Applying Human Mental Model to STAMP/STPA

3rd MIT STAMP/STPA Workshop

March 26, 2014

伸行　星野
Nobuyuki Hoshino (hoshino.nobuyuki@jamss.co.jp)

Go to Stars Safety !

Software Group
Safety and Product Assurance Department
Japan Manned Space Systems Corporation (JAMSS)

Contents

- Overview
- Background
- Human Mental Model
- Human Error Patterns
- Results
- Summary and Future

Overview

■JAXA, MIT, and JAMSS researched in 2012-13.

➢ **Issue :**

- Automatic controllers always perform control action as specification documents. So easy to identify hazard causal factors related to process model inconsistency by referring the specifications.

- However, human controllers do NOT always perform as operation manuals. So hard to indentify hazard causal factors by only referring the manuals.

➢**Goal :**

- Study feasibility of using Human Mental Model in STAMP/STPA.

- Identify hazard causal factor related to process model inconsistencies, particularly when human is a controller in the control loop diagram.

- Evaluate effectiveness of this model.

➢ **Approach :**

-Identify potential hazard causes in human controller by analyzing patterns of mistakes caused by cognitive behavior errors.

➢ **Result :**

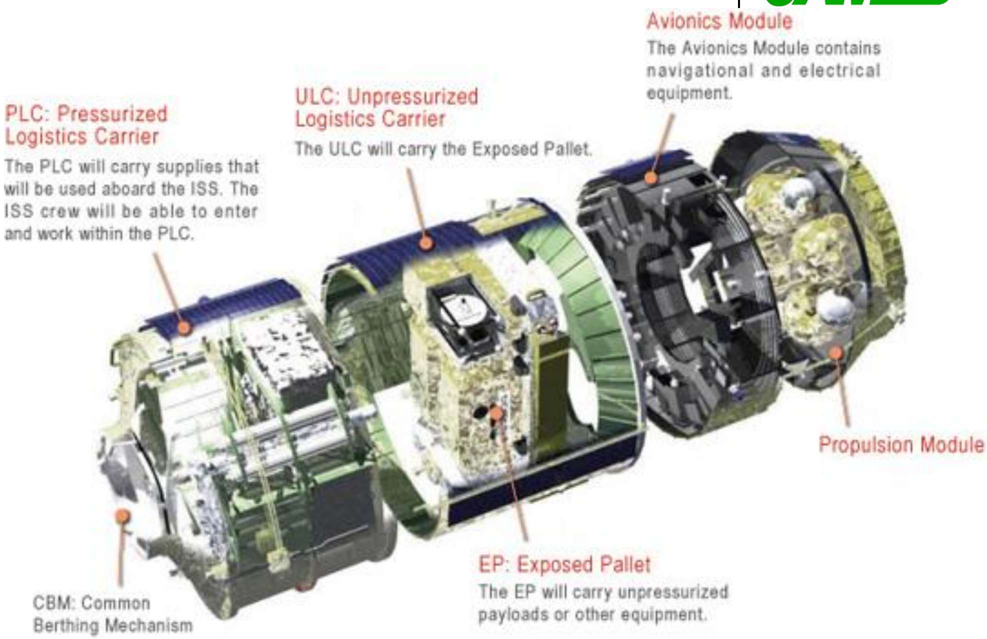
-Technique was applied to the analysis of HTV(Japanese Transfer Vehicle to ISS).

-Yielded more hazard causes and safety constraints.

-Using guide words of error patterns enabled to analyze systematically.

Background

- ■Applied STAMP/STPA to HTV in 2011.
  - ➢ **Target :**
    - - HTV(H-2 Transfer Vehicle).
    - - While berthing with ISS(International Space Station).
  - ➢ **Hazard :**
    - - Collision to ISS.



Avionics Module
The Avionics Module contains navigational and electrical equipment.

