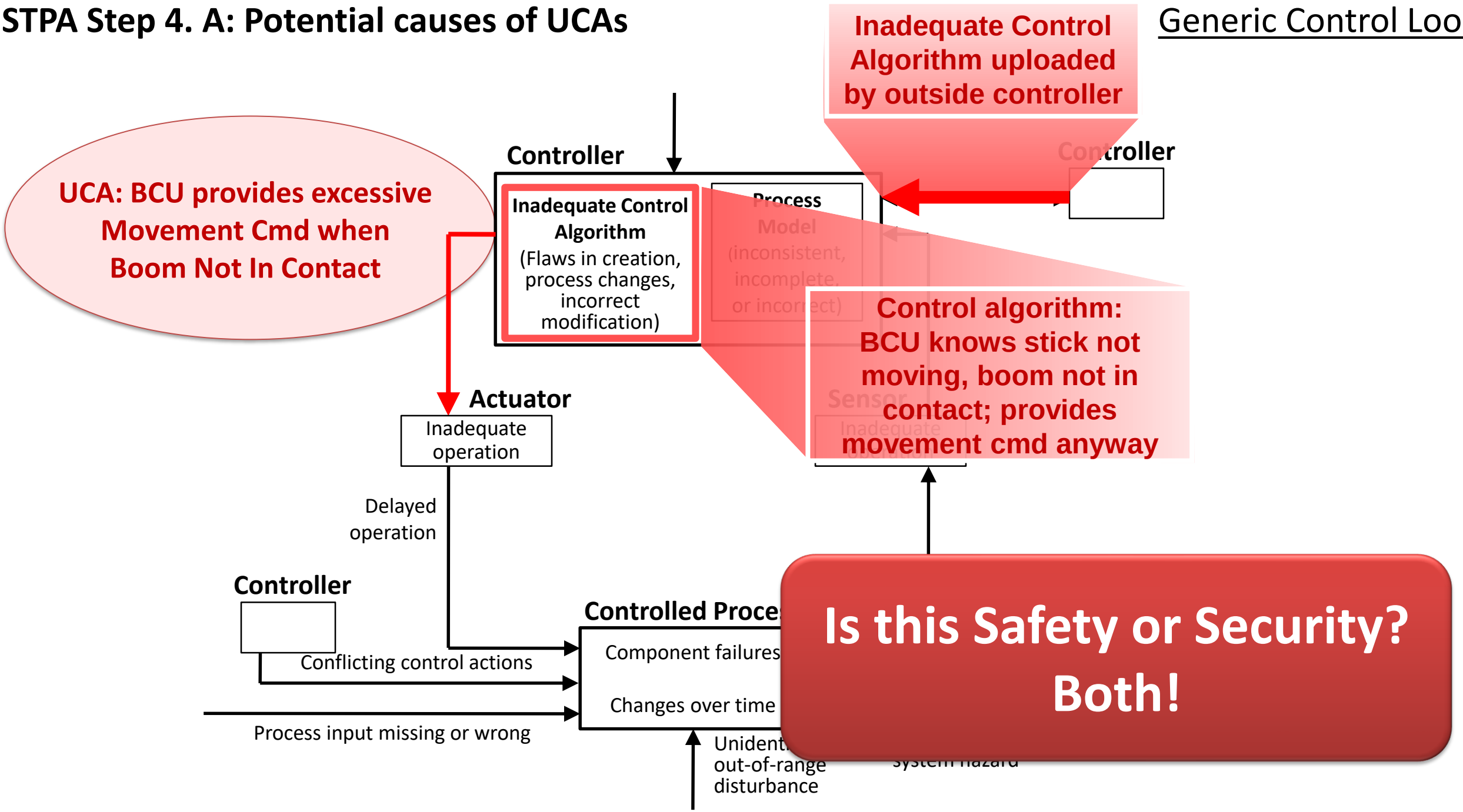
STPA Step 4. A: Potential causes of UCAs

Generic Control Loop



STPA Step 4. A: Potential causes of UCAs

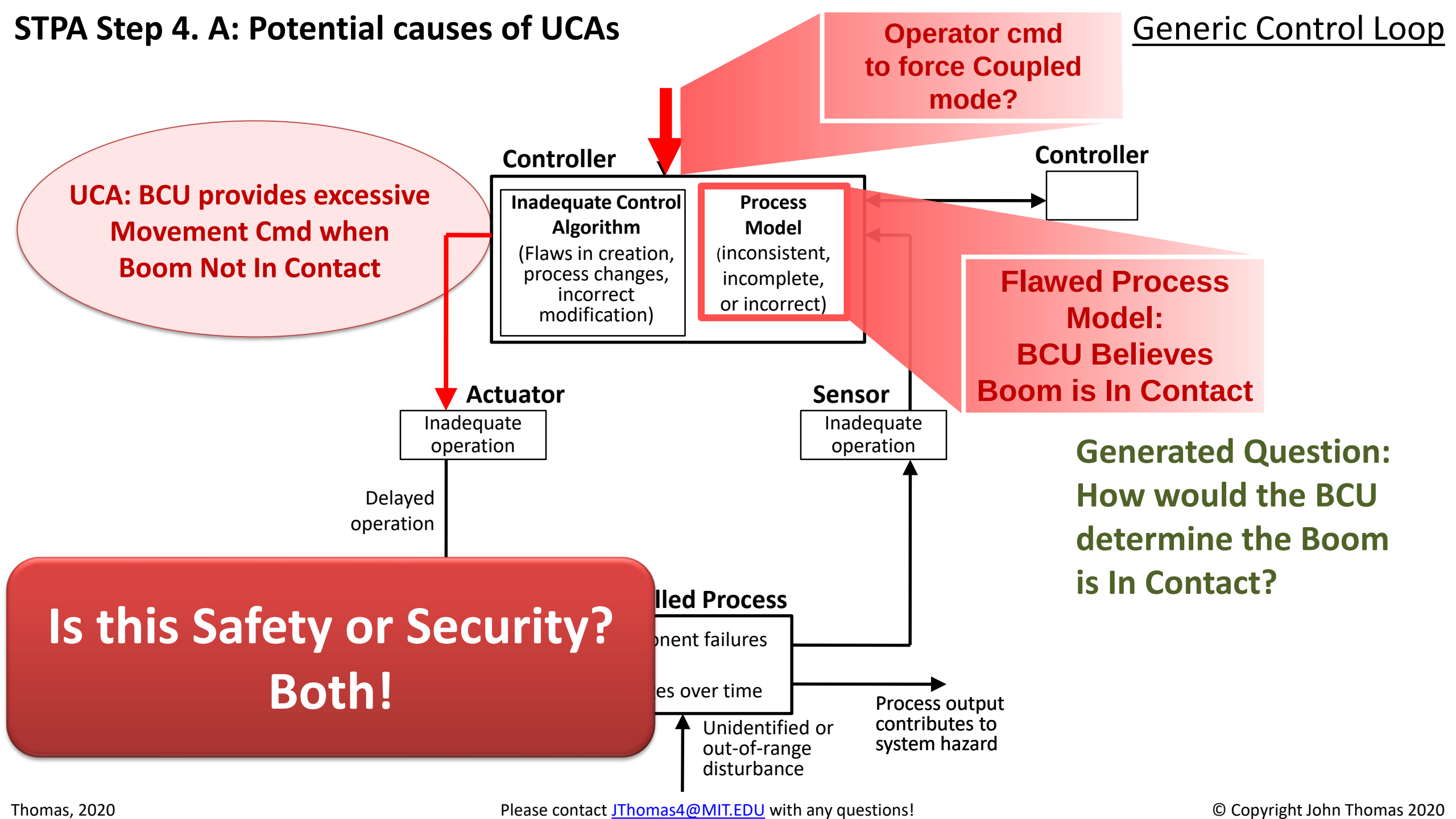
Generic Control Loop



Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. A: Potential causes of UCAs

