Safety-Guided Design

Safety-Guided Design

- Safety analysis and design should be integrated into system engineering process
  - Most important decisions related to design made in early concept development stage.
  - Once made, very difficult or impossible to change
  - So kludges made to try to fix the problems (usually expensive and not very effective)
  - Cheapest and most effective if design safety in from the beginning
  - Can save money and time doing this (less rework)

Process

1. Try to eliminate hazards from conceptual design
2. If cannot eliminate, identify controls at system level
3. Create system control structure
4. Refine constraints and design in parallel
    a. STPA step 1: identify potentially hazardous control actions. Restate as design constraints.
    b. STPA step 2: determine factors that could lead to violation of safety constraints
    c. Augment basic design to eliminate or control
    d. Iterate and refine design

Thermal Tile Robot Example

1. **Identify high-level functional requirements and environmental constraints.**

   e.g. size of physical space, crowded area

2. **Identify high-level hazards**

Accidents?

Hazards

Hazards

- Violation of minimum separation between mobile base and objects (including orbiter and humans)
- Mobile robot becomes unstable (e.g., could fall over)
- Manipulator arm hits something
- Fire or explosion
- Contact of human with DMES
- Inadequate thermal control (e.g., damaged tiles not detected, DMES not applied correctly)
- Damage to robot

Safety Constraints?

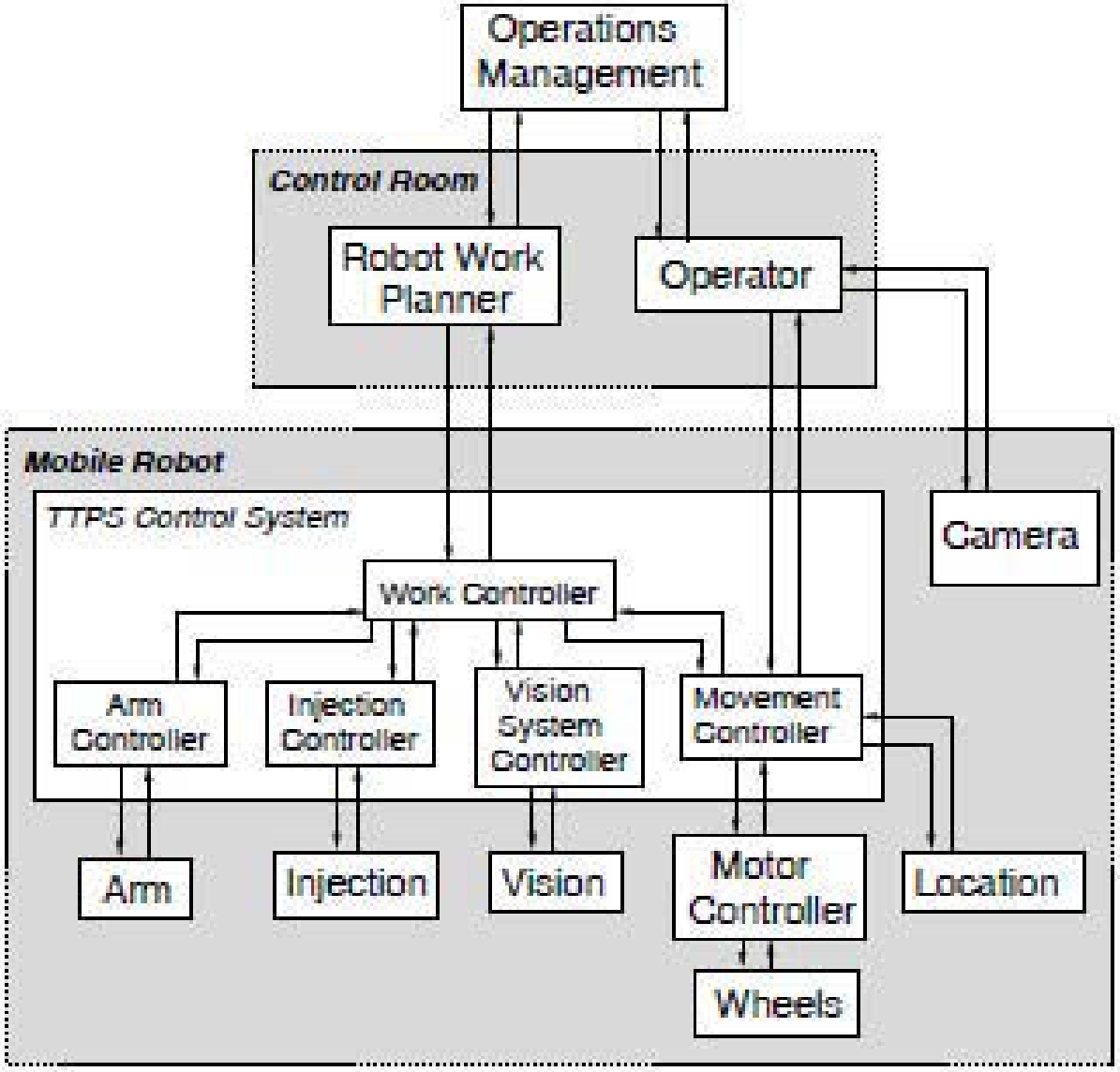
Safety Constraints?

For unstable base hazard

System Safety Constraint:

Mobile base must not be capable of falling over under worst case operational conditions

Define preliminary control structure and refine constraints and design in parallel.



From Leveson, Nancy (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, © Massachusetts Institute of Technology. Used with permission.

3. **Try to eliminate hazards from system conceptual design. If not possible, then identify controls and new design constraints.**

First Try to Eliminate

First try to eliminate:

1. Make base heavy

   Could increase damage if hits someone or something.

