April 19, 2012

Handling Multiple Controllers in STPA

Ryo Ujiie

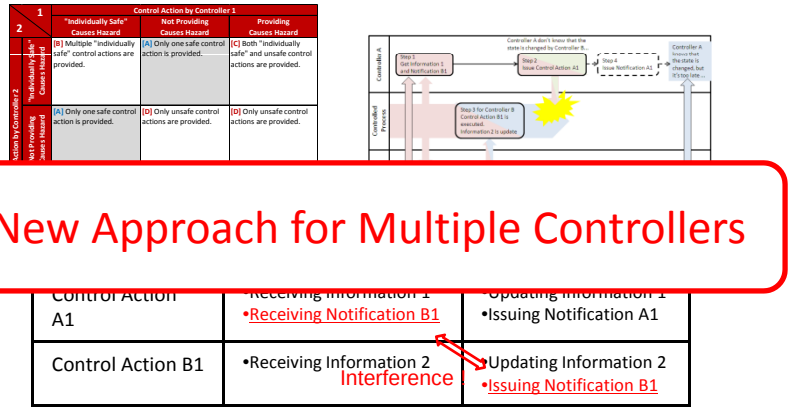
Japan Aerospace Exploration Agency (JAXA)

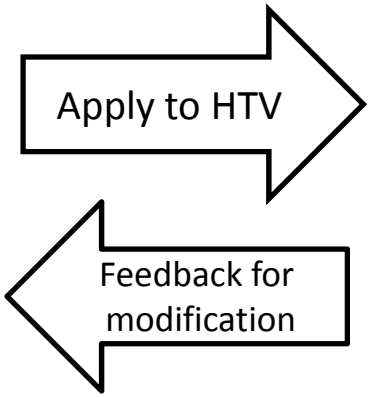
Takuto Ishimatsu

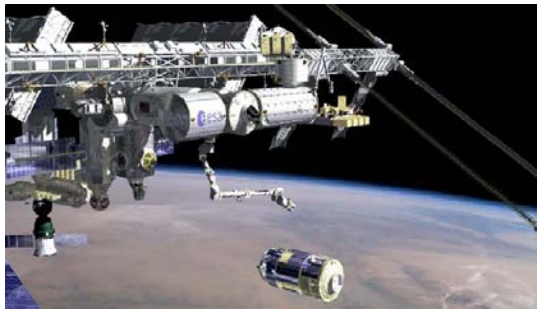
Massachusetts Institute of Technology (MIT)

Introduction

- Control by multiple controllers is more complex.
  - Interaction among multiple controllers is difficult to capture in traditional hazard analysis techniques
  - Control actions that would be “safe” in a single-controller situation might be unsafe in a multiple-controller situation
- Apply STPA to multiple-controller system using the JAXA’s HTV as a case study
  - Additional study is under way

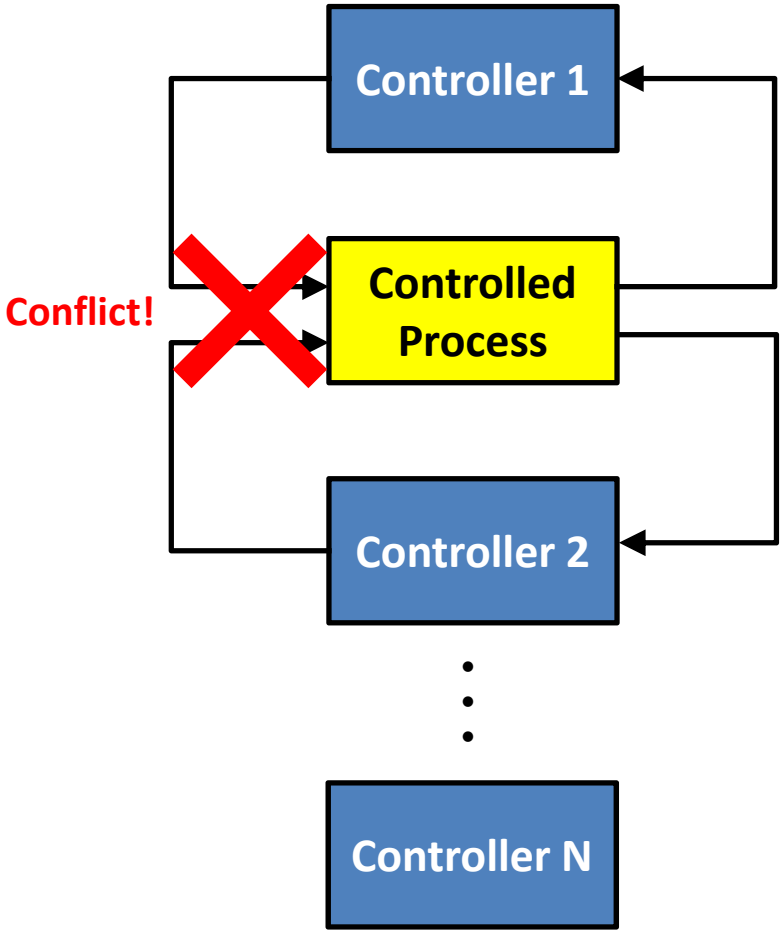






Multiple-Controller Problem

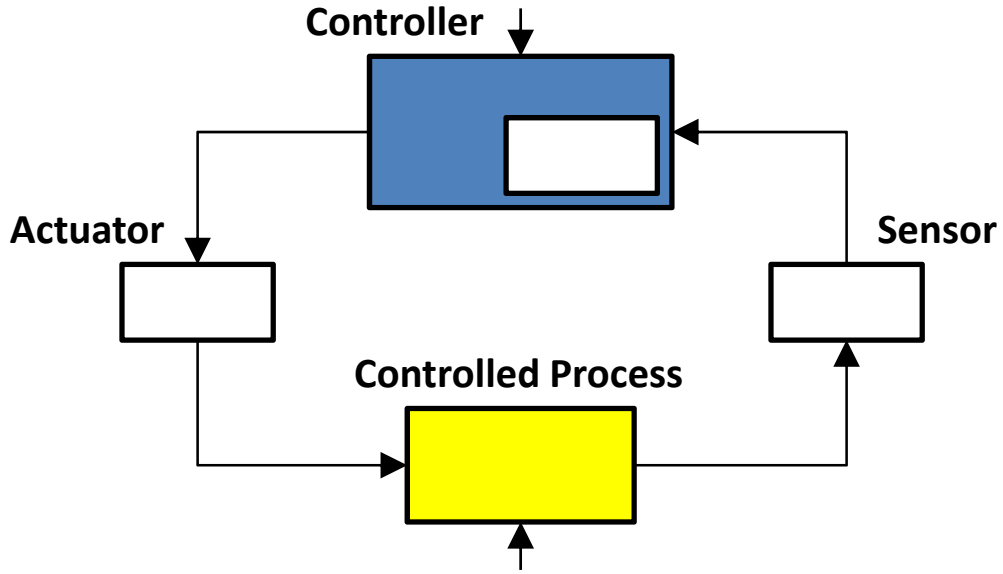
- **Conflicting control actions**
  - e.g., the 2002 Überlingen aircraft collision
- **Overriding between commands**
  - An unsafe command overrides a safe one
  - A safe one overrides another safe one while time runs out
- **"Someone else has done (will do)"**
  - Each controller thinks the other has done (will do) and nobody does
- **etc…**