Generic Control Loop



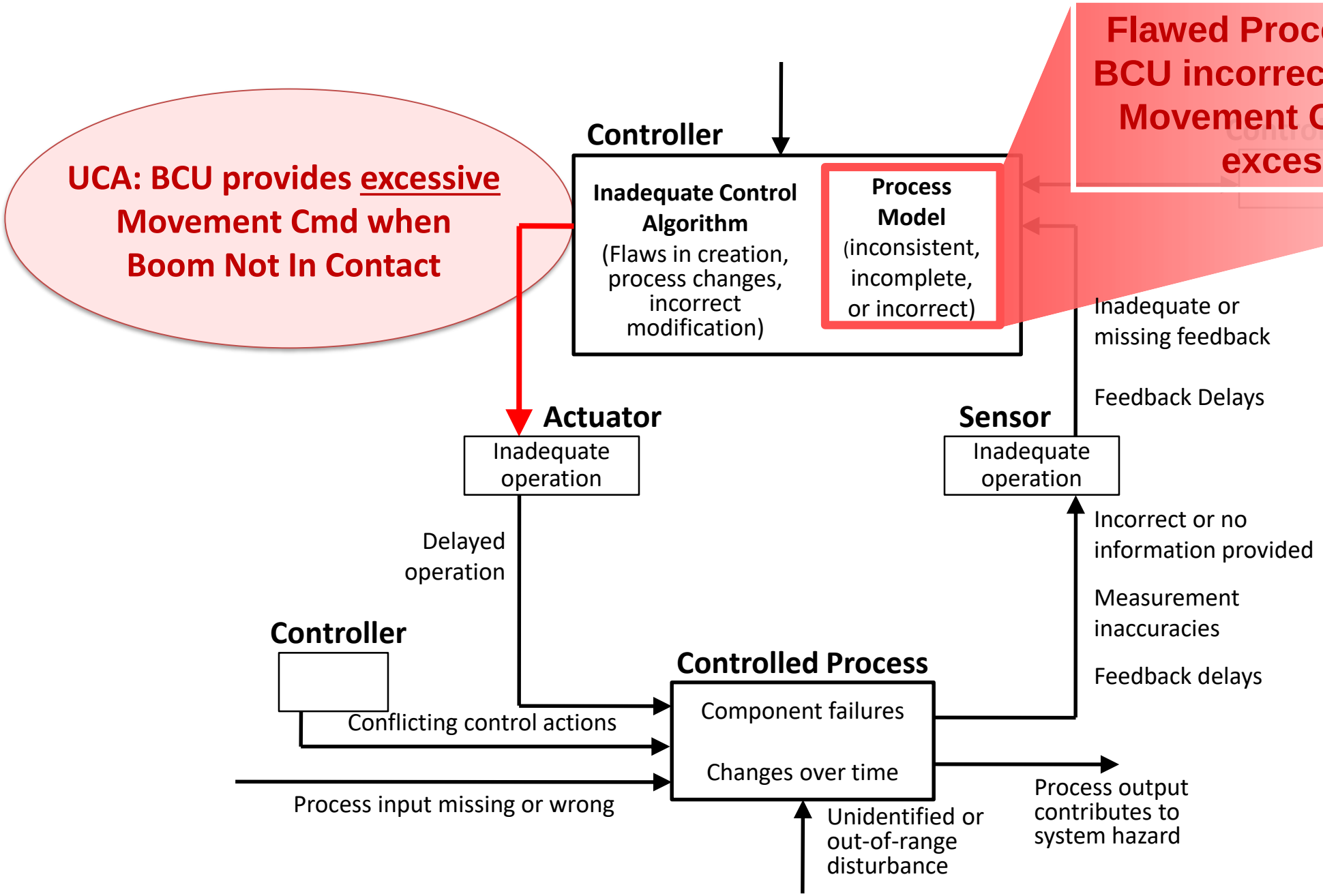
Generated Question: How would the BCU determine the Boom is In Contact?

Is this Safety or Security? Both!

Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. A: Potential causes of UCAs

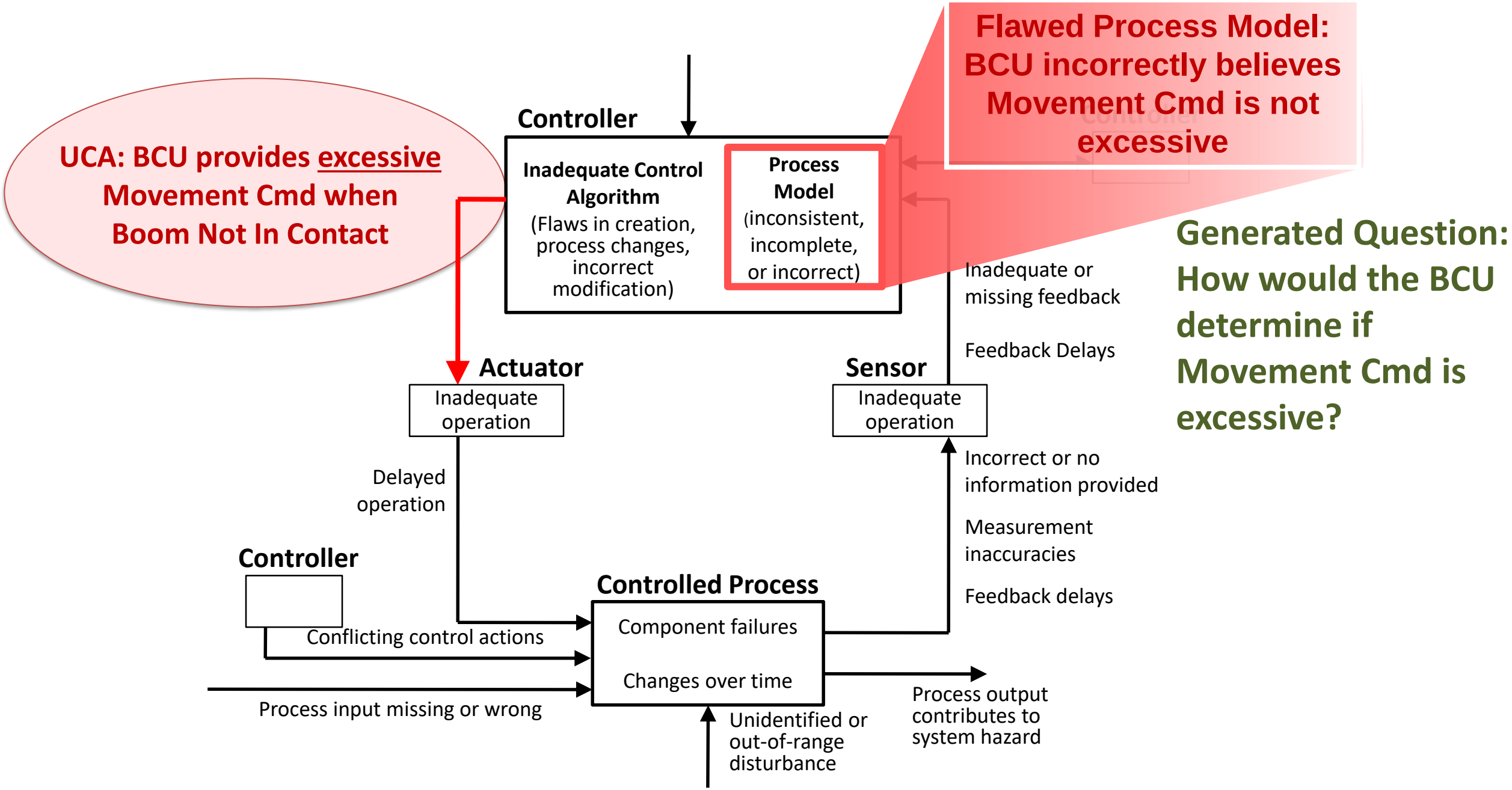
Generic Control Loop



Please contact JThomas4@MIT.EDU with any questions!