   Difficult to move out of way manually in emergency

2. Make base long and wide

   Eliminates hazard but violates environmental constraints

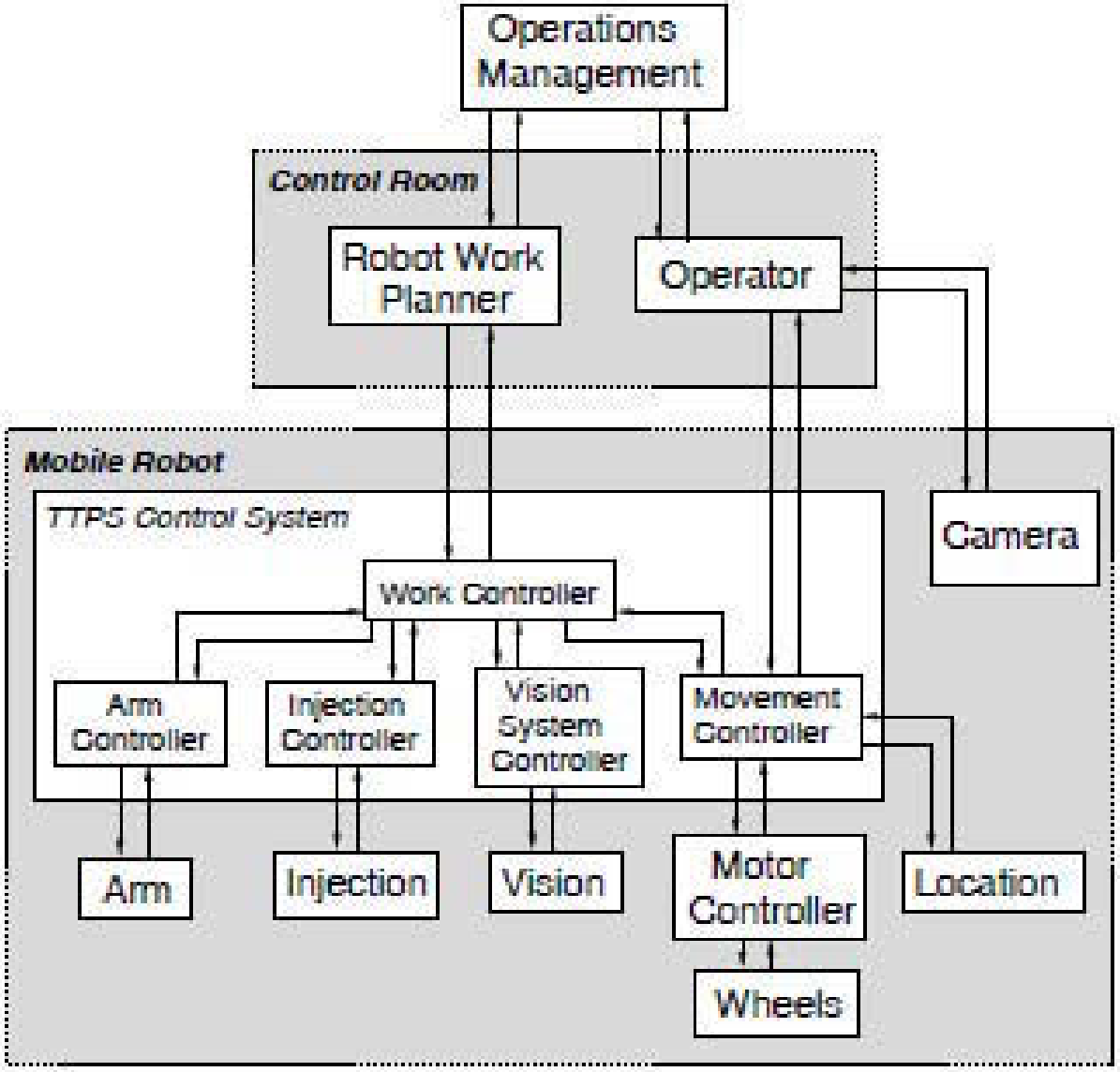
3. Use lateral stability legs that are deployed when manipulator arm extended but must be retracted when mobile base moves.

   Creates two new safety constraints. What are they?

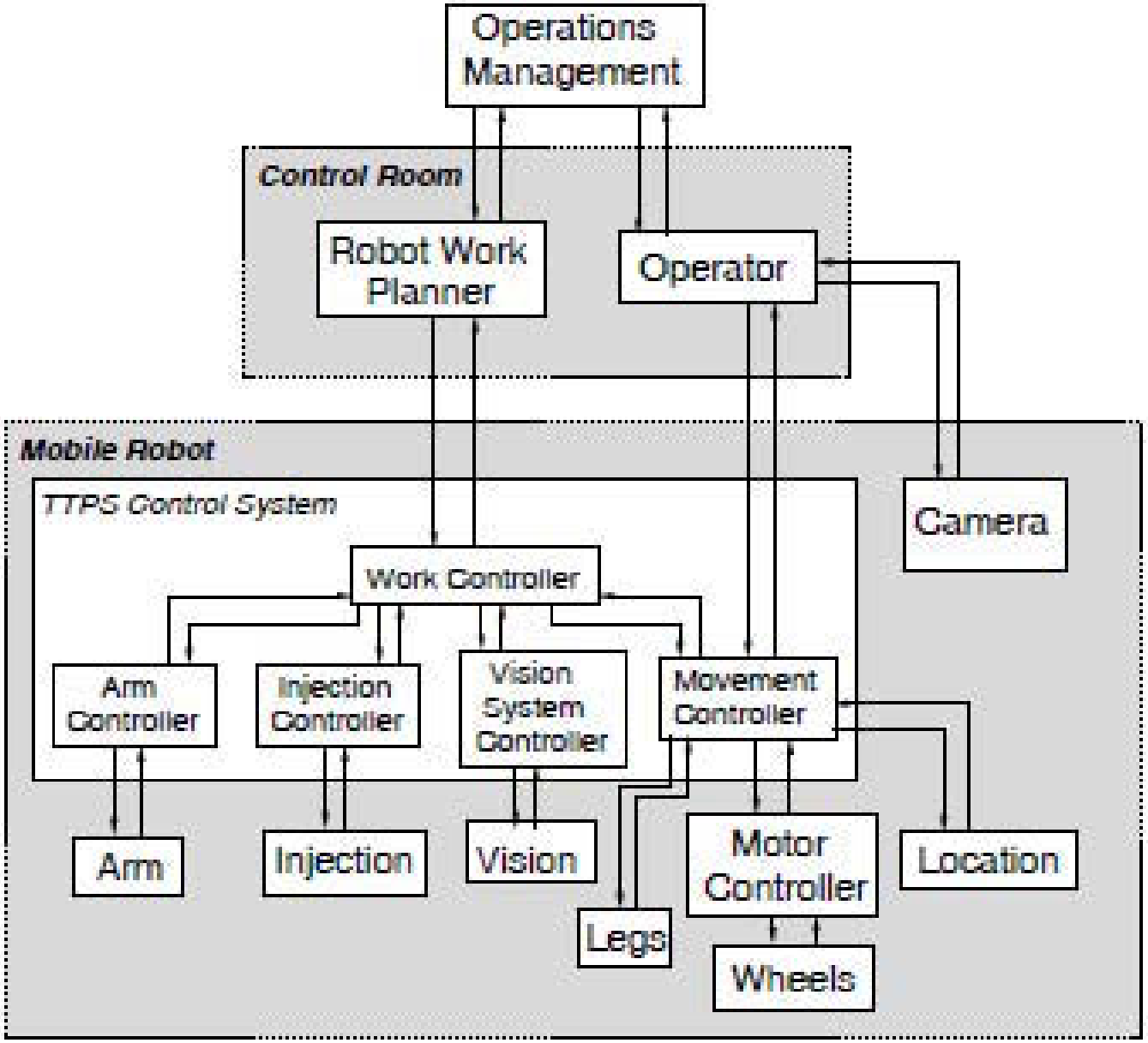
Lateral stability legs results in two new design constraints:

- Manipulator arm must move only when stabilizer legs are fully deployed
- Stabilizer legs must not be retracted until manipulator arm is fully stowed.

Define preliminary control structure and refine constraints and design in parallel.



From Leveson, Nancy (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, © Massachusetts Institute of Technology. Used with permission.



From Leveson, Nancy (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, © Massachusetts Institute of Technology. Used with permission.

