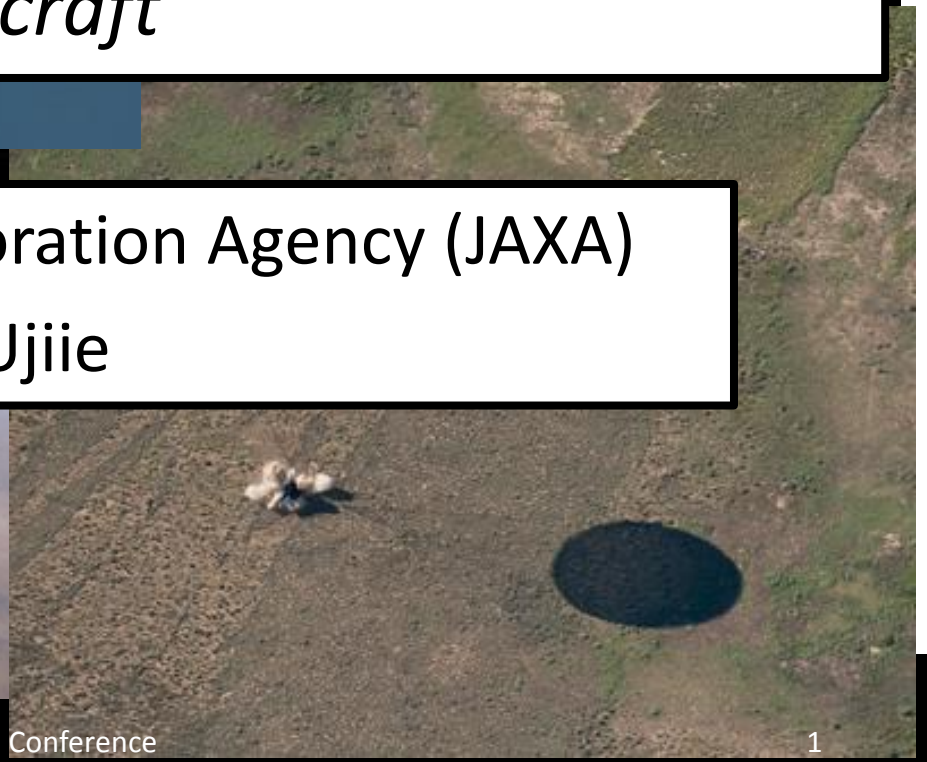
Using STPA in the Design of a new Manned Spacecraft

Japan Aerospace Exploration Agency (JAXA)

Ryo Ujiie



Contents

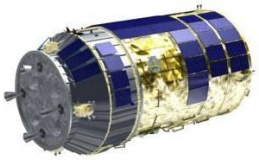
Abstract

- We have been applying STPA to JAXA's new Manned Spacecraft.
  - JAXA are studying a new Manned Spacecraft. It is NOT an actual project in JAXA yet.
  - The spacecraft is being designed. We are studying Safety Guided Design in this study project.

- Some characteristics of Safety Guided Design have been identified.
  - Each result from STPA step 1 & 2 can be fed back to system design.
  - Combination between General System Engineering Process & STPA process. It will be "Safer System Engineering Process" ?

Purpose

- Background
  - JAXA has never developed Manned Spacecraft.
    - ISS program project in JAXA
      - HTV: an unmanned resupply spacecraft used to resupply the International Space Station (ISS).
      - JEM: a Japanese science module for the International Space Station (ISS).



  - Manned Spacecraft study in JAXA from 2010
    - Severe Constraint for returning to the earth;
      - aerodynamic heating , landing point, ECLSS, …
    - Control by Crew
      - Pros: Flexible Control (e.g. fault detection by understanding trends of device's status)
      - Cons: Human Error

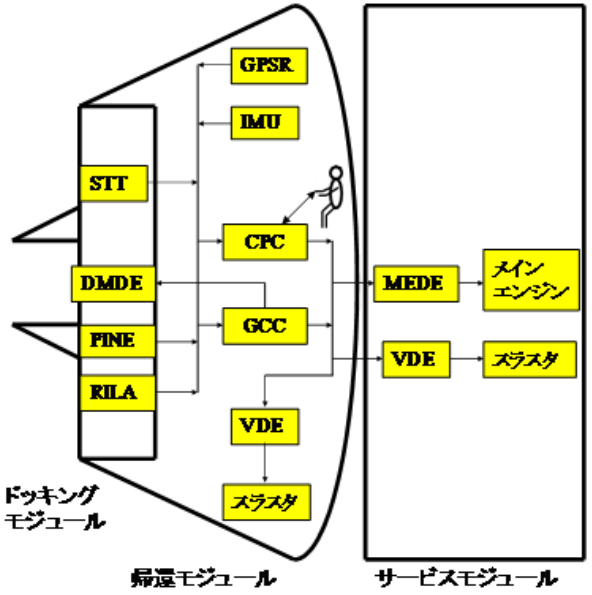
Now we needs to study how to design Safety in Manned Spacecraft.

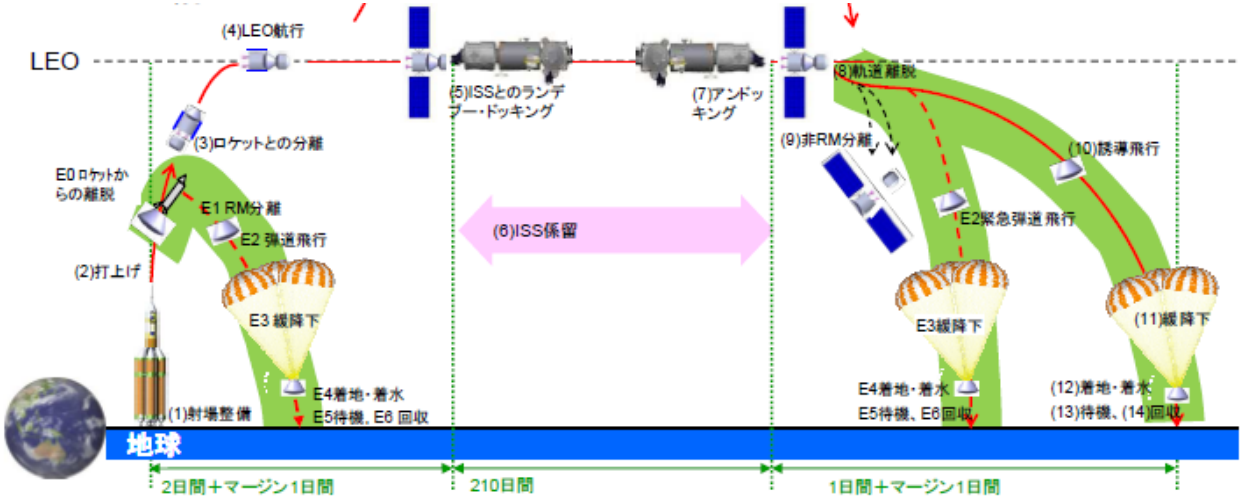
Our experiences of HTV and JEM are NOT enough. "Crew" changes our existing concept of safety in spacecraft.