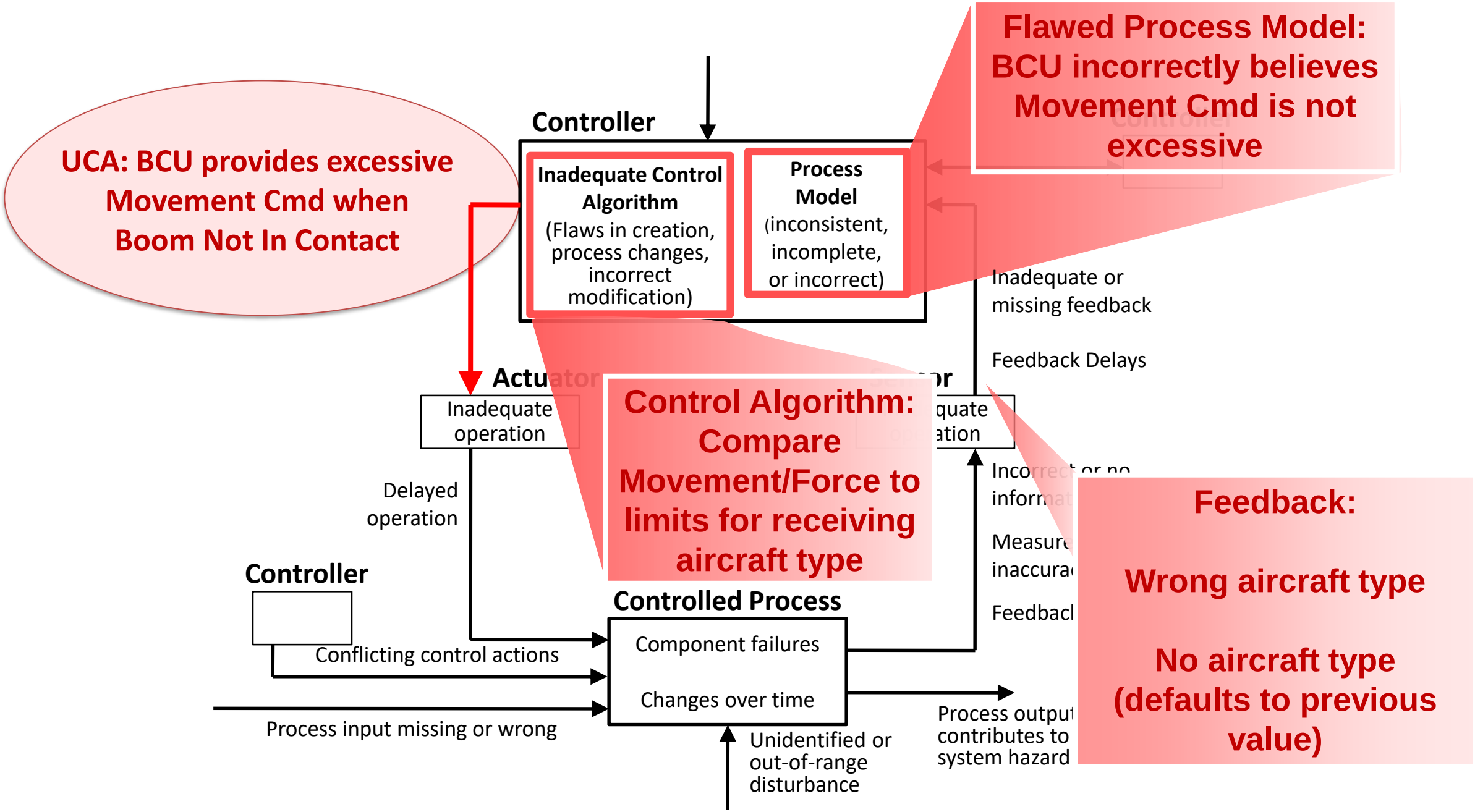
STPA Step 4. A: Potential causes of UCAs

Generic Control Loop



STPA Step 4. A: Potential causes of UCAs

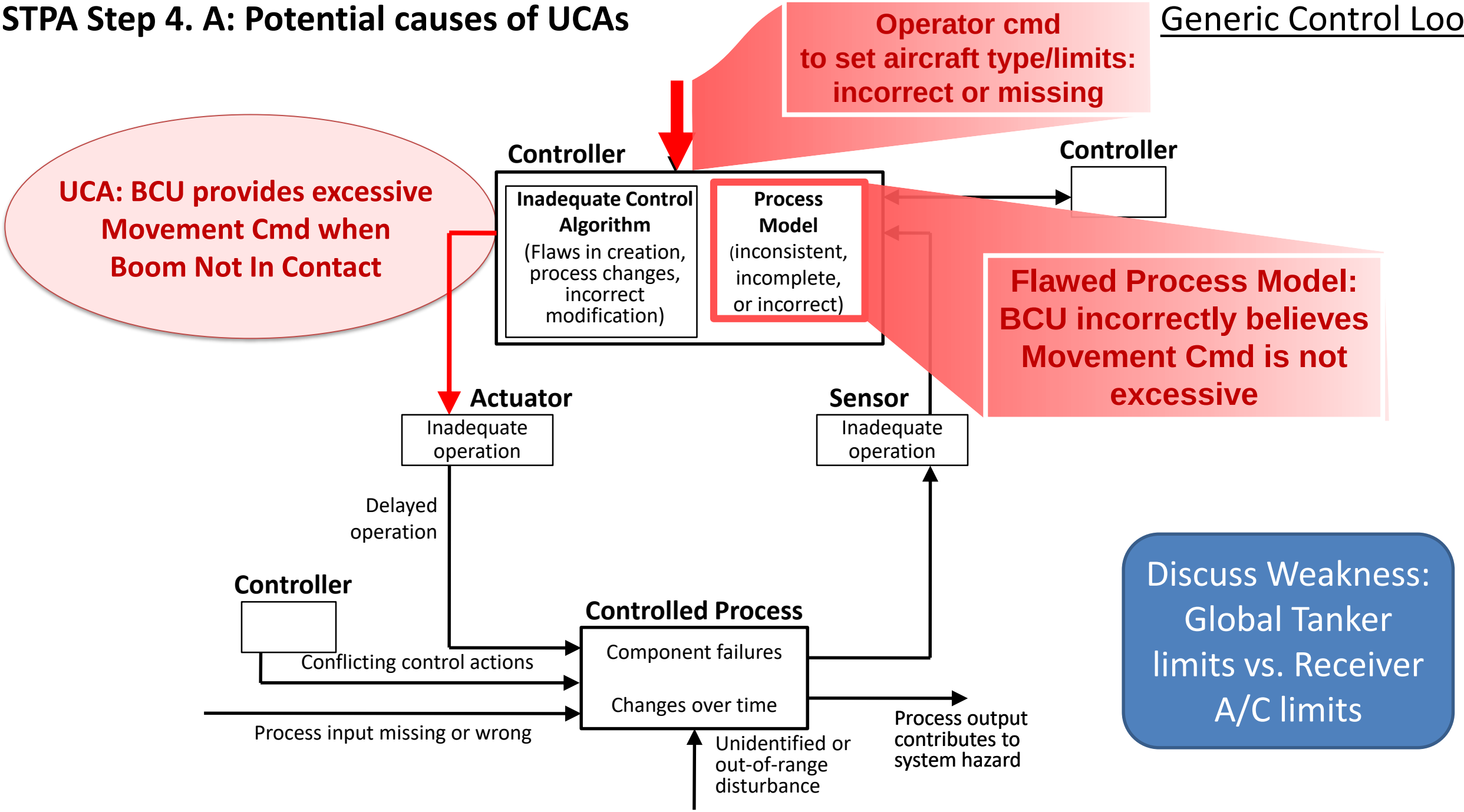
Generic Control Loop



Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. A: Potential causes of UCAs

