Massachusetts
Institute of
Technology

System-Theoretic Process Analysis (STPA) Introduction

Dr. John Thomas

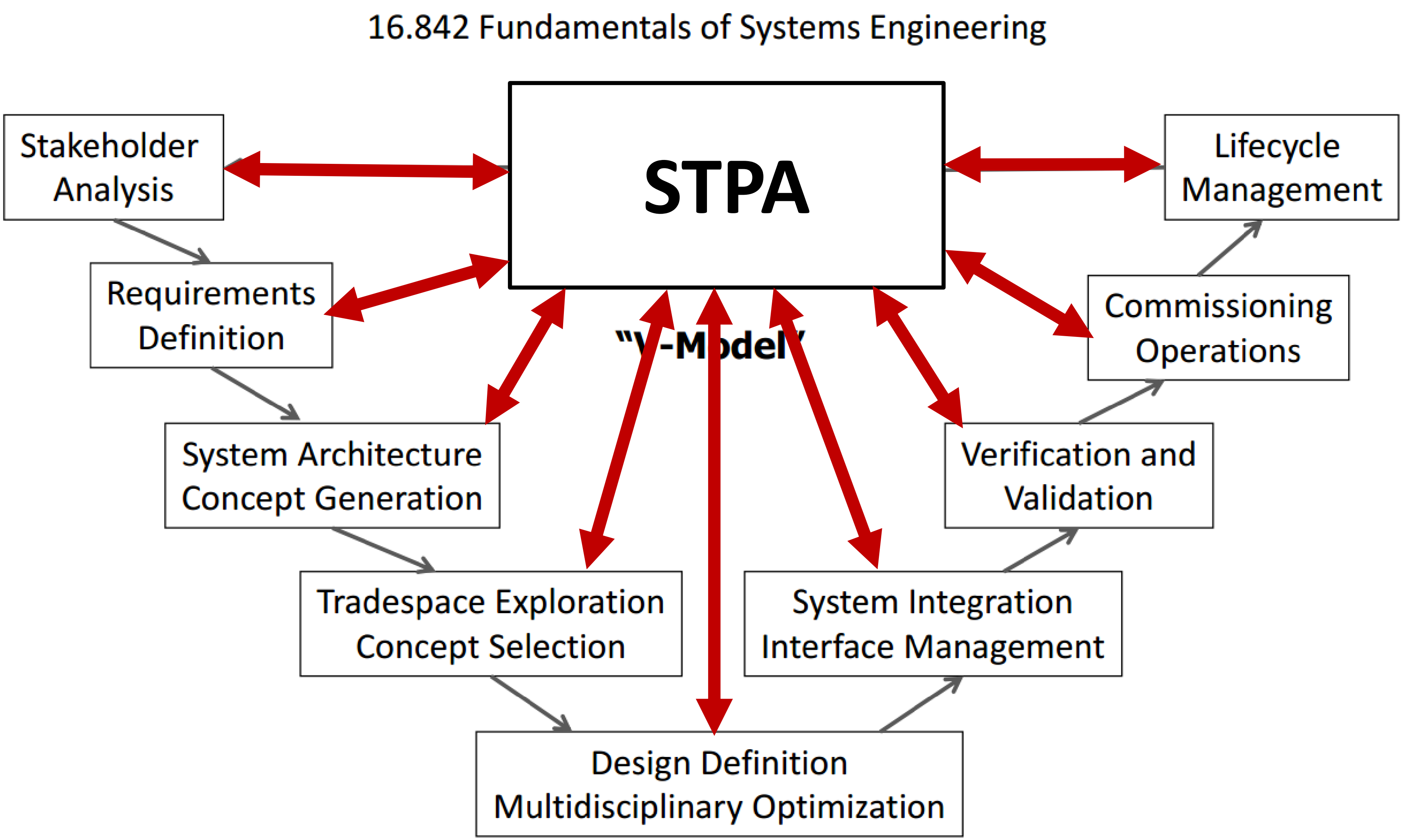
Any questions? Please email: jthomas4@mit.edu

Notes about these slides

- This is not our full STPA class, this is just a short introduction with a small exercise to introduce core concepts.
- The intent is to enable MIT STAMP workshop attendees to follow the workshop presentations and provide some familiarity with the basic process.

Any questions? Please email: jthomas4@mit.edu

The famous “V-Model” of Systems Engineering


16.842 Fundamentals of Systems Engineering
STPA
Stakeholder Analysis
Requirements Definition
System Architecture Concept Generation
Tradespace Exploration Concept Selection
Design Definition Multidisciplinary Optimization
System Integration Interface Management
Verification and Validation
Commissioning Operations
Lifecycle Management
“V-Model”

Many opportunities to address safety throughout!
We only have time to cover a few in this introduction

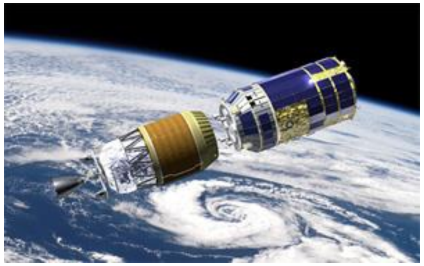
STPA Exercise
JAXA H-II Transfer Vehicle (HTV)

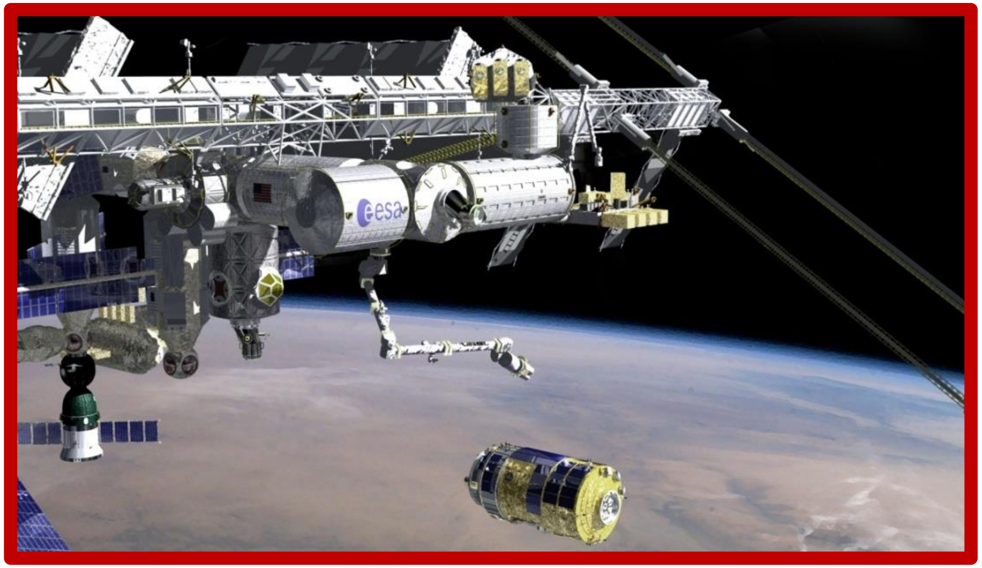
John Thomas

Takuto Isimatsu

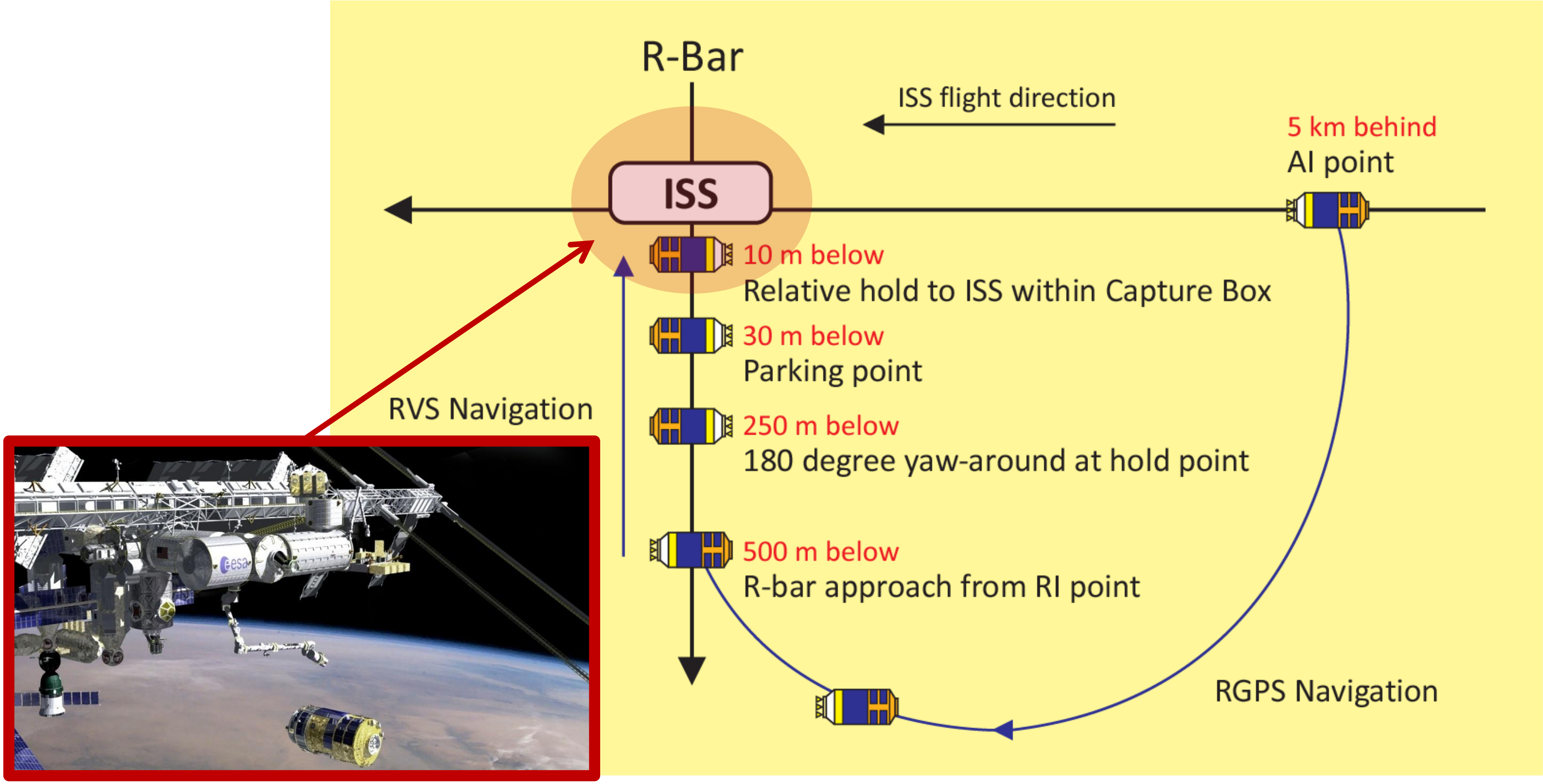
HTV: H-II Transfer Vehicle

- JAXA's unmanned cargo transfer spacecraft
  - Launched from the Tanegashima Space Center aboard the H-IIB rocket
  - Delivers supplies to the International Space Station (ISS)
  - HTV-1 (Sep '09) through HTV-7 (Sep '18) completed successfully
  - **Proximity operations** involve the ISS (including crew) and NASA and JAXA ground stations





Capture Operation



R-Bar

ISS flight direction

ISS

5 km behind
AI point

10 m below
Relative hold to ISS within Capture Box

30 m below
Parking point

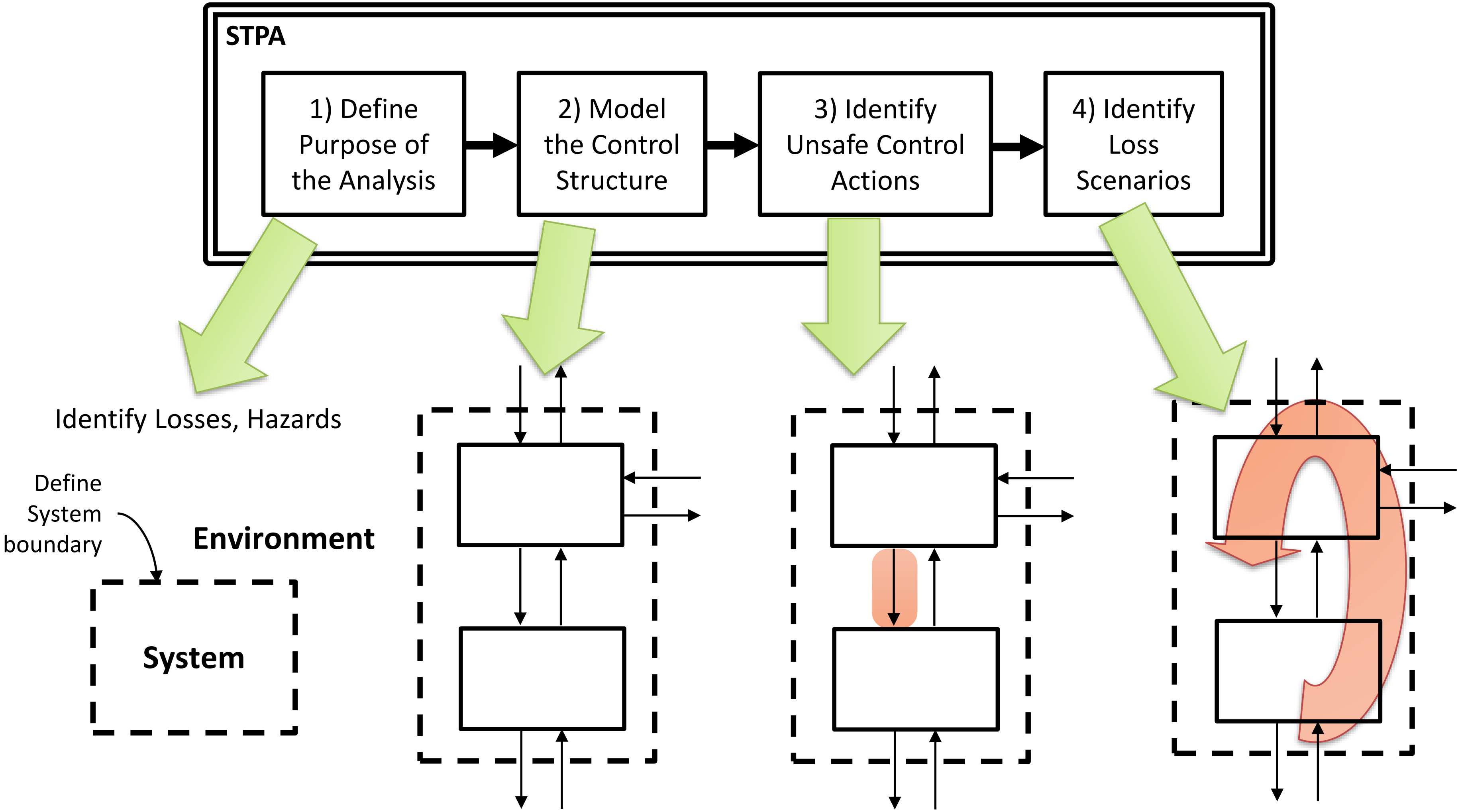
250 m below
180 degree yaw-around at hold point

