

September 17, 2010

NASA 2010 IV&V Annual Workshop

Modeling and Hazard Analysis using STPA

Takuto Ishimatsu, Nancy Leveson, John Thomas

Massachusetts Institute of Technology (MIT)

Masa Katahira, Yuko Miyamoto

Japan Aerospace Exploration Agency (JAXA)

Haruka Nakao

Japan Manned Space Systems Corporation (JAMSS)

Introduction

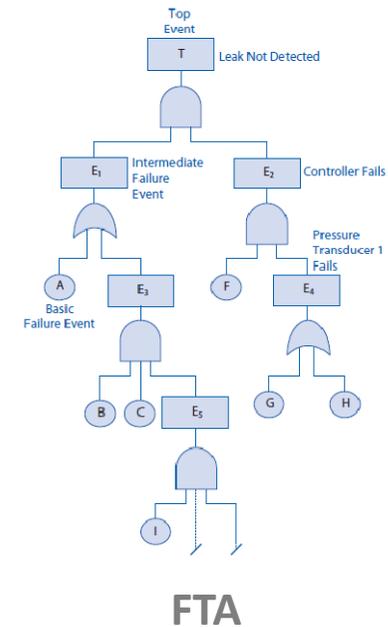
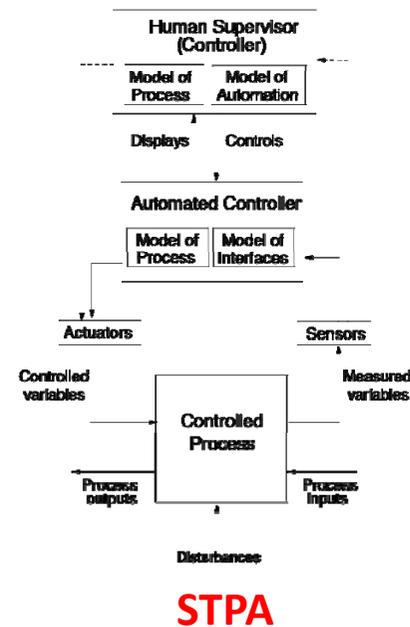
A joint research project between MIT and JAXA/JAMSS

Purpose: Determine the feasibility and usefulness of STPA

Case Study: JAXA HTV

❖ Comparison between **STPA results** and FTA-based hazard analysis results explicitly stated in the past hazard reports

- Problems identified?
- Resources required?



STAMP/STPA



STAMP/STPA

A new accident model:

STAMP (Systems-Theoretic Accident Model and Processes)

A new hazard analysis technique:

STPA (STAMP-Based Process Analysis)

- Views safety as a dynamic control problem rather than a component failure problem
- Accidents are the result of the inadequate control
 - Result from lack of enforcement of safety constraints

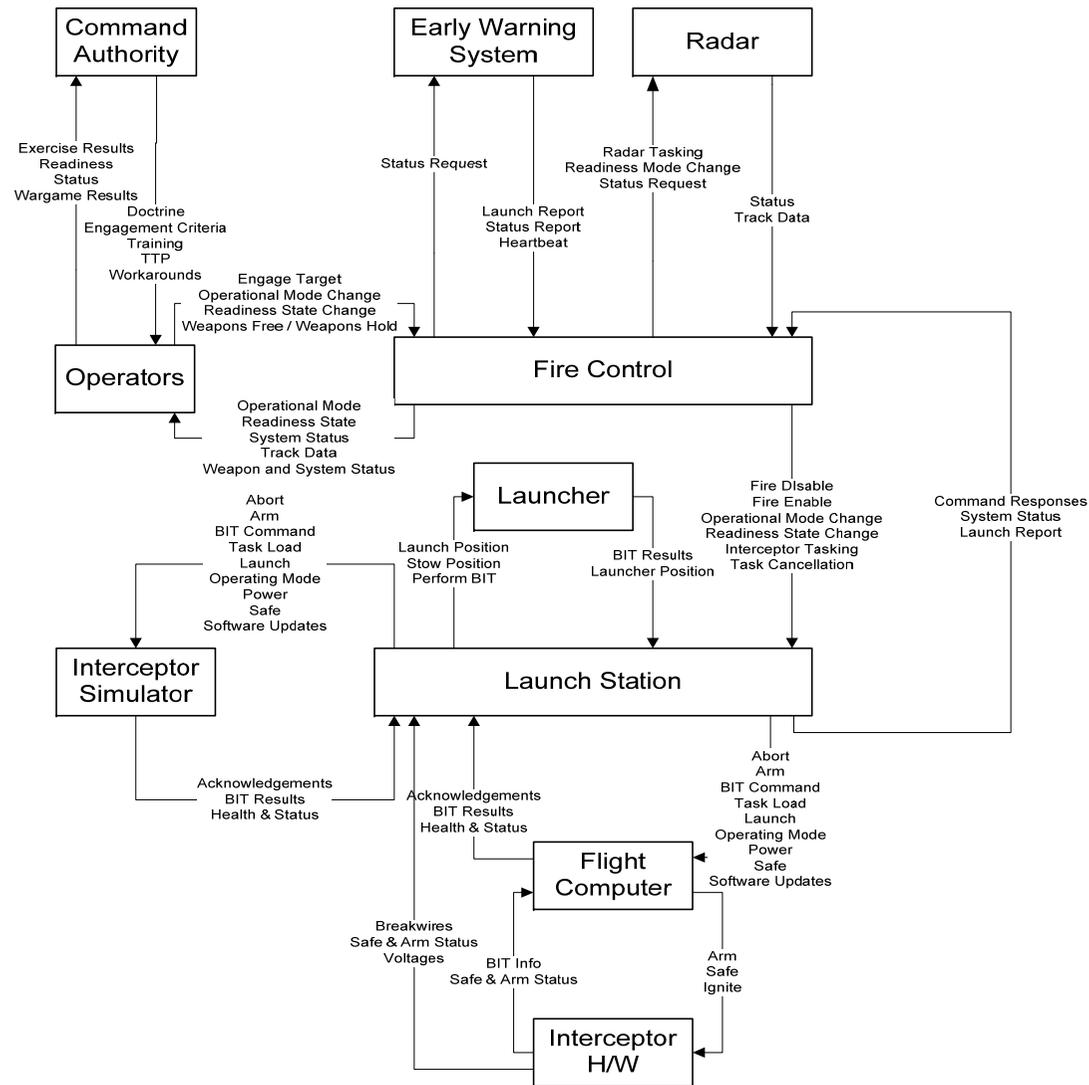
Prevent failures → Enforce safety constraints