Identify potentially hazardous control actions by each of system components

1. A required control action is not provided or not followed
2. An incorrect or unsafe control action is provided
3. A potentially correct or inadequate control action is provided too late or too early (at the wrong time)
4. A correct control action is stopped too soon.

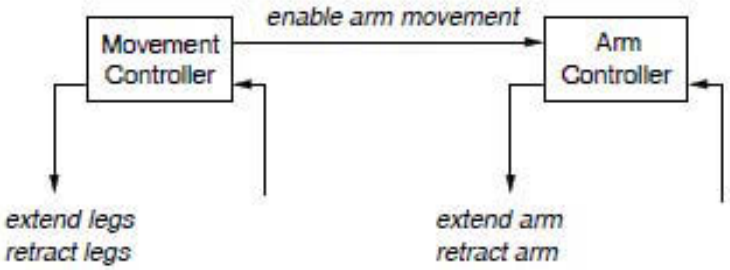
Hazardous control of stabilizer legs:

- Legs not deployed before arm movement enabled
- Legs retracted when manipulator arm extended
- Legs retracted after arm movements are enabled or retracted before manipulator arm fully stowed
- Leg extension stopped before they are fully extended

Create Step 1 Table

HAZARD1: Arm extended while legs retracted

HAZARD2: Legs extended during movement



Command	Missing	Incorrect	Timing/Sequencing	Stopped Too Soon
extend legs	Legs not extended before arm extended **H1**	Extend legs during movement **H2**	Extend arm before legs extended **H1**	Stop before fully extended **H1**
retract legs	Not retracted before movement **H2**	Retract while arm extended **H1**	Retract legs before arm fully stowed **H1**	Stop while still partially extended **H1**

Command	Missing	Incorrect	Timing/Sequencing	Stopped Too Soon
extend arm	Do not extend arm when commanded	Extend arm when legs retracted **H1**	Extend arm before legs fully extended **H1**	(tile processing hazard)
retract arm	Not retracted before movement **H2**	(tile processing hazard)	(tile processing hazard)	Stop retraction before fully arm fully stowed and movement starts or legs retracted **H1 H2**

From Leveson, Nancy (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, © Massachusetts Institute of Technology. Used with permission.

Restate as safety design constraints on components

Restate as safety design constraints on components

1. Controller must ensure stabilizer legs are extended whenever arm movement is enabled
2. Controller must not command a retraction of stabilizer legs when manipulator arm extended
3. Controller must not command deployment of stabilizer legs before arm movements are enabled. Controller must not command retraction of legs before manipulator arm fully stowed
4. Controller must not stop leg deployment before they are fully extended

Do same for all hazardous commands:

e.g., Arm controller must not enable manipulator arm movement before stabilizer legs are completely extended.

Create Process Models

- What must be in the process models for the arm controller and the leg controller?

To produce detailed scenarios for violation of safety constraints, augment control structure with process models

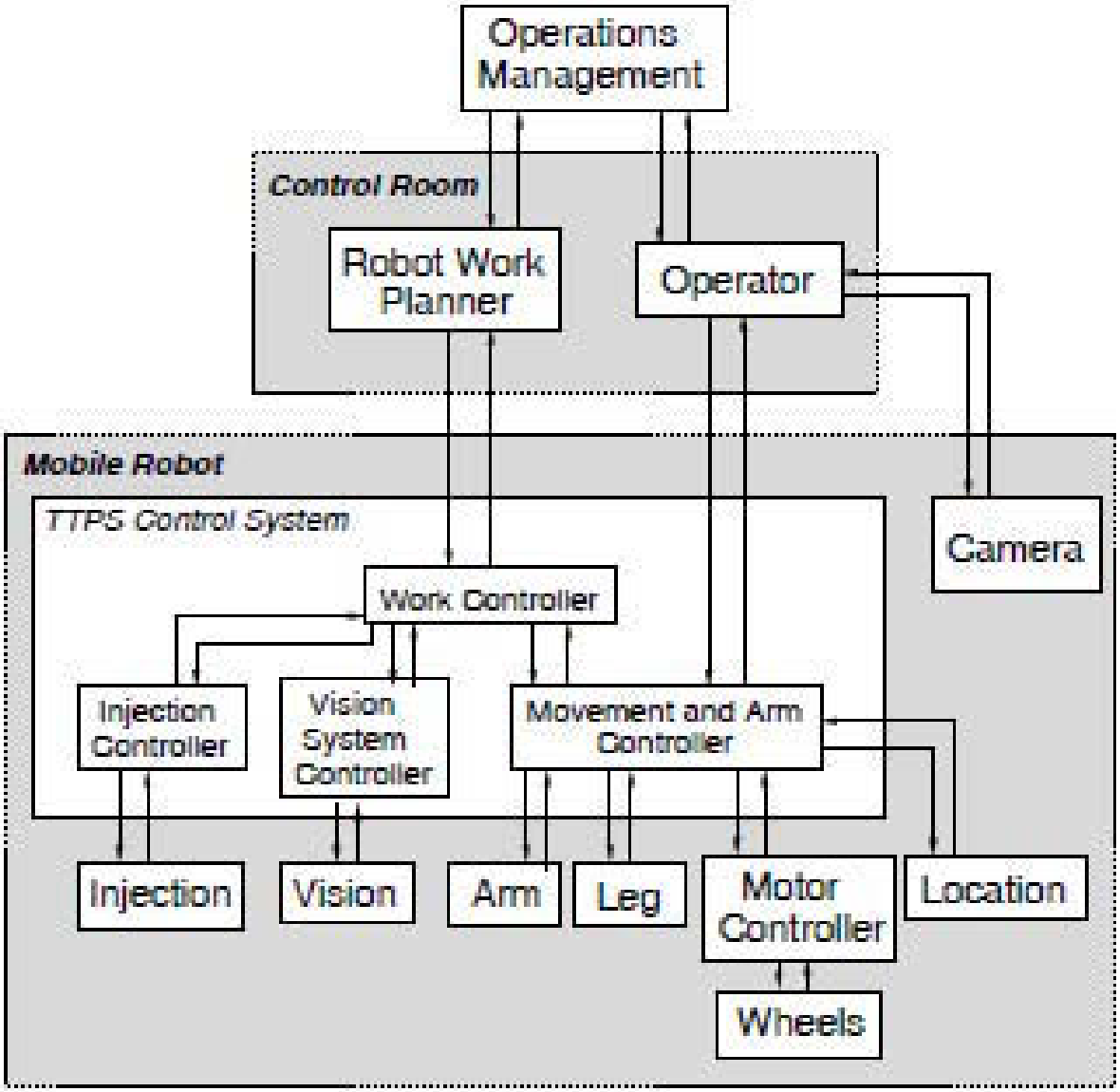
Arm Movement	**Stabilizer Legs**	**Manipulator Arm**
Enabled	Extended	Stowed
Disabled	Retracted	Extended
Unknown	Unknown	Unknown

How could become inconsistent with real state?

How could become inconsistent with real state?