500 m below
R-bar approach from RI point

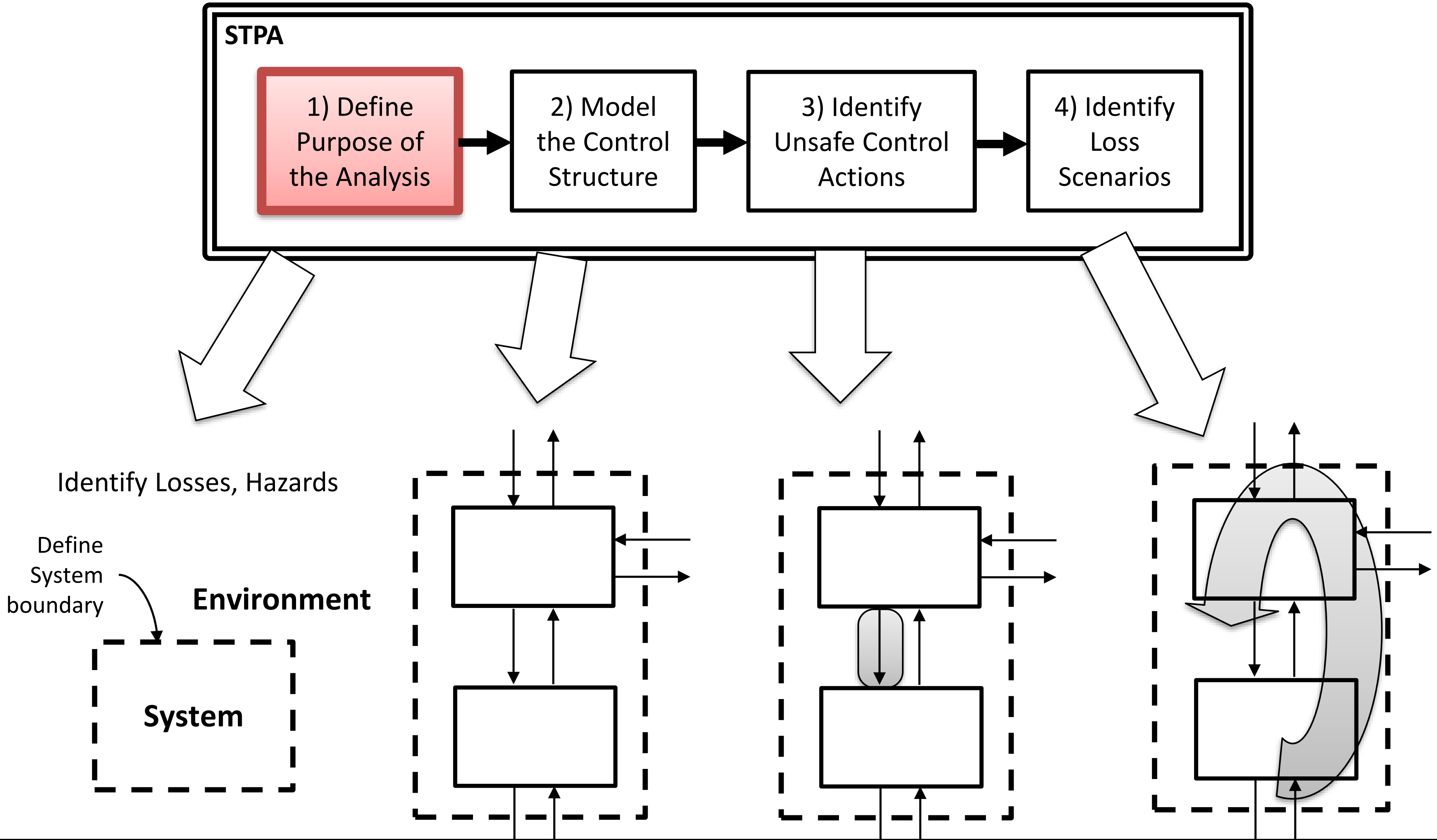
RVS Navigation

RGPS Navigation

System-Theoretic Process Analysis (STPA)


STPA
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
Identify Losses, Hazards
Define System boundary
Environment
System

System-Theoretic Process Analysis (STPA)


STPA
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
Identify Losses, Hazards
Define System boundary
Environment
System

Concept: Unmanned Space Vehicle

- Goal: To deliver cargo to ISS
- What (System): An unmanned space vehicle (HTV)
- How (Method): By means of autonomous navigation followed by manual capture

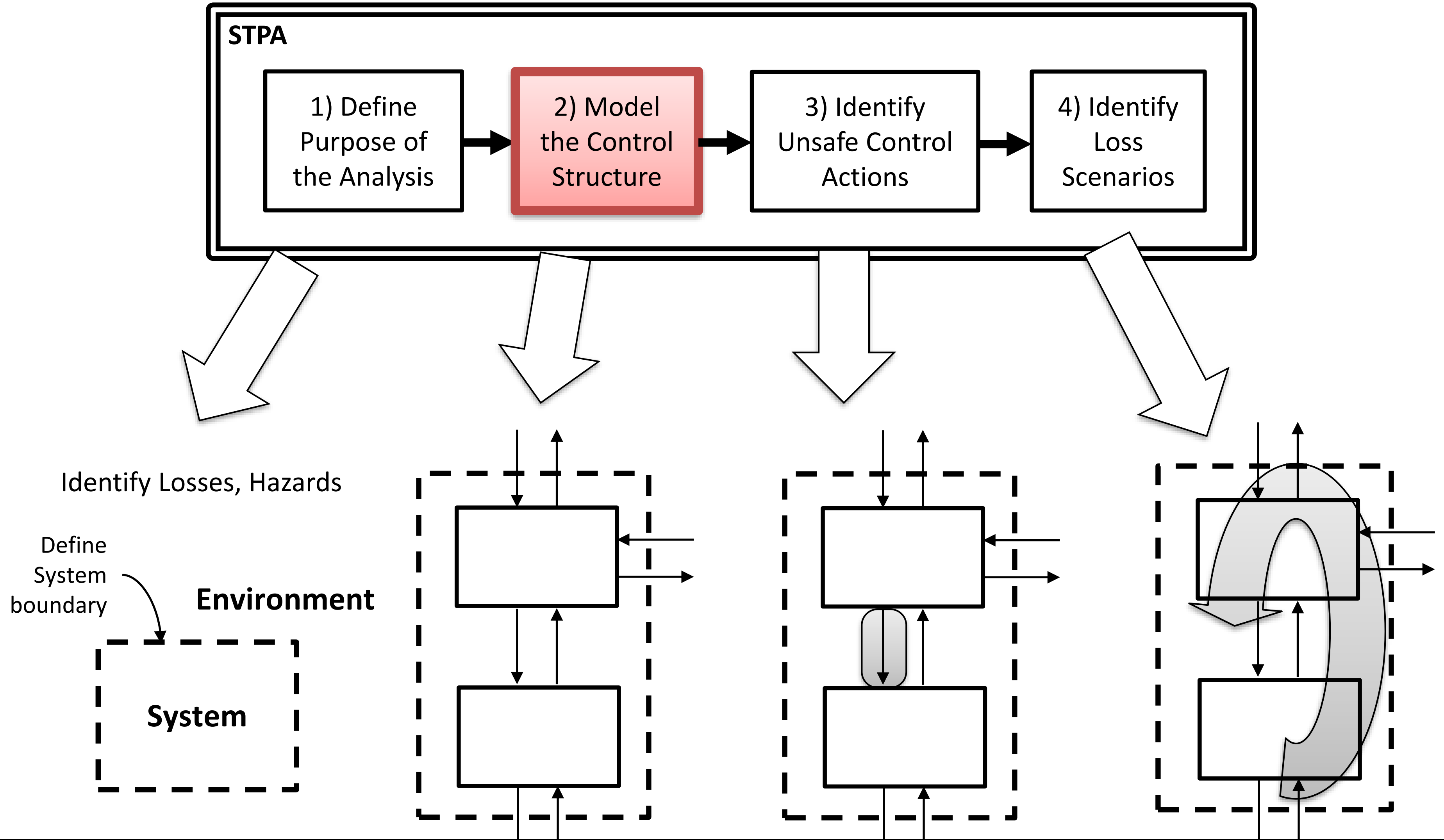
Losses / Hazards

- Losses
  - Death or injury to human astronauts
- System Hazards
  - HTV too close to ISS (for given speed)
    - Captures collisions, near misses

Losses / Hazards

- Losses
  - L-1: Death or injury to human astronauts
  - L-2: Loss of delivery mission
- System Hazards
  - H-1: HTV too close to ISS (for given operational phase)
  - H-2: HTV trajectory makes delivery impossible
- System Safety Constraints
  - ?

System-Theoretic Process Analysis (STPA)



STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

Identify Losses, Hazards

Define System boundary

Environment

System

Basic Information

Accident we want to prevent: **collision with ISS**

Main components in the system

- **HTV**
- **ISS (including crew)**
- **NASA ground station**
- **JAXA ground station**

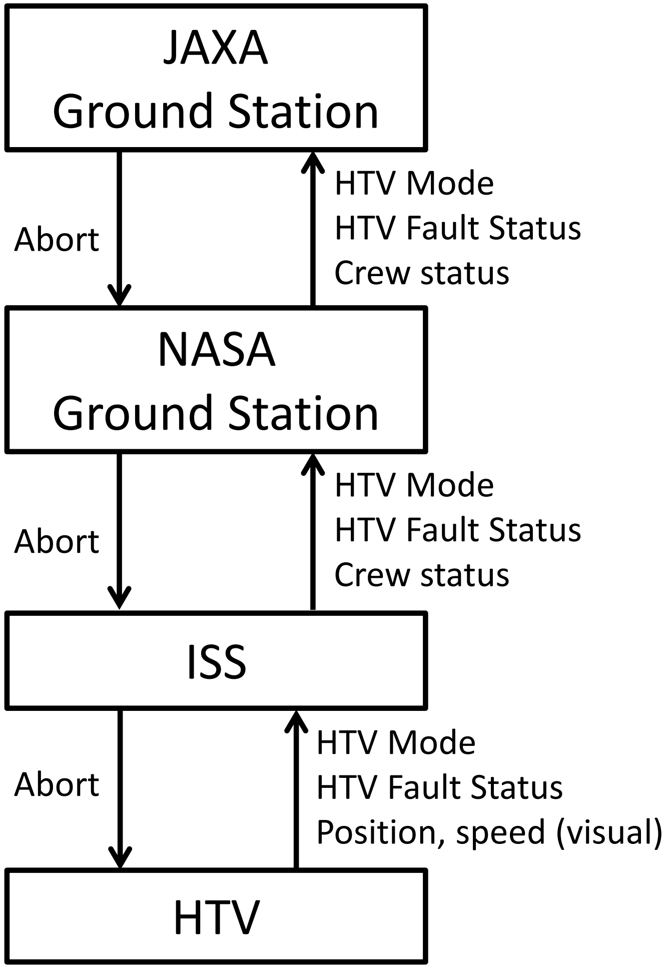
Typical capture operation

1. HTV autonomously reaches Capture Box (10 m below ISS), holds position (has laser)
2. ***Free Drift*** command sent to HTV
   - Deactivates HTV (by radio), disables the thrusters
3. HTV is **captured** by ISS crew using SSRMS (robotic arm)

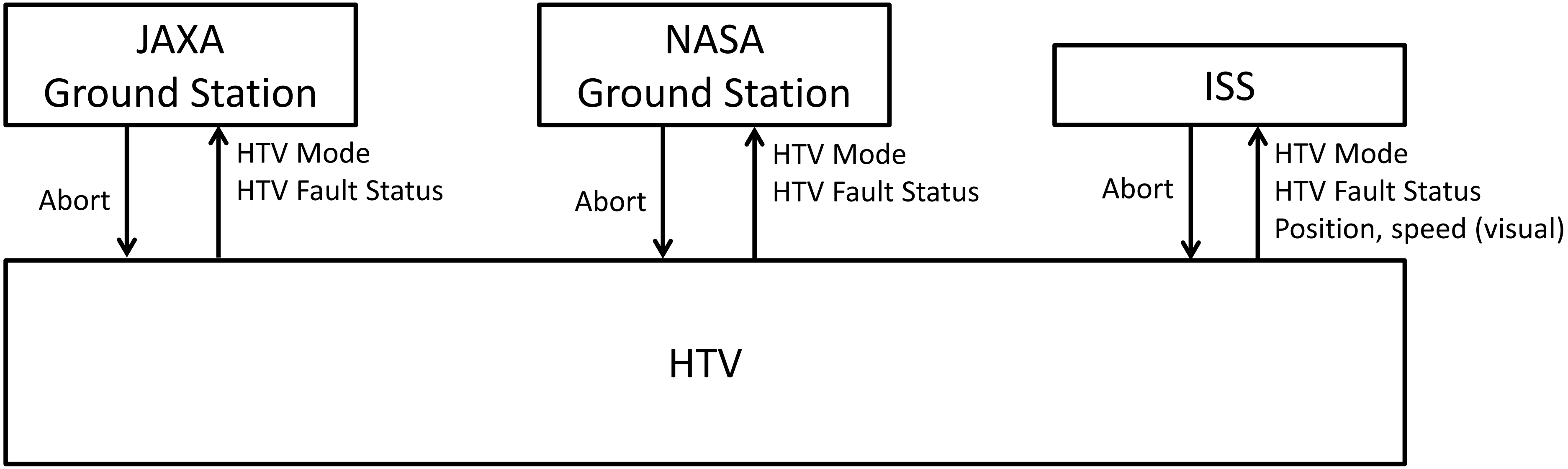
At any time:

- HTV sends back ***HTV Fault Status***
- ***Abort/Retreat/Hold*** commands can be sent to the HTV in case of emergency. HTV will immediately fire top thrusters to maneuver away from ISS. Abort is final (HTV ignores all future commands) and irrecoverable.