- Can be used to drive the earliest design decisions
 - **Safety-driven design**
- Can also be applied in an after-the-fact analysis and hazard assessment

STPA Steps

1. Identify hazards and translate them into high-level requirements and constraints on behavior.
2. Define a basic control structure.
→ Control Structure Diagram
- 3a. Identify potential inadequate control actions that could lead to a hazardous state.
- 3b. Use identified inadequate control actions to refine system safety design constraints.
4. Determine how potentially hazardous control actions could occur (scenarios of how constraints can be violated). Eliminate from design or control in design or operations.

Control Structure Diagram Example



Inadequate Control Actions

Inadequate control actions fall into the following four general categories:

1. “Not Provided”

A required control action to maintain safety is not provided.

2. “Incorrectly Provided”

An incorrect or unsafe control action is provided that induces a loss.

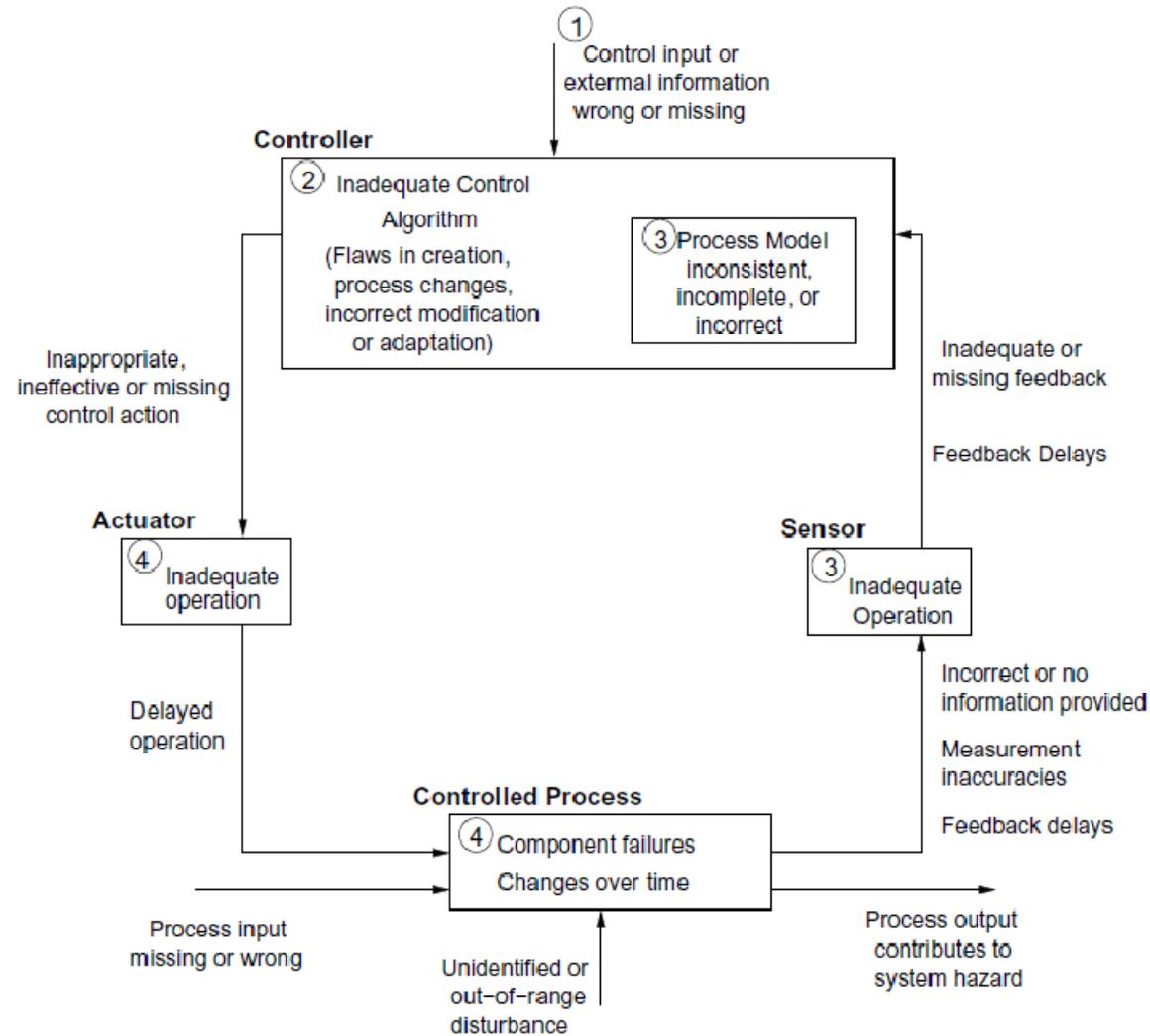
3. “Provided Too Early, Too Late, or Out of Sequence”

A potentially correct or adequate control action is provided too early, too late, or out of sequence.