- The HTV shall NOT collide with the ISS. Manned Spacecraft shall NOT only collide with the ISS but also shall keep Crew's life
- It will be difficult to predict mis-operation of Crew, but operation will be much more time critical.
- Reliability theory can NOT analyze the dynamic of system including crew behavior.

JAXA's Manned Spacecraft (CRV)

- Crew Return Vehicle (CRV)
  - CRV is a Manned Spacecraft like the Soyuz.
    - The missions are "docking ISS" and "returning to the Earth"
  - The landing points are very limited because Japan is an island.
  - "CPC (Cockpit Processing Computer)" will be an unique component.
    - Supporting Crew's Control, Partial back up of GCC, etc (TBD)



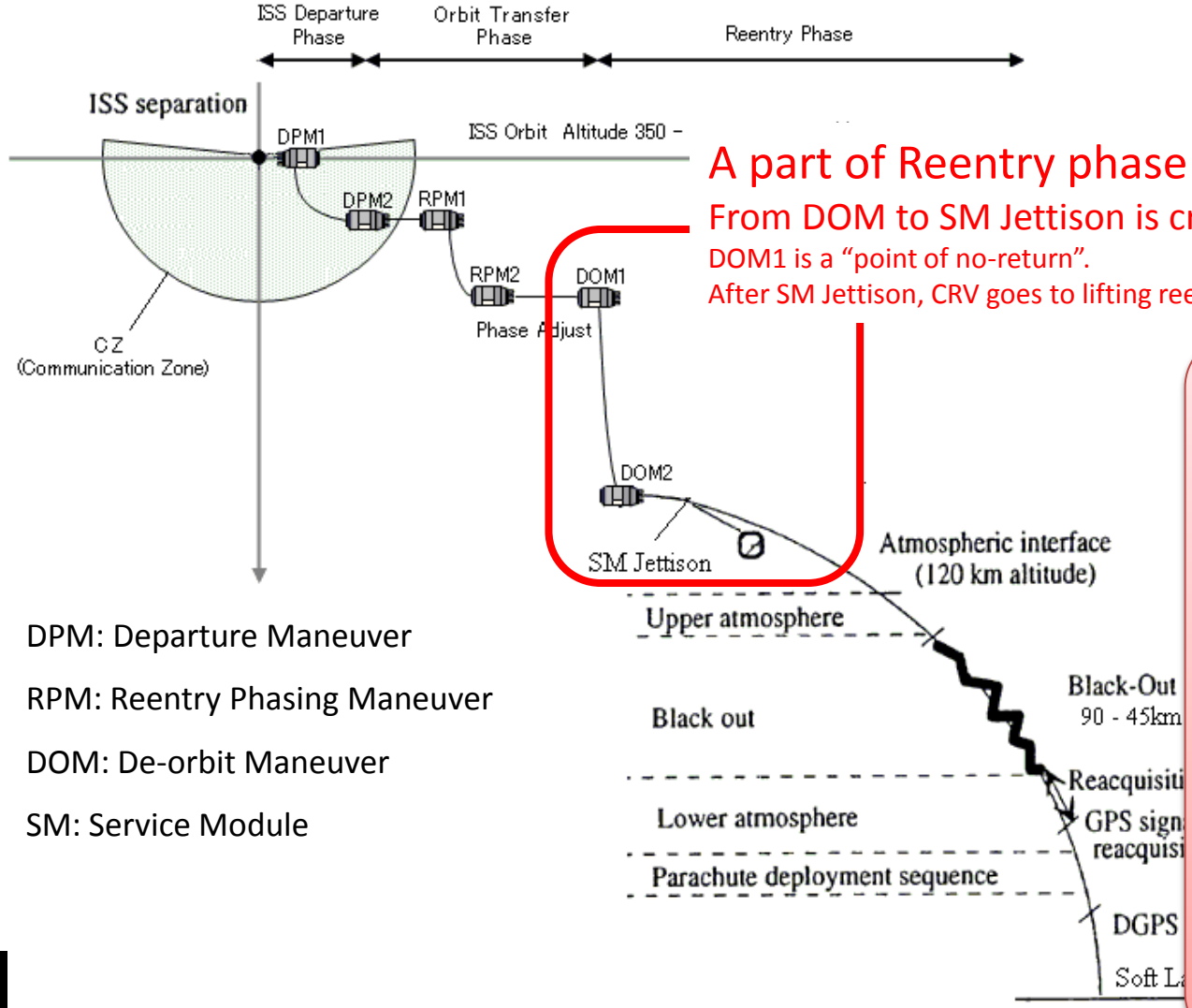


JAXA's Experience of STPA

- HTV, GPM/DPR (Satellite)
  - Analyzed HTV and GPM/DPR with STPA after they're designed.
- STPA Related Research
  - Multiple Controller Analysis in STPA
  - SpecTRM techniques to support STPA
  - New Mental Model in STPA

CRV is a NOT designed system.
We apply STPA to the CRV and study Safety Guided Design with STPA.

STPA in CRV
~Target~



A part of Reentry phase is Target Scenario of STPA.

From DOM to SM Jettison is critical operation.

DOM1 is a “point of no-return”.

After SM Jettison, CRV goes to lifting reentry phase.