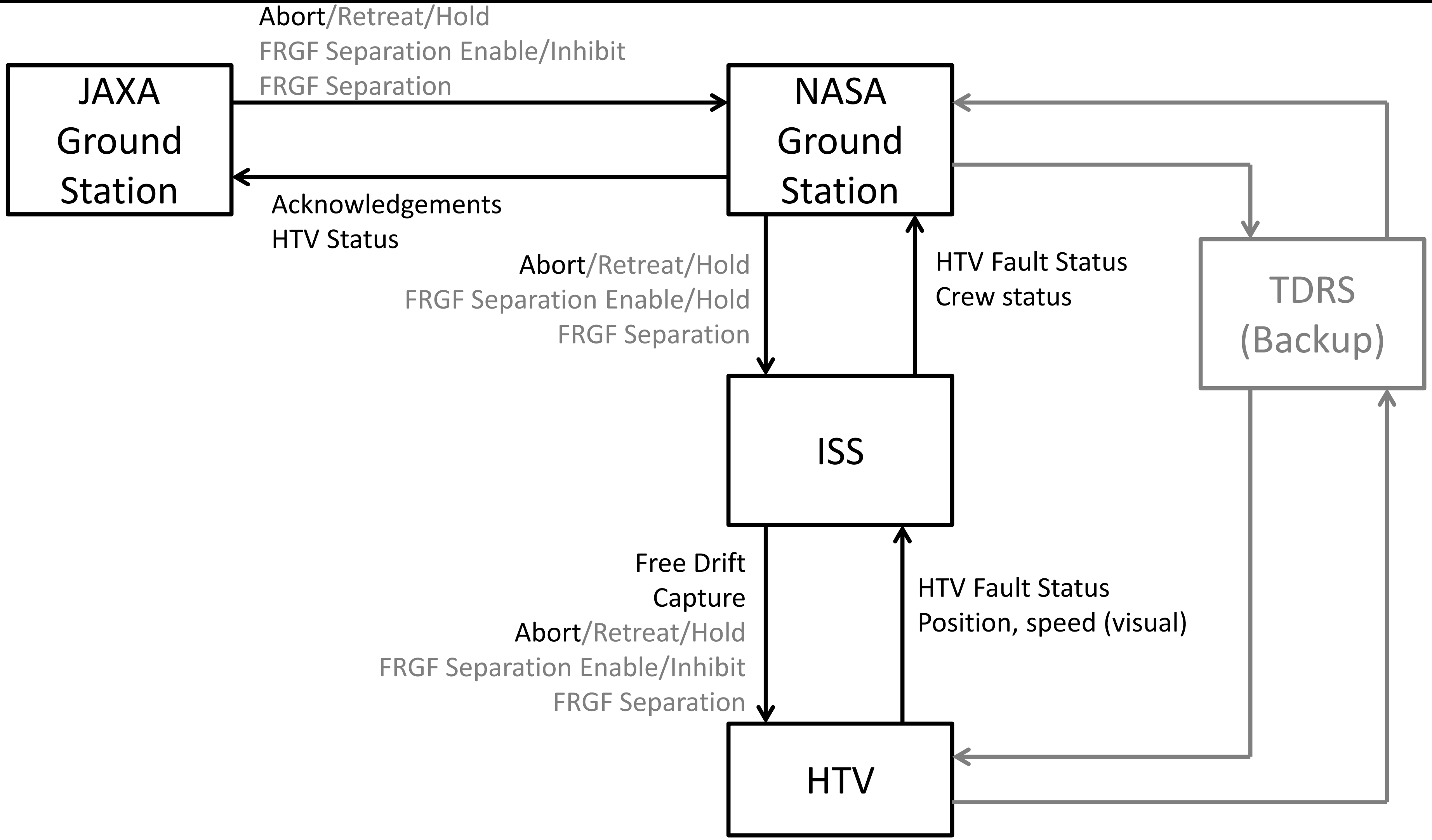
Proposal A: Clear Hierarchy



Proposal B: Any can directly abort



Actual Control Structure



JAXA Ground Station

Abort/Retreat/Hold
FRGF Separation Enable/Inhibit
FRGF Separation

NASA Ground Station

Acknowledgements
HTV Status

Abort/Retreat/Hold
FRGF Separation Enable/Hold
FRGF Separation

HTV Fault Status
Crew status

TDRS (Backup)

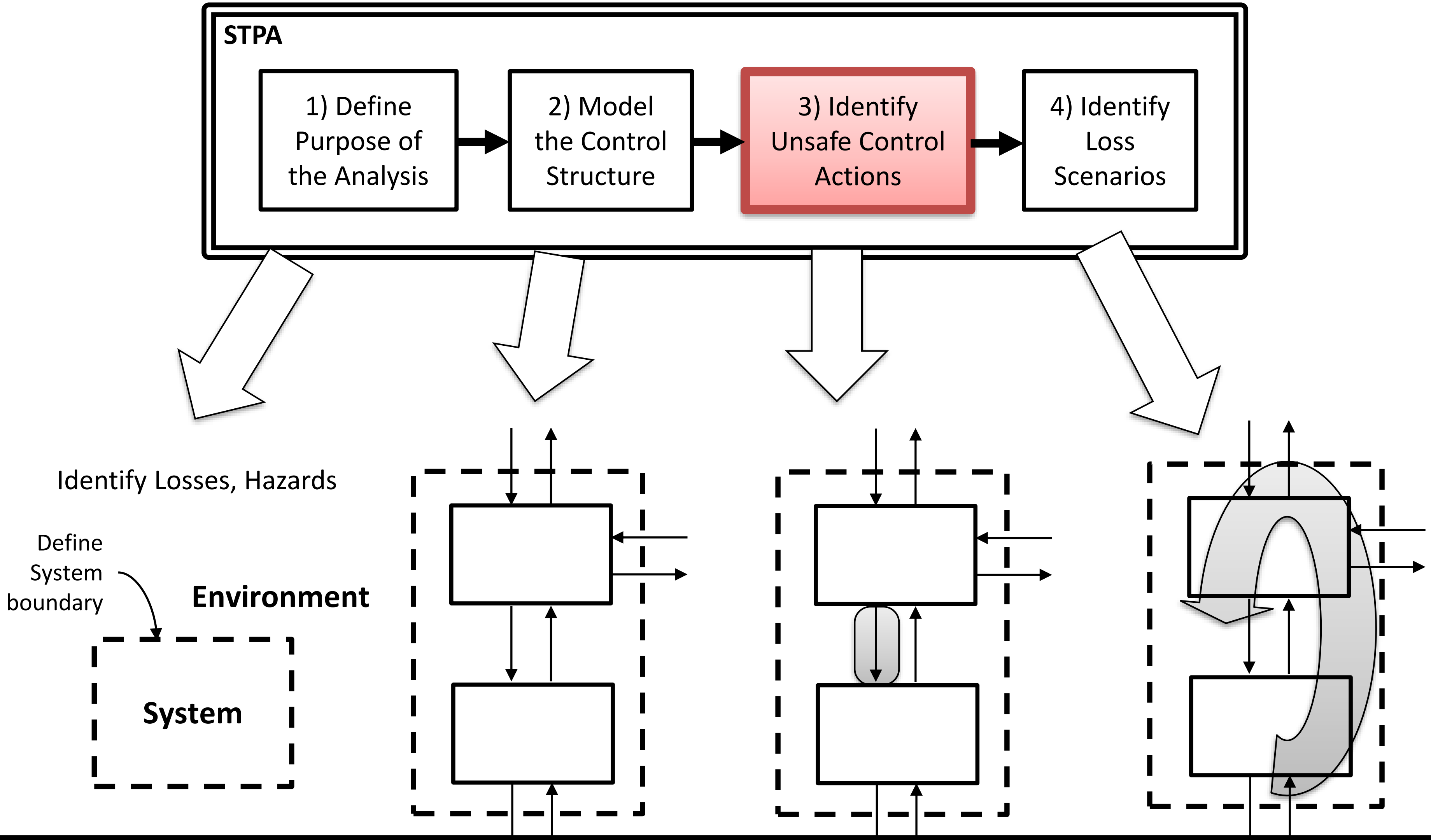
ISS

Free Drift
Capture
Abort/Retreat/Hold
FRGF Separation Enable/Inhibit
FRGF Separation

HTV Fault Status
Position, speed (visual)

HTV

System-Theoretic Process Analysis (STPA)



STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

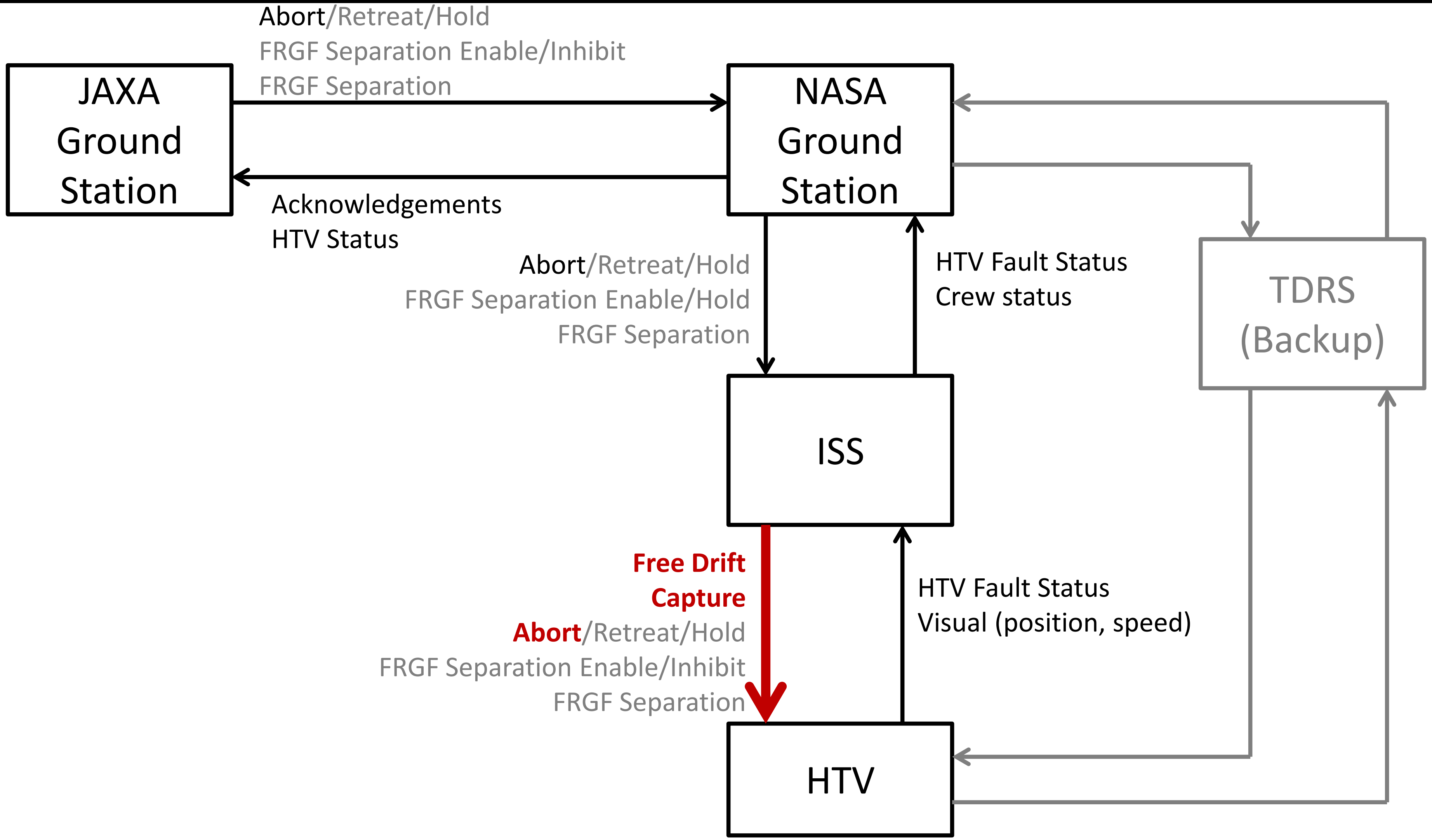
Identify Losses, Hazards

Define System boundary

Environment

System

Selecting Control Actions



JAXA Ground Station

Abort/Retreat/Hold
FRGF Separation Enable/Inhibit
FRGF Separation

NASA Ground Station

Acknowledgements
HTV Status

Abort/Retreat/Hold
FRGF Separation Enable/Hold
FRGF Separation

HTV Fault Status
Crew status

TDRS (Backup)

ISS

Free Drift
Capture
Abort/Retreat/Hold
FRGF Separation Enable/Inhibit
FRGF Separation

HTV Fault Status
Visual (position, speed)

HTV

Identifying Unsafe Control Actions

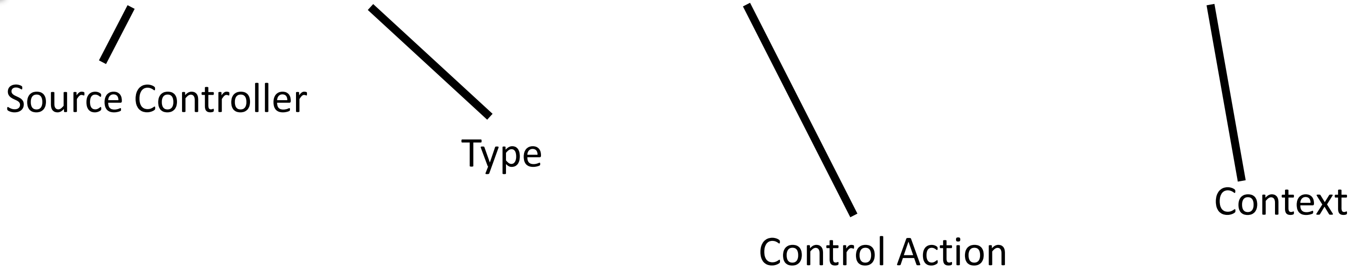
ISS Crew Actions

	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Abort				
Free Drift				
Capture				