Basic Approach in STPA

STPA has two main steps:

1. Identify potentially unsafe control actions
   - Not providing causes hazard
   - Providing causes hazard
   - Wrong timing/order causes hazard
   - Stopping too soon/applying too long causes hazard
2. Identify causal scenarios for unsafe control actions



Step 1: Unsafe Control Actions

2 \ 1	Control Action by Controller 1: "Individually Safe" Causes Hazard	Control Action by Controller 1: Not Providing Causes Hazard	Control Action by Controller 1: Providing Causes Hazard
Control Action by Controller 2: "Individually Safe" Causes Hazard	[B] Multiple "individually safe" control actions are provided.	[A] Only one safe control action is provided.	[C] Both "individually safe" and unsafe control actions are provided.
Control Action by Controller 2: Not Providing Causes Hazard	[A] Only one safe control action is provided.	[D] Only unsafe control actions are provided.	[D] Only unsafe control actions are provided.
Control Action by Controller 2: Providing Causes Hazard	[C] Both "individually safe" and unsafe control actions are provided.	[D] Only unsafe control actions are provided.	[D] Only unsafe control actions are provided.

Classification:

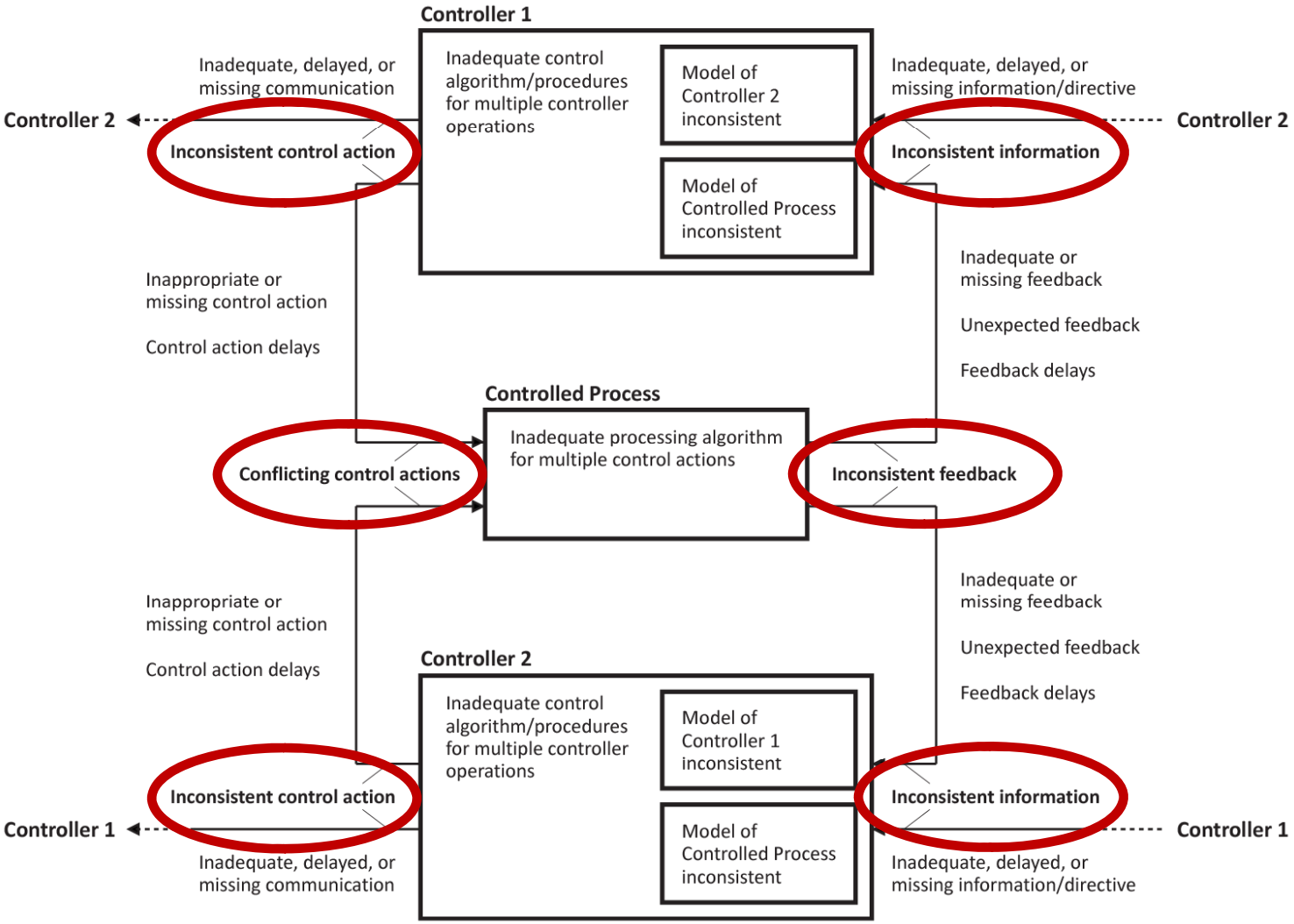
[A]:
Only a “safe” action provided

[B]:
Multiple “safe” actions provided

[C]:
Both “safe” and unsafe actions provided

[D]:
Only unsafe actions provided

Step 2: Causal Factors

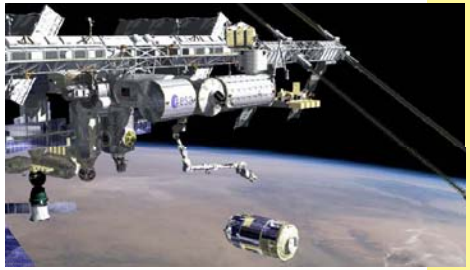


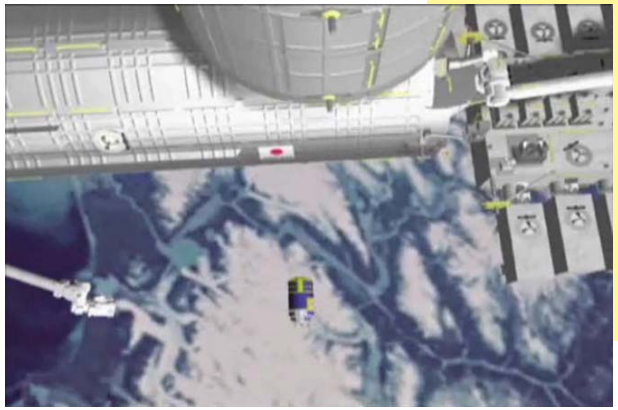
Step 2: Causal Scenarios

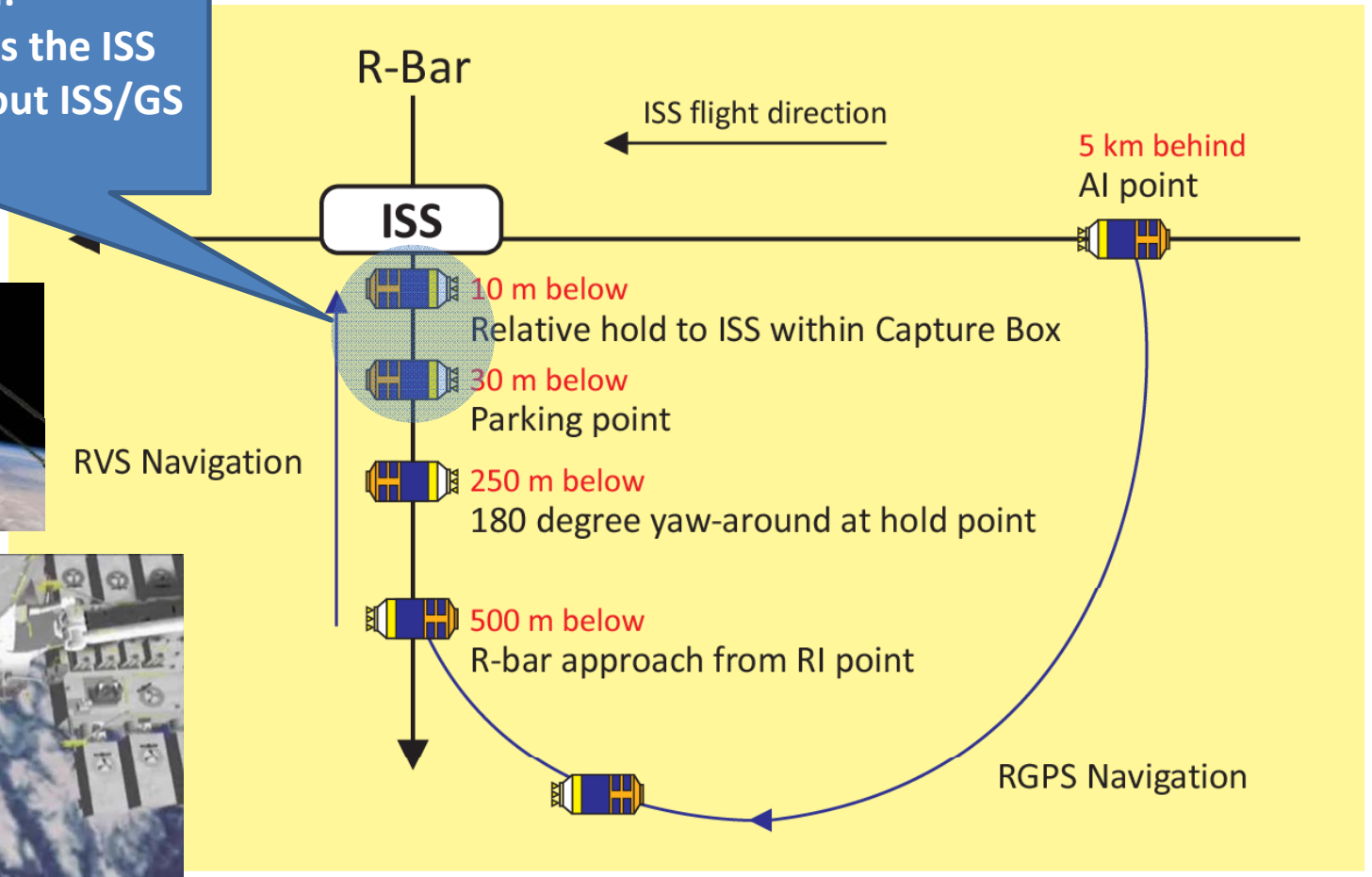
- Human controllers have many psychological pitfalls:
  - Rash control under pressure/desire to precede other controllers
  - Overlapping responsibilities
  - Unclear authority
  - Hesitation due to control actions of other controllers
  - Complacency to control actions or information from other controllers
  - Overconfidence in automation
  - Confusion by unexpected control actions or information/directives from other controllers
- After the causal factors have been identified for each controller, specific hazardous scenarios can be built by combining the causal factors from each controller

Case Study: HTV Final Approach Phase

HTV Final Approach:
The HTV approaches the ISS automatically without ISS/GS commands.







Control Structure & Off-Nominal Commands

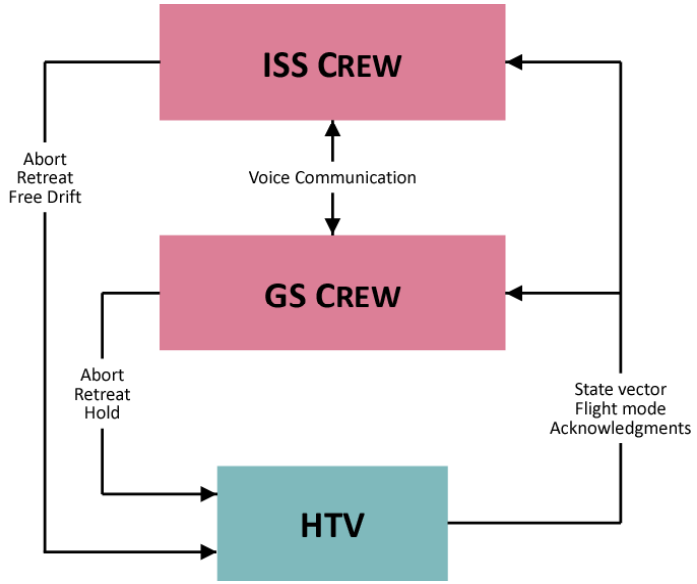
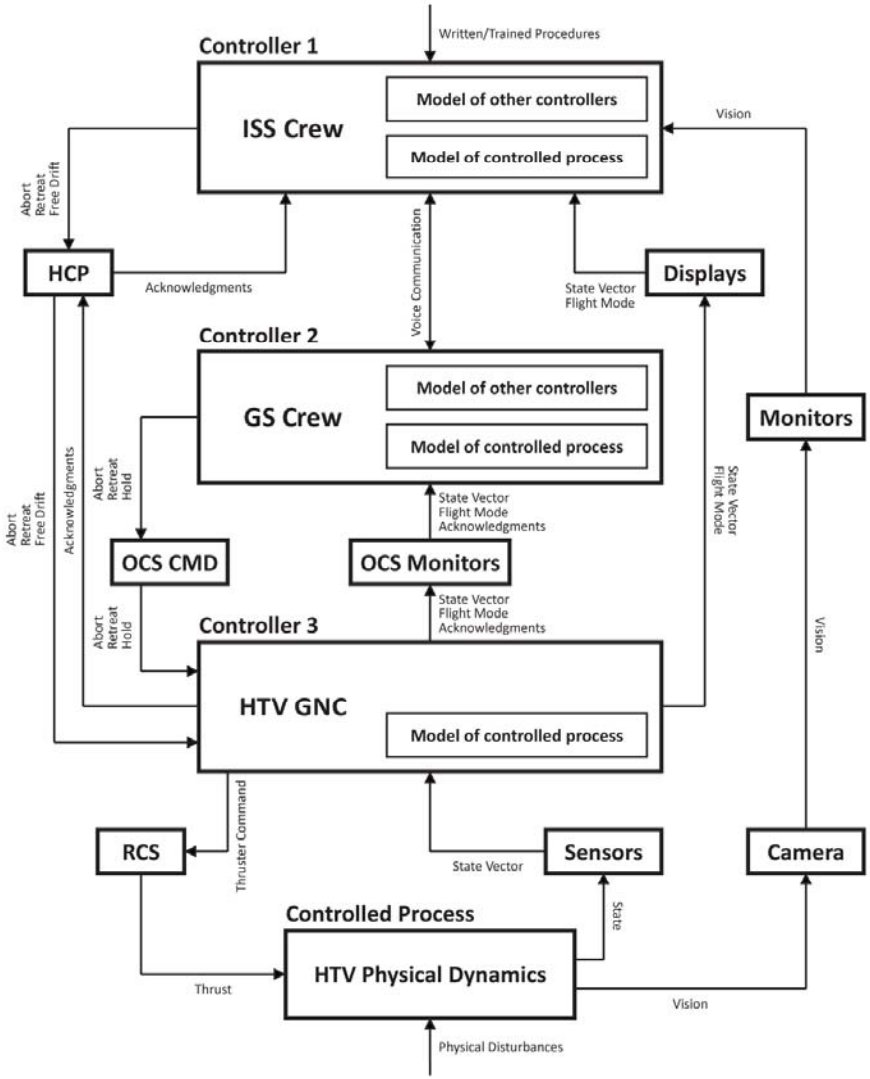