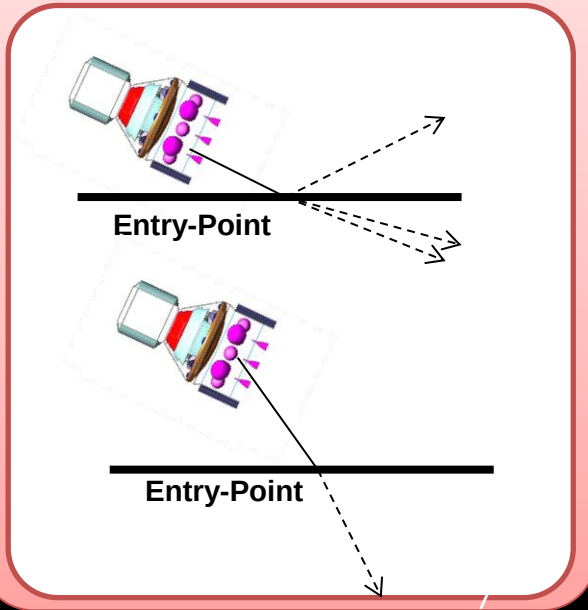
DPM: Departure Maneuver

RPM: Reentry Phasing Maneuver

DOM: De-orbit Maneuver

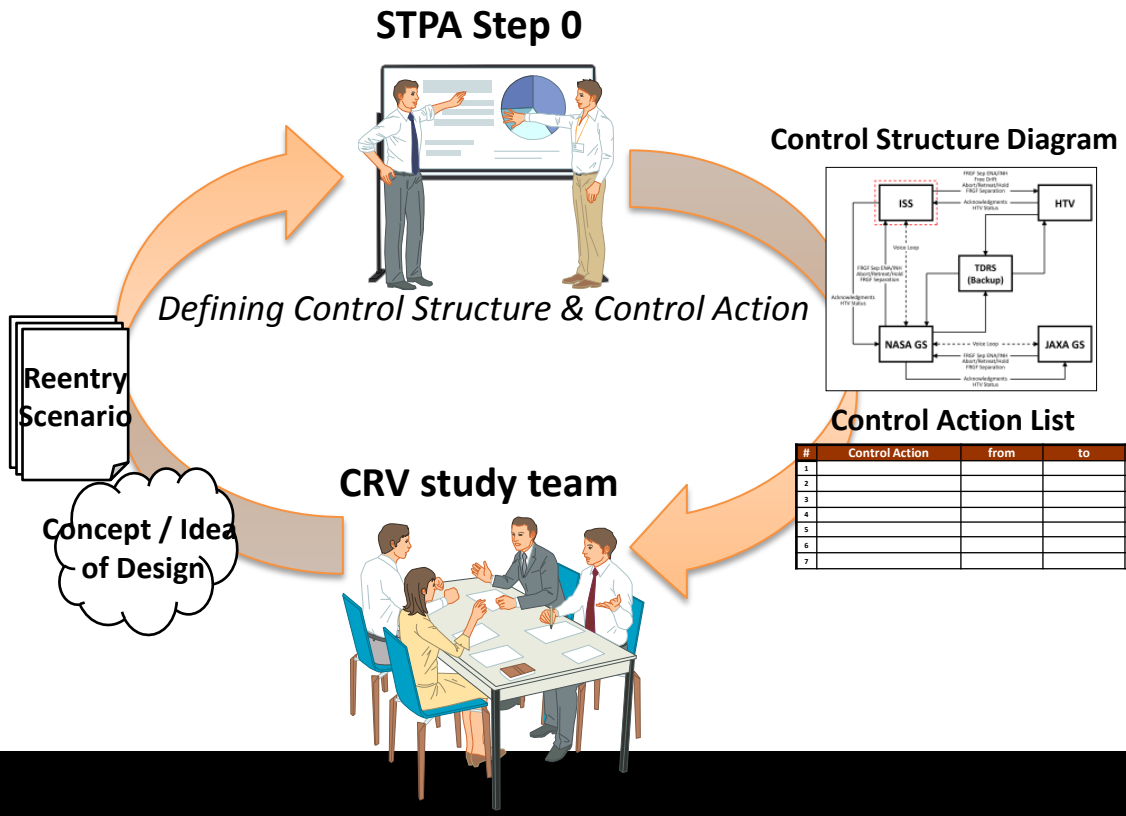
SM: Service Module

Target Hazard:
Fail in entry to return orbit



STPA in CRV
~ Step 0 ~

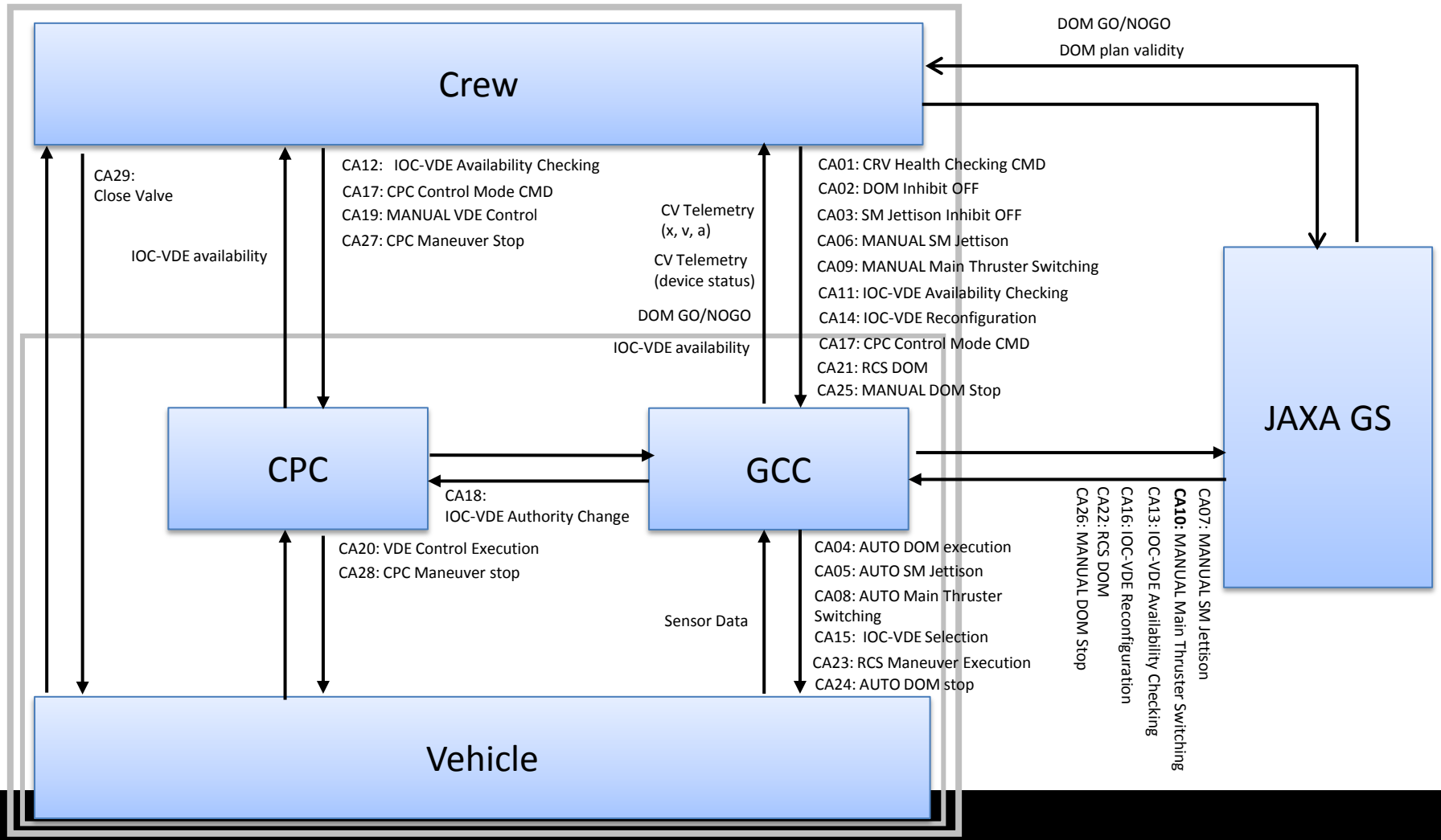
- STPA Step 0: Identifying Control Structure and Control Actions
  - Identify them based on the reentry scenario (documented) & concept design of CRV (NOT documented) from CRV study team.