- Issue command to extend stabilizer legs but external object could block extension
- Extension motor could fail
- Communication (messages) between the two controllers could be lost or delayed

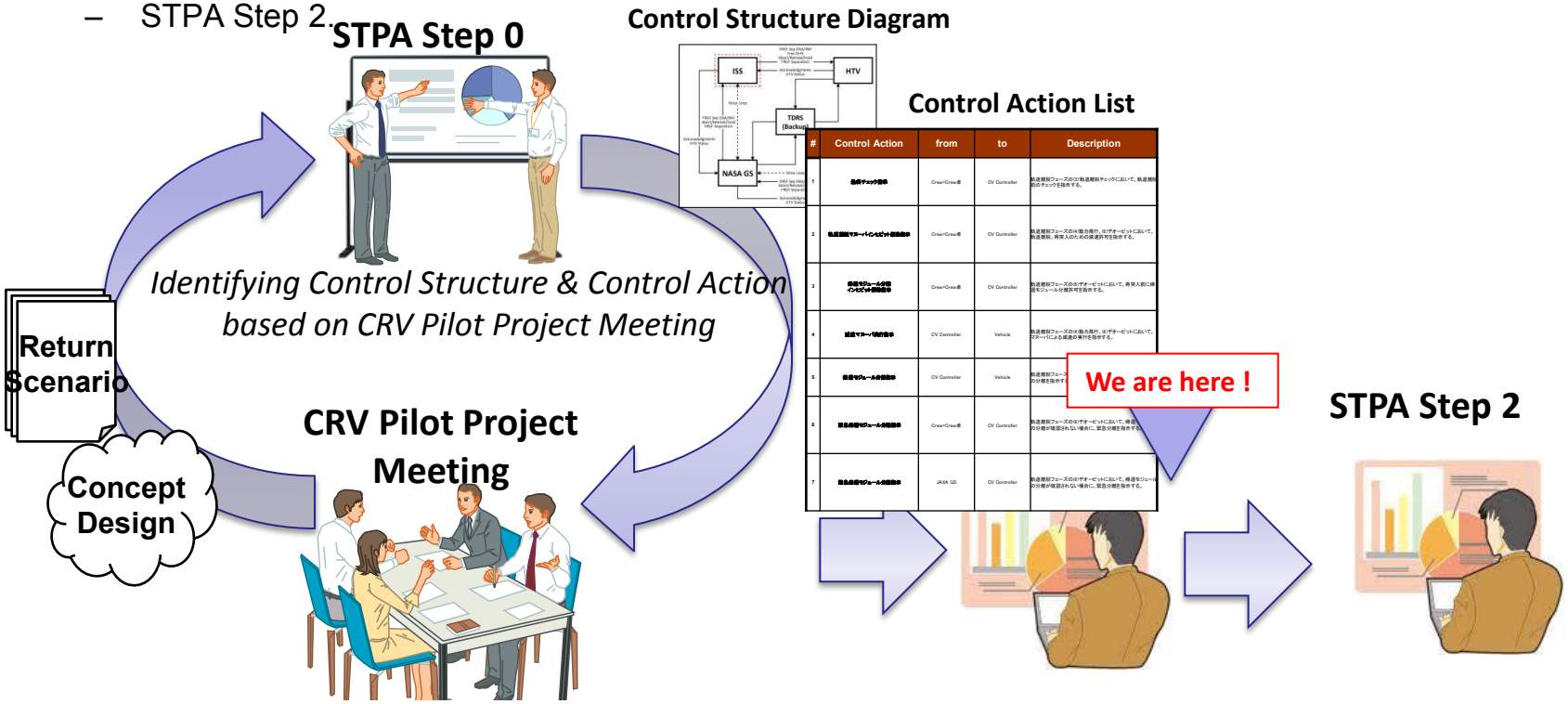
At this point, may decide to have arm controller and leg controller in same component



From Leveson, Nancy (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, © Massachusetts Institute of Technology. Used with permission.

STPA for Crew Return Vehicle
~Current Status~

- We are trying Safety Guided Design with STPA in Crew Return Vehicle …
  - Target Phase: De-orbiting Phase (see next slide), Target Hazard:
- Current Status
  - STPA Step 2



Discussing Concept Design & Return Scenario

STPA for Crew Return Vehicle
~Summary of CRV~

JAXA has started early study of Manned Spacecraft since 2010.

- Goal of the early study of Manned Spacecraft:
  - To obtain technical capability to initiate real project
- Duration:
  - 2010 ~ 2012 (3 years)

- Current status of the study
  - Define the mission
    - Mission goals, System overview, Operation flow
  - Identify functionalities that are needed in the mission
  - Identity and prioritize technical areas that are needed more studies / researches
    - There are 8 technical groups

STPA for Crew Return Vehicle
~Summary of CRV~

- Mission overview

Diagram removed due to copyright restrictions. See:
http://iaassconference2013.space-safety.org/wp-content/uploads/sites/19/2013/06/1440_Ujiie.pdf

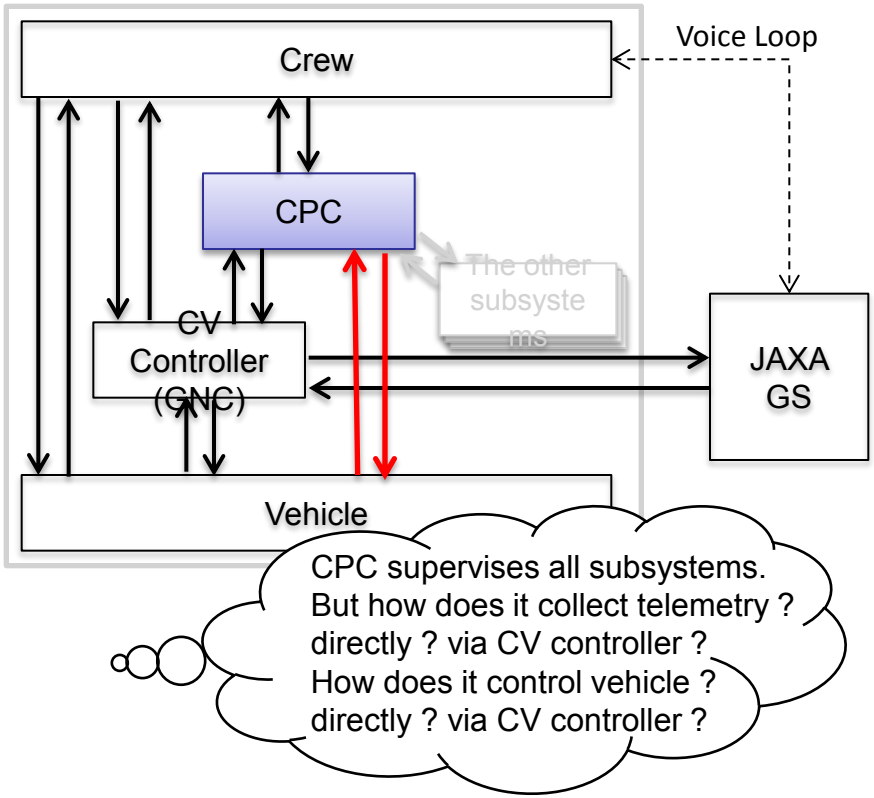
STPA for Crew Return Vehicle

~De-orbiting Scenario~

Diagram removed due to copyright restrictions. See:
http://iaassconference2013.space-safety.org/wp-content/uploads/sites/19/2013/06/1440_Ujiie.pdf

STPA for Crew Return Vehicle
~STPA step 0~

- STPA Step 0
  - Support to clarify the system (define the interaction among components and identify missing control action).