Generic Control Loop



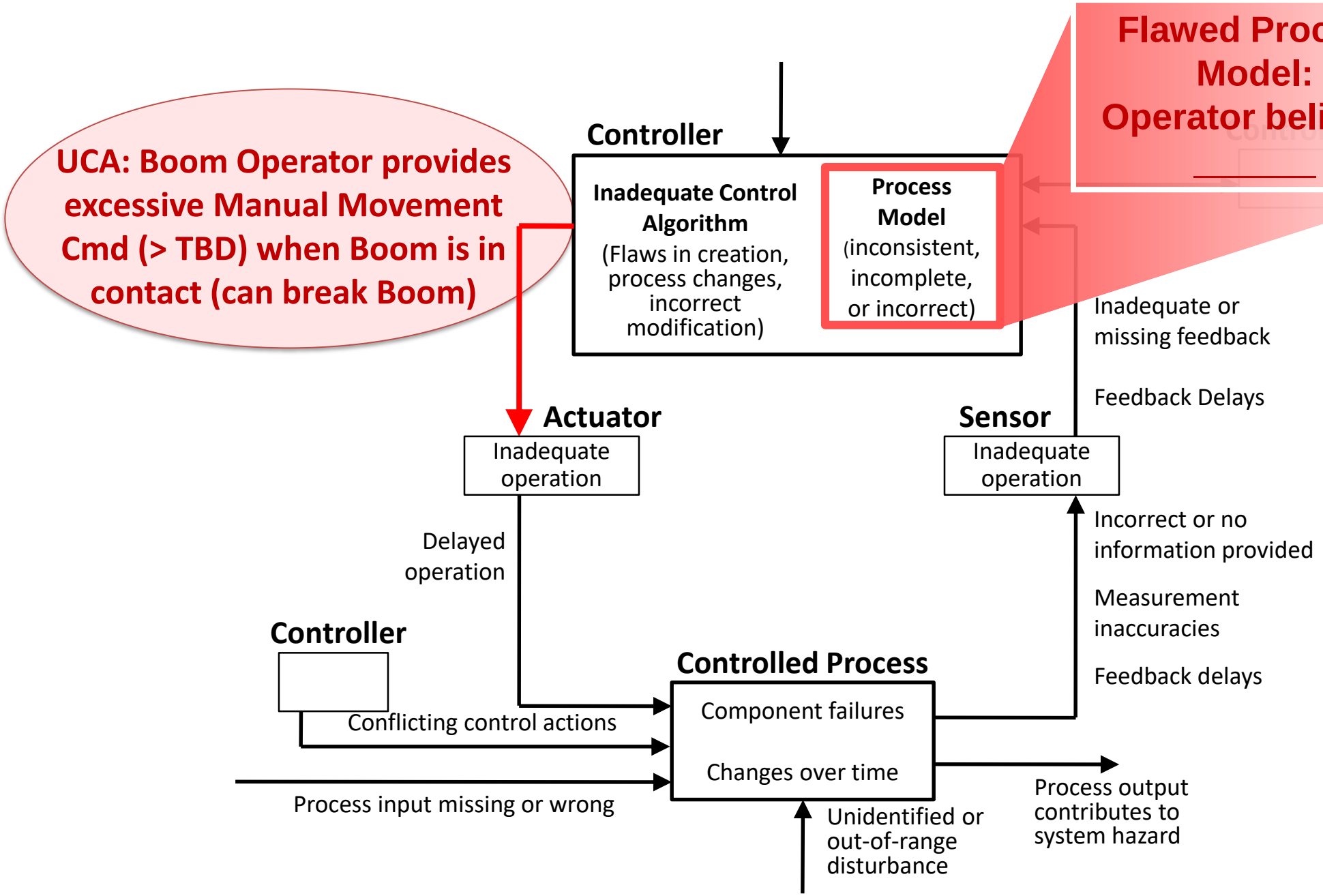
Please contact JThomas4@MIT.EDU with any questions!

Exercise Success!

Let’s look at Human Operator commands

STPA Step 4. A: Potential causes of UCAs

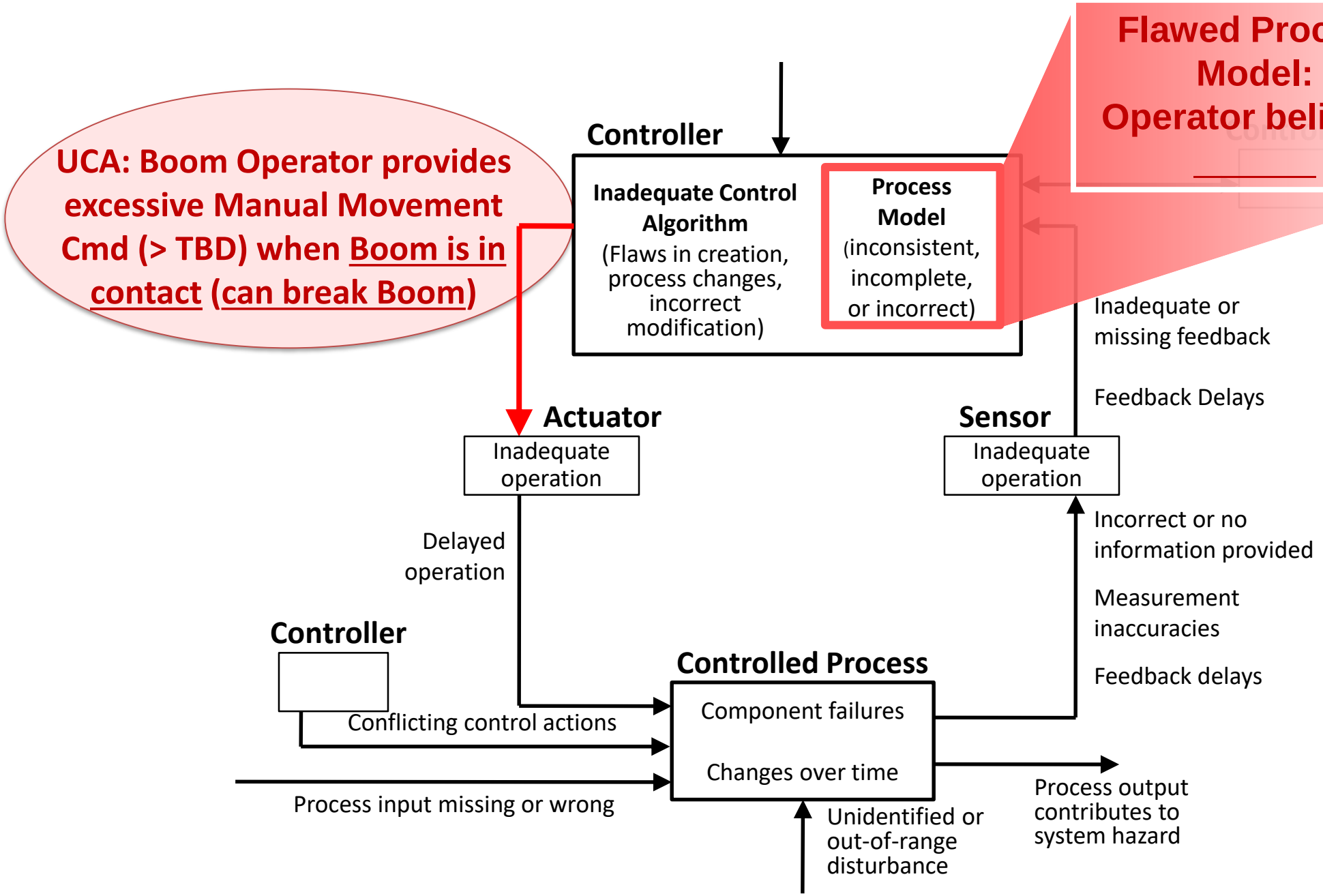
Generic Control Loop



Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. A: Potential causes of UCAs