4. “Stopped Too Soon”

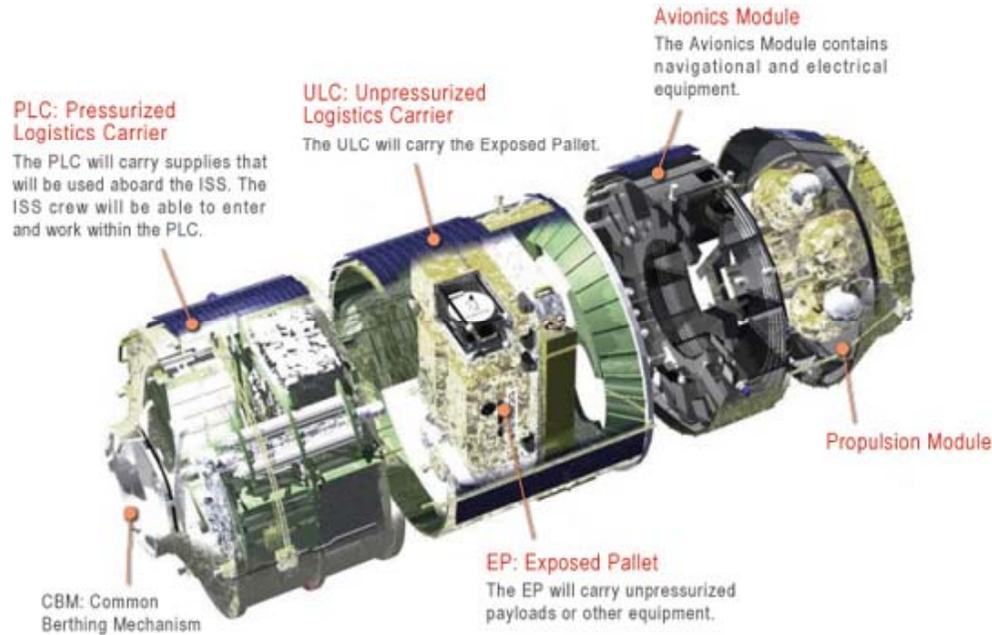
A correct control action is stopped too soon.

Causal Factors Leading to Hazards



JAXA's H-II Transfer Vehicle

HTV: H-II Transfer Vehicle



HTV Specifications

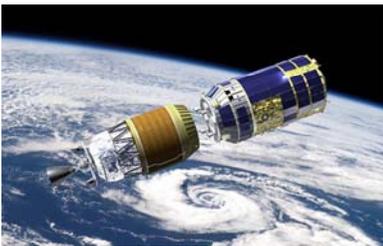
Items	Specifications
Length	9.8 m (including thrusters)
Diameter	4.4 m
Mass	10,500 kg
Propellant	Fuel: MMH Oxidizer: MON3 (Tetroxide)
Cargo capacity (supplies and equipment)	6,000 kg - Pressurized cargo: 4,500 kg - Unpressurized cargo: 1,500 kg
Cargo capacity (waste)	Max. 6,000 kg
Target orbit to ISS	Altitude: 350-460 km Inclination: 51.6 degrees
Max. mission duration	Solo flight: 100 hours Stand-by (on-orbit): > 1 week Berthed with ISS: Max. 30 days

HTV-1 (Sep 10 – Nov 2): **successful**

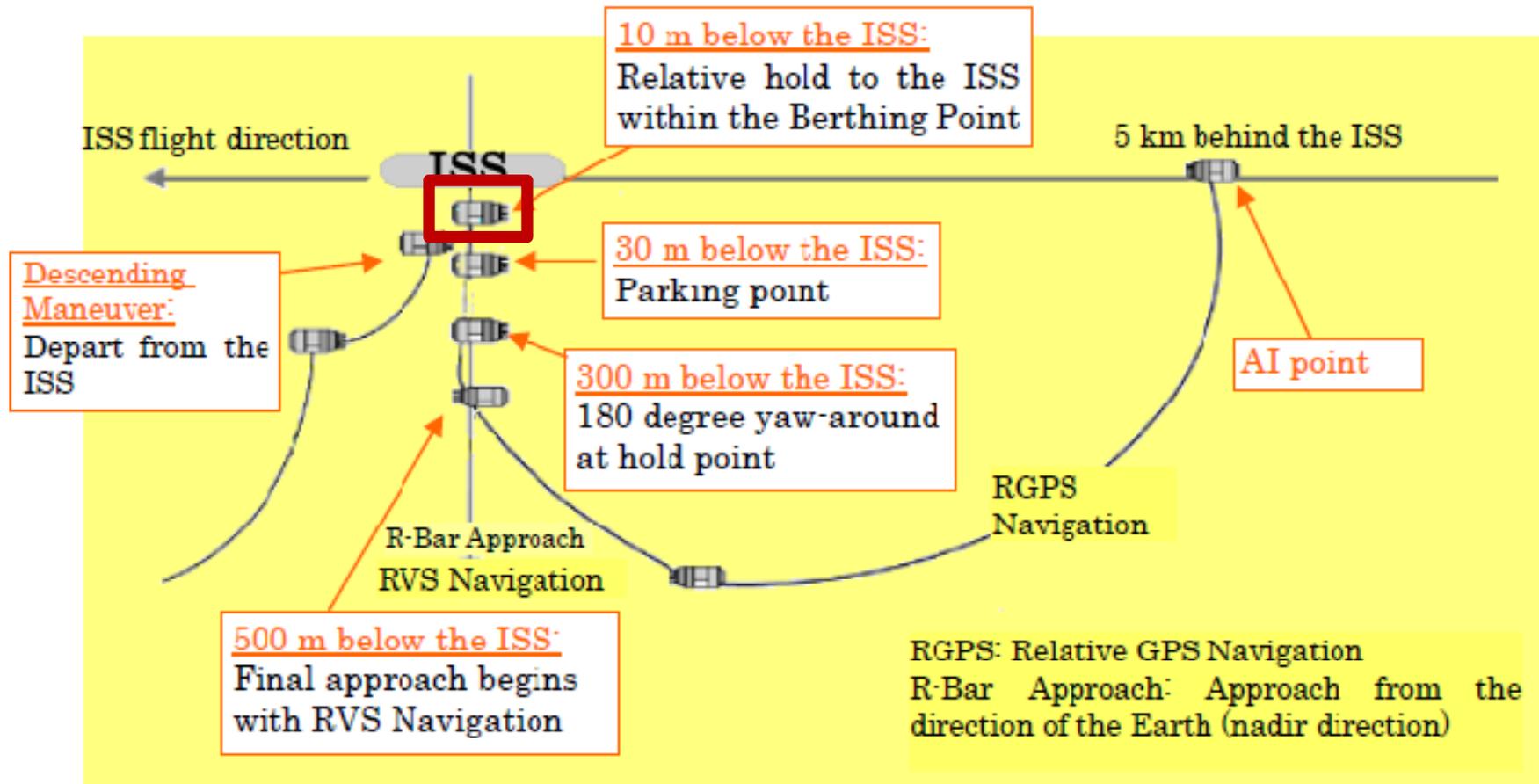
- Launched at the TNSC aboard the H-IIB rocket
- Performed the demonstration tests
- Rendezvoused and berthed with the ISS
- Released and departed from the ISS
- Performed the fiery re-entry and disintegration