#	Control Action	From	to	Description
…	…	…	…	…
3	**Release Inhibition of SM separation**	Crew	CV Controller	Permit to execute SM separation
4	…	…	…	…
5	**SM Separation**	CV Controller	Vehicle	CV controller separates SM from Vehicle.
6	**SM Separation (emergent situati**			
7	**(emergent situation)**			SM if schedule.

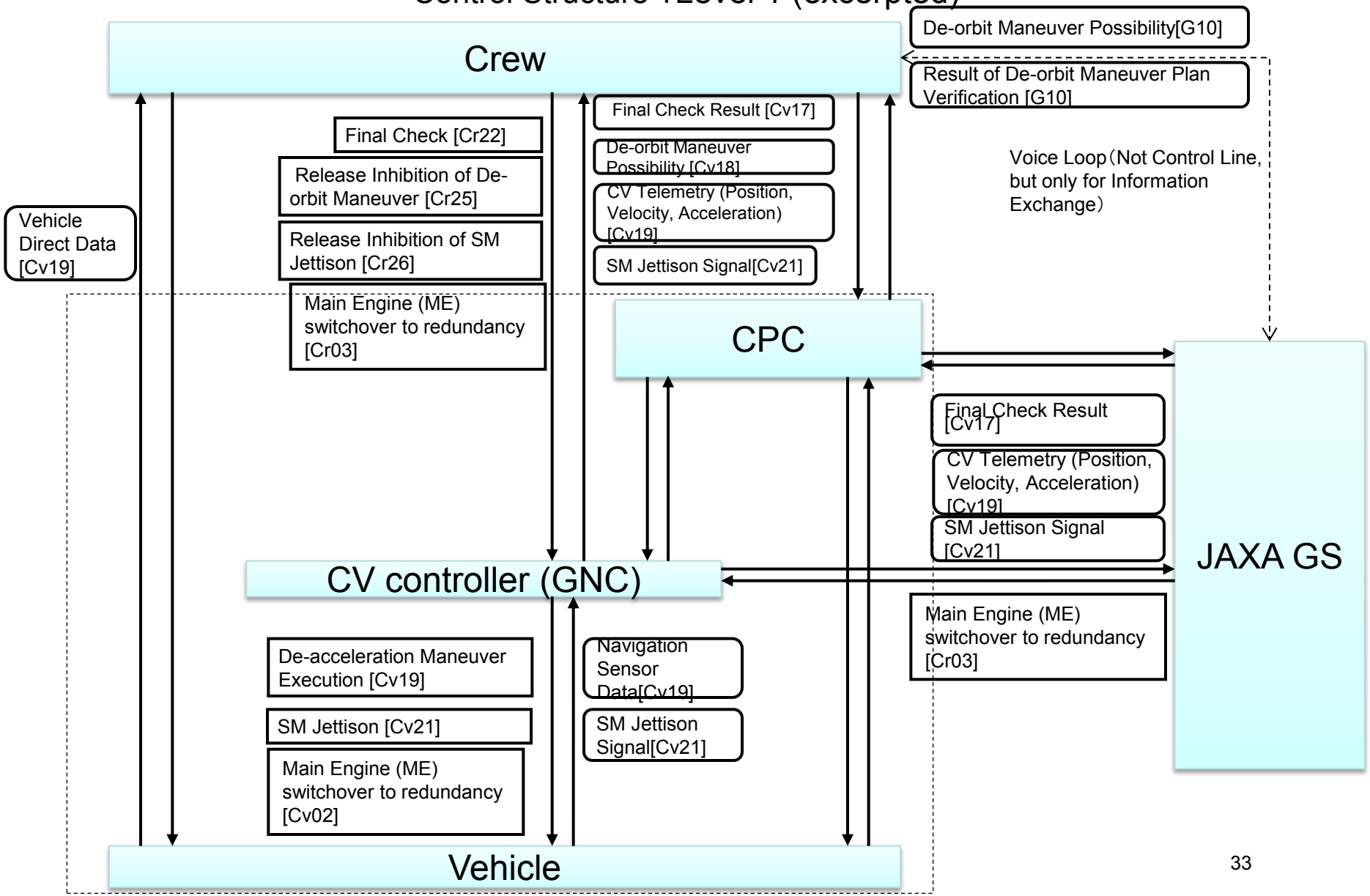
Crew, CV Controller and JAXA GS can execute SM separation.
But it's inhibition can be unlocked by only Crew… Is it better that JAXA GS can also unlock it ?

System and Scenario were brushed up by iterating STPA step 0 and system design

STPA for Crew Return Vehicle

~STPA step 0~

Control Structure：Level 1 (excerpted)



□：Control Action (CA) ▭：Feedback Data (FB)

STPA for Crew Return Vehicle
~STPA step 0~

- Control Action List (excerpted)

#	Control Action	From	to	Description
1	**Final Check**	Crew	CV Controller	At De-orbit Check of Orbit Transfer phase, command check for de-orbit
2	**Release Inhibition of De-orbit Maneuver**	Crew	CV Controller	At Powered Flight and De-orbit of Orbit Transfer phase, command de-orbit and allow de-acceleration for reentry
3	**Release Inhibition of SM(Service Module) Jettison**	Crew	CV Controller	At De-orbit of Orbit Transfer phase, allow SM Jettison before reentry
4	**De-acceleration**	CV Controller	Vehicle	At Powered Flight and De-orbit of Orbit Transfer phase, command de-acceleration with maneuver
5	**SM(Service Module) Jettison**	CV Controller	Vehicle	At De-orbit of Orbit Transfer phase, perform SM Jettison before reentry
6	**Main Engine (ME) switchover to redundancy**	CV Controller	Vehicle	Automatic Main Engine switchover to redundancy by the CV controller
7	**Main Engine (ME) switchover to redundancy**	Crew	CV Controller	Manual Main Engine switchover to redundancy by the crew if automatic switchover is unavailable
8	**Main Engine (ME) switchover to redundancy**	JAXA GS	CV Controller	Manual Main Engine switchover to redundancy by the JAXA GS if switchover by crew is unavailable

STPA for Crew Return Vehicle
~STPA step 1~

- STPA Step 1
  - Some assumptions of system are needed when analyzing an unsafe control action results in hazard or not.

#	Control Action	from	to	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopping Too Soon /Applying Too Long Causes Hazard
2	**Main Engine (ME) switchover to redundancy**	Crew	CV Controll…	…	When ME is normal, this control action can result in hazard **if the thrusting value of ME is initialized when switching the redundant ME.**	…	…

When ME is switched to redundant one, thrusting value of ME succeeded to the redundant one immediately ? If succeeded, this control action doesn't cause hazard …

These assumptions are important information to design system.
It depends on our experience how much assumptions we can find.