Step 0 is the preparation of STPA. But it supported system design activity in this case.

STPA in CRV

~ Step 0 ~



STPA in CRV

~ Step 0 ~

#	Control Action	from	To	Description
1	CRV Health Checking CMD	Crew	CV Controller	Check the CRV's devices are readied for DOM
2	DOM Inhibit OFF	Crew	CV Controller	Set the inhibit of DOM off (= Approve DOM)
3	SM Jettison Inhibit OFF	Crew	CV Controller	Set the inhibit of SM jettison off (= Approve SM jettison)
4	AUTO DOM execution	CV Controller	Vehicle	Execute DOM following DOM plan
5	AUTO SM Jettison	CV Controller	Vehicle	Execute SM Jettison following DOM plan
6	MANUAL SM Jettison	Crew	CV Controller	Execute SM Jettison by Crew's order
7	MANUAL SM Jettison	JAXA GS	CV Controller	Execute SM Jettison by JAXA GS's order
8	AUTO Main Thruster Switching	CV Controller	Vehicle	Switch Main Thruster to redundant one when a planned thrusting is NOT started
9	MANUAL Main Thruster Switching	Crew	CV Controller	Switch Main Thruster to redundant one by Crew's order
10	MANUAL Main Thruster Switching	JAXA GS	CV Controller	Switch Main Thruster to redundant one by JAXA GS's order
11	IOC-VDE Availability Checking	Crew	CV Controller	Check and Show available IOC-VDE combination to Crew
12	IOC-VDE Availability Checking	Crew	CPC	Check and Show available IOC-VDE combination to Crew
13	IOC-VDE Availability Checking	JAXA GS	CV Controller	Check and Show available IOC-VDE combination to JAXA GS
14	IOC-VDE Reconfiguration	Crew	CV Controller	Reconfigure IOC-VDE combination
15	IOC-VDE Selection	CV Controller	Vehicle	Set IOC-VDE to be used following IOC-VDE Reconfiguration CMD
16	IOC-VDE Reconfiguration	JAXA GS	CV Controller	Reconfigure IOC-VDE combination
17	CPC Control Mode CMD	Crew	Vehicle (CPC+CV Controller)	Set CPC to be a controller of IOC-VDE
18	IOC-VDE Authority Change	CPC	CV Controller	Get the authority to control IOC-VDE
19	MANUAL VDE Control	Crew	CPC	Set (Select) a thrusting quantity
20	VDE Control Execution	CPC	Vehicle	Execute DOM following MANUAL VDE Control
21	RCS DOM	Crew	CV Controller	Plan and Start DOM with using RCS
22	RCS DOM	JAXA GS	CV Controller	Plan and Start DOM with using RCS
23	RCS Maneuver Execution	CV Controller	Vehicle	Execute RCS DOM following RCS Maneuver plan
24	AUTO DOM stop	CV Controller	Vehicle	Stop Main Thruster Maneuver when a thrusting is NOT stopped as planed
25	MANUAL DOM Stop	Crew	CV Controller	Stop Main Thruster Maneuver by Crew's order
26	MANUAL DOM Stop	JAXA GS	CV Controller	Stop Main Thruster Maneuver by JAXA GS's order
27	CPC Maneuver Stop	Crew	CPC	Stop Main Thruster Maneuver by Crew's order
28	CPC Maneuver stop	CPC	Vehicle	Stop Main Thruster Maneuver by Crew's order
29	Close Valve	Crew	Vehicle	Close the valve of Main Thruster to stop maneuver

