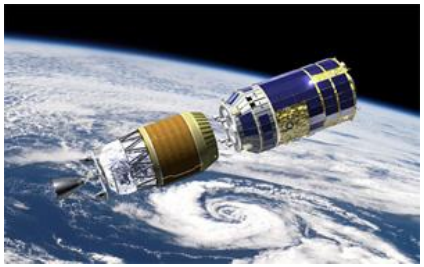
April 17, 2012

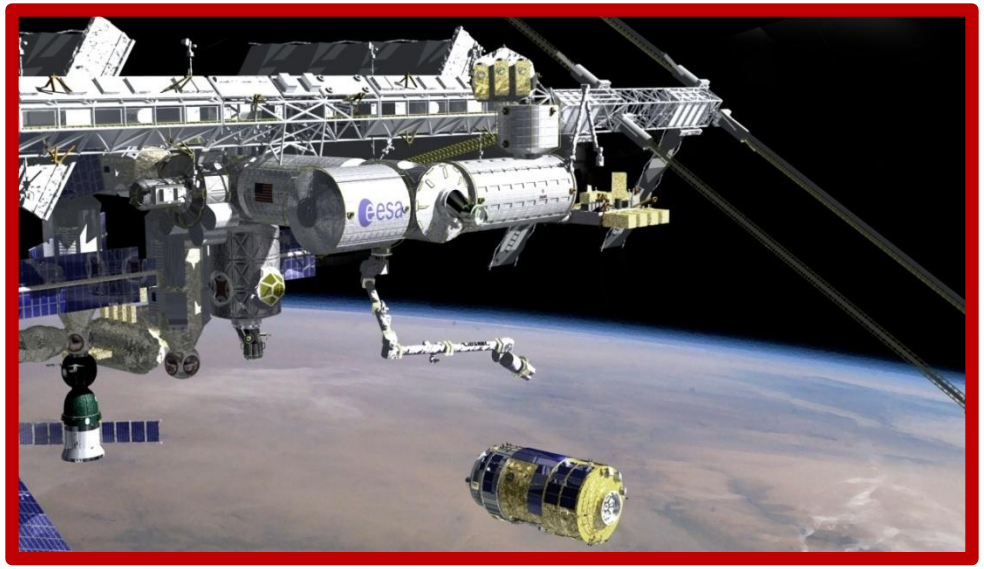
STAMP/STPA – Advanced Tutorial

JAXA H-II Transfer Vehicle (HTV)