STPA for Crew Return Vehicle
~STPA step 1~

- Summary of assumptions

No.	Related UCA	Category	Assumption
1	Base Scenario UCA4-x	Assumption of Criticality of Actions	We assume the criticality of both DM (De- acceleration Maneuver) 1 and DM 2 at de-orbit is equal; therefore, we analyze DM 1 and DM 2 as same
2	Base Scenario UCA6-3b	Assumption of Criteria for Judging Unsafe	We assume there is time limit when the command of SM Jettison is too late.
3	Emergent Start UCA1-x, 2-x, 3-x	Assumption of Operation Sequence	For Main Engine switchover to redundancy when nominal switchover is impossible, we assume Crew commands it first, but it cannot be done, and the ground controller commands it.
4	Emergent Start UCA1-3a, 2-3a, 3-3a	Assumption of Design	We assume even if ME switchover happens, the controlled variable can be inherited
5	Emergent Start UCA7-x, 8-x, 9-x	Assumption of Design	The actual content of selection of IOC and VDE is not decided. Are they automatically selected by selecting failed thrusters or is it selected by crews at first.
6	Emergent Start UCA10-x, 11-x	Assumption of Design	It is needed to switch the right of control from CV Controller to CPC in order to control Vehicle with CPC.

STPA for Crew Return Vehicle

~STPA step 1~

Step1 result (excerpted)

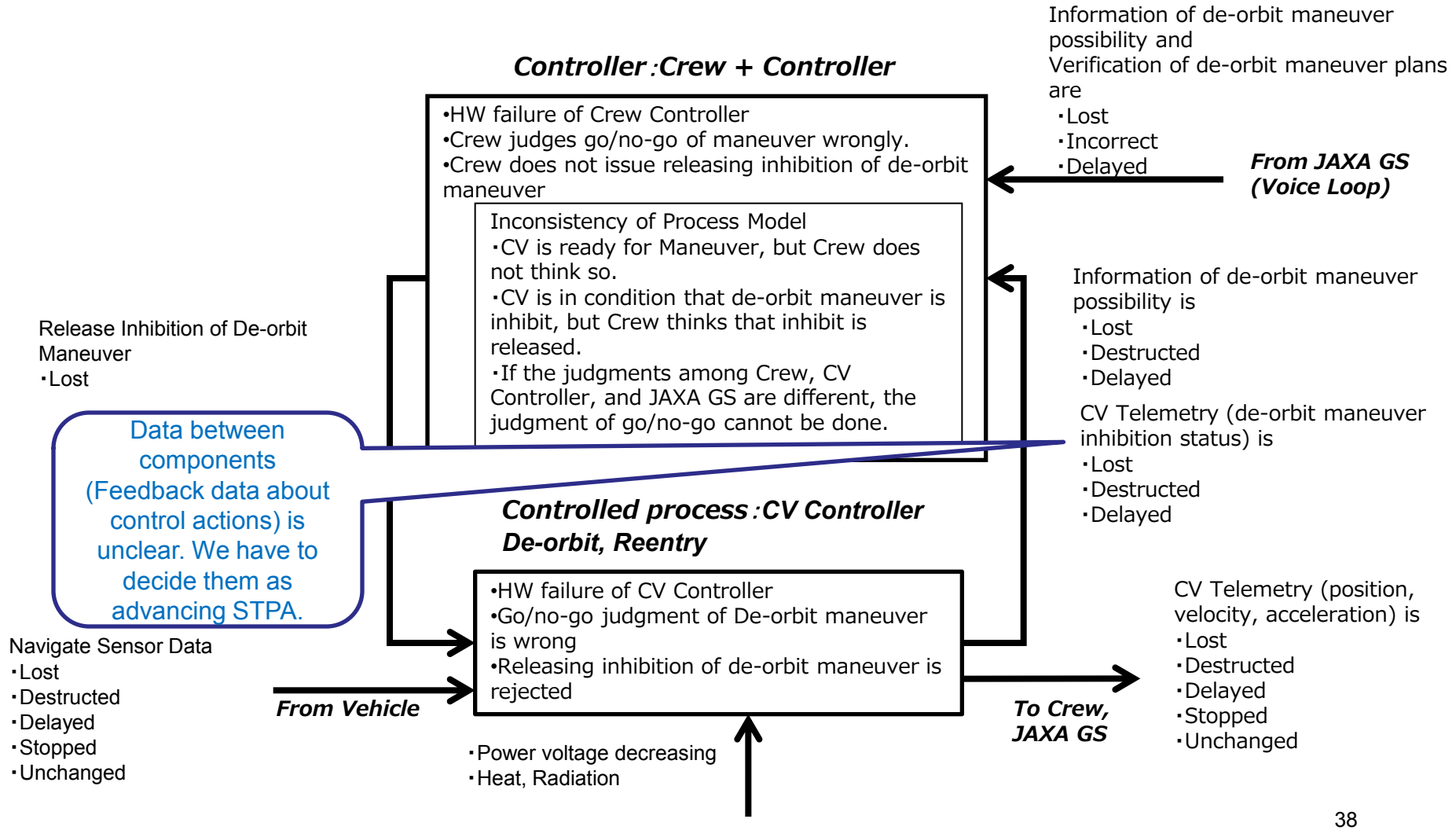
#	Control Action	From	To	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopping Too Soon /Applying Too Long Causes Hazard
1	**Final Check**	Crew	CV Controller	[UCA1-1] The command of Final Check for maneuver start is not processed, go/no-go of maneuver cannot be judged, and then de-orbit cannot be done. Finally, reentry cannot be done.	[UCA1-2] If an invalid command is issued, go/no-go of maneuver cannot be judged, and then de-orbit cannot be done. Finally, reentry cannot be done.	[UCA1-3a] Final Check timing is too early. When Final Check is done while it is not in final condition but at phase adjustment, if Crew finds it and finally executes it at appropriate timing, it is safe. [UCA1-3b] Final Check timing is too late. Judging go/no-go of maneuver becomes late, and planned de-orbit time will be past. Planned de-orbit cannot be done. Finally, planned reentry cannot be done. (The landing point can be apart from planned one)	[UCA1-4] N/A because of single command
2	**Release Inhibition of De-orbit Maneuver**	Crew	CV Controller	[UCA2-1] The command of releasing inhibition for maneuver start is not processed, maneuver cannot be done, and then de-orbit cannot be done. Finally, reentry cannot be done.	[UCA2-2a] If inhibition is set adversely or an invalid command is issued when release of inhibition is tried, maneuver cannot be done, and then de-orbit cannot be done. Finally, reentry cannot be done. [UCA2-2b] (same as [UCA2-3a]) If unintentionally inhibition of maneuver is released though it is not the time for maneuver, and maneuver is executed because of GNC failure, then planned de-orbit cannot be done. Finally, planned reentry cannot be done. (The landing point can be apart from planned one) (It is hazard because of multiple failures)	[UCA2-3a] (same as [UCA2-2b]) Release Inhibition of De-orbit Maneuver is too early. If moreover maneuver is executed too early because of GNC failure, then planned de-orbit cannot be done. Finally, planned reentry cannot be done. (The landing point can be apart from planned one) (It is hazard because of multiple failures) [UCA2-3b] Release Inhibition of De-orbit Maneuver is too late. Planned de-orbit time is past. Planned de-orbit cannot be done. Finally, planned reentry cannot be done. (The landing point can be apart from planned one)	[UCA2-4] N/A because of single command