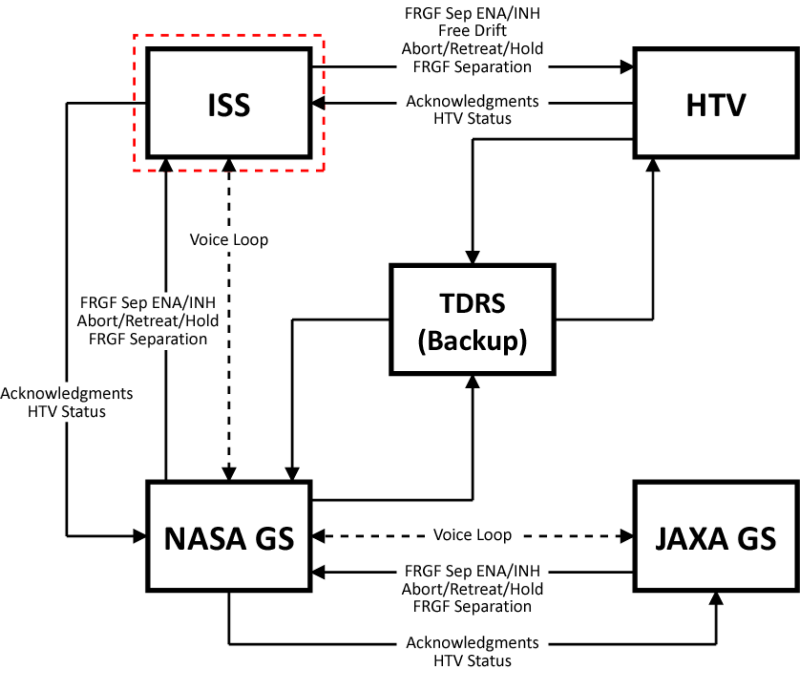
PLC: Pressurized Logistics Carrier
The PLC will carry supplies that will be used aboard the ISS. The ISS crew will be able to enter and work within the PLC.

ULC: Unpressurized Logistics Carrier
The ULC will carry the Exposed Pallet.

Propulsion Module

EP: Exposed Pallet
The EP will carry unpressurized payloads or other equipment.

CBM: Common Berthing Mechanism



ISS

HTV

TDRS (Backup)

NASA GS

JAXA GS

FRGF Sep ENA/INH
Free Drift
Abort/Retreat/Hold
FRGF Separation

Acknowledgments
HTV Status

Voice Loop

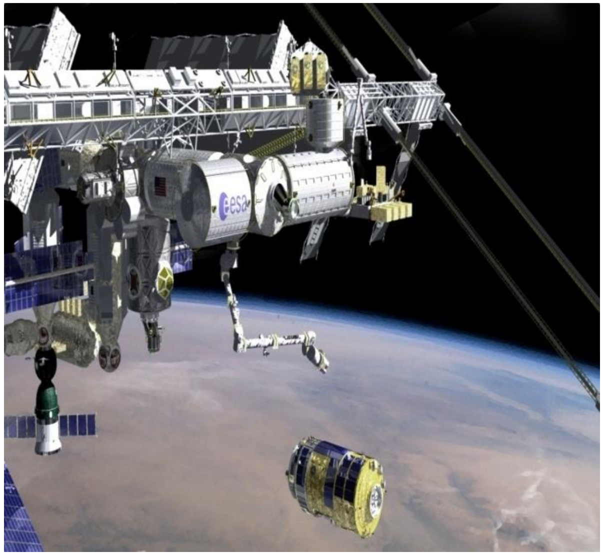
FRGF Sep ENA/INH
Abort/Retreat/Hold
FRGF Separation

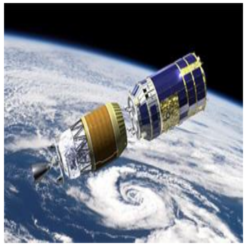
Acknowledgments
HTV Status

Voice Loop

FRGF Sep ENA/INH
Abort/Retreat/Hold
FRGF Separation

Acknowledgments
HTV Status





Background

■Result of Applying STAMP/STPA to HTV in 2011.

- **Unsafe Control Actions :**

  - Activation Command is NOT provided when HTV is drifting out from capture box.