HTV Operations

1. Launch
2. Rendezvous flight to the ISS
3. Berthing with the ISS
4. Docked operations
5. Undock/Departure from the ISS
6. Reentry



PROX Operations



HTV's approach sequence during PROX Operations

STPA for HTV Capture Phase

HTV Proximity Operations



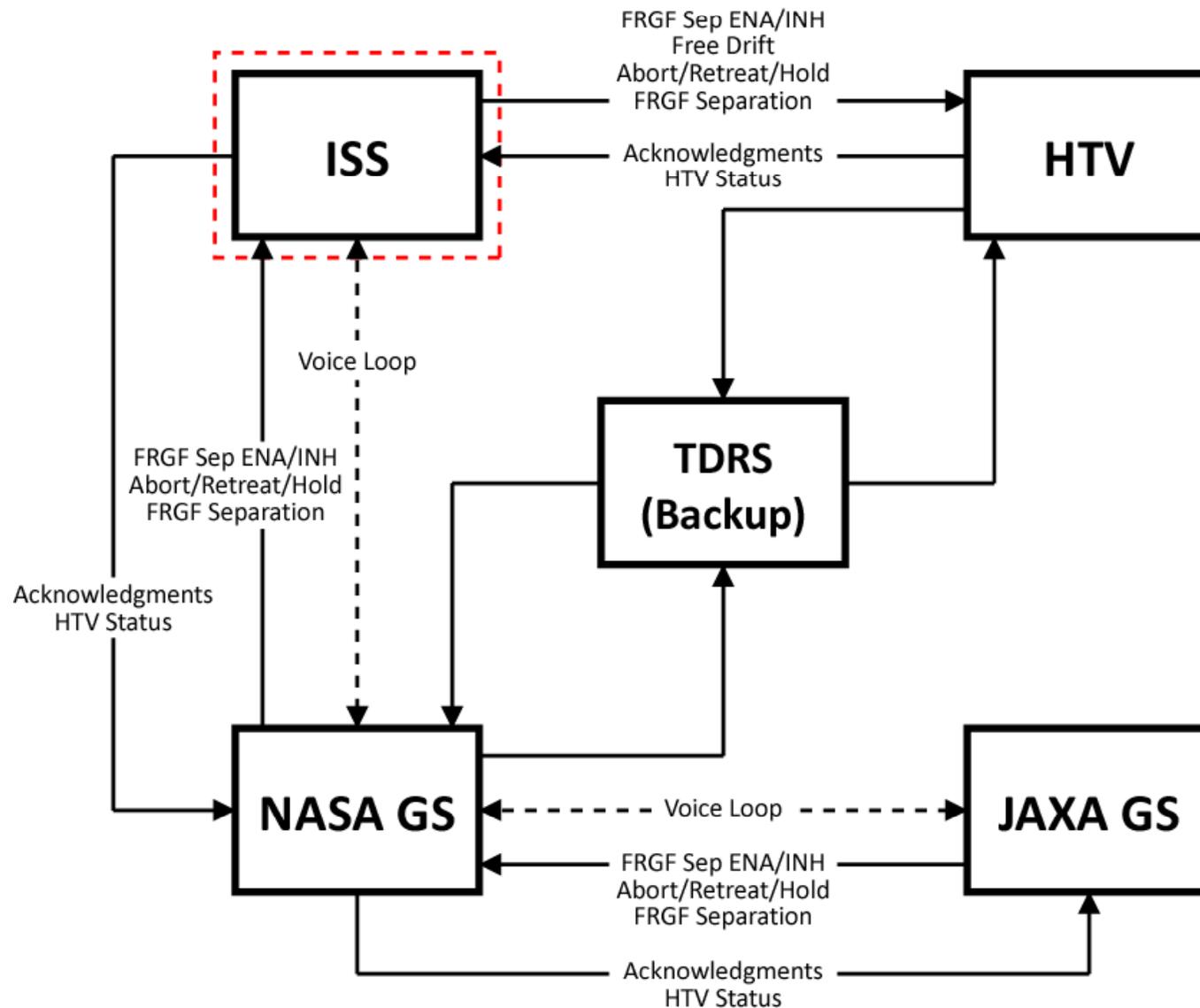
Hardware Command Panel (HCP)