Four elements for an Unsafe Control Action

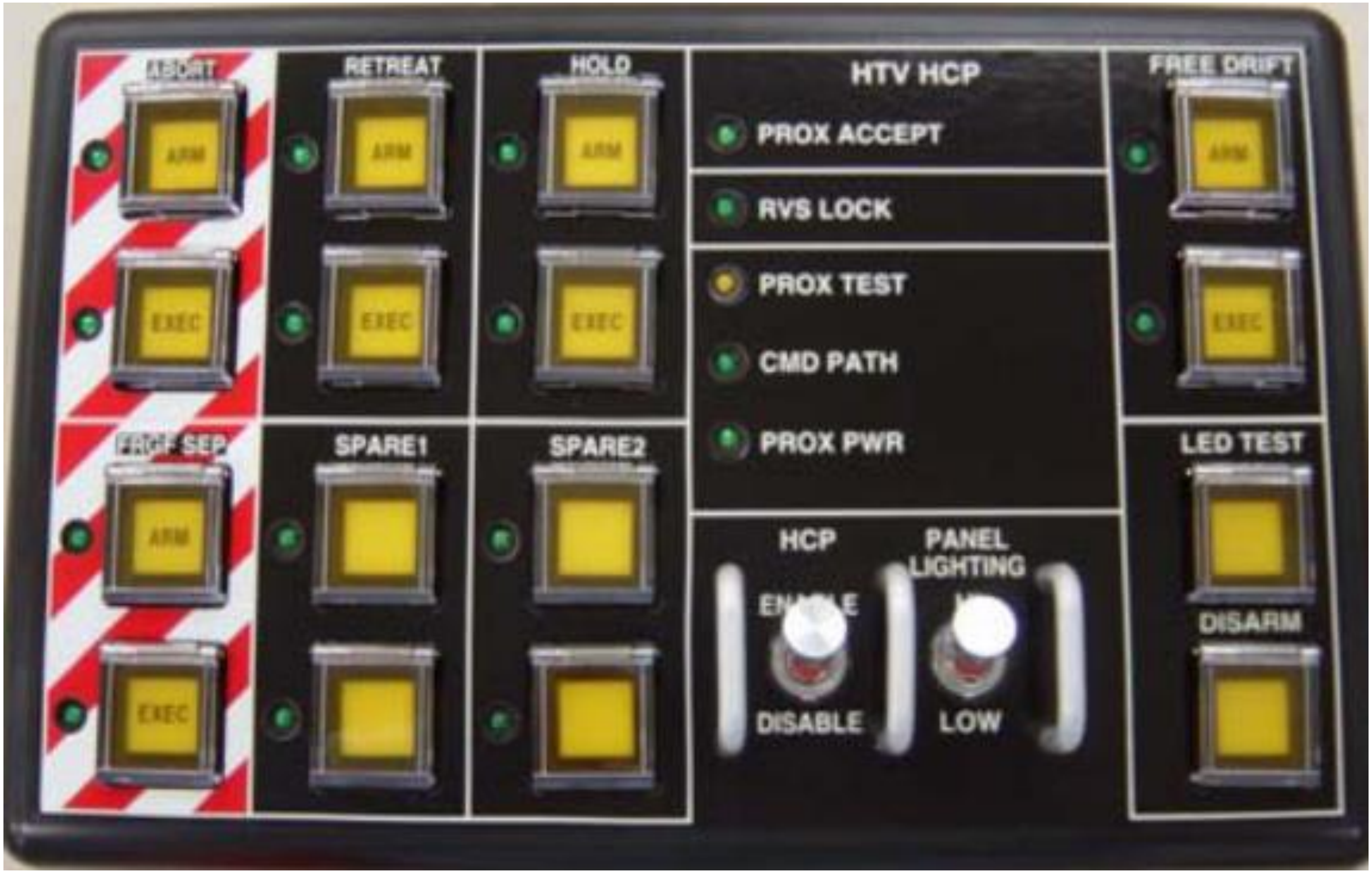
Example:

"ISS crew does not provide Abort Cmd when emergency condition exists*"

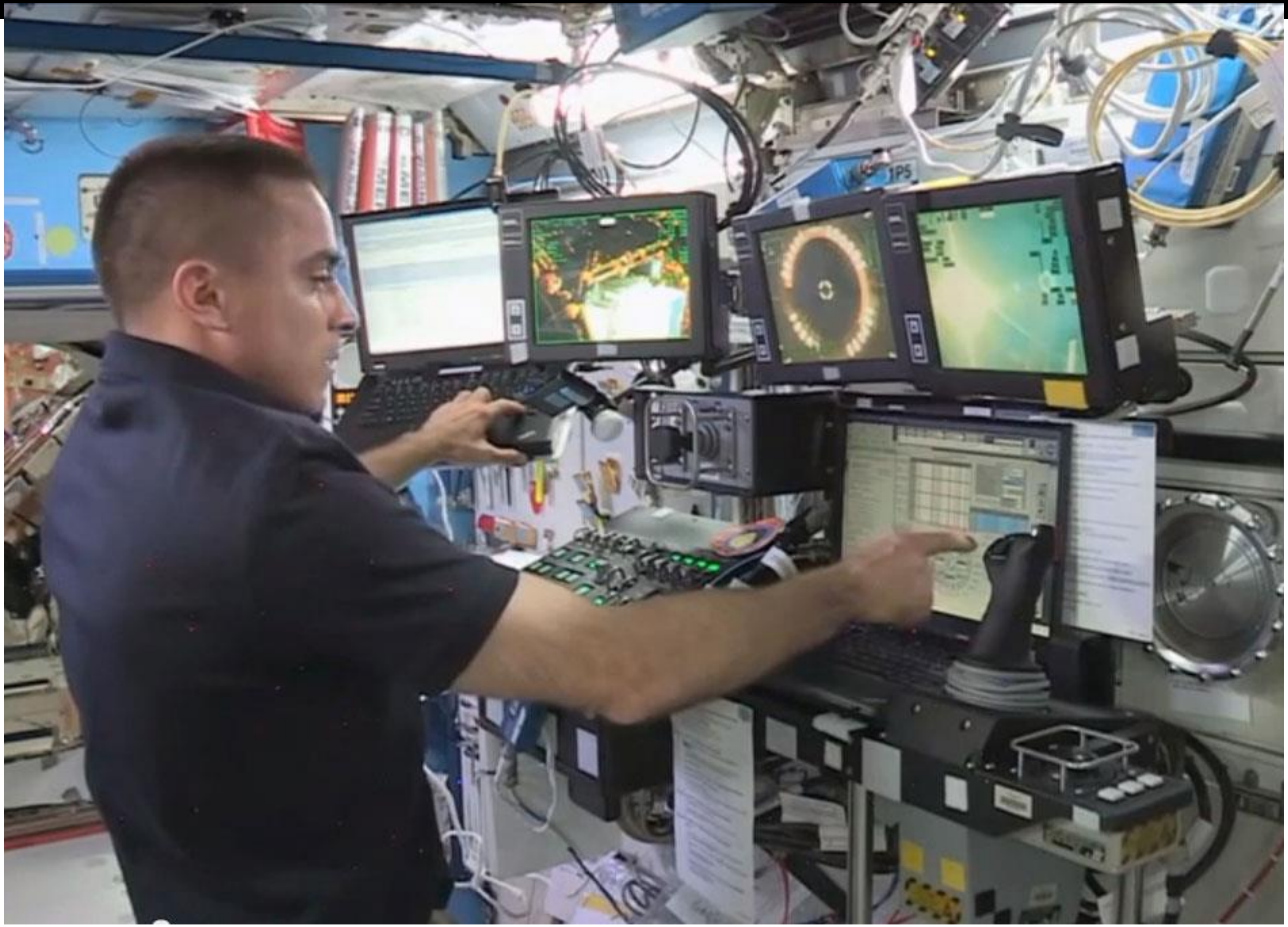


	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Abort	🟥			
Free Drift				
Capture				

Actual Astronaut Control Interface

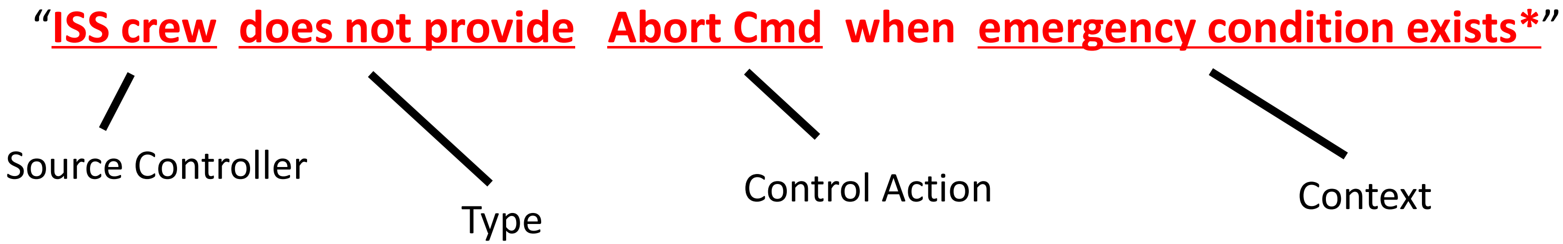


SSRMS Control Station



STPA: Identify Unsafe Control Actions

Example:



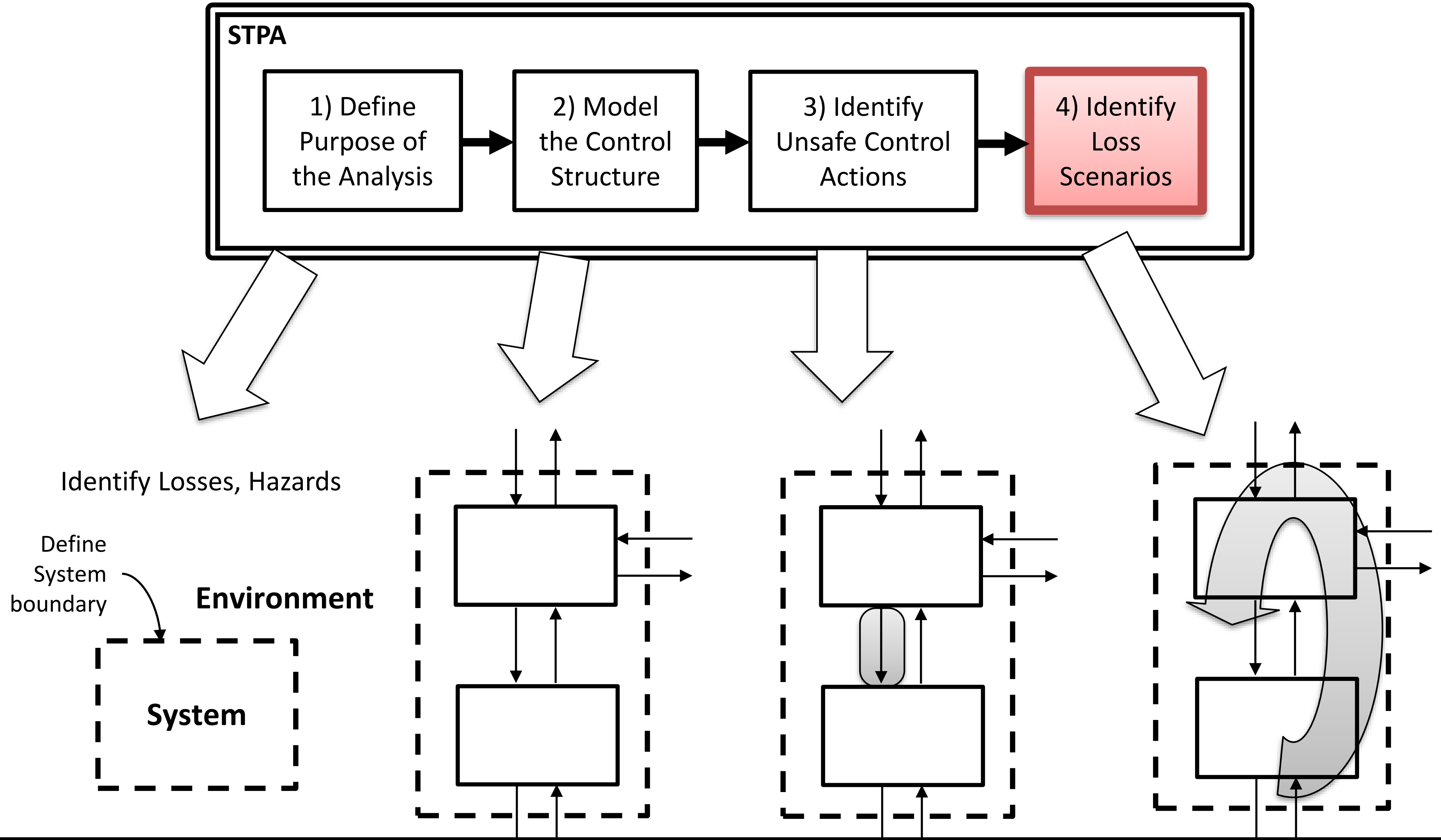
"ISS crew does not provide Abort Cmd when emergency condition exists*"

	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Abort Cmd	ISS crew does not provide abort when ______	ISS crew provides abort when ______	ISS crew provides abort too late after ______	
Free Drift Cmd				
Capture				