  - …

- **Causal Factors :**

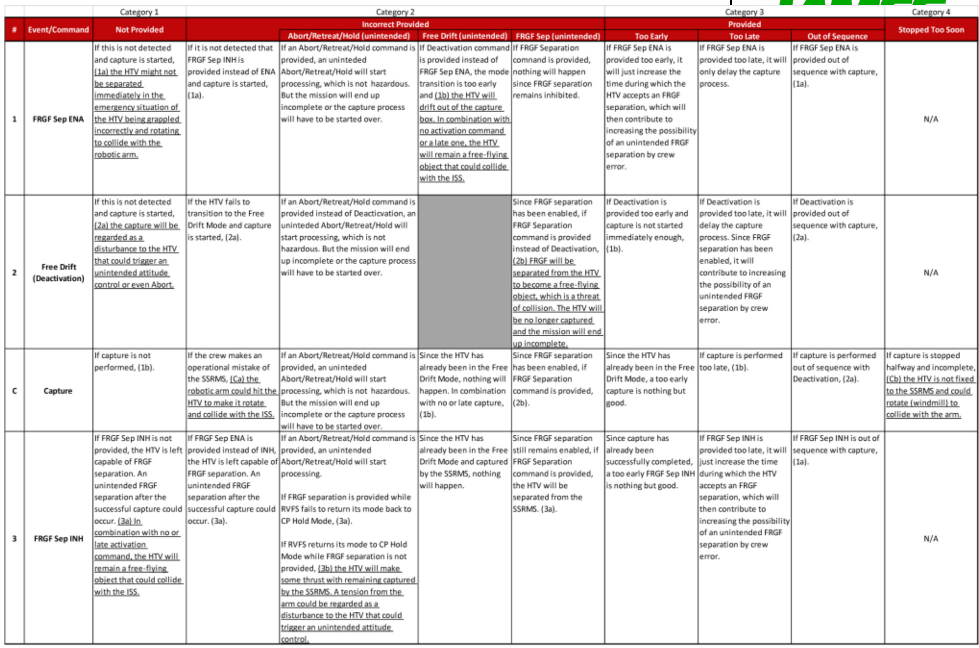
  - Crew process model inconsistent.

    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*.

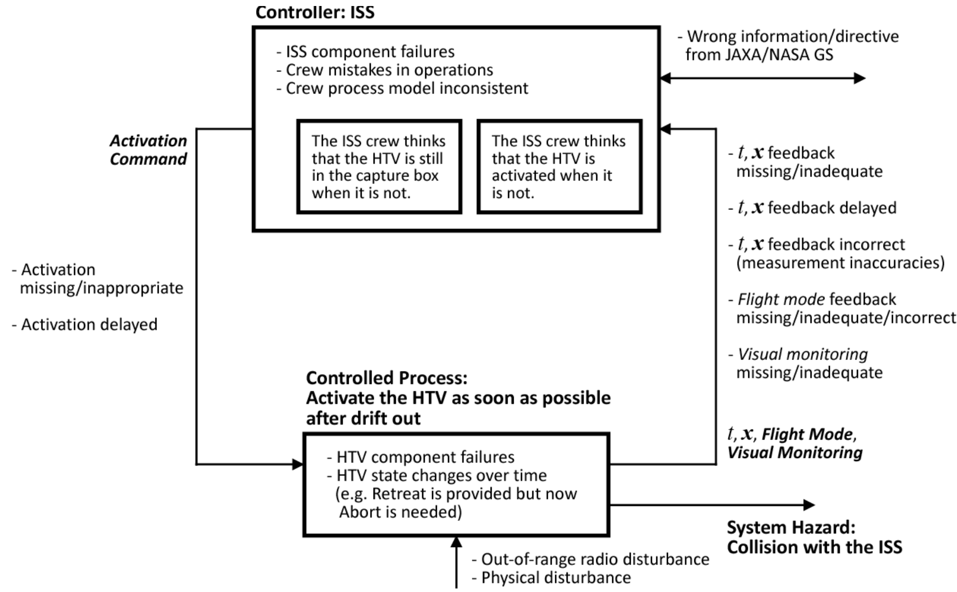
  - …

Other factors of crew process model inconsistency?

How to identify more detailed factors systematically?