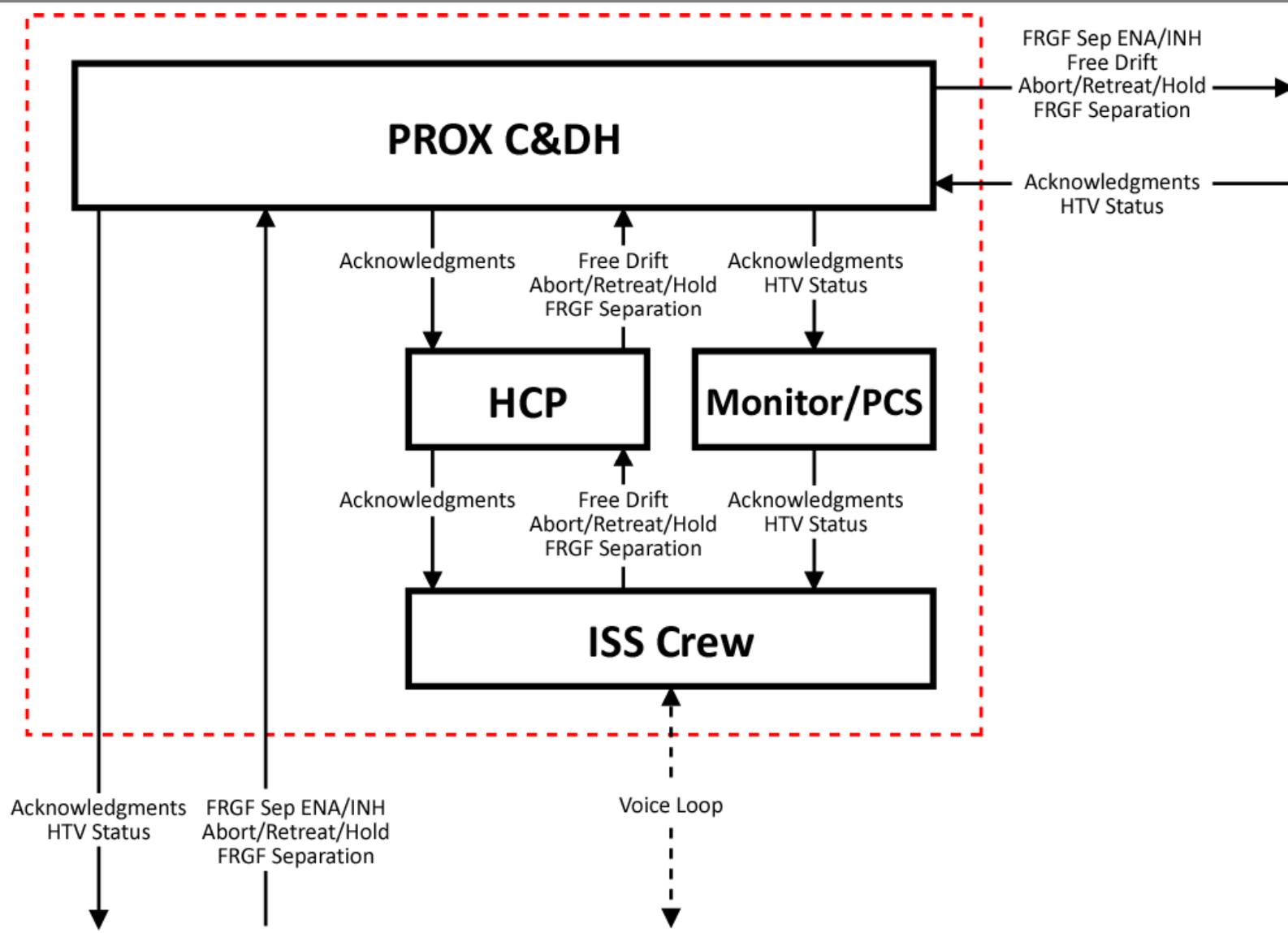
HCP key functions:

- ABORT
- RETREAT
Retreat to 30 m or 100 m below the ISS
- HOLD
Hold the approach
- FREE DRIFT
Disable the HTV thrusters
- FRGF SEP
Separate the Flight Releasable Grapple Fixture (FRGF)

Control Structure Diagram – Level 0



Control Structure Diagram – ISS Level 1



Command Sequence (Capture Phase)

#	Event/Command	from	to	Description
1	FRGF Sep ENA	JAXA GS	HTV	Enable FRGF separation in case of emergency
2	Free Drift (Deactivation)	ISS (Crew)	HTV	Transition from "Capture Point Hold Mode" to "Free Drift Mode" to disable the HTV guidance and control functions
C	Capture	ISS (Crew)	HTV	Manipulate the SSRMS to capture FRGF of the HTV
3	FRGF Sep INH	JAXA GS	HTV	Inhibit FRGF separation to prevent an unintended separation after the capture

Hazardous Control Behavior Table

#	Event/Command	Category 1	Category 2			Category 3			Category 4
		Not Provided	Incorrectly Provided			Provided			Stopped Too Soon
			Abort/Retreat/Hold (unintended)	Free Drift (unintended)	FRGF Sep (unintended)	Too Early	Too Late	Out of Sequence	
1	FRGF Sep ENA	If this is not detected and capture is started, (1a) the HTV might not be separated immediately in the emergency situation of the HTV being grappled incorrectly and rotating to collide with the robotic arm.	If it is not detected that	If Deactivation command is provided instead of FRGF Sep ENA, the mode transition is too early and (1b) the HTV will drift out of the capture box. In combination with no activation command or a late one, the HTV will remain a free-flying object that could collide with the ISS.	If FRGF Separation command is provided, nothing will happen since FRGF separation remains inhibited.	FRGF Sep ENA is	If FRGF Sep ENA is	If FRGF Sep ENA is	N/A
2	Free Drift (Deactivation)	If this is not detected and capture is started, (2a) the capture will be regarded as a disturbance to the HTV that could trigger an unintended attitude control or even Abort.	If the HTV fails to transition to the Free Drift Mode and capture is started, (2a).	If an Abort/Retreat/Hold command is provided instead of Deactivation, an unintended Abort/Retreat/Hold will start processing, which is not hazardous. But the mission will end up incomplete or the capture process will have to be started over.	Since FRGF separation has been enabled, if FRGF Separation command is provided instead of Deactivation, (2b) FRGF will be separated from the HTV to become a free-flying object, which is a threat of collision. The HTV will be no longer captured and the mission will end up incomplete.	Deactivation is provided too early and capture is not started immediately enough, (2b).	If Deactivation is provided too late, it will delay the capture process. Since FRGF separation has been enabled, it will contribute to increasing the possibility of an unintended FRGF separation by crew error.	If Deactivation is provided out of sequence with capture, (2a).	N/A
C	Capture	If capture is not performed, (1b).	If the crew makes an operational mistake of the SSRMS, (Ca) the robotic arm could hit the HTV to make it rotate and collide with the ISS.	If an Abort/Retreat/Hold command is provided, an unintended Abort/Retreat/Hold will start processing, which is not hazardous. But the mission will end up incomplete or the capture process will have to be started over.	Since the HTV has already been in the Free Drift Mode, nothing will happen. In combination with no or late capture, (1b).	Since the HTV has already been in the Free Drift Mode, a too early capture is nothing but good.	If capture is performed too late, (1b).	If capture is performed out of sequence with Deactivation, (2a).	If capture is stopped halfway and incomplete (Cb) the HTV is not fixed to the SSRMS and could rotate (windmill) to collide with the arm.
3	FRGF Sep INH	If FRGF Sep INH is not provided, the HTV is left capable of FRGF separation. An unintended FRGF separation after the successful capture could occur. (3a) In combination with no or late activation command, the HTV will remain a free-flying object that could collide with the ISS.	If FRGF Sep ENA is provided instead of INH, the HTV is left capable of FRGF separation. An unintended FRGF separation after the successful capture could occur. (3a).	If an Abort/Retreat/Hold command is provided, an unintended Abort/Retreat/Hold will start processing. If FRGF separation fails, CP Hold Mode will be provided, some thrusters by the SSRMS could trigger an attitude control.	Since the HTV has already been in the Free Drift Mode and captured by the SSRMS, nothing will happen.	Since capture has already been successfully completed, too early FRGF Sep INH is nothing but good.	If FRGF Sep INH is provided too late, it will just increase the time during which the HTV accepts an FRGF separation, which will then contribute to increasing the possibility of an unintended FRGF separation by crew error.	If FRGF Sep INH is out of sequence with capture, (1a).	N/A