Identifying Unsafe Control Actions

	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Abort	ISS crew does not provide Abort Cmd when emergency condition* exists [H-1]	ISS crew provides Abort Cmd when HTV is captured [H-1] ISS crew provides Abort Cmd when ISS is in Abort path [H-1]	ISS crew provides Abort Cmd too late to avoid collision [H-1] ISS crew provides Abort Cmd too early before capture is released [H-1]	N/A
Free Drift	ISS crew does not provide Free Drift Cmd when HTV is stopped in capture box [H-1]	ISS crew provides Free Drift Cmd when HTV is approaching ISS [H-1]	ISS crew provides Free Drift Cmd too late, more than X minutes after HTV stops [H-1] ISS crew provides Free Drift Cmd too early before HTV stops [H-1]	N/A
Capture	ISS crew does not perform Capture when HTV is in capture box in free drift [H-1]	ISS crew performs Capture when HTV is not in free drift [H-1] ISS crew performs Capture when HTV is aborting [H-1] ISS crew performs Capture with excessive/insufficient movement (can impact HTV, cause collision course) [H-1]	ISS crew performs Capture too late, more than X minutes after HTV deactivated [H-1] ISS crew performs Capture too early before HTV deactivated [H-1]	ISS crew continues performing Capture too long after emergency condition* exists [H-1]

System-Theoretic Process Analysis (STPA)



STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

Identify Losses, Hazards

Define System boundary

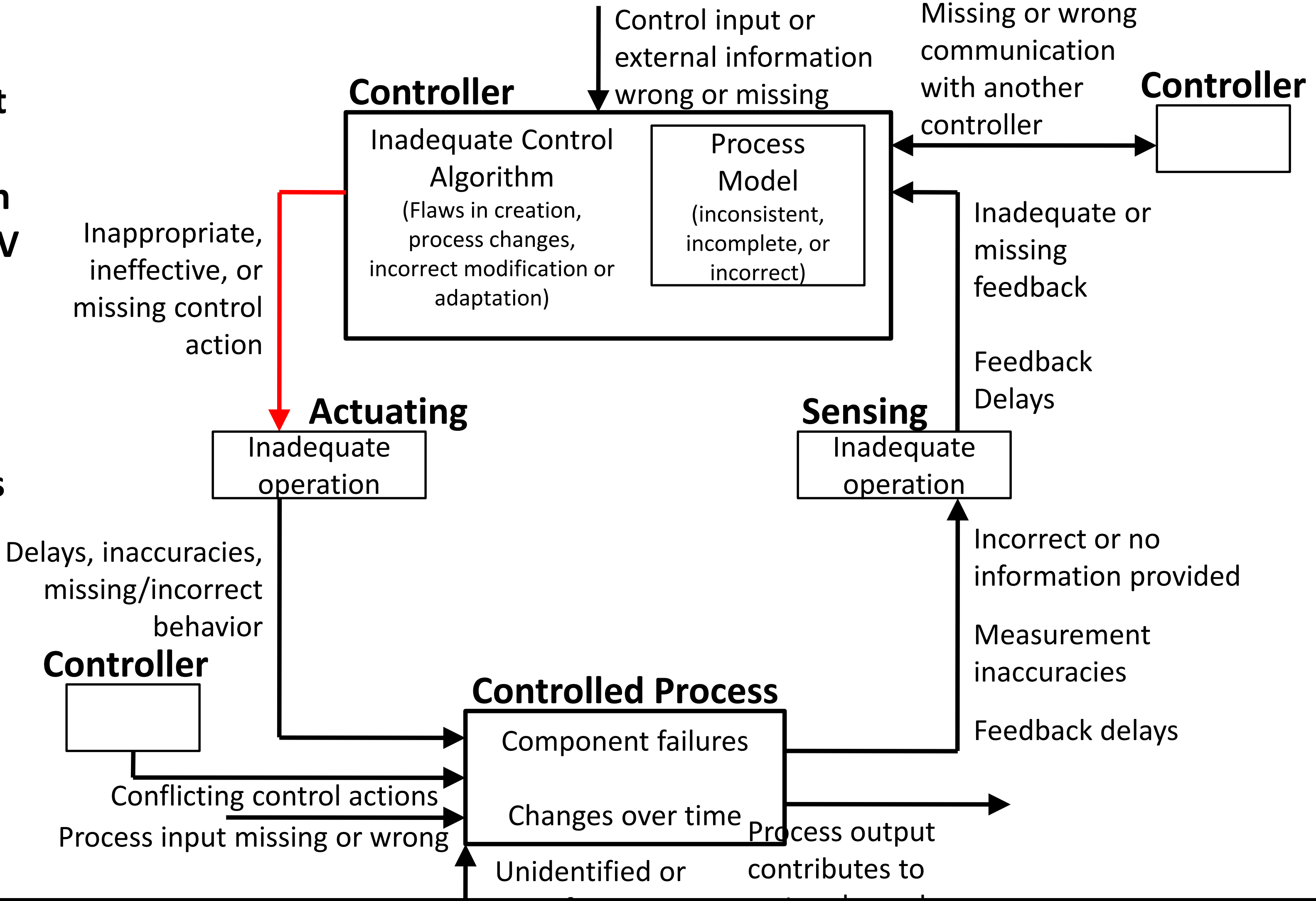
Environment

System

Identifying Accident Scenarios

UCA-1: ISS Crew does not perform capture within X sec after HTV deactivation [H-1, H-2]

UCA-2: ISS Crew provides free drift command while HTV approaching ISS [H-1, H-2]



Controller

Control input or external information wrong or missing

Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification or adaptation)

Process Model
(inconsistent, incomplete, or incorrect)

Missing or wrong communication with another controller

Controller

Inappropriate, ineffective, or missing control action

Inadequate or missing feedback

Feedback Delays

Actuating

Inadequate operation

Sensing

Inadequate operation

Delays, inaccuracies, missing/incorrect behavior

Incorrect or no information provided

Measurement inaccuracies

Feedback delays

Controller

Controlled Process

Component failures

Changes over time

Conflicting control actions

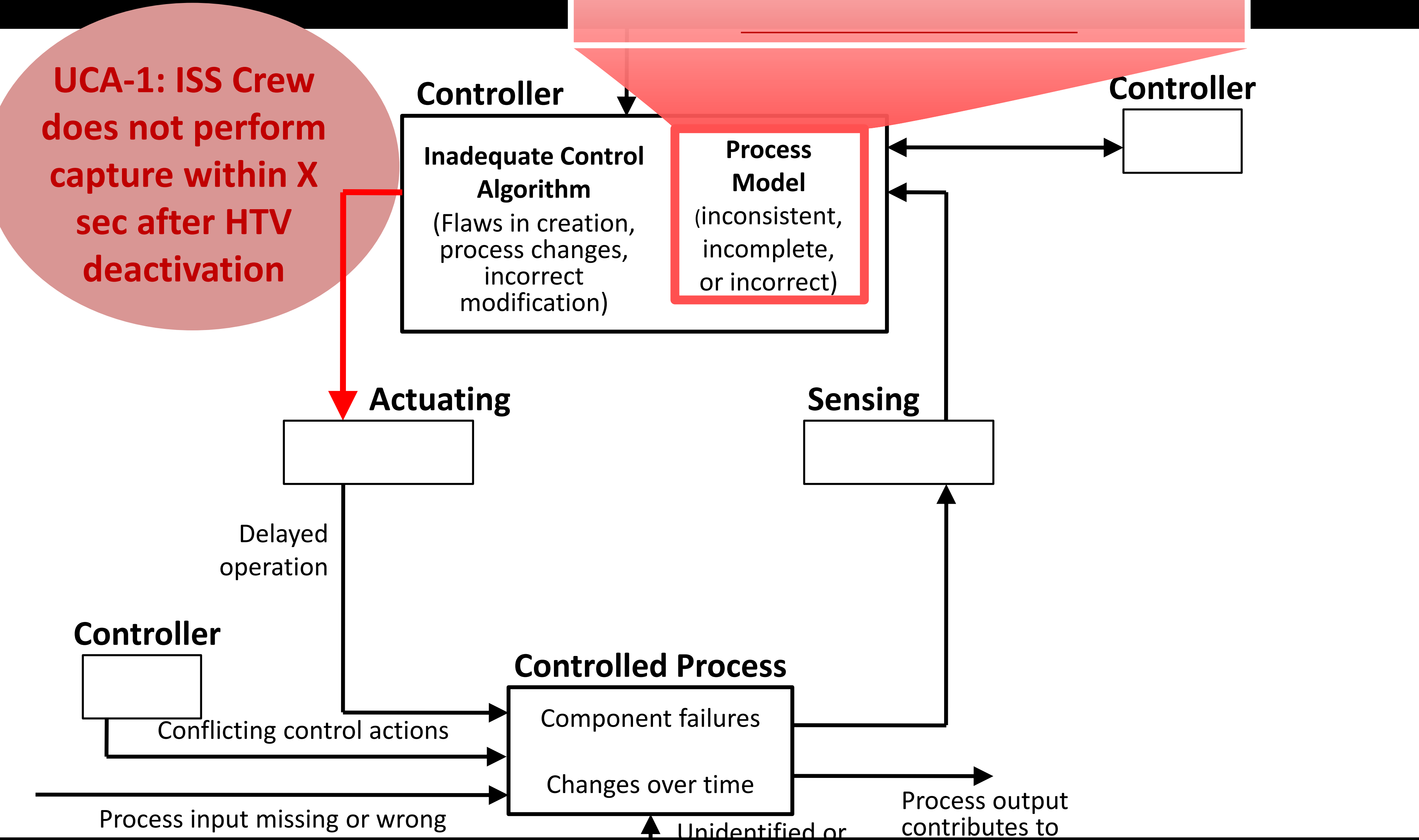
Process input missing or wrong

Unidentified or

Process output contributes to

Flawed Process Model:
ISS Crew incorrectly believes

____



UCA-1: ISS Crew does not perform capture within X sec after HTV deactivation

Controller

Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification)

Process Model
(inconsistent, incomplete, or incorrect)