		Category 1	Category 2				Category 3			Category 4
#	Event/Command	Not Provided	Incorrect 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 FRGF Sep INH is provided instead of ENA and capture is started, (1a).	If an Abort/Retreat/Hold command is provided, an uninteded 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.	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 comnand is provided, nothing will happen since FRGF separation remains inhibited.	If FRGF Sep ENA is provided too early, 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 ENA is provided too late, it will only delay the capture process.	If FRGF Sep ENA is provided out of sequence with capture, (1a).	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 Deacticvation, an uninteded 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.	If Deactivation is provided too early and capture is not started immediately enough, (1b).	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 uninteded 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 FRGF separation has been enabled, if FRGF Separation command is provided, (2b).	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 is provided while RVFS fails to return its mode back to CP Hold Mode, (3a). If RVFS returns its mode to CP Hold Mode while FRGF separation is not provided, (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 could trigger an unintended attitude control.	Since the HTV has already been in the Free Drift Mode and captured by the SSRMS, nothing will happen.	Since FRGF separation still remains enabled, if FRGF Separation command is provided, the HTV will be separated from the SSRMS. (3a).	Since capture has already been successfully completed, a 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



Controller: ISS

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

The ISS crew thinks that the HTV is still in the capture box when it is not.

The ISS crew thinks that the HTV is activated when it is not.

- Wrong information/directive from JAXA/NASA GS

Activation Command

- Activation missing/inappropriate
- Activation delayed

- $t, \boldsymbol{x}$ feedback missing/inadequate
- $t, \boldsymbol{x}$ feedback delayed
- $t, \boldsymbol{x}$ feedback incorrect (measurement inaccuracies)
- *Flight mode* feedback missing/inadequate/incorrect
- *Visual monitoring* missing/inadequate

$t, \boldsymbol{x}$, Flight Mode, Visual Monitoring

Controlled Process: Activate the HTV as soon as possible after drift out

- HTV component failures
- HTV state changes over time (e.g. Retreat is provided but now Abort is needed)

System Hazard: Collision with the ISS

- Out-of-range radio disturbance
- Physical disturbance

Human Mental Model

- **General process of human cognitive behavior**

  (1) *Detection* (recognize)
  (2) *Identification* (classify)
  (3) *Decision* (judge)
  (4) *Action* (act)

- **Rasmussen Model of Human Error**

  Dr. Nancy introduced us Rasmussen Model.
  Analyze by classifying human error patterns into 3 layers .

  (I) Skill-based behavior

  – After "*Detection*", automatically executes "*Action*"
  – Very accustomed task

  (II) Rule-based behavior

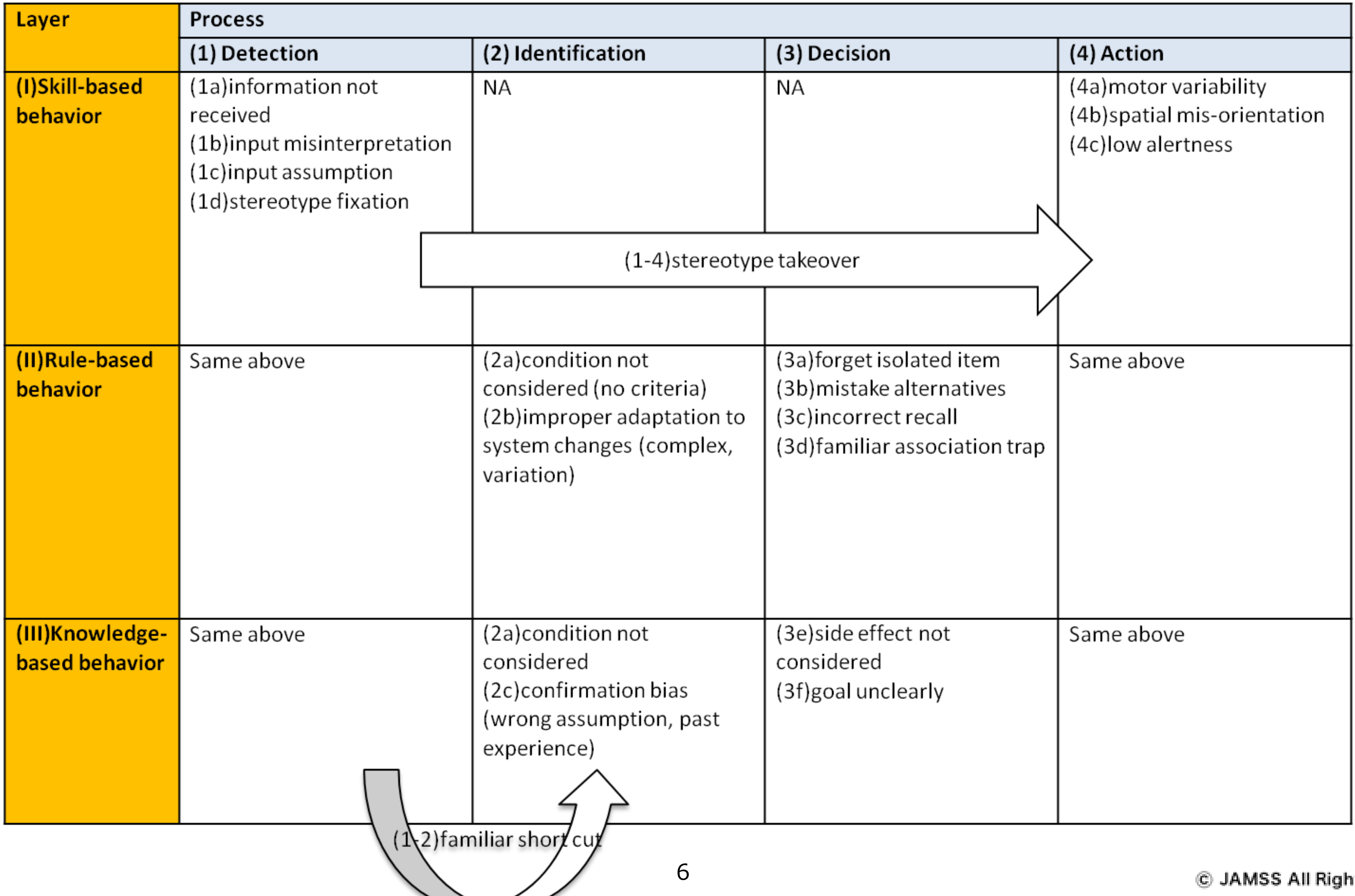
  – After "*Detection*" and "*Identification*", "*Decision*" and "*Action*" are executed as specified by the manuals.
  – Task not very familiar