Hazardous Control Behaviors

(1a) The HTV might not be separated immediately in the emergency situation of the HTV being grappled incorrectly and rotating to collide with the robotic arm.

(1b) The HTV will drift out of the capture box. In combination with no activation command or a late one, the HTV will remain a free-flying object that could collide with the ISS.

(2a) The capture will be regarded as a disturbance to the HTV that could trigger an unintended attitude control or even Abort.

(2b) FRGF will be separated from the HTV to become a free-flying object, which is a threat of collision. The HTV will be no longer captured and the mission will end up incomplete.

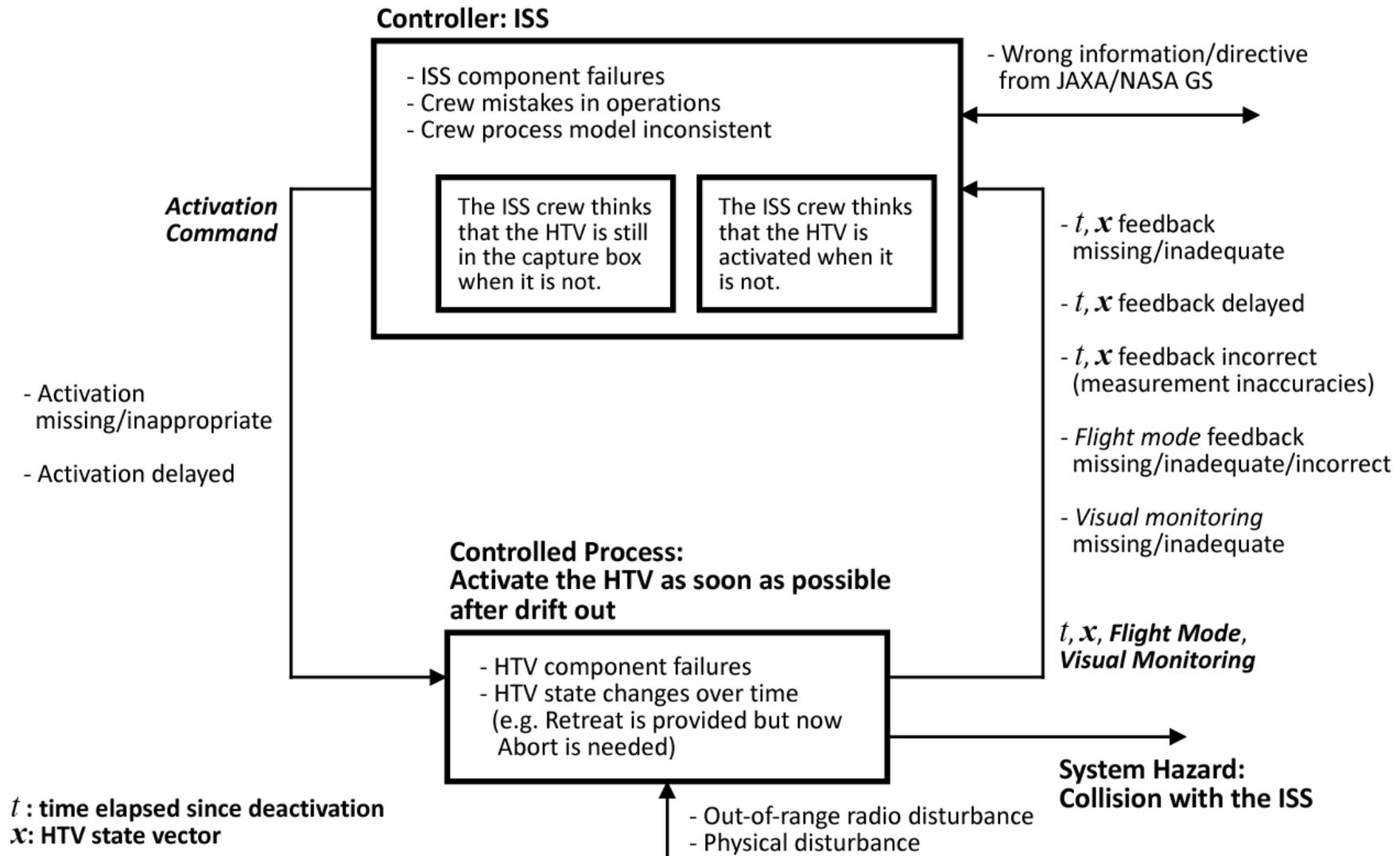
(Ca) The robotic arm could hit the HTV to make it rotate and collide with the ISS.

(Cb) The HTV is not fixed to the SSRMS and could rotate (windmill) to collide with the arm.

(3a) In combination with no or late activation command, the HTV will remain a free-flying object that could collide with the ISS.

(3b) The HTV will make some thrust with remaining captured by the SSRMS. A tension from the arm could be regarded as a disturbance to the HTV that might trigger an unintended attitude control.