Generic Control Loop

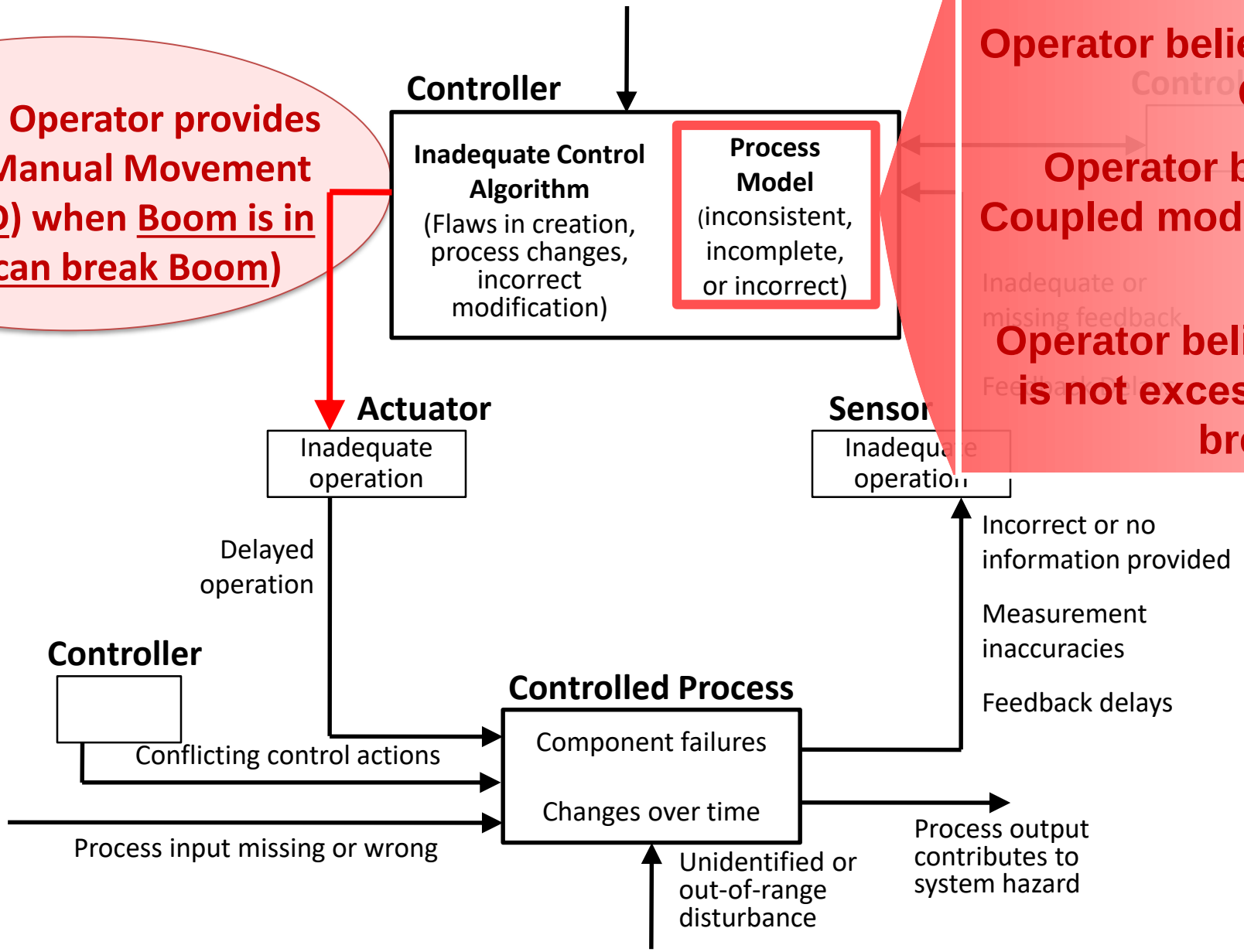


Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. A: Potential causes of UCAs

Generic Control Loop

UCA: Boom Operator provides excessive Manual Movement Cmd (> TBD) when Boom is in contact (can break Boom)



Flawed Process Models:

Operator believes Boom not yet In Contact

Operator believes BCU is in Coupled mode (will ignore manual cmds)

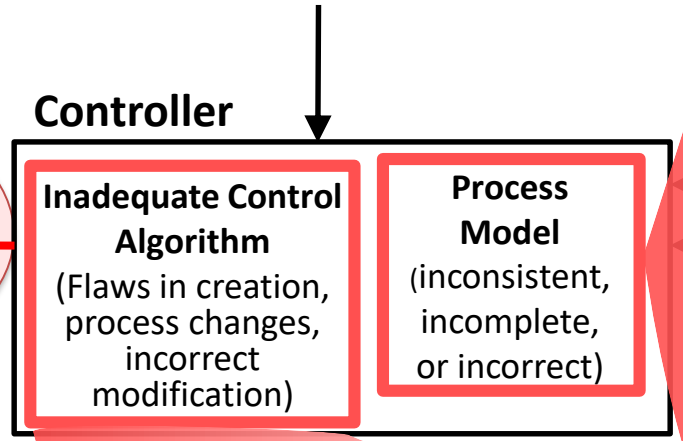
Operator believes the movement is not excessive (<TBD), won't break boom

Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. A: Potential causes of UCAs

Generic Control Loop

UCA: Boom Operator provides excessive Manual Movement Cmd (> TBD) when Boom is in contact (can break Boom)



Flawed Process Models:

Operator believes Boom not yet In Contact

Operator believes BCU is in Coupled mode (will ignore manual cmds)

Operator believes the movement is not excessive (<TBD), won't break Boom

Control Algorithm:

Operators develop habit to release stick upon contact (per procedure)

Inadequate operation

Delayed operation

Incorrect or no information provided

Controller

Controlled Process

failures

er time

Unidentified or out-of-range disturbance

Process outp contributes to system hazard

Feedback:
Operator sees the Boom make contact (but BCU didn't sense it)

What features could we incorporate to mitigate this?

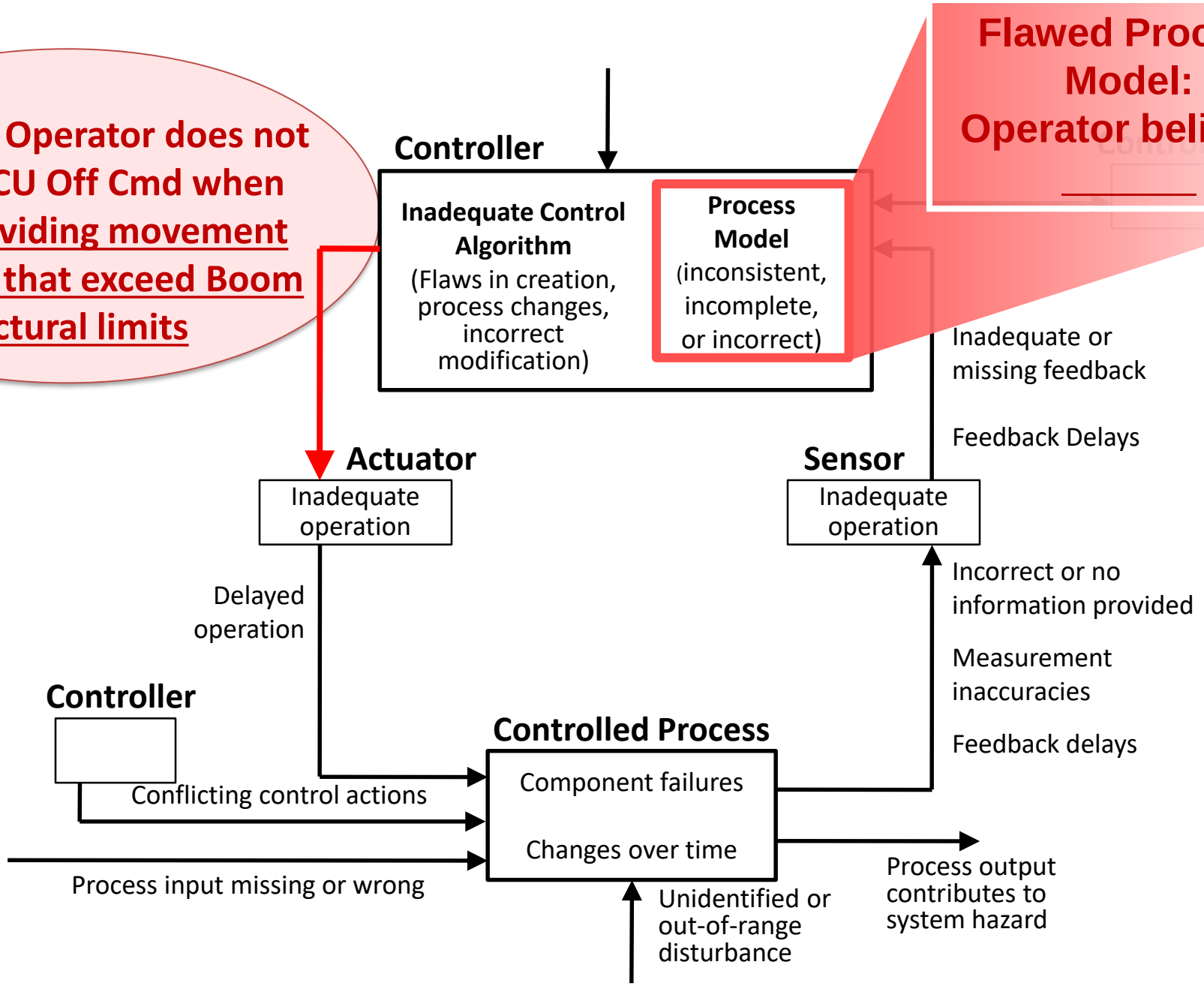
Please contact JThomas4@MIT.EDU with any questions!