TABLE. Off-nominal commands availability and range

Command	Controller			Range
	ISS Crew	GS Crew	HTV GNC	
Hold	☑	✓	×	30 m — 15 m
Retreat	✓	✓	×	15 m — 10 m
Abort	✓	✓	✓	10 m (Capture Box) — (HTV GNC: anywhere)

✓: allowed to issue (by the design/flight rules)
☑: not allowed but available
× : not available (by the software design)



STPA Step 1: 3D UCA Table

HTV GNC *Abort*: "Individually Safe" Causes Hazard

GS \ ISS		ISS Crew *Abort*			
		"Individually Safe" Causes Hazard	Not Providing Causes Hazard	Providing Causes Hazard	
				Retreat	*Free Drift*
GS Crew *Abort*	"Individually Safe" Causes Hazard	**[B1]** Triple *Abort* commands are redundantly provided by ISS crew, GS crew, and HTV GNC	**[B2]** Double *Abort* commands are redundantly provided by GS crew and HTV GNC	**[C1]** Double *Abort* commands are provided by GS crew and HTV GNC while a *Retreat* command is provided by ISS crew	**[C2]** Double *Abort* commands are provided by GS crew and HTV GNC while a *Free Drift* command is provided by ISS crew
	Not Providing Causes Hazard	**[B3]** Double *Abort* commands are redundantly provided by ISS crew and HTV GNC	**[A1]** Only a single *Abort* command is provided by HTV GNC	**[C3]** An *Abort* command is provided by HTV GCN while a *Retreat* command is provided by ISS crew	**[C4]** An *Abort* command is provided by HTV GNC while a *Free Drift* command is provided by ISS crew
	Providing Causes Hazard: *Retreat*	**[C5]** Double *Abort* commands are provided by ISS crew and HTV GNC while a *Retreat* command is provided by GS crew	**[C6]** An *Abort* command is provided by HTV GNC while a *Retreat* command is provided by GS crew	**[C7]** An *Abort* command is provided by HTV GNC while double *Retreat* commands are provided by ISS crew and GS crew	**[C8]** An *Abort* command is provided by HTV GNC while a *Retreat* command is provided by GS crew and a *Free Drift* command is provided by ISS crew
	Providing Causes Hazard: *Hold*	**[C9]** Double *Abort* commands are provided by ISS crew and HTV GNC while a *Hold* command is provided by GS crew	**[C10]** An *Abort* command is provided by HTV GNC while a *Hold* command is provided by GS crew	**[C11]** An *Abort* command is provided by HTV GNC while a *Retreat* command is provided by ISS crew and a *Hold* command is provided by GS crew	**[C12]** An *Abort* command is provided by HTV GNC while a *Free Drift* command is provided by ISS crew and a *Hold* command is provided by GS crew

STPA Step 1: 3D UCA Table

HTV GNC *Abort* : Not Providing Causes Hazard

GS \ ISS	ISS Crew *Abort*: "Individually Safe" Causes Hazard	ISS Crew *Abort*: Not Providing Causes Hazard	ISS Crew *Abort*: Providing Causes Hazard — *Retreat*	ISS Crew *Abort*: Providing Causes Hazard — *Free Drift*
GS Crew *Abort*: "Individually Safe" Causes Hazard	[B4] Double *Abort* commands are redundantly provided by ISS crew and GS crew	[A2] Only a single *Abort* command is provided by GS crew	[C13] An *Abort* command is provided by GS crew while a *Retreat* command is provided by ISS crew	[C14] An *Abort* command is provided by GS crew while a *Free Drift* command is provided by ISS crew
GS Crew *Abort*: Not Providing Causes Hazard	[A3] Only a single *Abort* command is provided by ISS crew	[D1] No *Abort* command is provided by any of the three controllers	[D2] Only a *Retreat* command is provided by ISS crew	[D3] Only a *Free Drift* command is provided by ISS crew
GS Crew *Abort*: Providing Causes Hazard — *Retreat*	[C15] An *Abort* command is provided by ISS crew while a *Retreat* command is provided by GS crew	[D4] Only a *Retreat* command is provided by GS crew	[D5] Double *Retreat* commands are provided by ISS crew and GS crew	[D6] A *Free Drift* command is provided by ISS crew and a *Retreat* command is provided by GS crew
GS Crew *Abort*: Providing Causes Hazard — *Hold*	[C16] An *Abort* command is provided by ISS crew while a *Holde* command is provided by GS crew	[D7] Only a *Hold* command is provided by GS crew	[D8] A *Retreat* command is provided ISS crew and a *Hold* command is provided by GS crew	[D9] A *Free Drift* command is provided by ISS crew and a *Hold* command is provided by GS crew