Causal Factors Leading to Hazard (1b)



Causal Factors Identified by STPA

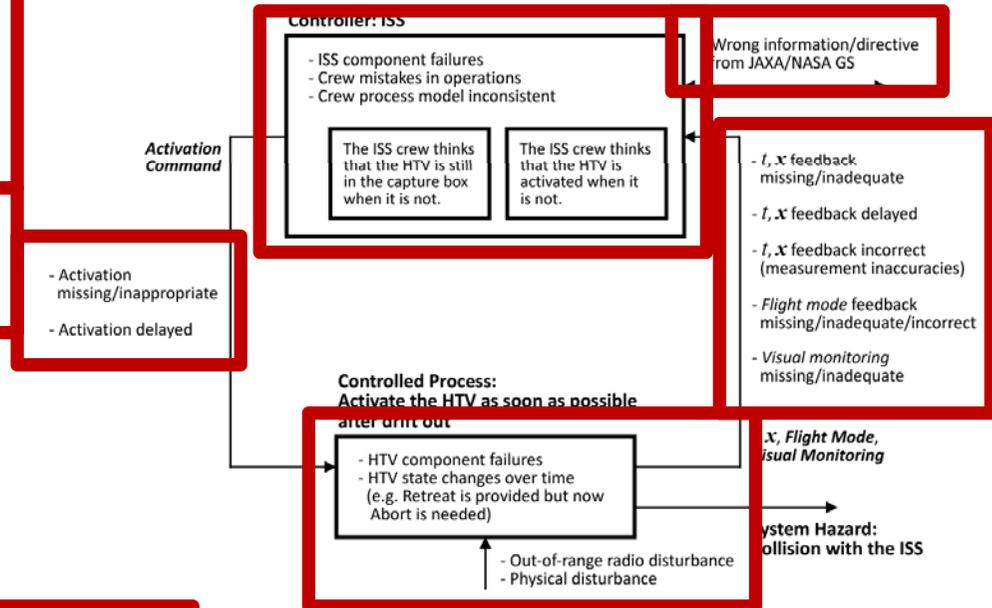
- ISS component failures
- Crew mistakes in operation
- Crew process model inconsistent

- Activation missing/inappropriate
- Activation delayed

- HTV component failures
- HTV state changes over time
- Out-of-range radio disturbance
- Physical disturbance

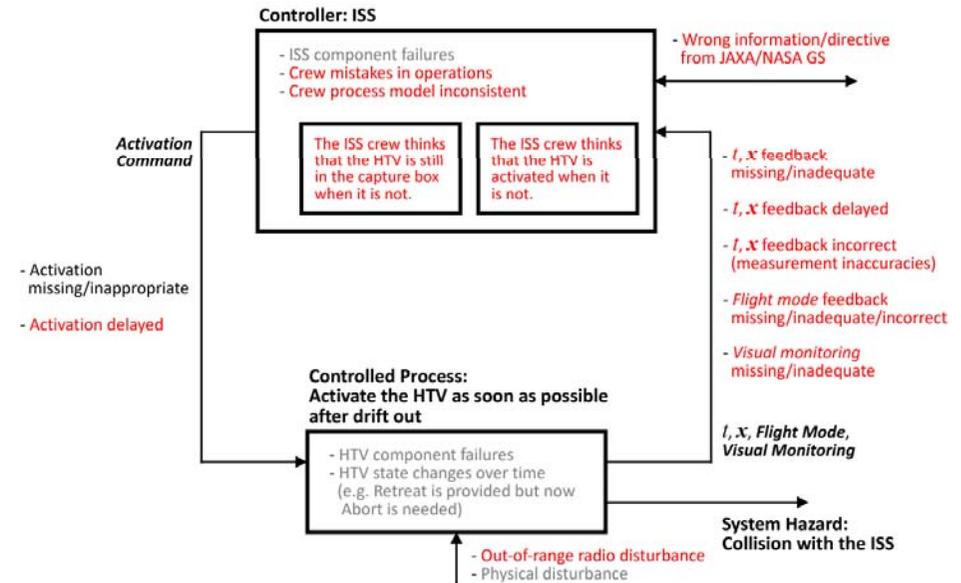
- t, x feedback missing/inadequate
- t, x feedback delayed
- t, x feedback incorrect
- Flight Mode feedback missing/inadequate
- Flight Mode feedback incorrect
- Visual Monitoring missing/inadequate

- Wrong information/directive from JAXA/NASA GS



Comparison between STPA and HR (Hazard Reports)

- ISS component failures
- **Crew mistakes in operation**
- **Crew process model inconsistent**
- Activation missing/inappropriate
- **Activation delayed**
- HTV component failures
- HTV state changes over time
- **Out-of-range radio disturbance**
- Physical disturbance
- **t, x feedback missing/inadequate**
- **t, x feedback delayed**
- **t, x feedback incorrect**
- **Flight Mode feedback missing/inadequate**
- **Flight Mode feedback incorrect**
- **Visual Monitoring missing/inadequate**
- **Wrong information/directive from JAXA/NASA GS**