Let’s try a different UCA

STPA Step 4. A: Potential causes of UCAs

Generic Control Loop

UCA: Boom Operator does not provide BCU Off Cmd when BCU is providing movement commands that exceed Boom structural limits

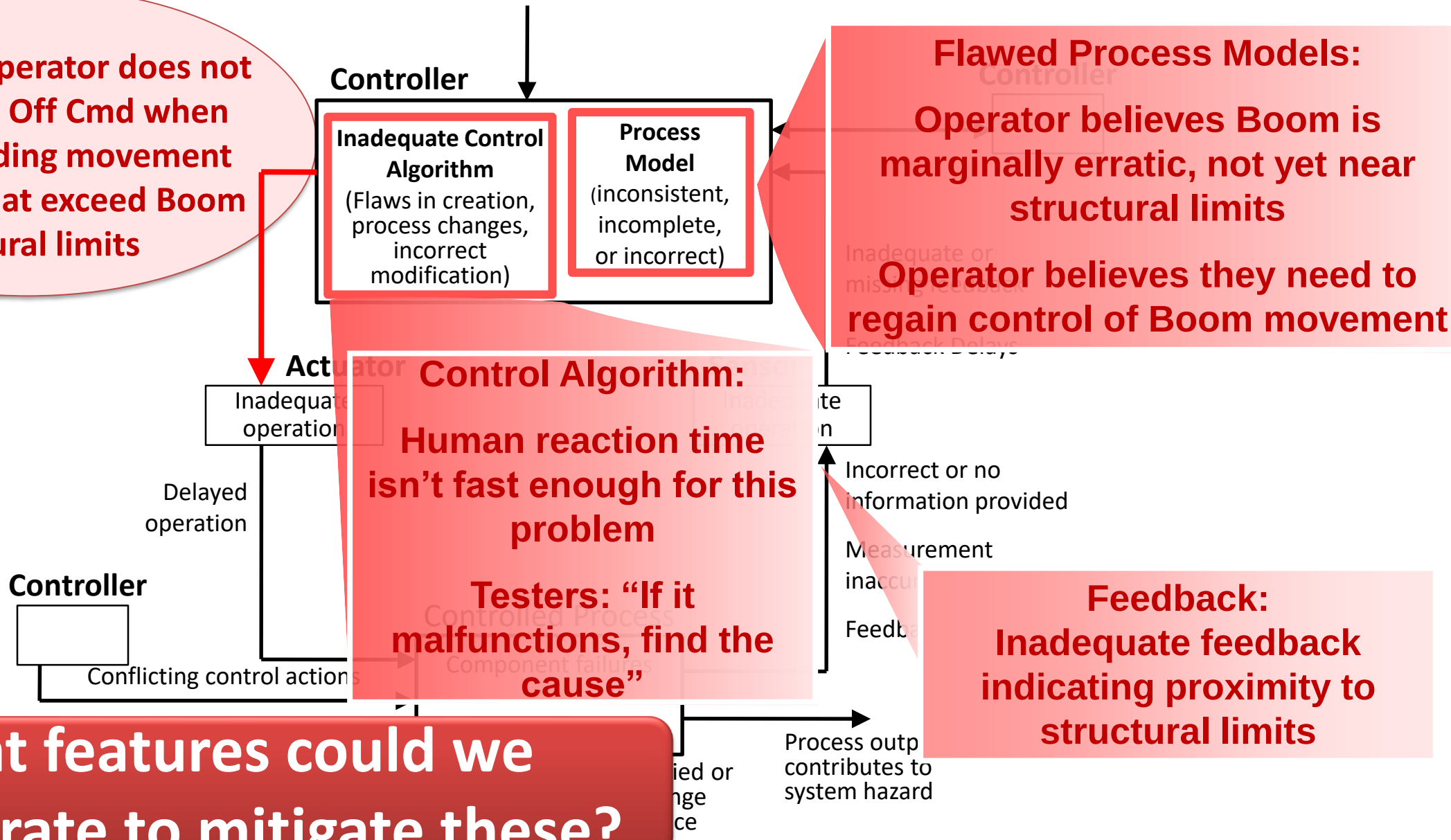


Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. A: Potential causes of UCAs

Generic Control Loop

UCA: Boom Operator does not provide BCU Off Cmd when BCU is providing movement commands that exceed Boom structural limits



Flawed Process Models:

Operator believes Boom is marginally erratic, not yet near structural limits

Operator believes they need to regain control of Boom movement

Control Algorithm:

Human reaction time isn't fast enough for this problem

Testers: "If it malfunctions, find the cause"

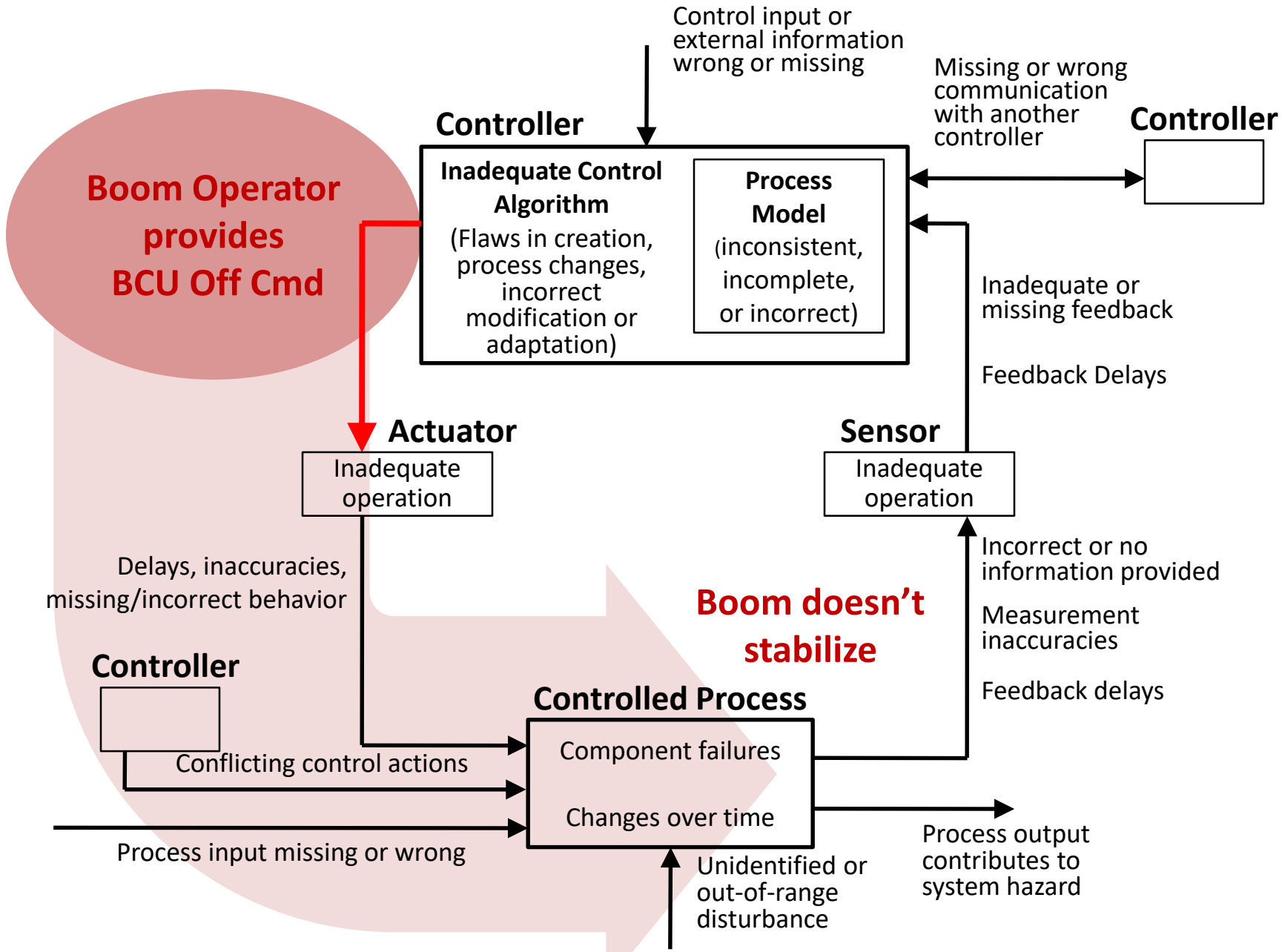
Feedback:
Inadequate feedback indicating proximity to structural limits

What features could we incorporate to mitigate these?

Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. B: Control Actions not Properly Followed

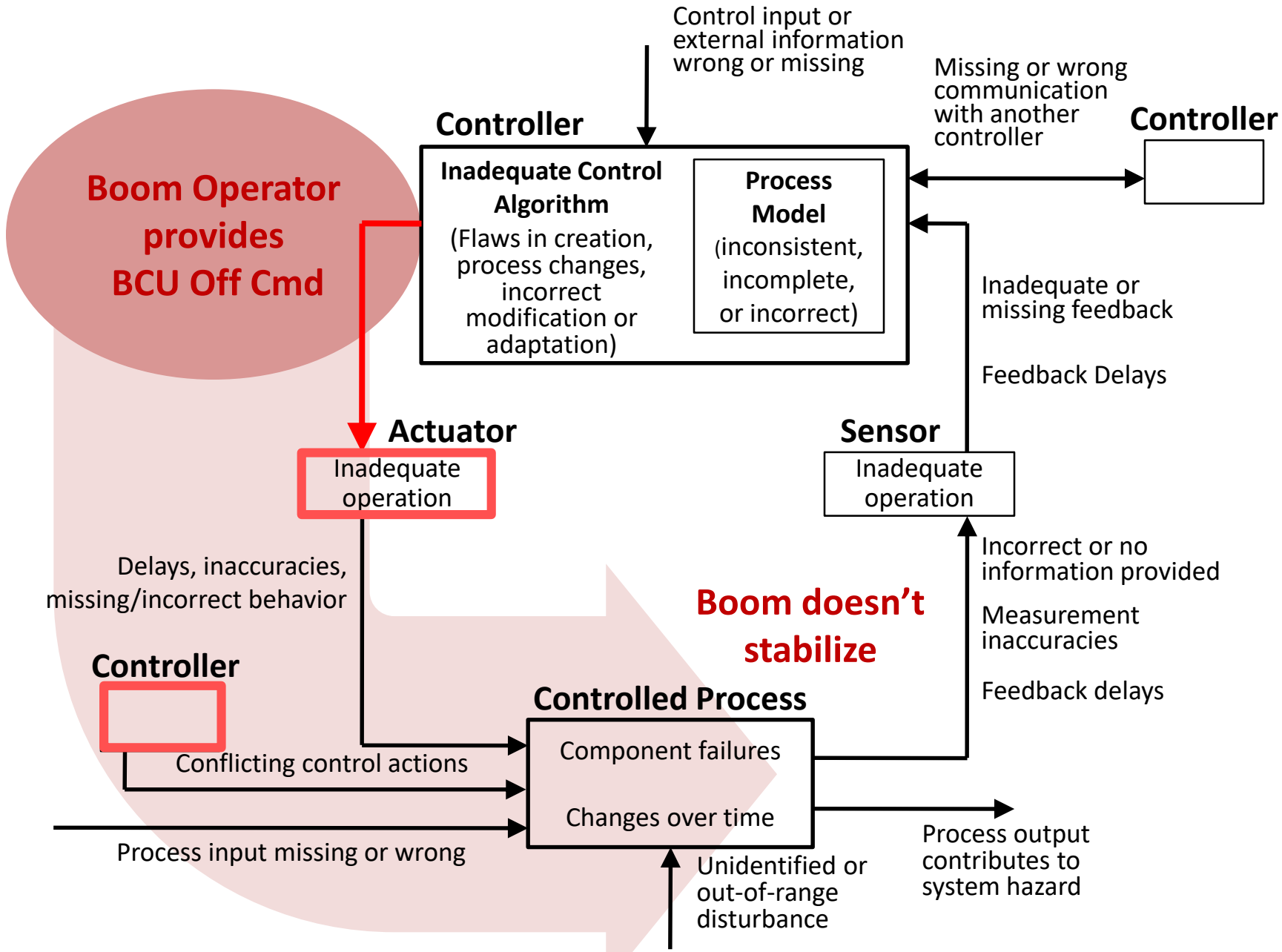
Generic Control Loop



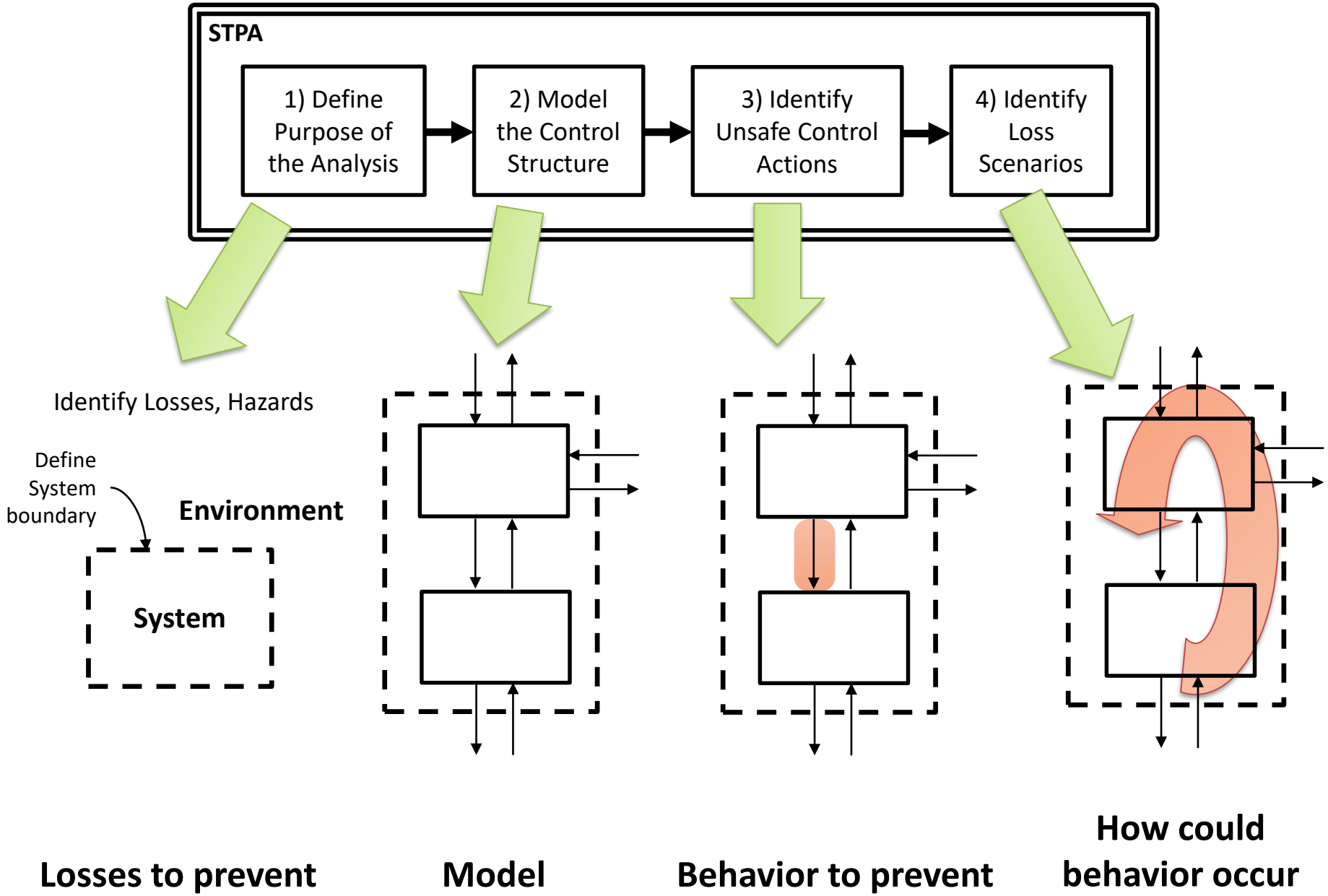
Please contact JThomas4@MIT.EDU with any questions!