STPA in CRV
~ Step 1 ~

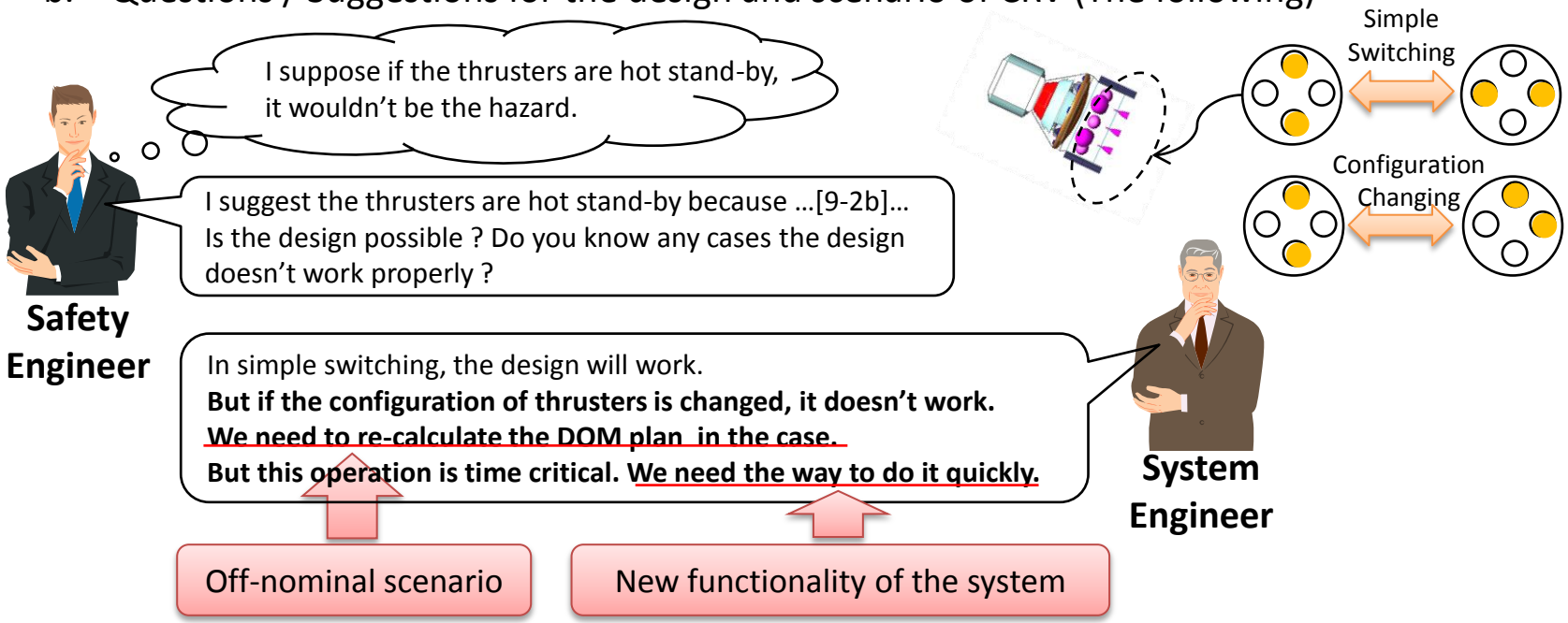
- STPA Step 1: Identifying Unsafe Control Action
  - The 29 Control Actions have been analyzed

Control Action	from	to	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopping Too Soon /Applying Too Long Causes Hazard
AUTO Main Thruster switching	CV Controller	Vehicle	[UCA9-1] This CA NOT provided when one of the 2 main thrusters doesn't work properly, CRV keeps using the broken thruster. It result in the hazard. **Unsafe Control Action**	[UCA9-2a] The incorrect CA provided, CRV uses the inappropriate thruster or the switching doesn't happen. It result in the hazard. **Unsafe Control Action** [UCA9-2b] The CA provided when CRV is executing DOM properly, Case A: Hot Stand-by CRV keeps executing DOM. It doesn't result in the hazard. Case B: Cold Stand-by DOM is stopped. It can result in the hazard.	[UCA9-3a] This CA provided too early when one of the 2 main thrusters doesn't work properly, the result is same as UCA9-2b. [UCA9-3b] This CA provided too late when one of the 2 main thrusters doesn't work properly, DOM is delayed. It can result in the hazard. **Unsafe Control Action**	[UCA9-4] This CA is a discrete command

It depends on the design of CRV whether UCA9-2b can be Unsafe or not.

STPA in CRV
~ Step 1 ~

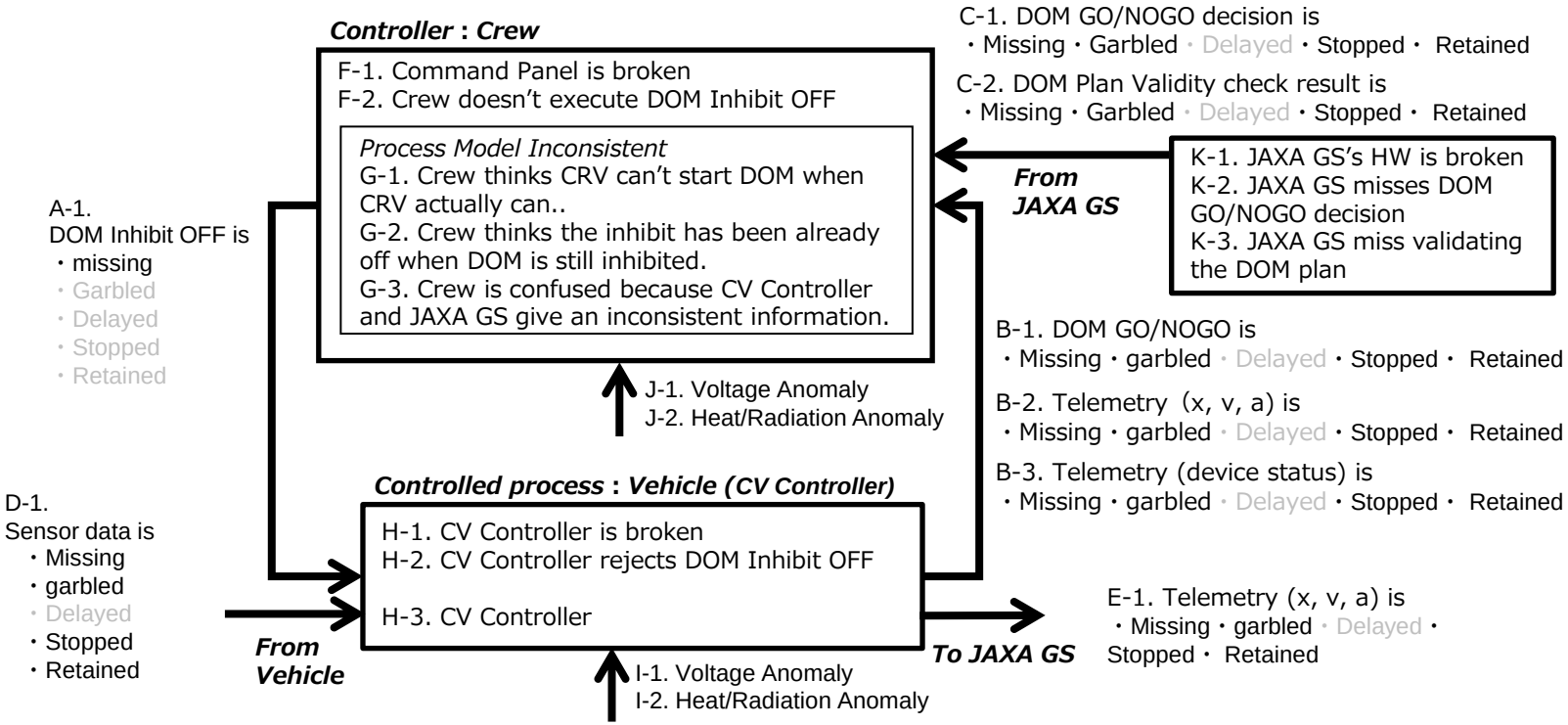
- Outcomes from Step 1
  a. 127 Unsafe Control Actions
  b. Questions / Suggestions for the design and scenario of CRV (The following)



STPA can facilitate designing off-nominal scenario and related functionality
STPA can find the points of system design that are generally overlooked by system engineer

STPA in CRV
~ Step 2 ~

- STPA Step 2: Identifying Causal Scenarios for Unsafe Control Actions
  - 11 of the 127 Unsafe Control Actions have been analyzed because of the limitation of time
  - The following example is “UCA2-1：DOM Inhibit OFF is NOT provided”.