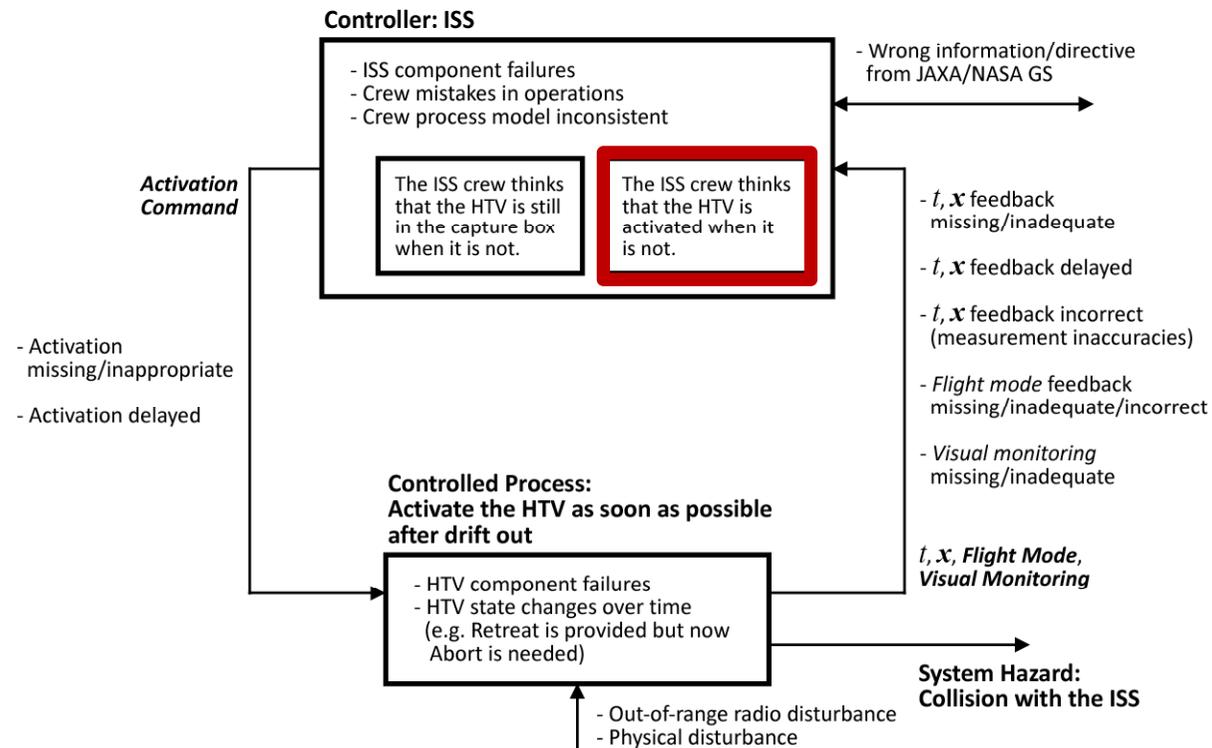


Identified by both (STPA and HR)
Identified by STPA only

Causal Factor Example

- **Crew process model inconsistent**

Due to an inadequate *Flight Mode* feedback, the crew might think that the HTV is activated when it is not and therefore the crew might not send the *Activation Command*.



Actual Hazard Control in HTV Design

In fact, most of the hazard causes identified by STPA are eliminated/mitigated by the HTV design and operations.

For example,

- Causal factors:
 - t, x feedback missing/inadequate/incorrect
 - *Flight Mode* feedback missing/inadequate/incorrect
- These hazard causes (**MISSING** or **INCORRECT**) are mitigated by FDIR (Fault Detection Isolation and Recovery) for communication system
 - **INCORRECT**: parity errors and packet format errors
 - Integrity Check and Validity Check
 - *meet the ISS Safety Requirements (CBCS Safety Requirements)
 - **MISSING**: loss of communication
 - “Heartbeat” signal between ISS and HTV, redundancy switching
 - If a failure of communication system is detected, the ISS crew is notified by sound (Caution)

Conclusion and Future Work

- The research collaboration has been partially completed and is still continuing.
- The potential benefit of using STPA, such as feasibility and usefulness for safety critical space system, has been found so far.
- Most of the hazard causes identified by STPA are eliminated or controlled by the current HTV design and operations, but not stated in the hazard reports (not considered as hazard cause and control in an explicit way).

For the next steps,

- The remaining seven hazardous scenarios other than (1b) will be analyzed to verify the benefit of using STPA.
- Causal factors identified by STPA will be confirmed that the current HTV design and operations have already enforced safety constraints for them.
- A safety-driven design process using STPA will be studied for use in future JAXA projects.

Thank You!

Causal Factors Identified by STPA

- **ISS component failures**

Due to the component failures, the ISS might not send the Activation Command or receive the feedback from the HTV.

- **Crew mistakes in operation**

The ISS crew might make an error in using the HCP.

- **Crew process model inconsistent**

Due to inadequate feedback (late, missing, spurious, or incorrect), the ISS crew might think that the HTV is still in the capture box when it is not, which could delay the activation commanding by the crew.

Due to an inadequate *Flight Mode* feedback, the crew might think that the HTV is activated when it is not and therefore the crew might not send the *Activation Command*.

- **Activation missing/inappropriate**

The *Activation Command* could disappear (i.e., not be received) or be corrupted during transmission.

- **Activation delayed**

The *Activation Command* could be delayed during transmission.

- **HTV component failures**

Due to the component failures, the HTV might not receive the *Activation Command*, execute the activation, or send the acknowledgment or feedback to the ISS.

- **HTV state changes over time**

Due to the changes in the HTV's state (position and attitude) relative to the ISS over time because it is floating, the crew might send a Retreat command without knowing that when the HTV now needs an Abort command for the safe escape trajectory.

- **Out-of-range radio disturbance**

Out-of-range radio disturbance could interfere with the *Activation Command* coming in and *t, x, Flight Mode* feedback going out.

- **Physical disturbance**

An unintended physical touch by the SSRMS could...

Causal Factors Identified by STPA

- ***t, x* feedback missing/inadequate**

Either or both of *t* and *x* feedback could be missing during transmission.

- ***t, x* feedback delayed**

t and *x* feedback could be delayed during transmission and arrive too late for the crew to execute the capture within 99 seconds or to issue an Abort command.

- ***t, x* feedback incorrect**

t and *x* feedback could be incorrect due to the measurement inaccuracies.

- ***Flight Mode* feedback missing/inadequate**

The *Flight Mode* feedback could disappear (i.e., not be received) or be corrupted during transmission.

- ***Flight Mode* feedback incorrect**

The *Flight Mode* feedback could be incorrect (e.g., activated when deactivated).

- ***Visual Monitoring* missing/inadequate**

The *Visual Monitoring* through camera and monitor could be missing or inadequate, which could delay the capture operation or activation commanding by the crew.

- **Wrong information/directive from JAXA/NASA GS**

Due to incorrect or delayed information to the JAXA/NASA GS, they might tell the ISS crew to capture the HTV when the crew should now issue an Abort command, which could confuse the crew.