STPA for Crew Return Vehicle

~STPA step 2~

- Step 2 result (excerpted)

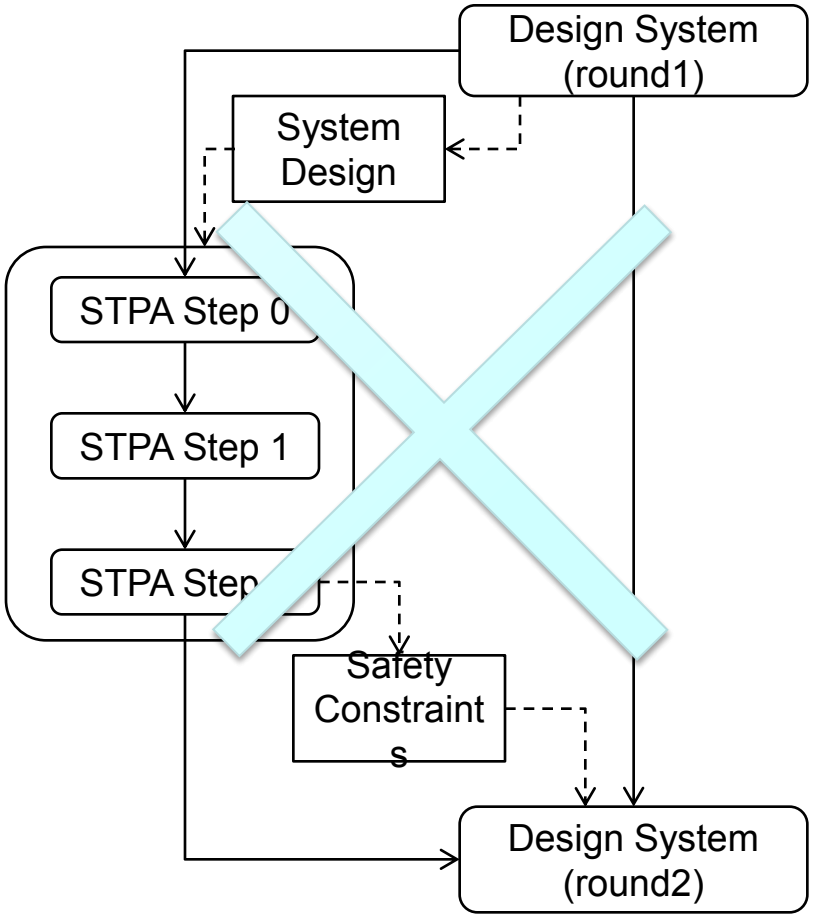
UCA2-1：The command of releasing inhibition for maneuver start is not processed, maneuver cannot be done, and then de-orbit cannot be done. Finally, reentry cannot be done.