STPA in CRV
~ Step 2 ~

- Identifying Safety Constraints / Requirements from Causal Scenario. Design candidates are also required to concretely discuss a safer design with the system engineers.

From Design to STPA result

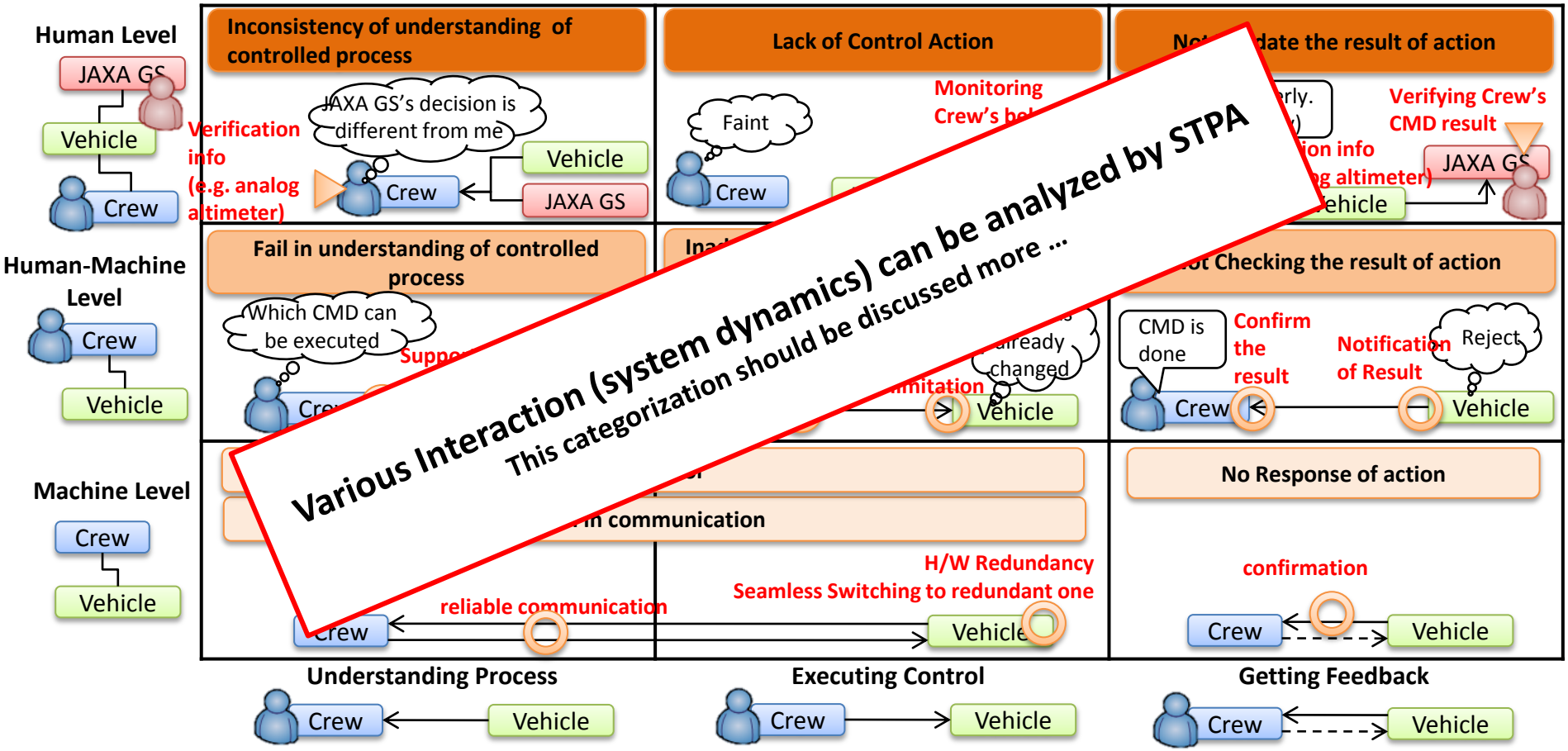
From STPA result to Design

#	Causal Scenario	Safety Constraint / Requirement	Design Candidate
13	**G-2.** **Crew thinks the inhibit has been already off when DOM is still inhibited,** and then Crew doesn't provide DOM Inhibit OFF to Vehicle.	Crew shall keep understanding the actual state of the inhibit.	CV Controller alerts if the inhibit is not OFF a few minutes before planned DOM time. Crew shall keep checking the state of the inhibit from after the final checking and to DOM start time. JAXA GS shall notify the state of the inhibit to Crew.

If some design candidates are adopted to the design, the Control Loop will be changed and STPA step 2 again.