STPA Step 2: Causal Factors leading to D2

Controller	Causal Factor
ISS Crew	• The ISS crew thinks that *Retreat* is still safe enough due to incorrect/delayed state vector feedback and issues a *Retreat* command
	• The ISS crew issues a Retreat command before the HTV initiates a self-abort because they do not want to waste time and fuel by starting all the final approach process over again (Rash control under desire to precede other controllers)
GS Crew	• Because a *Retreat* command has been provided by the ISS crew, the GS crew holds back from any control action and waits and sees for a while (Hesitation due to control actions of other controllers)
	• The GS crew is satisfied with *Retreat* provided by the ISS crew and no longer pays close attention (Complacency to control actions from other controllers)
	• The GS crew is confused by the ISS crew's unexpected *Retreat* command and does not issue an *Abort* command (Confusion by unexpected control actions of other controllers)
HTV GNC	• The HTV makes an error in decision-making on self-abort • The HTV thinks that it is still in a safe position due to inaccurate measurement and that it does not need to self-abort • The HTV thinks that it is still in a safe position due to incorrect/delayed state vector feedback and that it does not need to self-abort
	• Because a *Retreat* command has been provided by the ISS crew, the HTV GNC does not self-abort

Building up one possible hazardous scenario leading to unsafe interaction D2

STPA Handling Multiple Controllers

- STPA can handle multiple controllers and identify possible unsafe interactions among them and their causal scenarios
  - This multiple-controller problem cannot be captured by FTA
- While this case study considered unsafe interactions by looking at the combinations of control actions, the context of each control action is also a key factor involved in unsafe interactions
  - Temporal context
  - Preconditions under which each control action is provided
  - etc.

What Is Difficult/Complex?

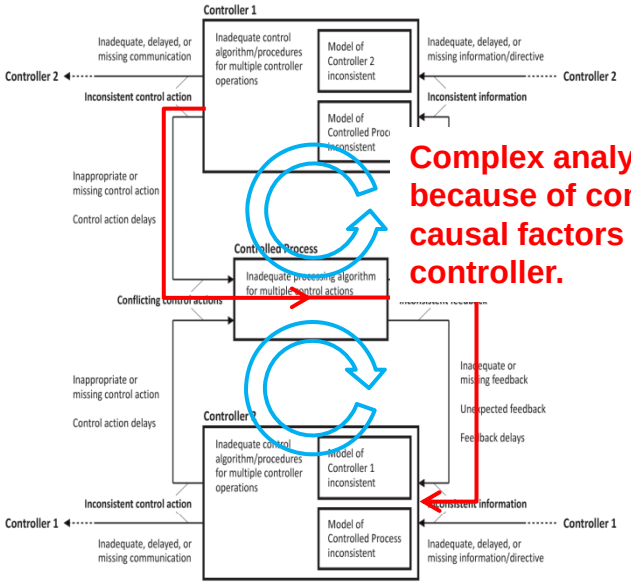
- Problem of STPA in Multiple Controller case
  - In multiple controllers case, it is important to understand interaction (interference) among controllers. However, it is difficult …

The table can represent all combination between the actions well.

2 \ 1	Control Action by Controller 1: "Individually Safe" Causes Hazard	Control Action by Controller 1: Not Providing Causes Hazard	Control Action by Controller 1: Providing Causes Hazard
Control Action by Controller 2: "Individually Safe" Causes Hazard	[B] Multiple "individually safe" control actions are provided.	[A] Only one safe control action is provided.	[C] Both "individually safe" and unsafe control actions are provided.
Control Action by Controller 2: Not Providing Causes Hazard	[A] Only one safe control action is provided.	[D] Only unsafe control actions are provided.	[D] Only unsafe control actions are provided.
Control Action by Controller 2: Providing Causes Hazard	[C] Both "individually safe" and unsafe control actions are provided.	[D] Only unsafe control actions are provided.	[D] Only unsafe control actions are provided.

Various contexts about 2 control actions in each box

The control loop can represent how an inadequate control action occurs well.

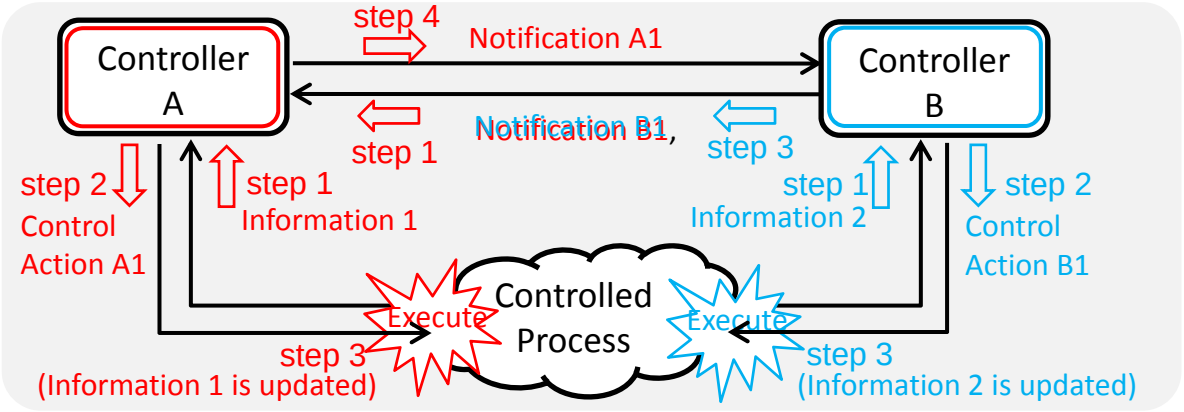


Complex analysis because of combining the causal factors from each controller.

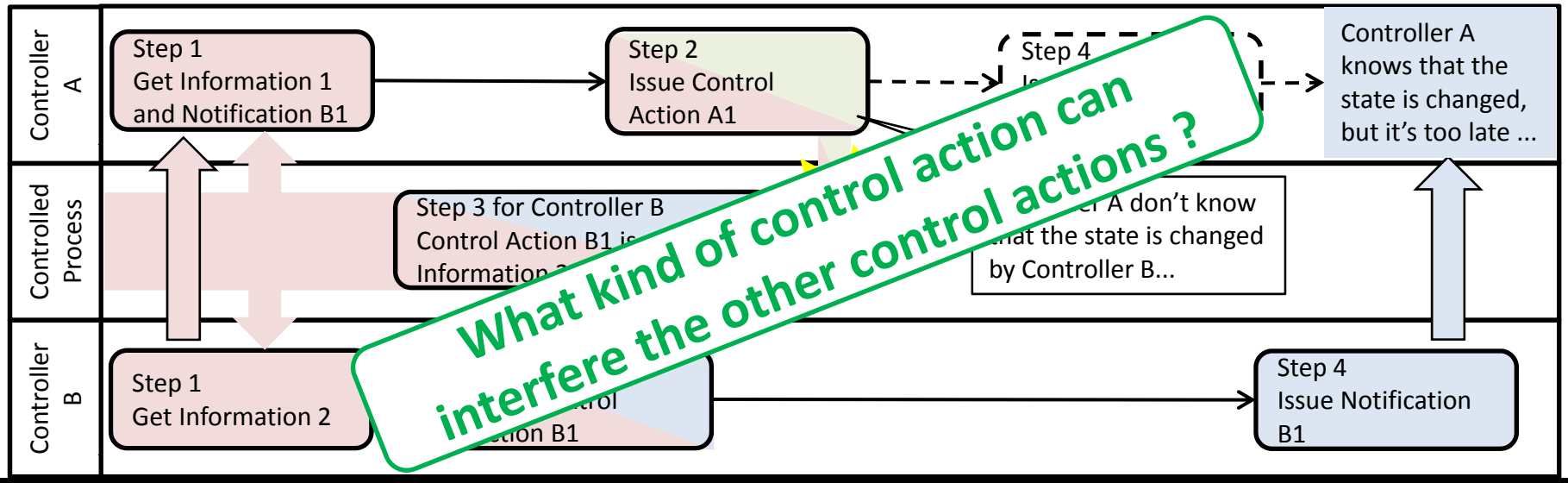
In order to understand the interaction clearly, we need an extended methodology of STPA.