  (III) Knowledge-based behavior

  – After "*Detection*" and "*Identification*", "*Decision*" and "*Action*" are executed based on knowledge and experience.
  – Familiar task, or task not defined by rule.

Human Error Patterns

- JAXA/JAMSS proposed a new mental model based on Ramussen Model.
- Constructed a matrix of Human Error Patterns by taking into consideration Layer and Process.



Layer	Process			
	(1) Detection	(2) Identification	(3) Decision	(4) Action
(I)Skill-based behavior	(1a)information not received (1b)input misinterpretation (1c)input assumption (1d)stereotype fixation	NA	NA	(4a)motor variability (4b)spatial mis-orientation (4c)low alertness
(II)Rule-based behavior	Same above	(2a)condition not considered (no criteria) (2b)improper adaptation to system changes (complex, variation)	(3a)forget isolated item (3b)mistake alternatives (3c)incorrect recall (3d)familiar association trap	Same above
(III)Knowledge-based behavior	Same above	(2a)condition not considered (2c)confirmation bias (wrong assumption, past experience)	(3e)side effect not considered (3f)goal unclearly	Same above

Results

- Using this Human Mental Model, re-analyzed the Causal Factor rerated to Crew process model inconsistency.

Normal process of cognitive behavior is,

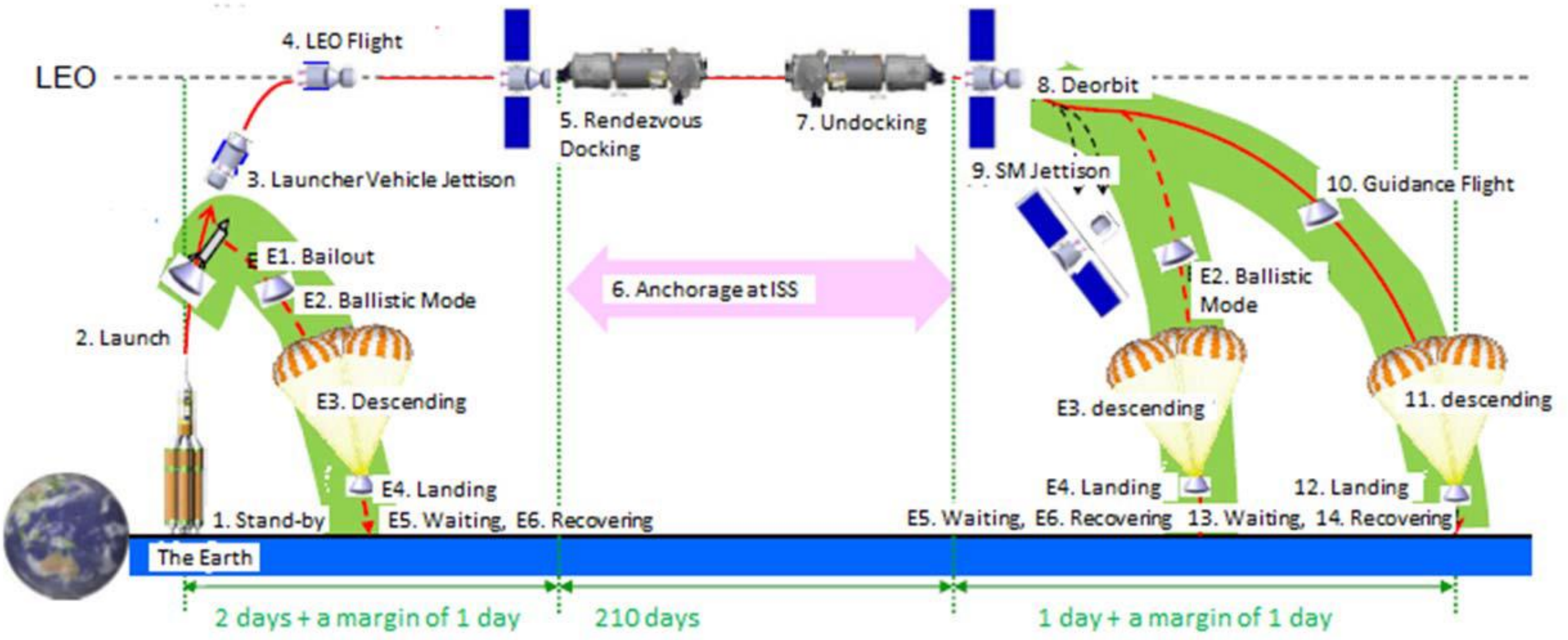
(1) Detection	Identify HTV Model information
(2) Identification	Recognize as “Uncontrolled state” when HTV is in Free Drift Mode
(3) Decision	Decide HTV’s activation
(4) Action	Execute activation command

ID	Causal Factor（abstract)	Safety Constraints（abstract)
1a	Will not look because the Ground Station is monitoring.	Prioritize crew’ decision and on-site visual confirmation (define in FR).