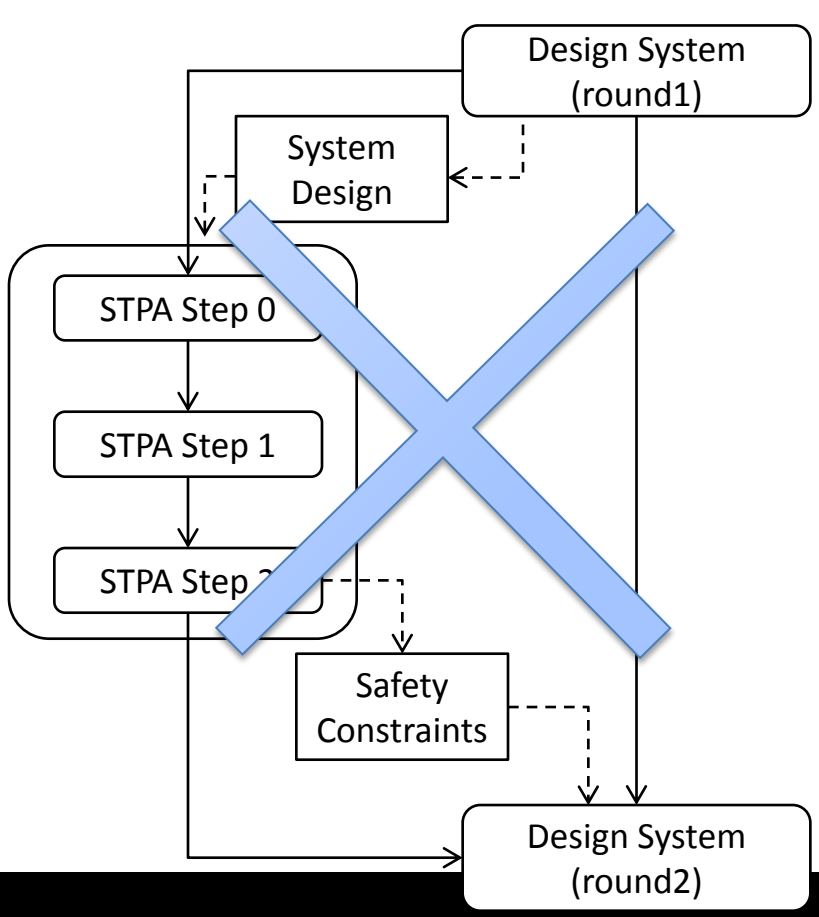
STPA in CRV
~ Step 2 ~

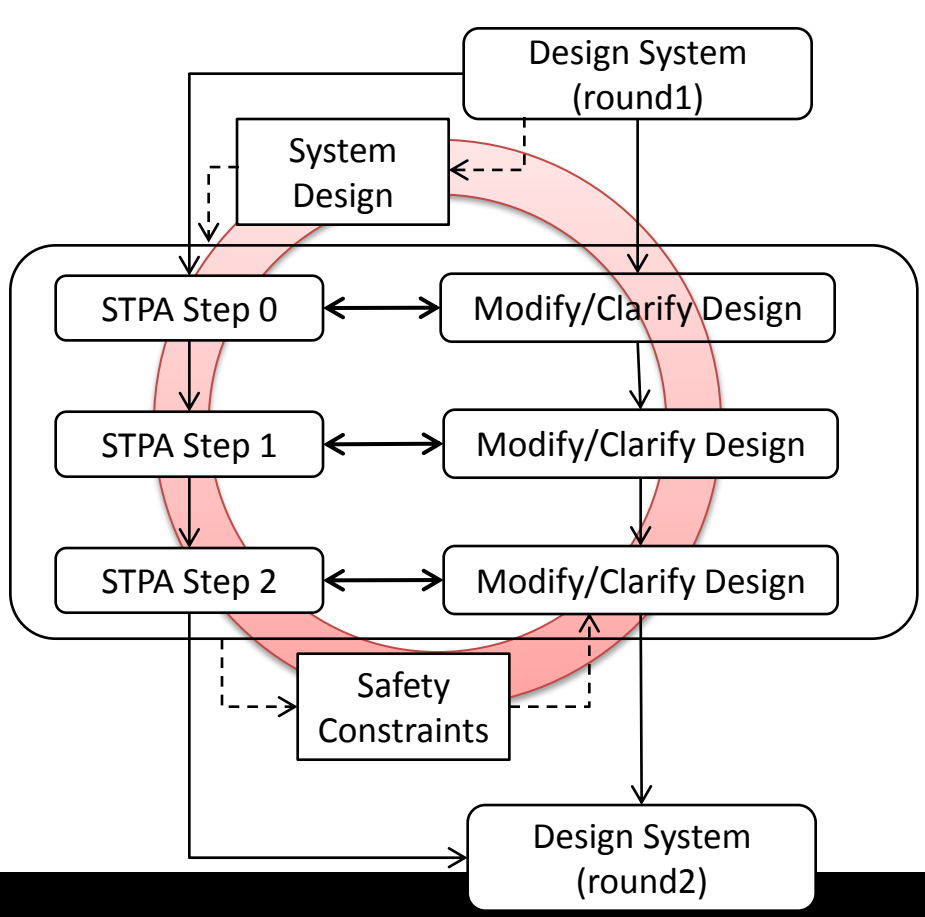
- Summary of Step2 results (Causal Scenario)



Discussion
~Safety Guided Design~

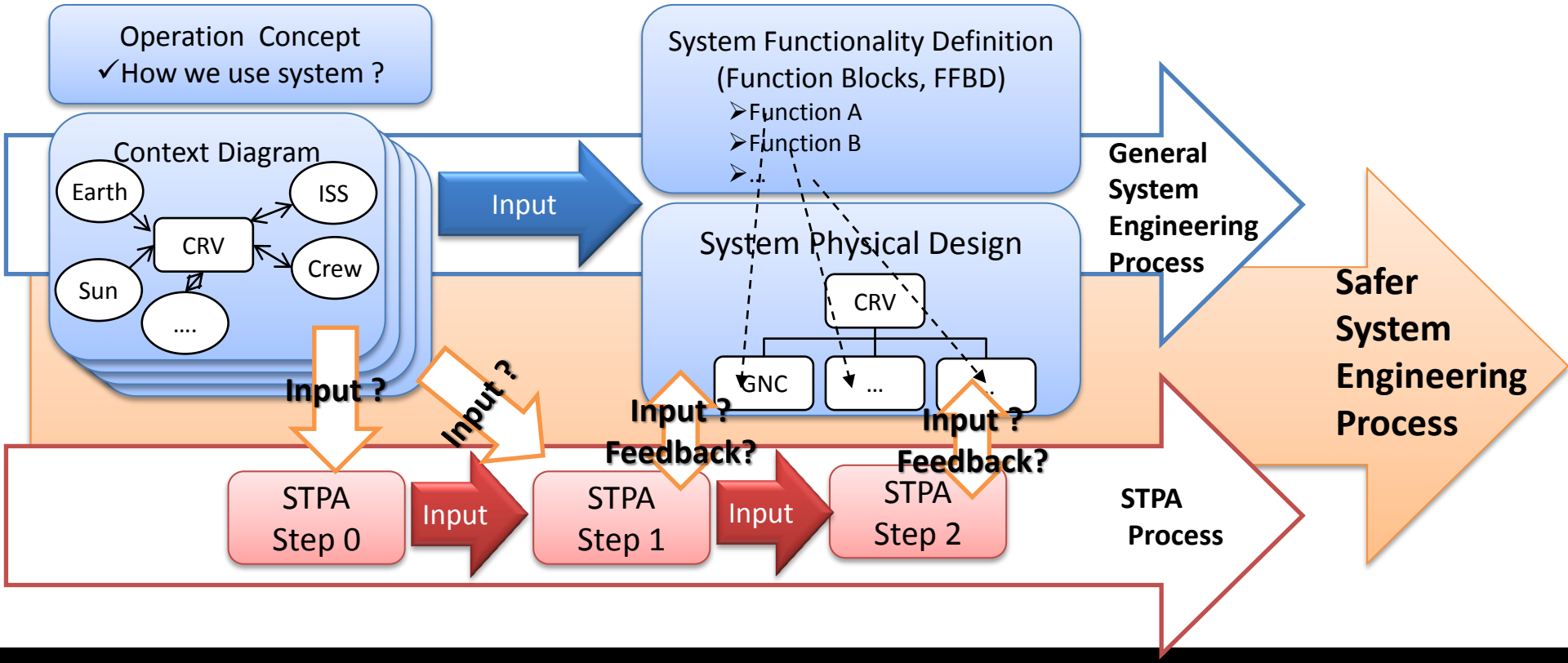
- In Safety Guided Design, STPA Process and System Design Process are much more inseparable than we expected