New Approach for Analysis of Multiple Controllers

- How interference (problematic interaction) among control actions occurs ?



Control loop is not enough to represent the context (process, time sequence, …) of interference.



New Approach for Analysis of Multiple Controllers

- Definition of "Interference"
  - We focus on "**Post-condition**" and "**Pre-condition**" of a control action.
    - *If "post-condition" of a control action changes "pre-condition" of the other control action, there will be an interference between the actions.*

	Precondition	**Postcondition**
Control Action A1	•Receiving Information 1 •Receiving Notification B1	•Updating Information 1 •Issuing Notification A1
Control Action B1	•Receiving Information 2 **Interference !**	•Updating Information 2 •Issuing Notification B1

  - This approach can be applied to Inadequate control actions.
    - An Inadequate control action is different in Pre/Post conditions from adequate case.

	Precondition	**Postcondition**
Too early Control Action A1	•Receiving Information 1 ~~•Receiving Notification B1~~	•Updating Information 1 •Issuing Notification A1
Incorrect Control Action B2 (when Control Action B1 is provided.)	•Receiving Information 2 **New Interference !**	•Updating ~~Information 2~~ Information 1 •Issuing Notification B1

New Approach for Analysis of Multiple Controllers

- Extended Step1 in STPA for Multiple Controllers case
  1. Identify the potential for inadequate control of the system that could lead to a hazardous state.

     (After analyzing each single controller)

     a. Identify combinations of control actions for each single controller.
        - A: Only one safe control action is provided.
        - B: Multiple "individually safe" control actions are provided.
        - C: Both "individually safe" and unsafe control actions are provided.
        - D: Only unsafe control actions are provided.

2 \ 1	"Individually Safe" Causes Hazard	Not Providing Causes Hazard	Providing Causes Hazard
"Individually Safe" Causes Hazard	[B] Multiple "individually safe" control actions are provided.	[A] Only one safe control action is provided.	[C] Both "individually safe" and unsafe control actions are provided.
Not Providing Causes Hazard	[A] Only one safe control action is provided.	[D] Only unsafe control actions are provided.	[D] Only unsafe control actions are provided.
Providing Causes Hazard	[C] Both "individually safe" and unsafe control actions are provided.	[D] Only unsafe control actions are provided.	[D] Only unsafe control actions are provided.

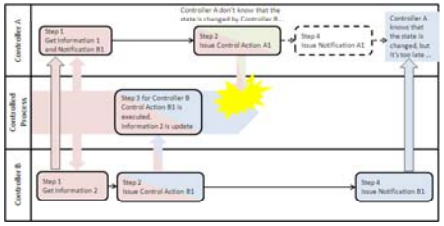
(Control Action by Controller 2 / Control Action by Controller 1)

     b. Identify interferences among the actions
        - Pre-condition
        - Post-condition

	Precondition	Postcondition
Control Action A1	•Receiving Information 1 •Receiving Notification B1	•Updating Information 1 •Issuing Notification A1
Control Action B1	•Receiving Information 2	•Updating Information 2 •Issuing Notification B1

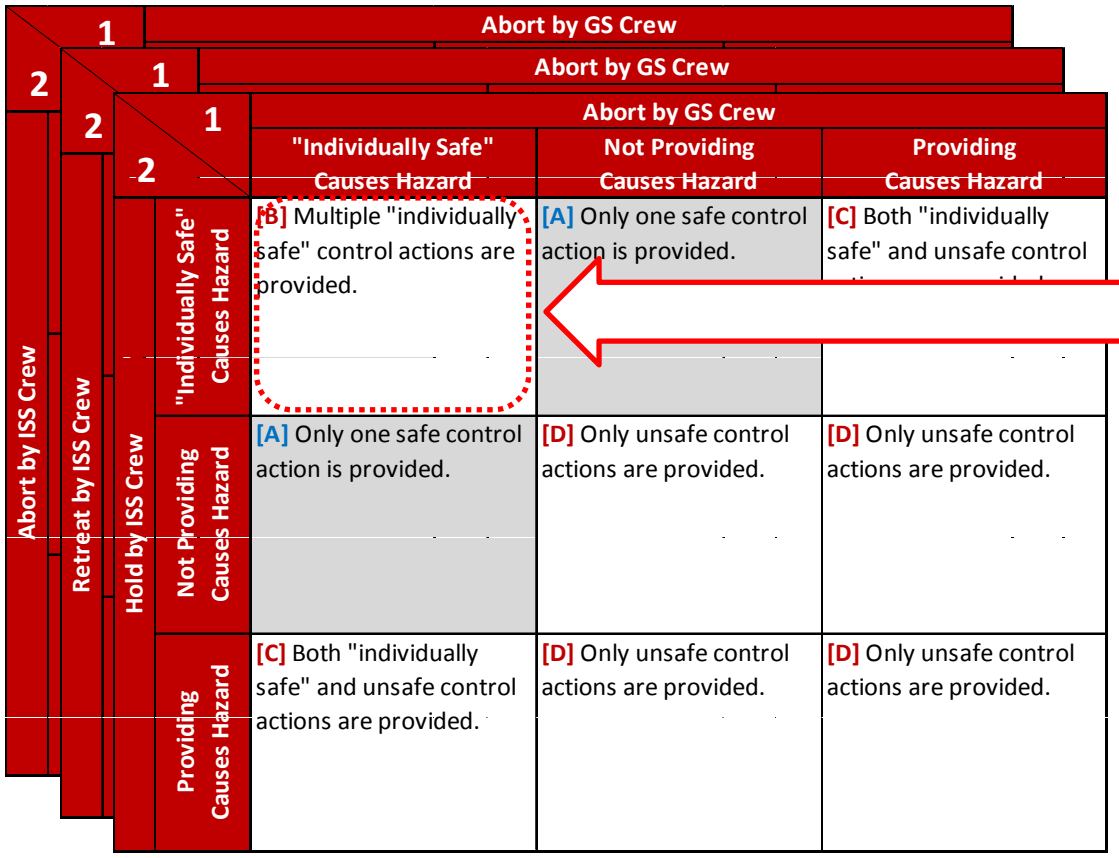
Interference !

     c. Analyze the interferences and Identify the potential of inadequate control
        - Process Flow Diagram



Trial of New Approach in HTV

- Step 1-a: Identify combinations of control actions for each single controller.
  - GS Crew vs. ISS Crew



Focus on this combination !
Abort by GS Crew
vs
Hold by ISS Crew

(Now we are analyzing the other combinations …)

Trial of New Approach in HTV

- Step 1-b: Identify interferences among the actions ...