Controller

Actuating

Sensing

Delayed operation

Controller

Conflicting control actions

Controlled Process

Component failures

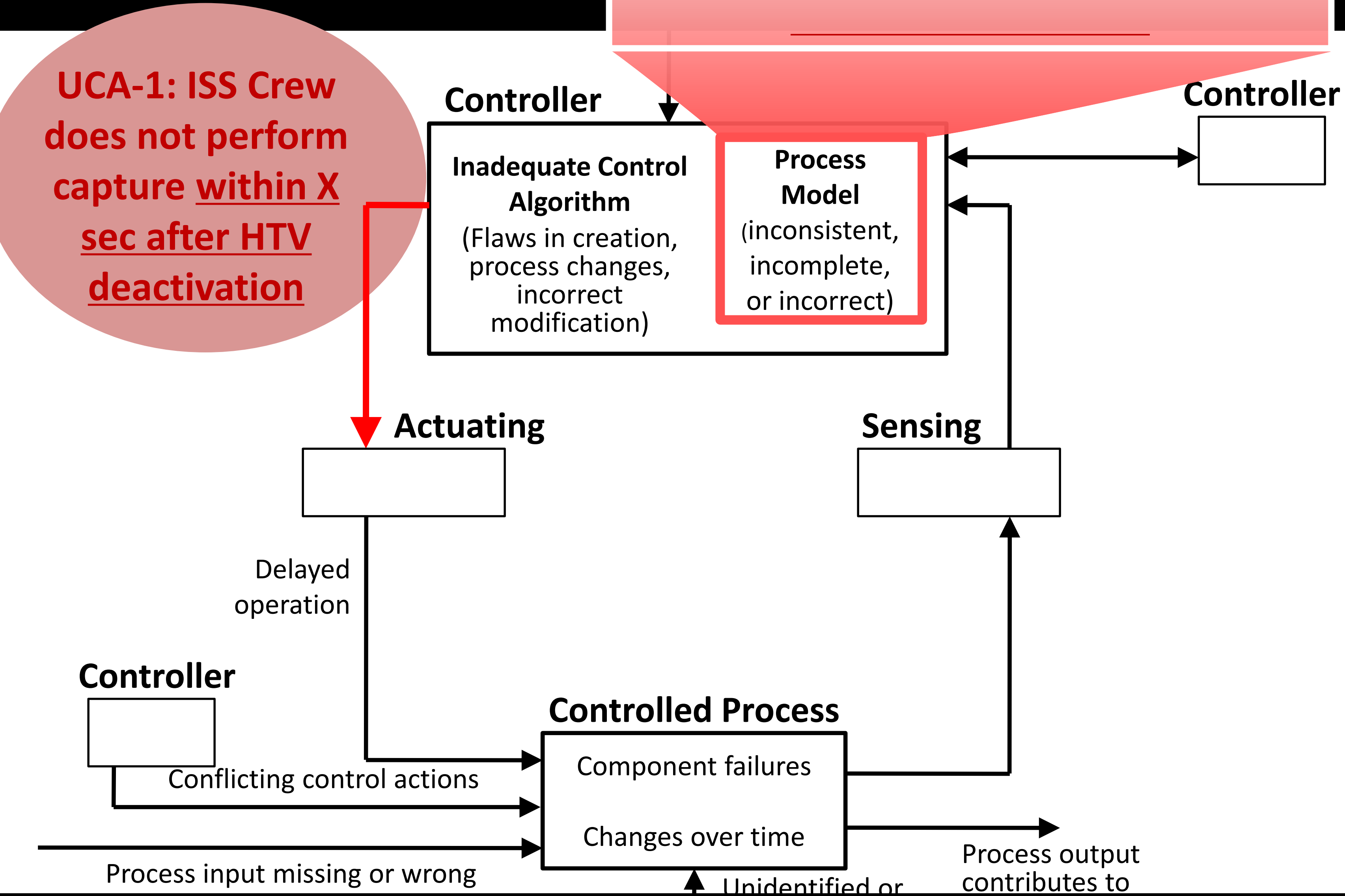
Changes over time

Process input missing or wrong

Unidentified or

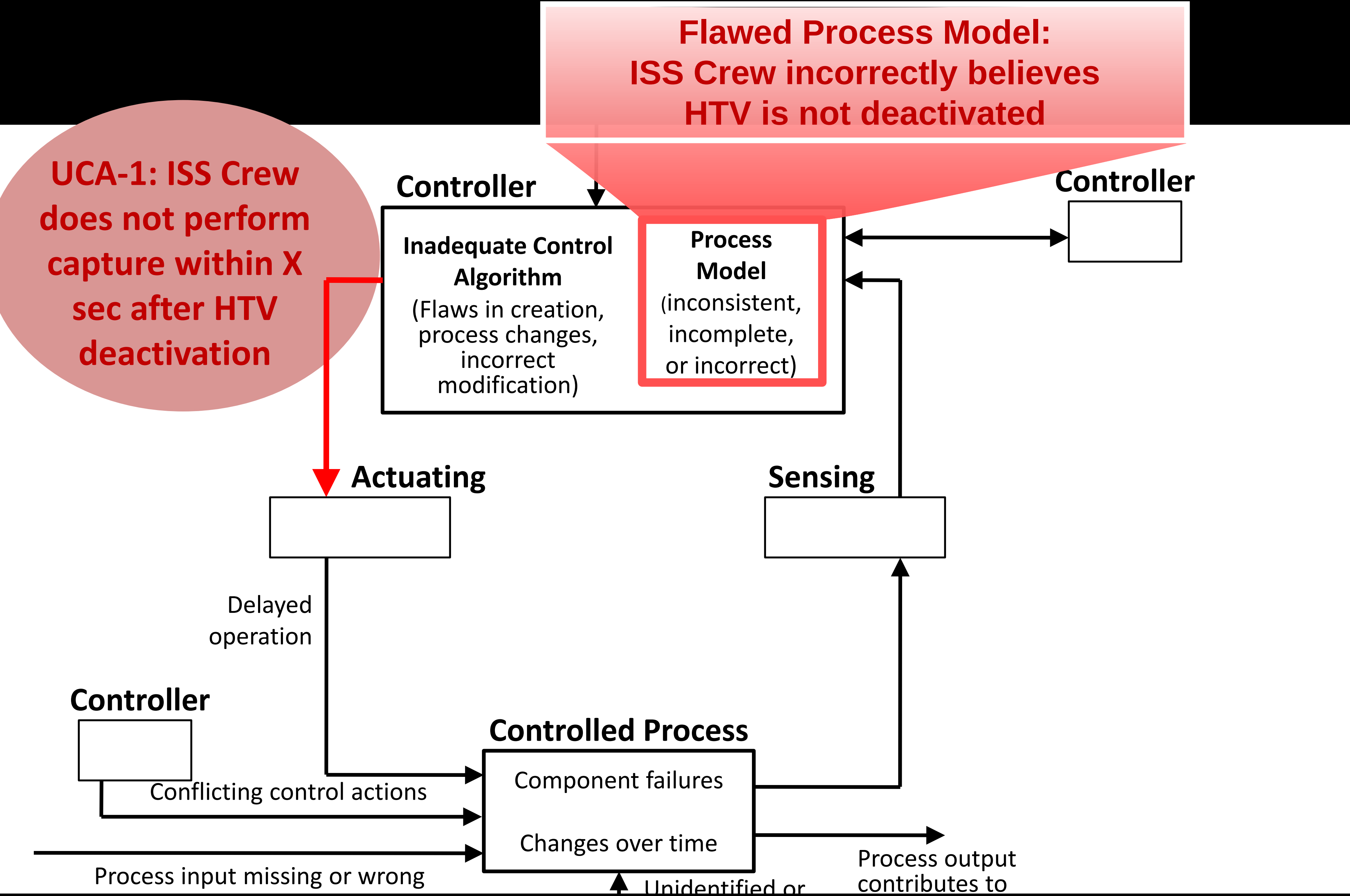
Process output contributes to

Flawed Process Model: ISS Crew incorrectly believes ______________



UCA-1: ISS Crew does not perform capture <u>within X sec after HTV deactivation</u>

Controller
Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification)
Process Model
(inconsistent, incomplete, or incorrect)
Controller
Actuating
Sensing
Delayed operation
Controller
Conflicting control actions
Controlled Process
Component failures
Changes over time
Process input missing or wrong
Unidentified or
Process output contributes to



Flawed Process Model:
ISS Crew incorrectly believes HTV is not deactivated

UCA-1: ISS Crew does not perform capture within X sec after HTV deactivation

Controller

Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification)

Process Model
(inconsistent, incomplete, or incorrect)

Controller

Actuating

Sensing

Delayed operation

Controller

Conflicting control actions

Controlled Process

Component failures

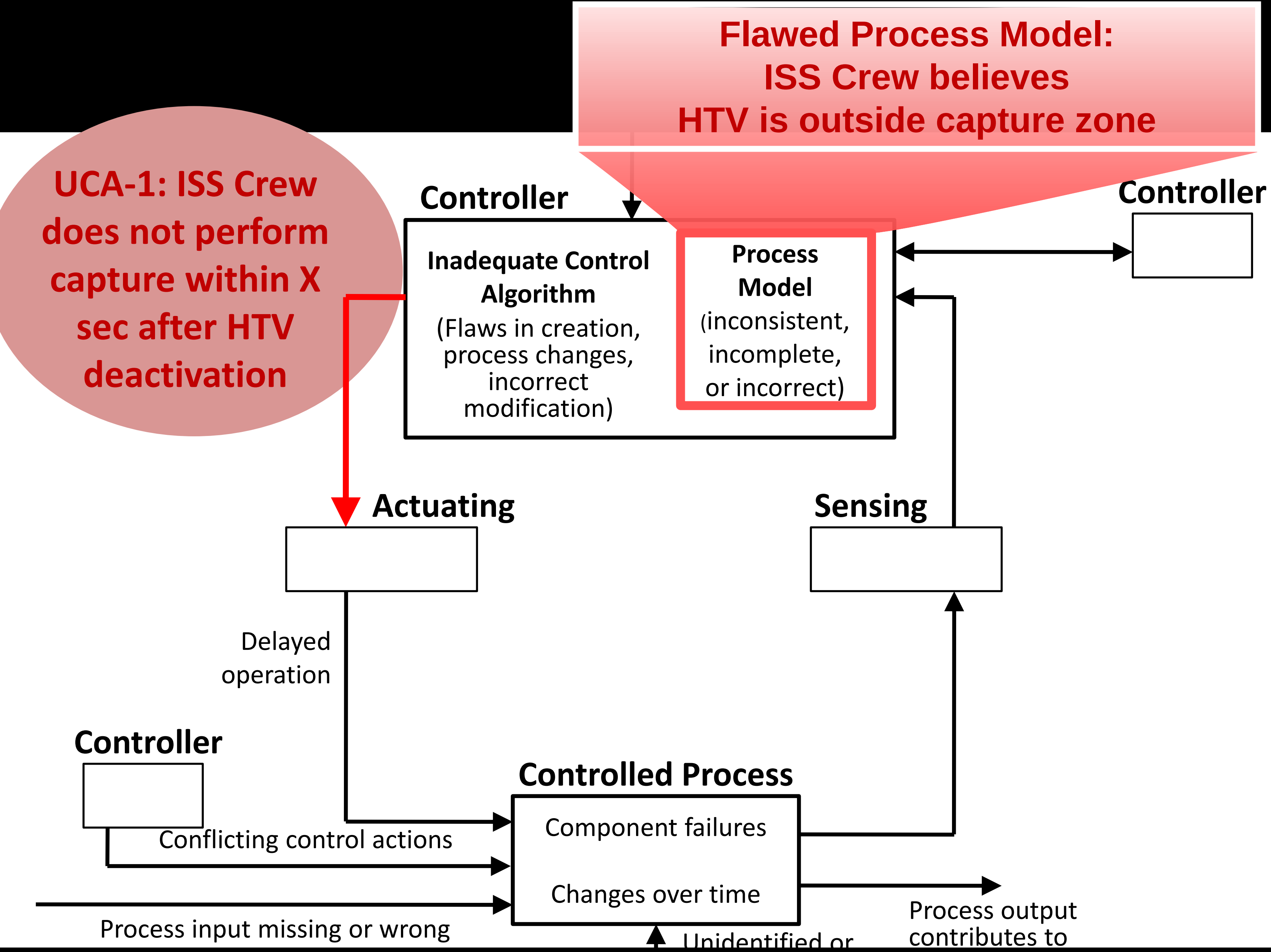
Changes over time

Process input missing or wrong

Unidentified or

Process output contributes to

Flawed Process Model: ISS Crew believes HTV is outside capture zone



UCA-1: ISS Crew does not perform capture within X sec after HTV deactivation

Controller

Inadequate Control Algorithm

(Flaws in creation, process changes, incorrect modification)

Process Model

(inconsistent, incomplete, or incorrect)

Controller

Actuating

Sensing

Delayed operation

Controller

Conflicting control actions

Controlled Process

Component failures

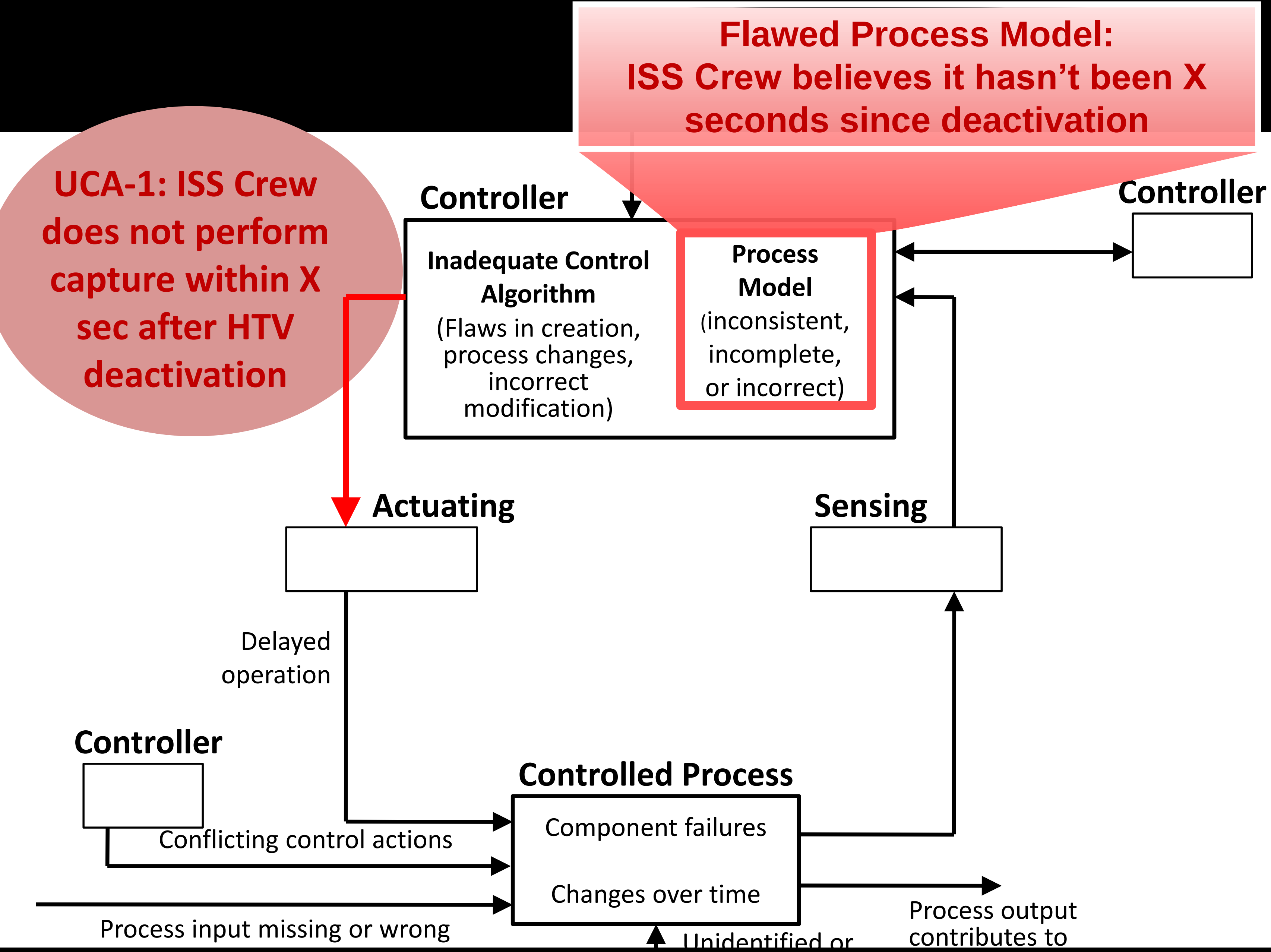
Changes over time

Process input missing or wrong

Unidentified or

Process output contributes to

Flawed Process Model: ISS Crew believes it hasn’t been X seconds since deactivation



UCA-1: ISS Crew does not perform capture within X sec after HTV deactivation

Controller

Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification)

Process Model
(inconsistent, incomplete, or incorrect)