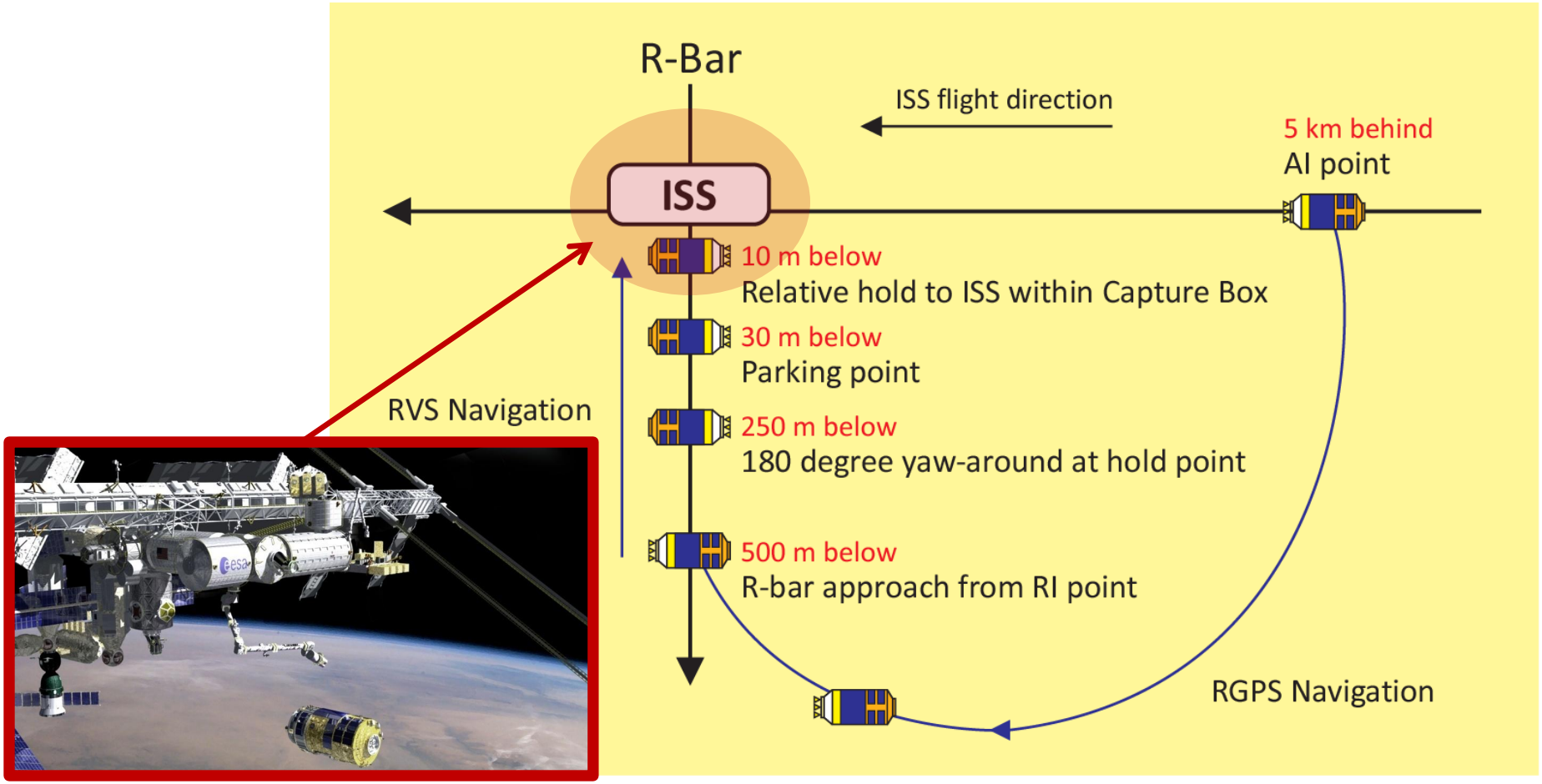
HTV: H-II Transfer Vehicle

- 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) and HTV-2 (Jan '11) were completed successfully
  - **Proximity operations** involve the ISS (including crew) and NASA and JAXA ground stations