GS Crew's control action

No.	Action	Pre-condition	Post-condition
1	Abort	(Flight Mode = Approach OR Flight Mode = Hold OR Flight Mode = Retreat) AND (State Vector3 > 70 M AND State Vector 4 = BETWEEN 250 M AND 200 M OR .....)	Flight Mode = Abort
2	Abort	..	...

Mathematical expression to check consistency

No.	Action	Pre-condition	Post-condition
1	...	...	...
2	Abort	...	...
3	Abort	...	...
...	...	...	...

Consistent

Interfere (Inconsistent)

No.	Action	Pre-condition	Post-condition
...	...	...	...
7	Hold	...	...
8	Hold	...	...
...	...	...	...

We would like to find the combinations of control actions that satisfy the followings;

- one pre-condition is consistent with the other's pre-condition.

The 2 actions can be issued simultaneously at least for interference

- one post-condition is inconsistent with the other's pre-condition.

This is our "interfere" definition.

Indentify the interferences automatically

SpecTRM model

Trial of New Approach in HTV

GS Crew's control action

No.	Action	Pre-condition	Post-condition
1	Abort	(Flight Mode = Approach OR Flight Mode = Hold OR Flight Mode = Retreat) AND (State Vector3 > 70 M AND State Vector 4 = BETWEEN 250 M AND 200 M OR State Vector3 > 40 M AND State Vector 4 = BETWEEN 200 M AND 100 M OR State Vector3 > 15 M AND State Vector 4 =BETWEEN 100 M AND 30 M OR State Vector3 > 5 M AND State Vector 4 = BETWEEN 30 M AND 15 M OR State Vector3 > 3.7 M AND State Vector 4 = BETWEEN 15 M AND CAPTURE POINT)	Flight Mode = Abort

Consistent

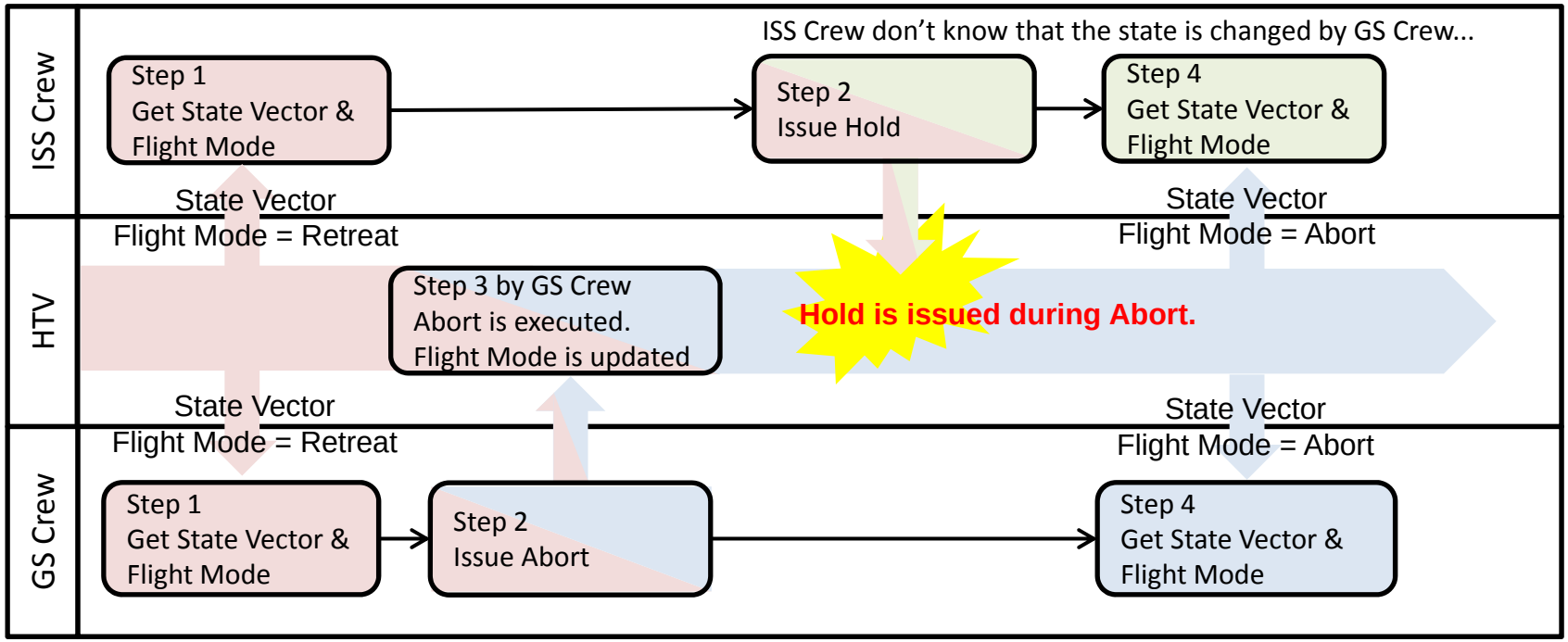
Interference (Inconsistent)

ISS Crew's control action

No.	Action	Pre-condition	Post-condition
1	Hold	State Vector 4 = BETWEEN 250 M AND 30 M AND Voice Communication = broken AND State Vector 1 = inside the KOS AND RVS Status = ONLY ONE FUNCTIONING AND State Vector 5 = GREATER THAN 15M OF THE PROX RANGE AND (Flight Mode = Approach OR Flight Mode = Retreat)	Flight Mode = Hold

Trial of New Approach in HTV

- Step 1-c: Analyze the interferences and Identify the potential for inadequate control



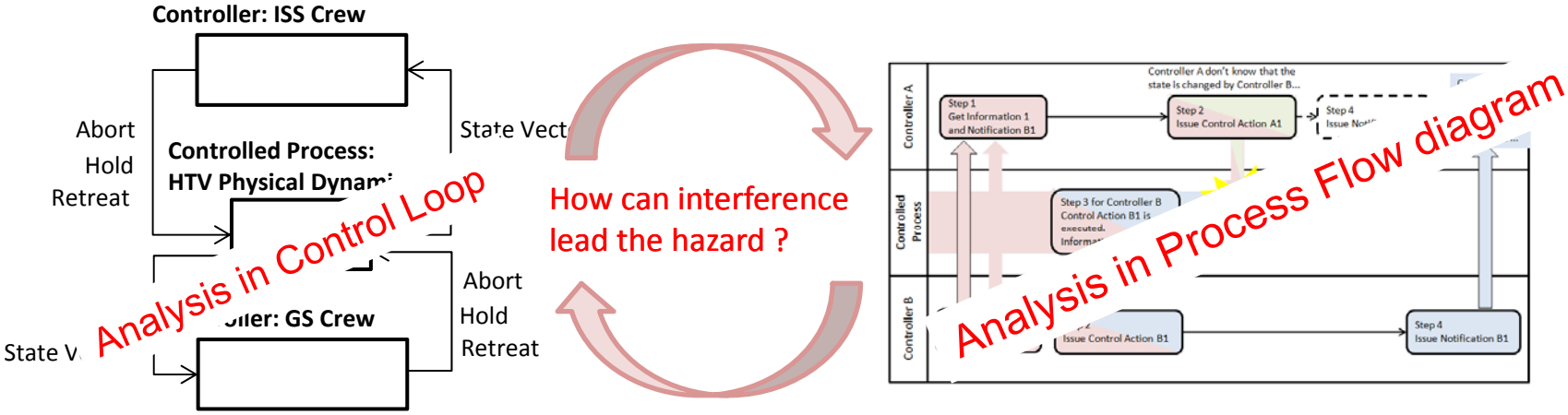
Executing Hold during HTV aborting could lead to collision with ISS.
This control by the double controllers could lead to a hazardous state !