Controller

Actuating

Sensing

Delayed operation

Controller

Conflicting control actions

Controlled Process

Component failures

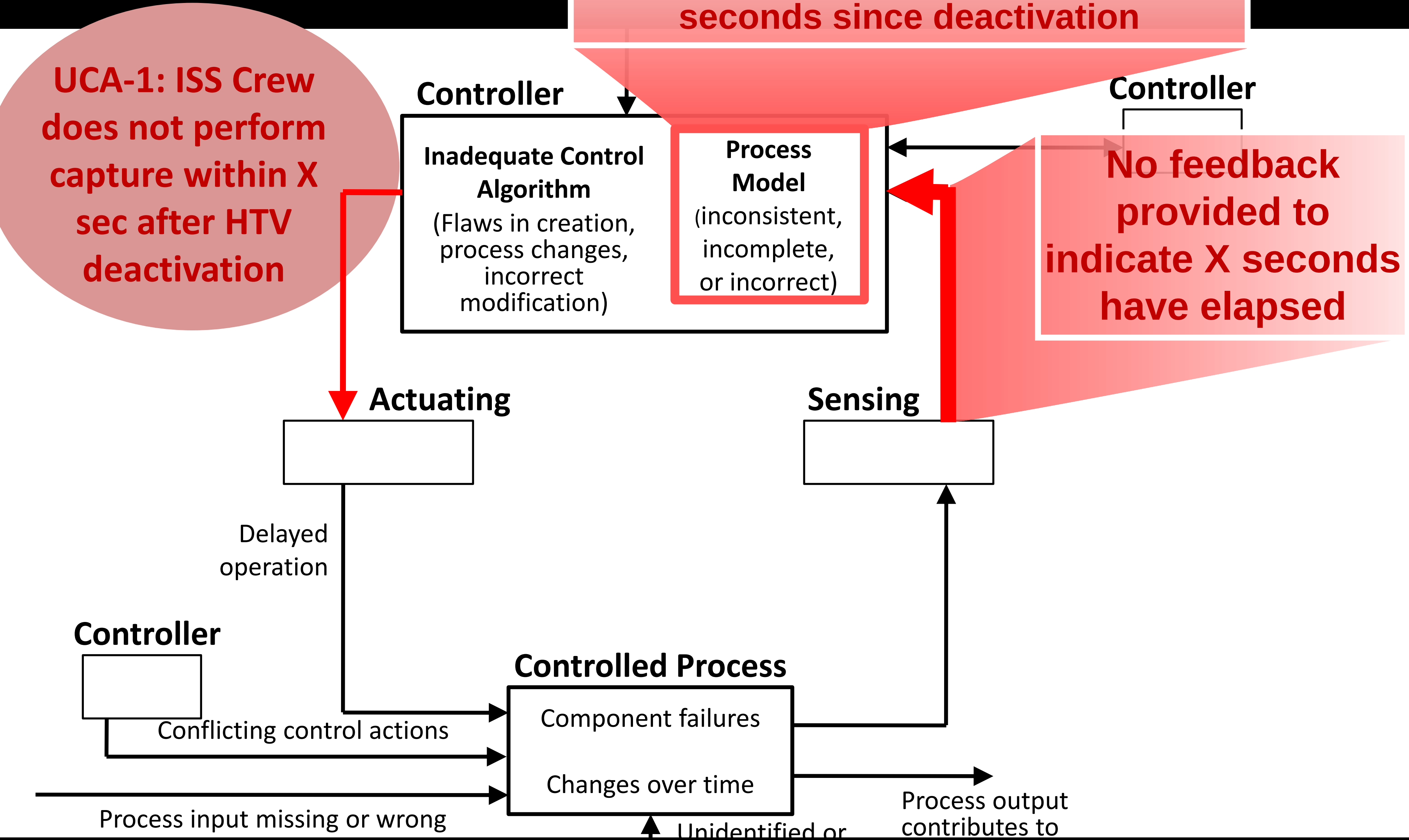
Changes over time

Process input missing or wrong

Unidentified or

Process output contributes to

Flawed Process Model:
ISS Crew believes it hasn't been X seconds since deactivation



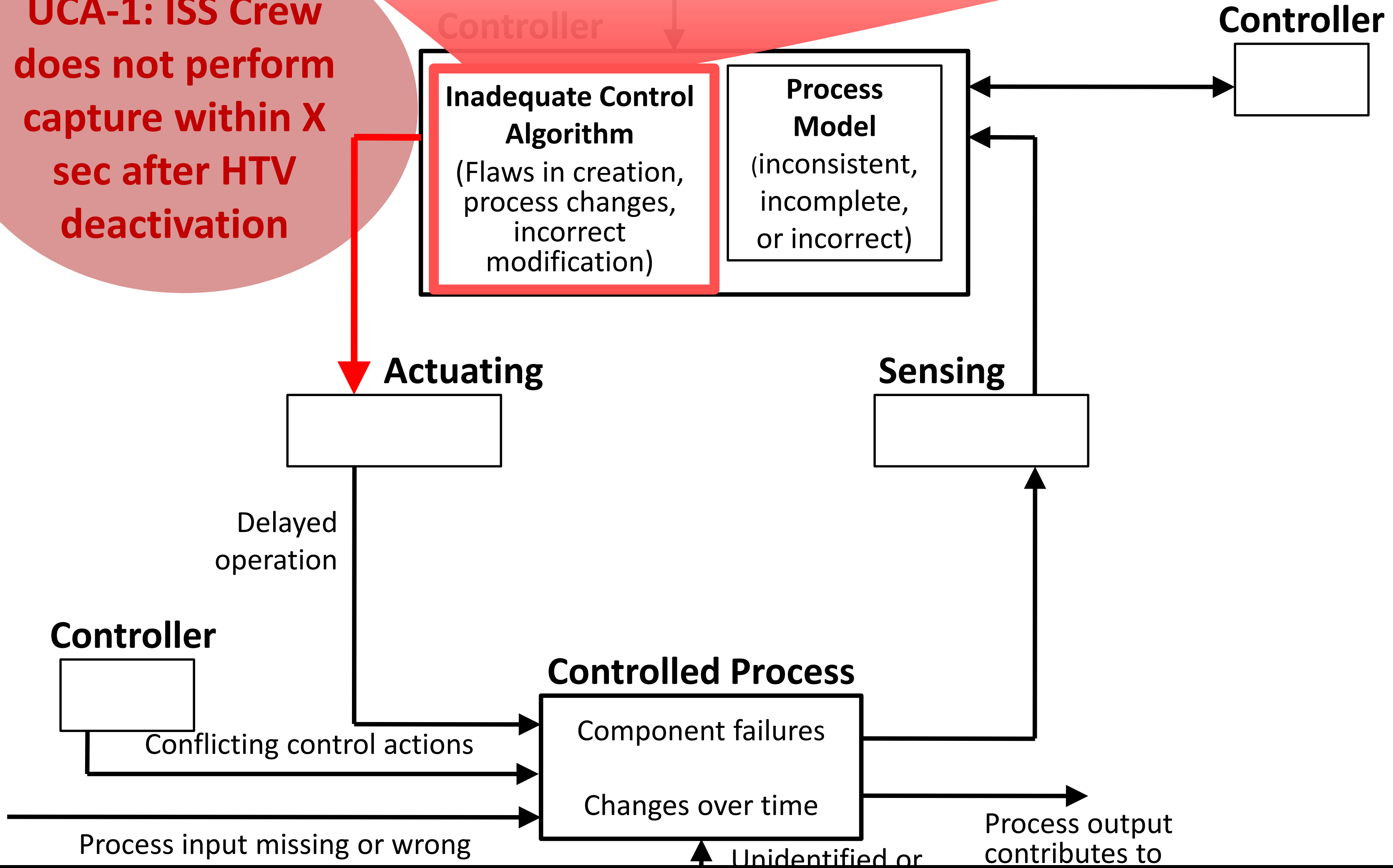
UCA-1: ISS Crew does not perform capture within X sec after HTV deactivation

No feedback provided to indicate X seconds have elapsed

Controller
Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification)
Process Model
(inconsistent, incomplete, or incorrect)
Controller
Actuating
Sensing
Delayed operation
Controller
Conflicting control actions
Controlled Process
Component failures
Changes over time
Process input missing or wrong
Unidentified or
Process output contributes to

Crew knows HTV is deactivated in capture box, but decide to let it drift closer (may be easier to capture)

UCA-1: ISS Crew does not perform capture within X sec after HTV deactivation



Controller

Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification)

Process Model
(inconsistent, incomplete, or incorrect)

Controller

Actuating

Sensing

Delayed operation

Controller

Conflicting control actions

Controlled Process

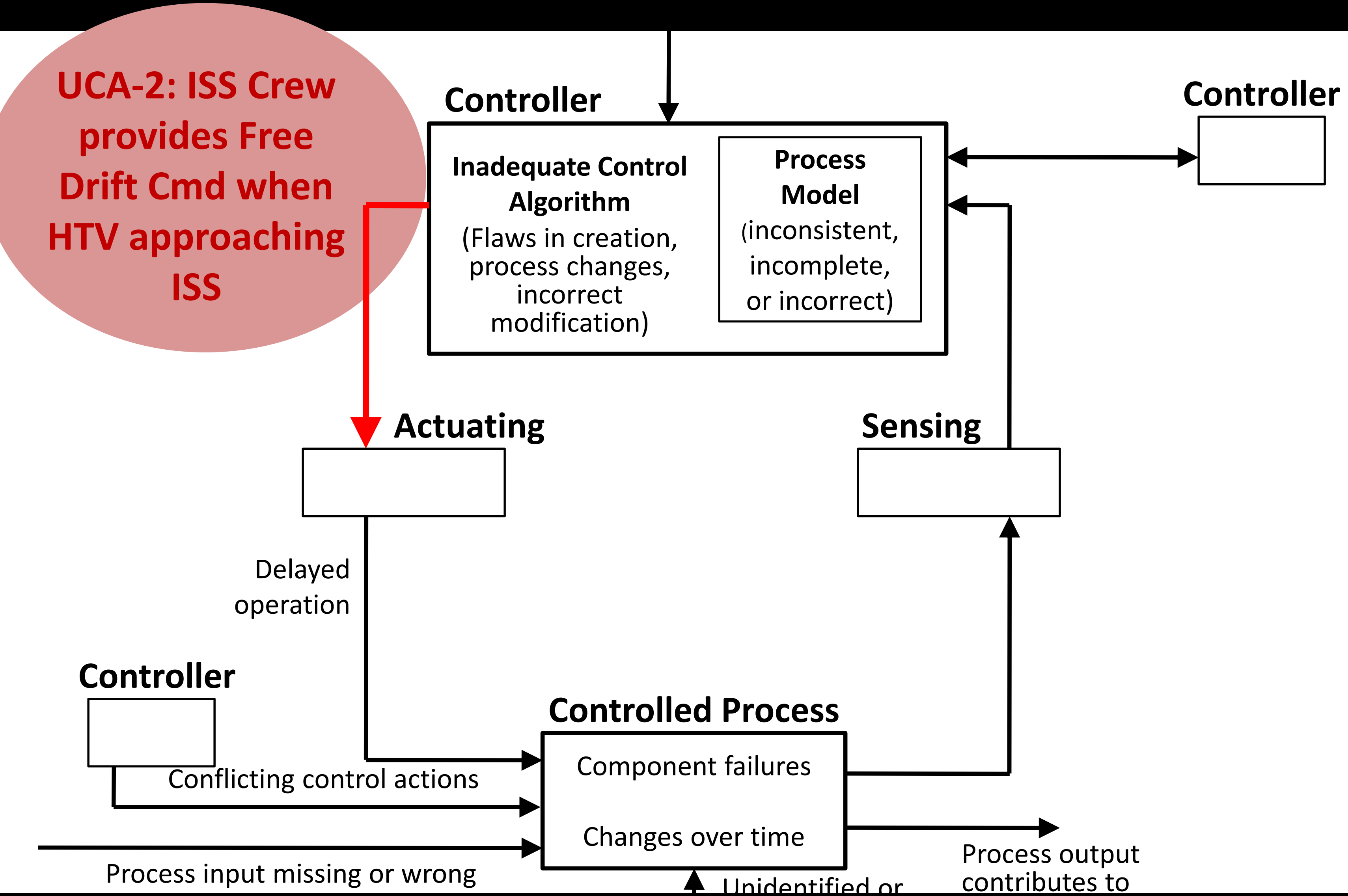
Component failures

Changes over time

Process input missing or wrong

Unidentified or

Process output contributes to



UCA-2: ISS Crew provides Free Drift Cmd when HTV approaching ISS

Controller

Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification)

Process Model
(inconsistent, incomplete, or incorrect)

Controller

Actuating

Sensing

Delayed operation

Controller

Controlled Process

Component failures

Changes over time

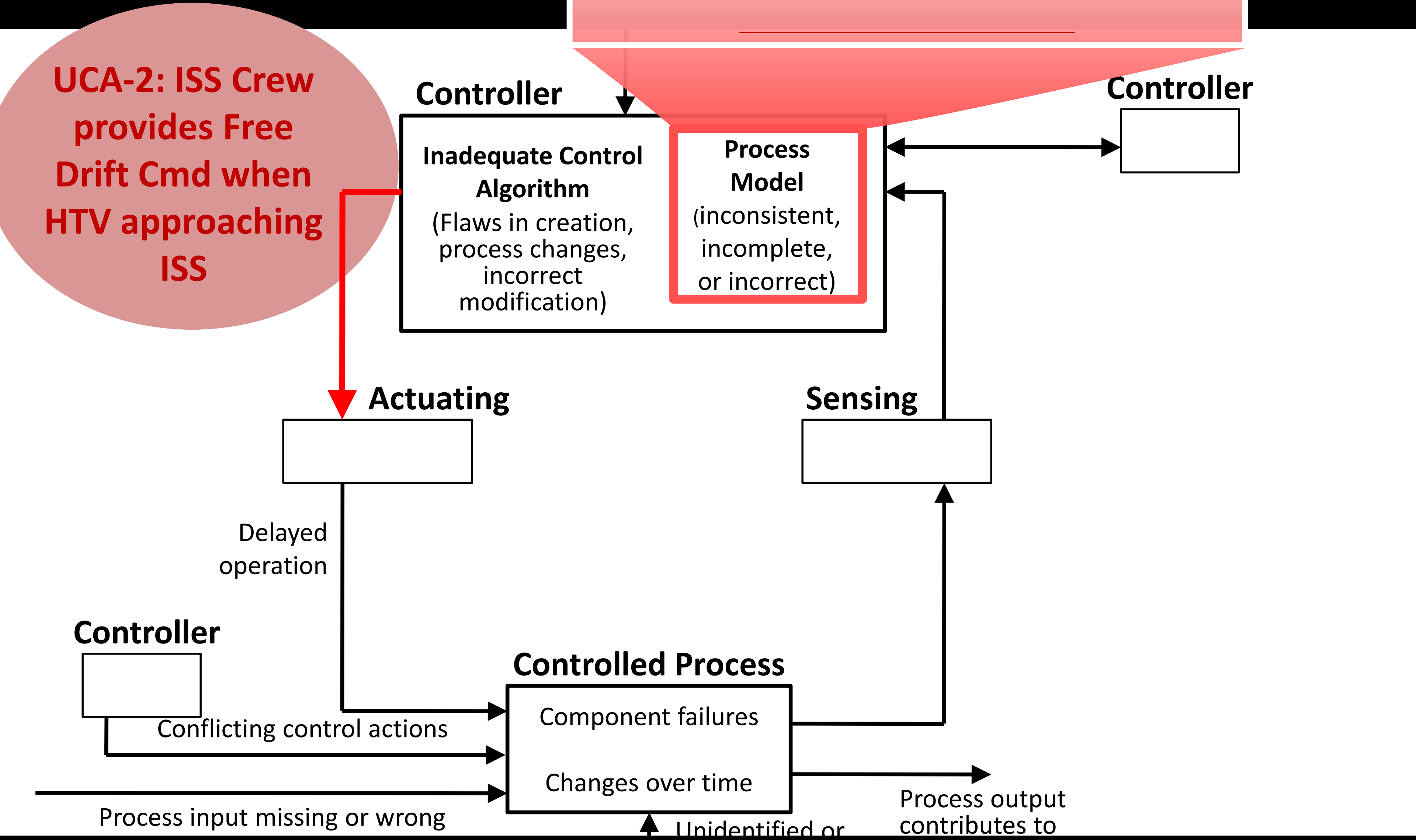
Conflicting control actions

Process input missing or wrong

Unidentified or

Process output contributes to

Flawed Process Model: ISS Crew incorrectly believes ____________



UCA-2: ISS Crew provides Free Drift Cmd when HTV approaching ISS

Controller

Inadequate Control Algorithm

(Flaws in creation, process changes, incorrect modification)