Capture Operation

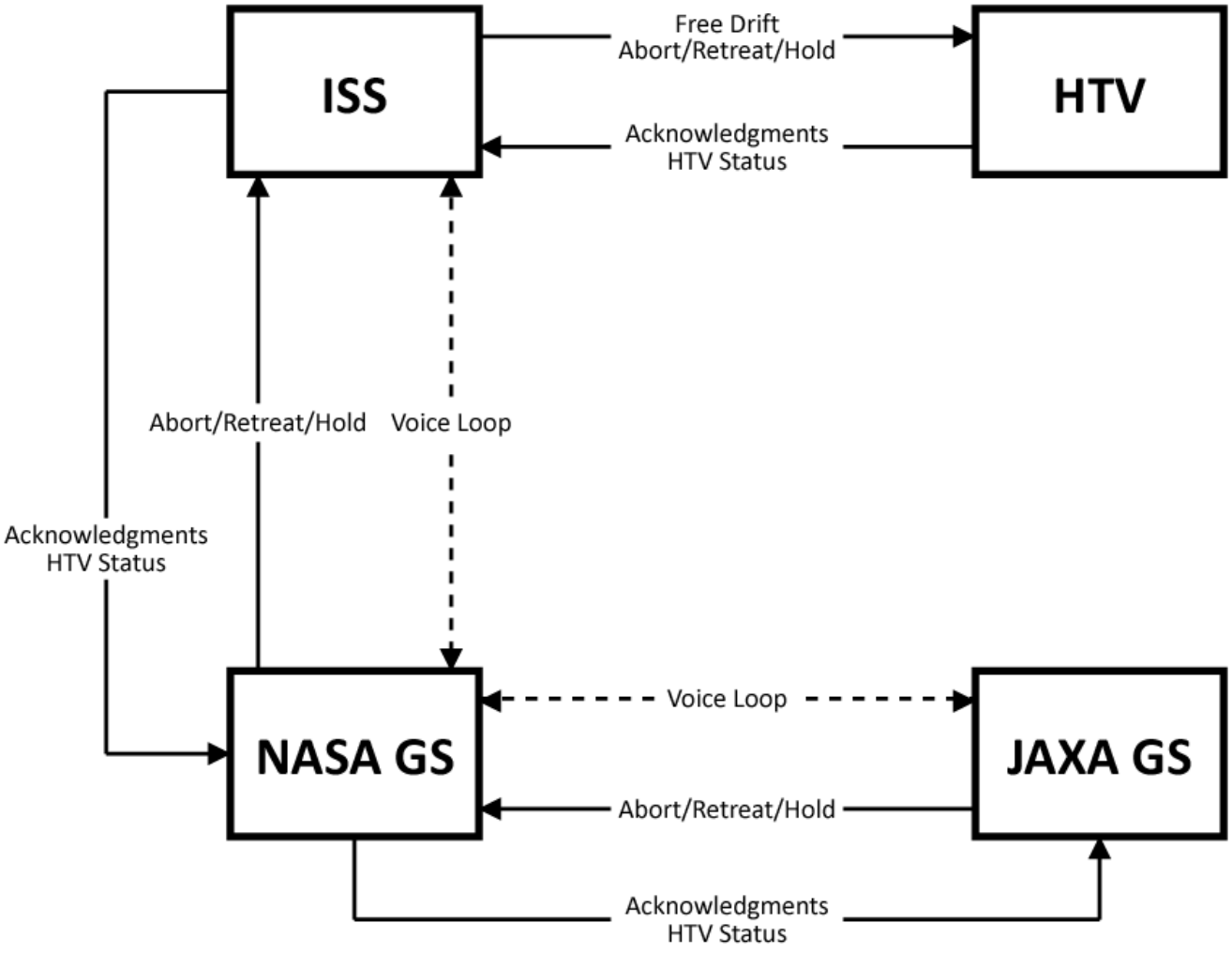


Basic Information

- Accident we want to prevent: **collision with ISS**
- Components in the system
  - **HTV**
  - **ISS (including crew)**
  - **NASA/JAXA ground stations**
- Capture operation
  - Once HTV reaches Capture Box (10 m below ISS),
    1. ISS crew sends a ***Free Drift*** command to HTV to disable the thrusters in preparation for capture
    2. HTV sends back **HTV status** (state vectors and flight mode)
    3. ISS crew manipulates SSRMS (robotic arm) to grapple HTV
  - If HTV drifts out of Capture Box before capture (since it is deactivated), either ISS crew or NASA/JAXA ground stations must activate HTV by sending ***Abort/Retreat/Hold*** commands
  - ISS crew and NASA/JAXA ground stations can communicate with each other using a **voice loop connection** through the entire operation