STPA Step 4. B: Control Actions not Properly Followed

Generic Control Loop



Please contact JThomas4@MIT.EDU with any questions!

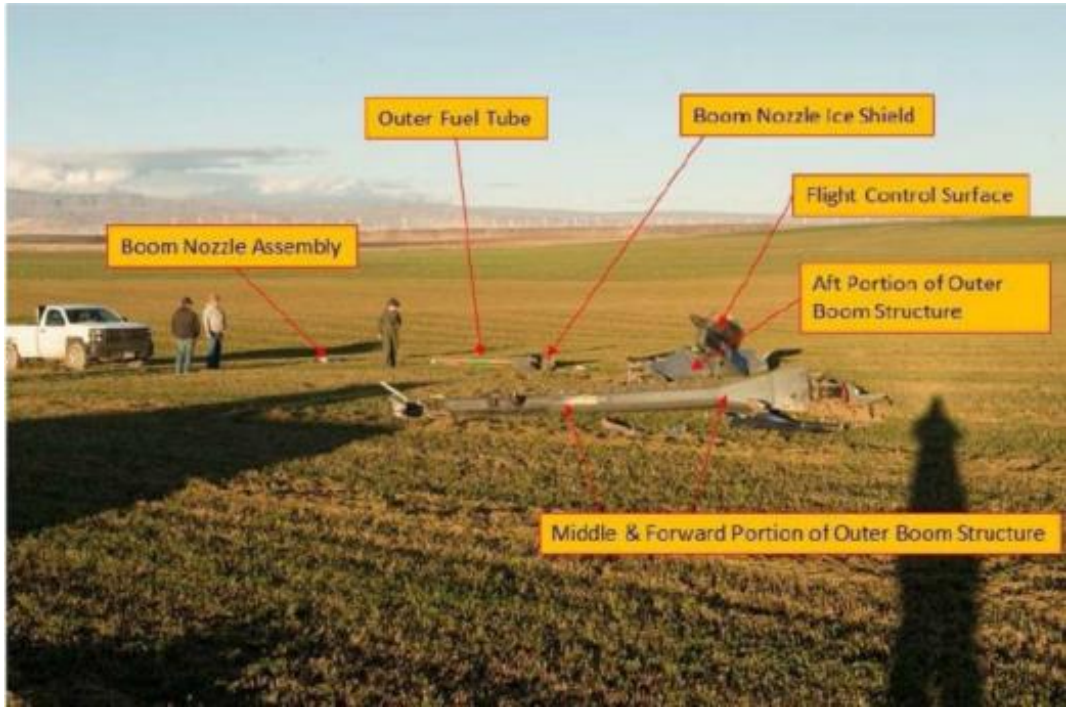


(Leveson and Thomas, 2018)

Let’s Review Previous Incidents

KC-10 Tanker Event

- Nov. 1, 2016
  - The boom operator lowered the boom
  - The boom immediately began to move erratically and well outside of its operational and structural limits.
  - The boom operator was not able to control the boom and the aircraft commander declared an in-flight emergency.
  - The boom fully detached from the fuselage and landed in an empty field
- Financial loss: $6.52 million



Official Causes

- Sheared DRVT rotary crank provided boom control unit (BCU) with continuous, inaccurate roll position indications. As a result, the BCU compensated with lateral movement commands in both directions, driving the boom beyond its structural limits. The boom oscillated violently, boom components and structures became so damaged that they failed and triggered multiple warning lights.
- “Boom operator’s failure to turn off the boom flight control switch in a timely manner.” “Turning off the boom flight control switch would have disabled the BCU. This would have neutralized the boom flight control surfaces, and prevented the boom from departing the aircraft.”

Please contact JThomas4@MIT.EDU with any questions!

Accident report

- “In my opinion, the flight control surfaces were erratic, and the [Boom Operator] should have begun the Flight Controls do not Respond to Command Inputs or Control Surfaces are Erratic checklist immediately. He would have turned off the flight control switch (Step 3) before the hoist cable broke […]”

Checklist

1) Flight Controls do not Respond to Command Inputs or Control Surfaces are Erratic (Applicable Steps)

- Step 1: disconnect the boom from receiver aircraft (if applicable)
- Step 2: retract the boom telescope (if able)
- Step 3: turn off the flight control switch (BCU control)
- Step 4: stow the boom using the hoist cable

Please contact JThomas4@MIT.EDU with any questions!

Boom Operators

"the boom is going crazy right now...it's moving left to right past 30 degrees"

"I don't know what to do honestly ... I have no control over this boom"

Engineers

We can use a single DRVT to sense boom roll and send signal to BCU.

Not a single point of failure—if it fails, the operators will just disable the BCU!

DRVT failure also very unlikely, replaced often!

Maintenance

"Maintenance personnel […] did not perform step 17, which instructs maintenance personnel to conduct a DRVT polarity test by lowering the boom onto a maintenance dolly and moving it to aircraft left. If the team had […] completed the remaining steps, they would have had an opportunity to detect the faulty component 17 days before the day of the mishap.

Please contact JThomas4@MIT.EDU with any questions!

Another Event

- The ARO made contact but the system didn’t recognize it, remaining in FREE FLIGHT while in contact.
- ARO released the stick, which commands the home (trail) position.
- Receiver wasn’t exactly at home position, so loads built up, breaking the tip.
- Tip flew out and struck the receiver tail.
- Receiver commanded disconnection which was sensed, toggling the boom to CONTACT mode, though now in free flight.
- Boom sensed air loads, generating a positive feedback, fly-up command.
- Boom struck tanker fuselage, lost a fin, was unstable and departed.

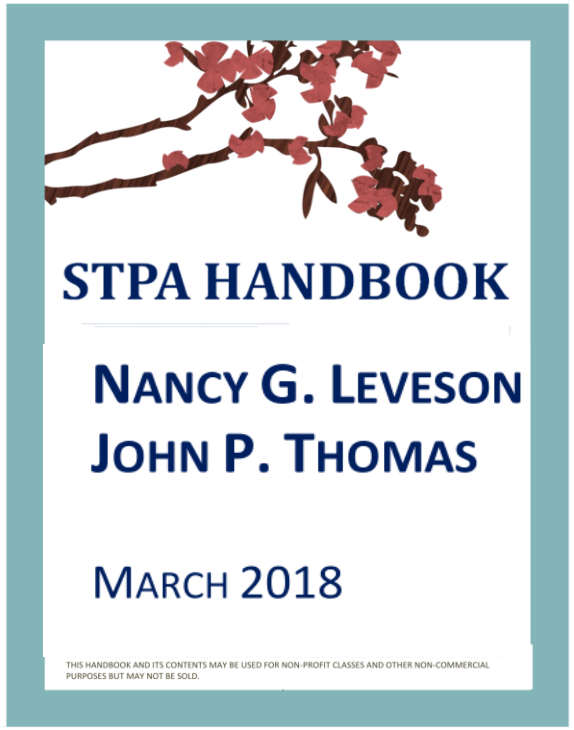
STPA in Industry Standards

- ISO/PAS 21448: SOTIF: Safety of the Intended Functionality
  - STPA used assess safety of digital 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”
- EPRI/Sandia
  - Recommending to use STPA for digital I&C

Please contact JThomas4@MIT.EDU with any questions!

For more information

- Google: “STPA Handbook”
- Email: jthomas4@mit.edu



Free PDF

Short Homework (the best kind!)

- http://psas.scripts.mit.edu/home/2020-stamp-workshop-presentations/
- Not graded, can be anonymous
- Choose an incident or loss event you’re familiar with
  1. Briefly describe the event
- Show how STPA might have anticipated the event before it happened
  2. Simple control structure (~3-5 boxes)
  3. Unsafe Control Action
  4. Process Model Flaws: controller believed _____?
  5. Why did the controller believe that?
- We’ll review and discuss together on Friday!

Enter Q’s on Slido.com
Event code #STPA2