Process Model

(inconsistent, incomplete, or incorrect)

Controller

Actuating

Sensing

Delayed operation

Controller

Controlled Process

Component failures

Changes over time

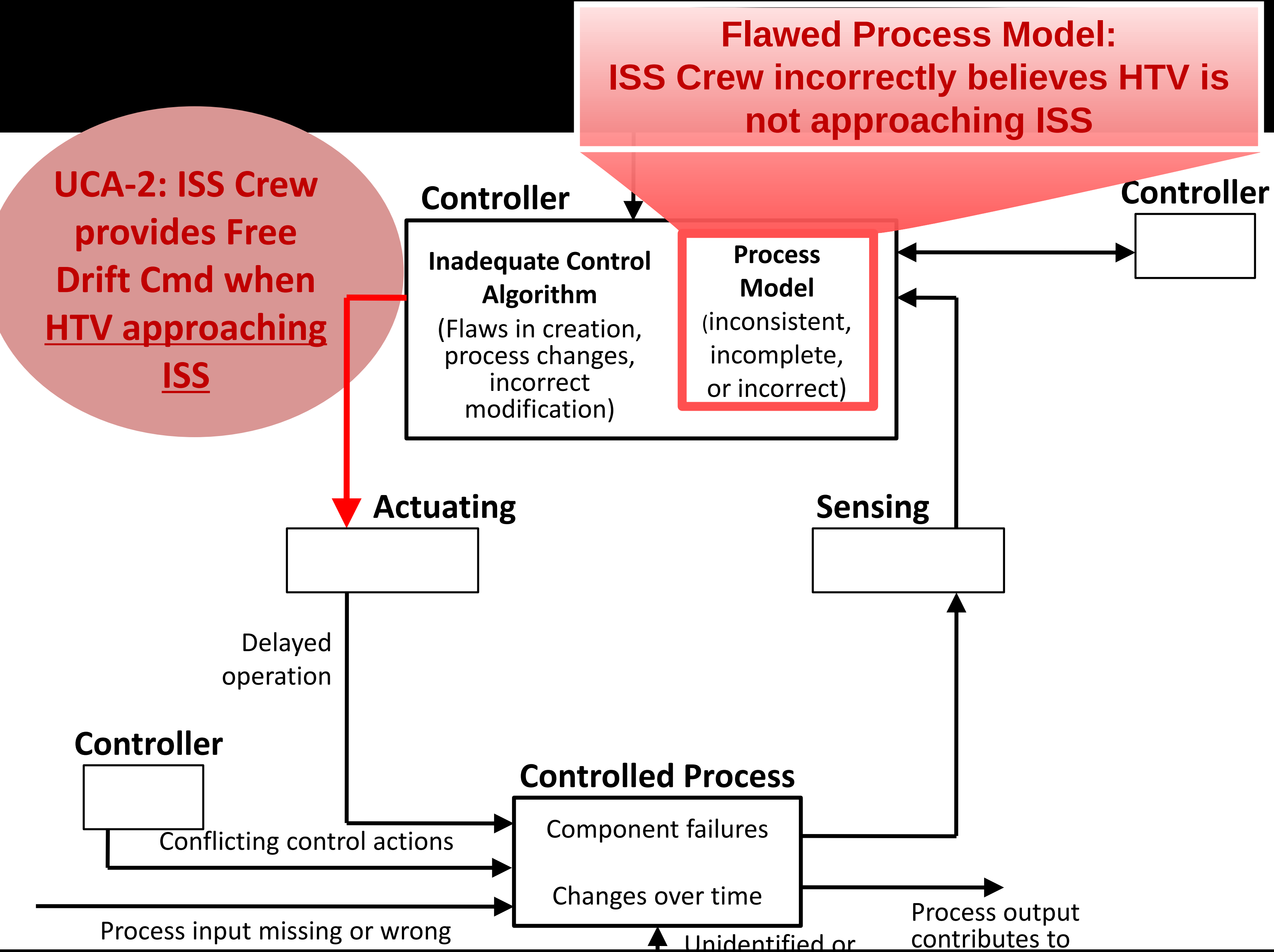
Conflicting control actions

Process input missing or wrong

Unidentified or

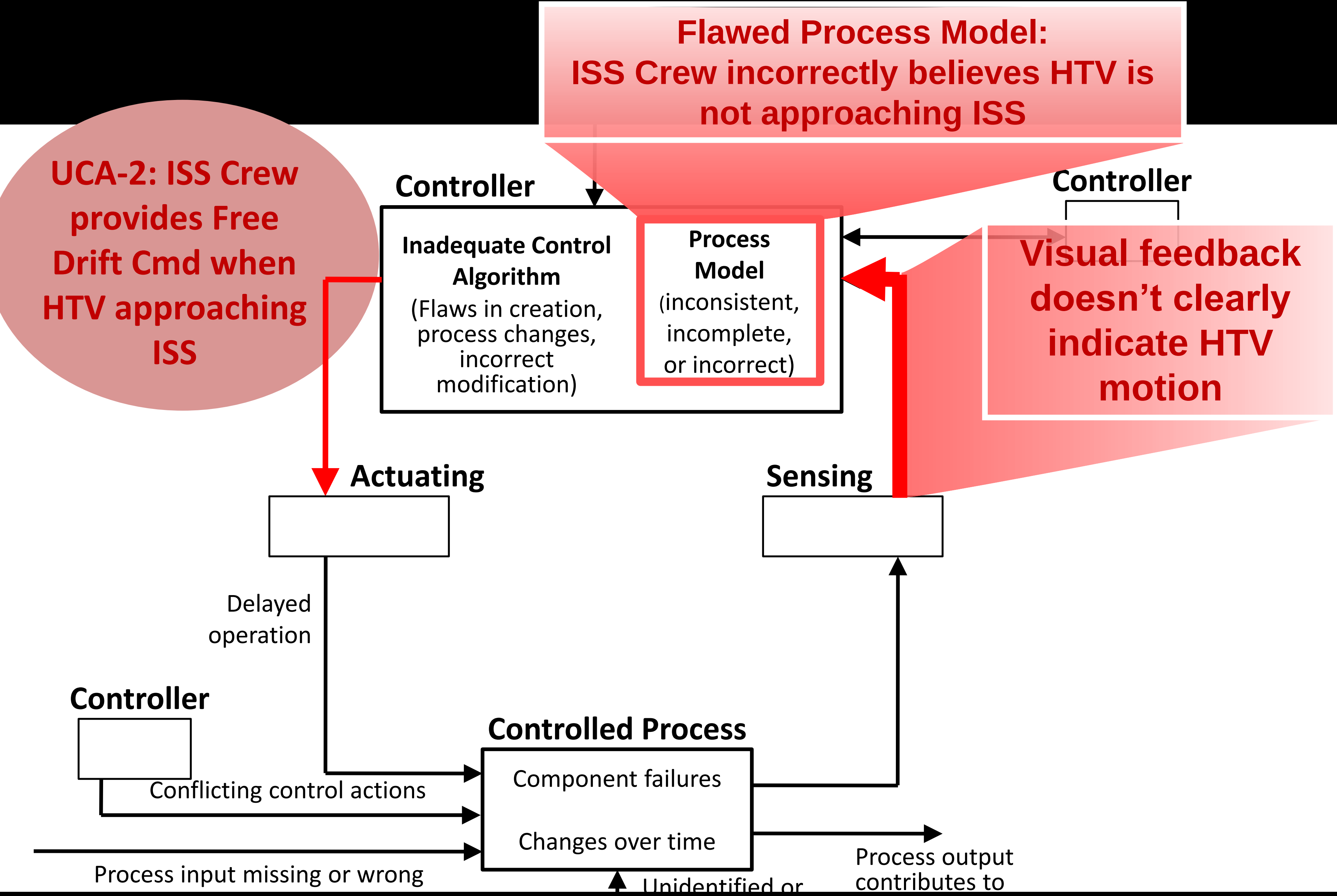
Process output contributes to

Flawed Process Model: ISS Crew incorrectly believes HTV is not approaching ISS



UCA-2: ISS Crew provides Free Drift Cmd when <u>HTV approaching ISS</u>

Controller
Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification)
Process Model
(inconsistent, incomplete, or incorrect)
Controller
Actuating
Sensing
Delayed operation
Controller
Controlled Process
Component failures
Changes over time
Conflicting control actions
Process input missing or wrong
Unidentified or
Process output contributes to



Flawed Process Model: ISS Crew incorrectly believes HTV is not approaching ISS

UCA-2: ISS Crew provides Free Drift Cmd when HTV approaching ISS

Controller

Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification)

Process Model
(inconsistent, incomplete, or incorrect)

Controller

Visual feedback doesn't clearly indicate HTV motion

Actuating

Sensing

Delayed operation

Controller

Conflicting control actions

Controlled Process

Component failures

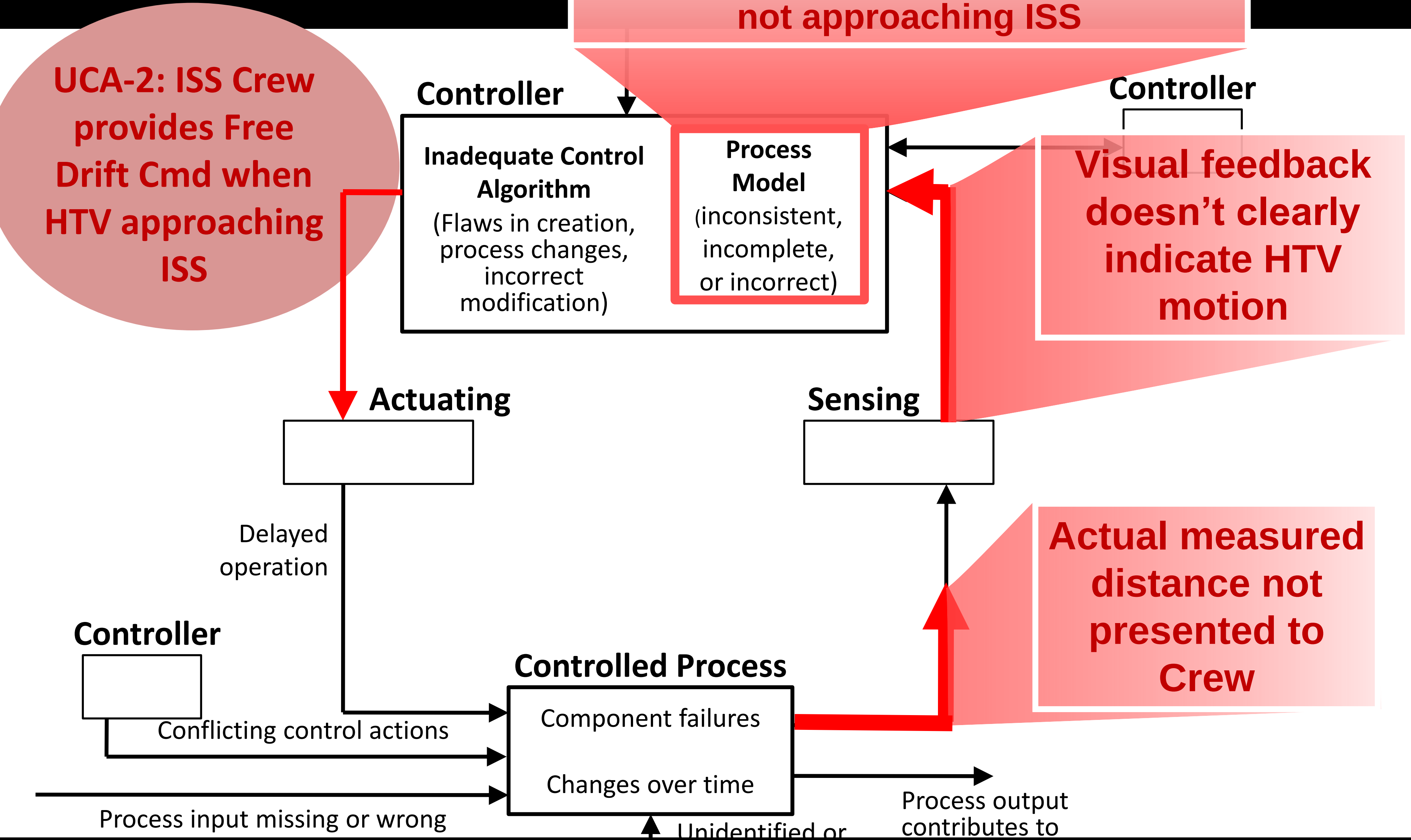
Changes over time

Process input missing or wrong

Unidentified or

Process output contributes to

Flawed Process Model:
ISS Crew incorrectly believes HTV is not approaching ISS



UCA-2: ISS Crew provides Free Drift Cmd when HTV approaching ISS

Visual feedback doesn't clearly indicate HTV motion

Actual measured distance not presented to Crew

Controller
Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification)
Process Model
(inconsistent, incomplete, or incorrect)
Controller
Actuating
Sensing
Delayed operation
Controller
Conflicting control actions
Controlled Process
Component failures
Changes over time
Process input missing or wrong
Unidentified or
Process output contributes to

If STPA had been used earlier, how might you address this problem? What would it cost?