Summary

Control Structure



Accident and Hazard List

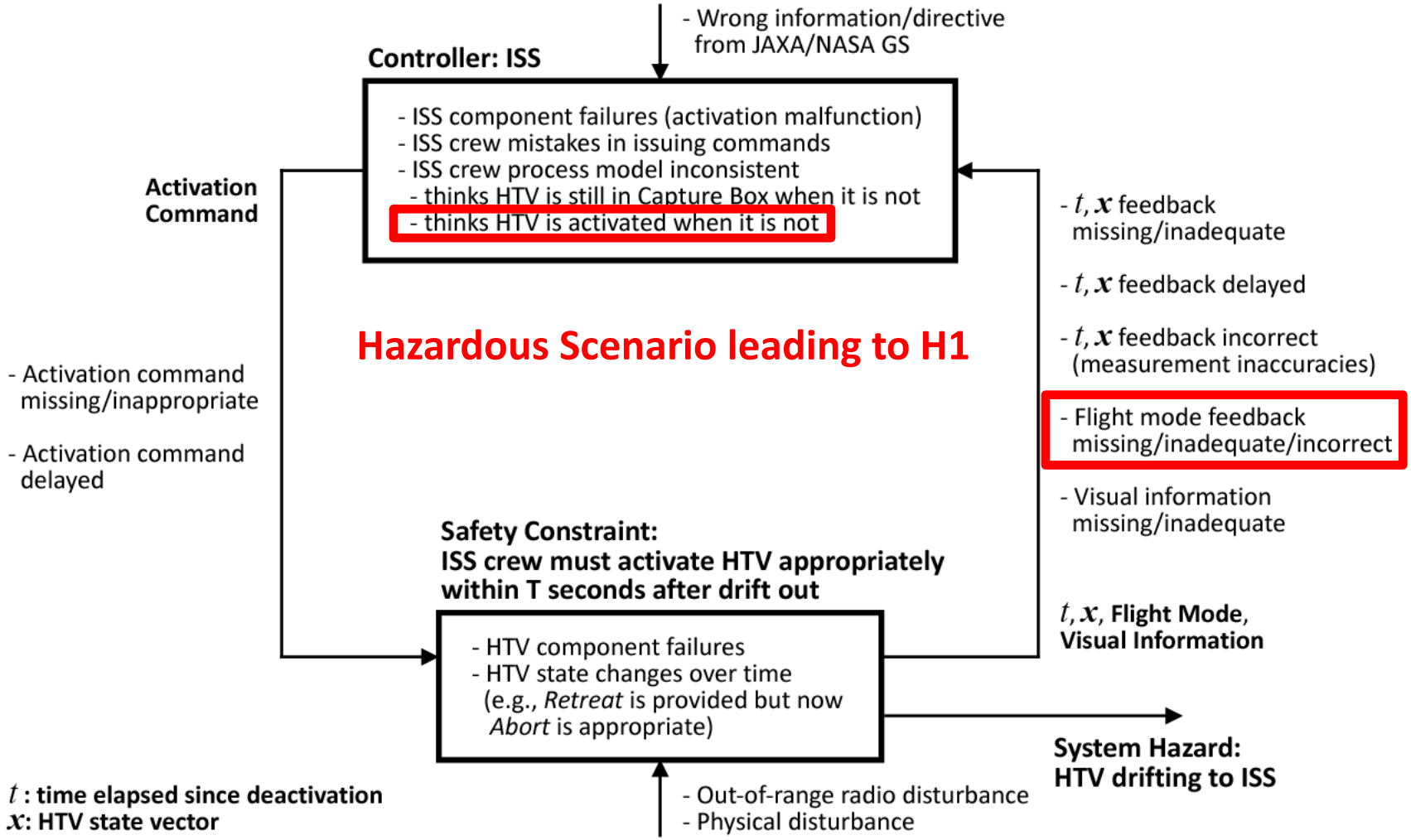
Accident		Hazard	
A1	Collision with ISS	H1	HTV is drifting to ISS while uncontrolled (deactivated)
A2	Damage to SSRMS	H3	HTV provides unintended attitude control in proximity to SSRMS
		H4	HTV is inclined by a large angle in proximity to SSRMS
		H5	HTV cannot be separated immediately when grappled unsafely (e.g., windmill)
		H6	HTV provides thrust while captured by SSRMS
A3	Loss of HTV mission	H7	FRGF is unintendedly separated from HTV before or during capture

Step 1: Unsafe Control Actions

Unsafe control actions leading to Hazard H1

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopping Too Soon /Applying Too Long Causes Hazard
Free Drift (Deactivation)	**[UCA4]** HTV is not deactivated when ready for capture	**[UCA5]** HTV is deactivated when not appropriate (e.g., while still approaching ISS)	EARLY: **[UCA6]** HTV is deactivated while not ready for immediate capture LATE: **[UCA7]** HTV is not deactivated for a long time while FRGF separation is enabled	
Execute Capture	**[UCA8]** Capture is not executed while HTV is deactivated	**[UCA9]** Capture is attempted when HTV is not deactivated **[UCA10]** SSRMS hits HTV inadvertently	EARLY: **[UCA11]** Capture is executed before HTV is deactivated LATE: **[UCA12]** Capture is not executed within a certain amount of time	**[UCA13]** Capture operation is stopped halfway and not completed
Abort Retreat Hold	**[UCA17]** Abort/Retreat/Hold is not executed when necessary (e.g., when HTV is drifting to ISS while uncontrolled)	**[UCA18]** Abort/Retreat/Hold is executed when not appropriate (e.g. after successful capture)	LATE: **[UCA19]** Abort/Retreat/Hold is executed too late when immediately necessary (e.g., when HTV is drifting to ISS while uncontrolled)	

Step 2: Causal Factors leading to H1



References

- Ishimatsu, T., Leveson, N., Thomas, J., Katahira, M., Miyamoto, Y., and Nakao, H., "Modeling and Hazard Analysis using STPA," *Proceedings of the 4th IAASS Conference*, Huntsville, AL, May 2010.
- Ishimatsu, T., Leveson, N., Thomas, J., Fleming, C., Katahira, M., Miyamoto, Y., Ujiie, R., Nakao, H., and Hoshino, N., "Hazard Analysis of Complex Spacecraft using STPA," (in preparation for journal submission).