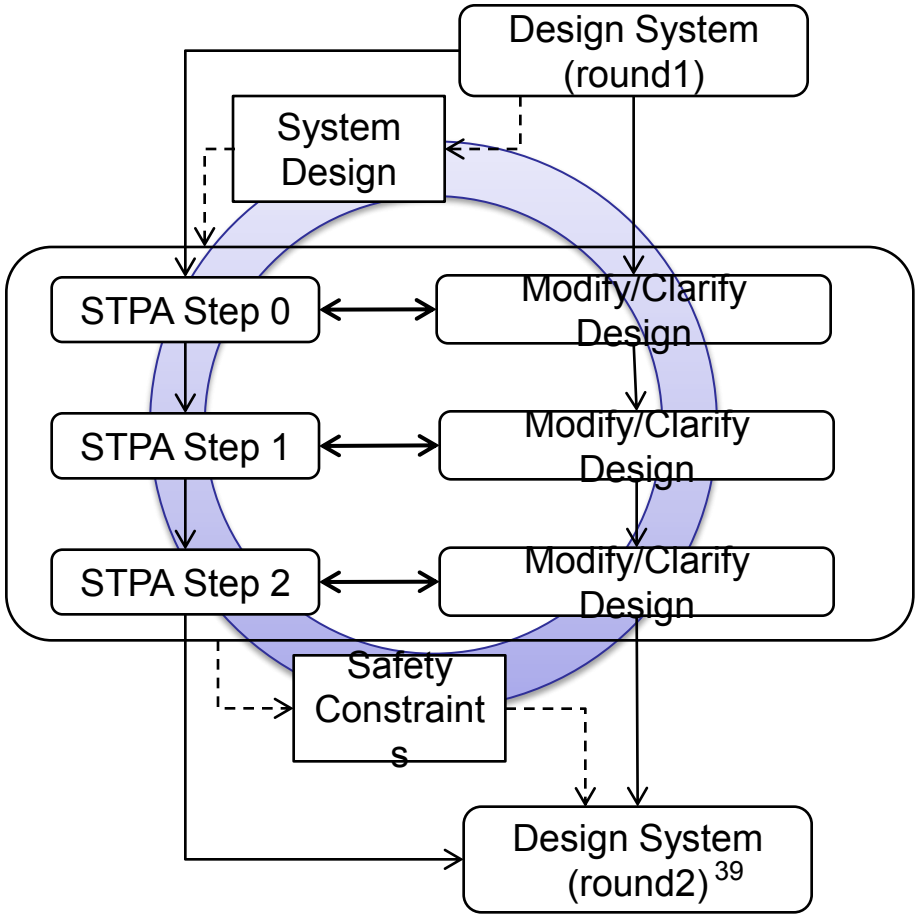


STPA for Crew Return Vehicle

~Summary~

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

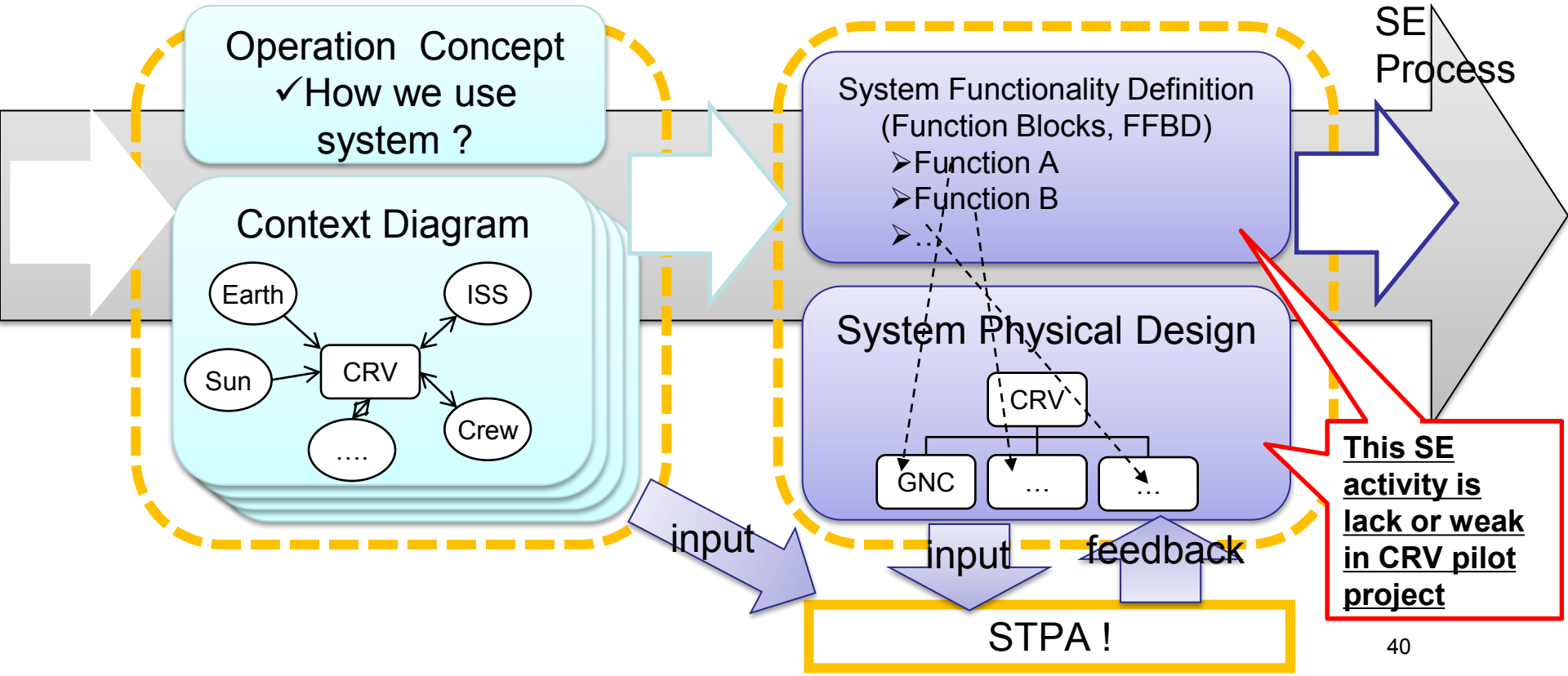




STPA for Crew Return Vehicle

~Problem to be solved~

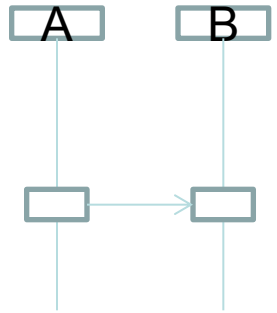
- What is the best precondition to start STPA?
  - We started STPA based on operation scenario of CRV. We could clarify the specification of CRV system during STPA. However it needed more work load to analysis.



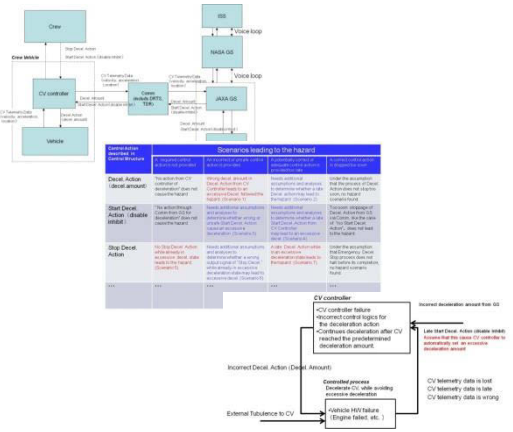
STPA for Crew Return Vehicle

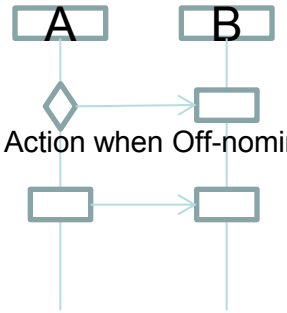
~Problem to be solved~

- When we consider a hazard scenario, it is necessary to analyze off-nominal scenario. Does Off-nominal scenario need to be defined to start STPA?
  - In early system concept design phase, it tend to be not enough considered the behaviors while off-nominal. On the other hand, STPA is more effective by including control actions while off-nominal.
  - We think we can consider the system behaviors while off-nominal by safety guided design. So we can analyze off-nominal scenarios by applying STPA to nominal scenarios.
  - In the case of CRV, off-nominal scenarios are considered based on experience of project team member. If we have approach to apply STPA to nominal scenarios, we could considered off-nominal scenarios systematically.



Nominal scenario





Off-nominal scenario

STPA for Crew Return Vehicle

~STPA step 1~

Discussion point (General)

1. Analysis Scope of CA

We now analyze including all backup CAs, for example, The CA "ME switchover to redundancy" has the following three ways:

(1) Automatic CA by the CV controller
(2) Manual CA by the crew if (1) is unavailable
(3) Manual CA by the ground if (2) is unavailable

Question: When a backup CA is available, might we analyze hazard scenarios enough only UCA of the backup CA?

				Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopping Too Soon /Applying Too Long Causes Hazard
1	**Main Engine switchover to redundancy**	CV Controller	Vehicle	[UCA1-1] Not Providing ME switchover by CV Controller results - Impossible to de-orbit as planned - Possible to return (Because there is a backup CA by Crew)	[UCA1-2a] Providing incorrect ME switchover results - Impossible to de-orbit as planned - Possible to return (Because there is a backup CA by Crew) [UCA1-2b] Providing unintentional ME switchover while maneuvering Normally results - Impossible to de-orbit as planned - Impossible to return as planned (Because return orbit is off the nominal)	[UCA1-3a] Providing ME switchover too early results no hazard. [UCA1-3b] Providing ME switchover too late results - Impossible to de-orbit as planned - Impossible to return as planned (Because return orbit is off the nominal)	[UCA1-4] NA (Single command)
2	**Main Engine switchover to redundancy**	Crew	CV Controller	[UCA1-1] Not Providing ME switchover by Crew results - Impossible to de-orbit as planned - Possible to return (Because there is a buck up CA by JAXA GS)	…	…	…
3	**Main Engine switchover to redundancy**	JAXA GS	CV Controller	[UCA1-1] Not Providing ME switchover by JAXA GS results - Impossible to de-orbit as planned - Possible to return (Because there is a buck up CA (RCS maneuvering, etc.))			

2. Guide word application policy

•Providing Causes Hazard:
Erroneous CAs which result in an unsafe situation
(1) Erroneous instructions (invalid, opposite, excessively large, excessively small, etc.)
(2) Erroneous instruction conditions (system status) excluding the temporal conditions

•Wrong Timing/Order Causes Hazard:
Erroneous CA sequences which result in an unsafe situation (the temporal conditions)

16.63J / ESD.03J System Safety
Fall 2012