In actual HTV, any commands(Hold, Retreat, Free Drift) are rejected until aborting finishes.
This control is NOT happen in actual system ...

This can be happen in actual system ?

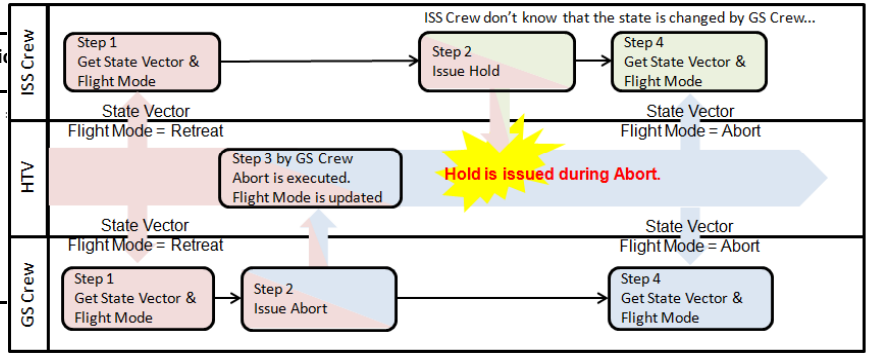
Problem To Be Solved

- Process Flow diagram is still useful in Step 2 ?



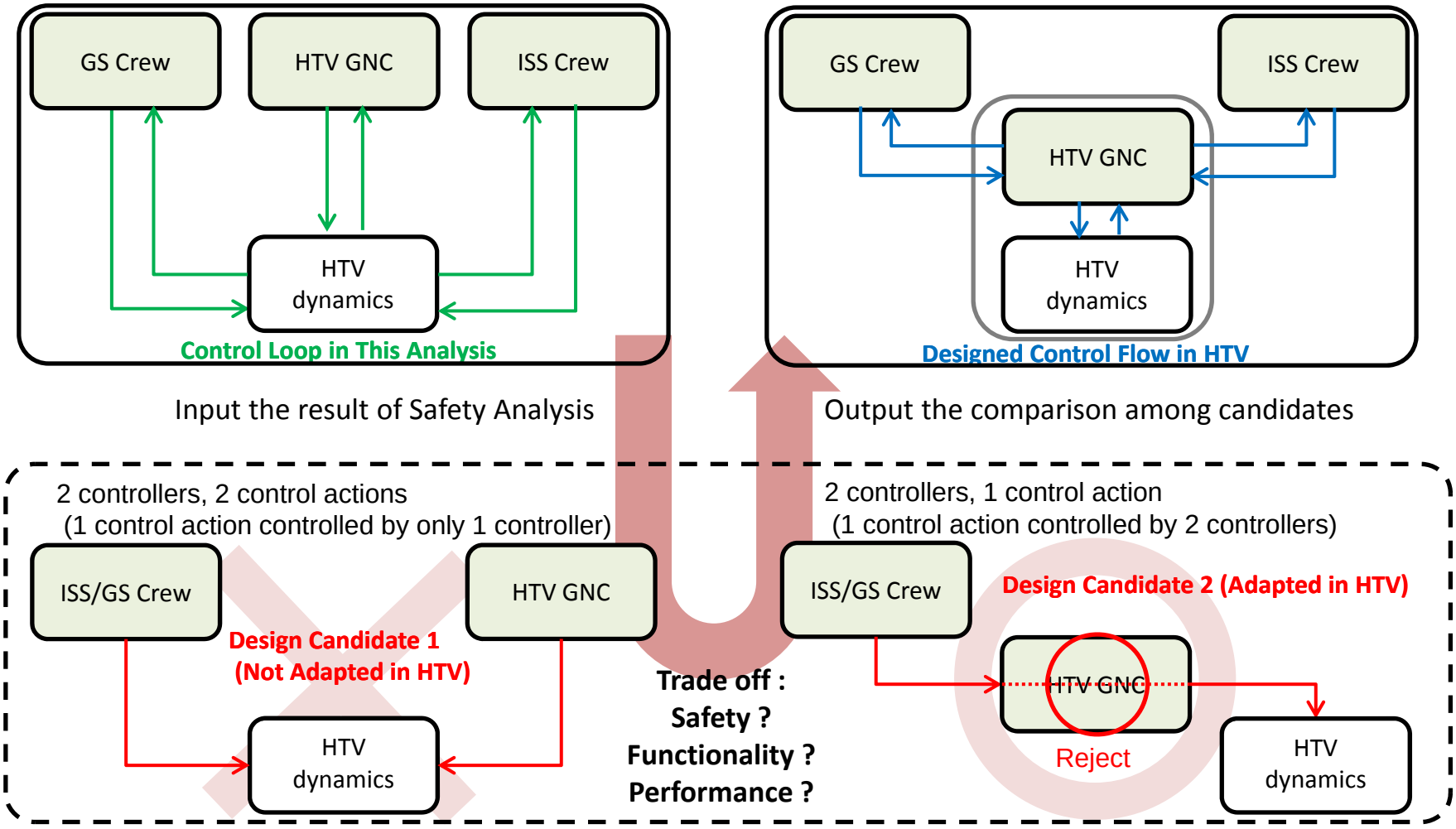
- How to define Pre- & Post- conditions and Process Flow Diagram should be clarified more …

No.	Action	Pre-condition	Post-conditi
1	Abort	(Flight Mode = Approach OR Flight Mode = Hold OR Flight Mode = Retreat) AND (State Vector3 > 70 M AND State Vector 4 = BETWEEN 250 M AND 200 M OR …..)	Flight Mode



Problem To Be Solved

- Design of hierarchy among controllers can be guided by STPA ?



Future Plan

- Establish a more clear and practical approach
  - Analyze all combinations in the HTV case
    - Develop a more formal process flow diagram
    - Define pre- & post- conditions more clearly
    - Study “2 controllers, 1 control action” case
    - etc …
- Use multiple-controller analysis in **safety guided design**
  - Apply this approach to “Crew Space Vehicle”
    - HTV is an existing system so that actual control flow has been already designed.
    - Crew Space Vehicle is in early development phase (NOT designed yet). It’s good target of safety guided design !