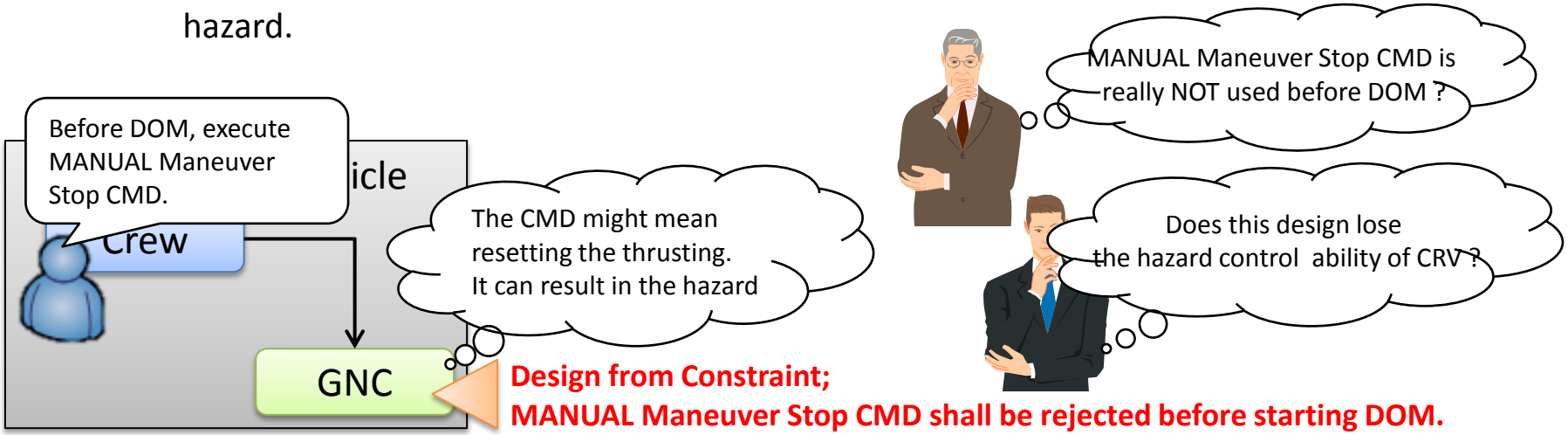
Discussion
~Safety Guided Design~

- How to combine STPA process and General System Engineering process ?
  - More efficient collaboration between SE & STPA process.
    - It is supposed STPA workload is high in the CRV study case because of lack of system engineering activity.



Discussion
~ Constraint vs. Flexibility ~

- Safety Constraint loses Crew's flexible Control ? Does it result in deteriorating safety ?
  - Sometimes human's flexible control might keep system safe. In the other case, it result in hazard.

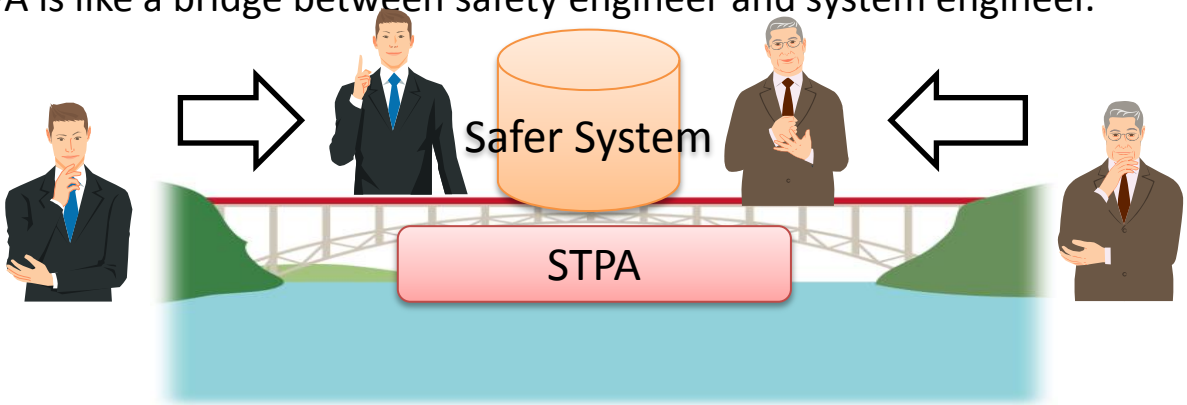


Design from Constraint;
MANUAL Maneuver Stop CMD shall be rejected before starting DOM.
If crew want to suspend DOM before DOM, DOM Inhibit CMD shall be executed.

How we evaluate human's flexible control in safety ?
How we select better design for system including human ?
At least, STPA could clarify the points to be discussed in CRV study.

Conclusion & Future Work

- Conclusion
  - STPA is like a bridge between safety engineer and system engineer.



- Future Works
  - Keep considering “Safer System Engineering Process
  - Multiple Controller Analysis in Safety Guided Design
    - The methodology of the analysis has been developed.
    - Analyze and Design the safer relationship among controllers.
  - Crew Mental Model for analyzing crew behavior in detail
    - A new mental model has been developed.
    - Analyze and Design the safer relationship between Crew and Computer system