1b	Value is not valid (old value)	Do not mistake the meaning of input information (show unit, validity)
1c	No need to check frequently because the value does not change drastically.	Get attention when changes in input information occurs (notify by sound alarm when changes occur). Get attention when HTV mode changes (define in FR)
1d	Confirming through other telemetry data (relative distance, speed) will be sufficient.	Get attention to all necessary input information (Summarize all information in one screen)
2a	Not aware that the Free Drift Mode is in “Uncontrolled state”.	Assign meaning to input information (show threshold values, danger zones, etc) .
2b	Not aware that other conditions has arised (ISS in proximity, out of capture range, exceeds Free Drift Timer limit).	Get attention to all necessary information (define in FR)
2c	Assume that it will not turn into dangerous “uncontrolled state” immediately after changing to Free Drift Mode.	Convey dangerous situation　(generate alarms)

Summary and Future

-The Human Mental Model enabled to make in-depth analysis of the hazard causes and safety constraints in STPA Causal Factor Analysis.

- In future work, apply to the other HTV cases or other projects (Crew Return Vehicle, etc.) and Modify the model itself and how to use the model.


LEO
4. LEO Flight
3. Launcher Vehicle Jettison
2. Launch
1. Stand-by
E1. Bailout
E2. Ballistic Mode
E3. Descending
E4. Landing
E5. Waiting, E6. Recovering
5. Rendezvous Docking
6. Anchorage at ISS
7. Undocking
8. Deorbit
9. SM Jettison
10. Guidance Flight
E2. Ballistic Mode
E3. descending
11. descending
E4. Landing
12. Landing
E5. Waiting, E6. Recovering 13. Waiting, 14. Recovering
The Earth
2 days + a margin of 1 day
210 days
1 day + a margin of 1 day