KiboCUBE Academy

Lecture 5

Introduction of Safety Review Process

Japan Aerospace Exploration Agency
Human Spaceflight Technology Directorate

This lecture is NOT specifically about KiboCUBE and covers GENERAL engineering topics of space development and utilization for CubeSats.
The specific information and requirements for applying to KiboCUBE can be found at:
https://www.unoosa.org/oosa/en/ourwork/psa/hsti/kibocube.html

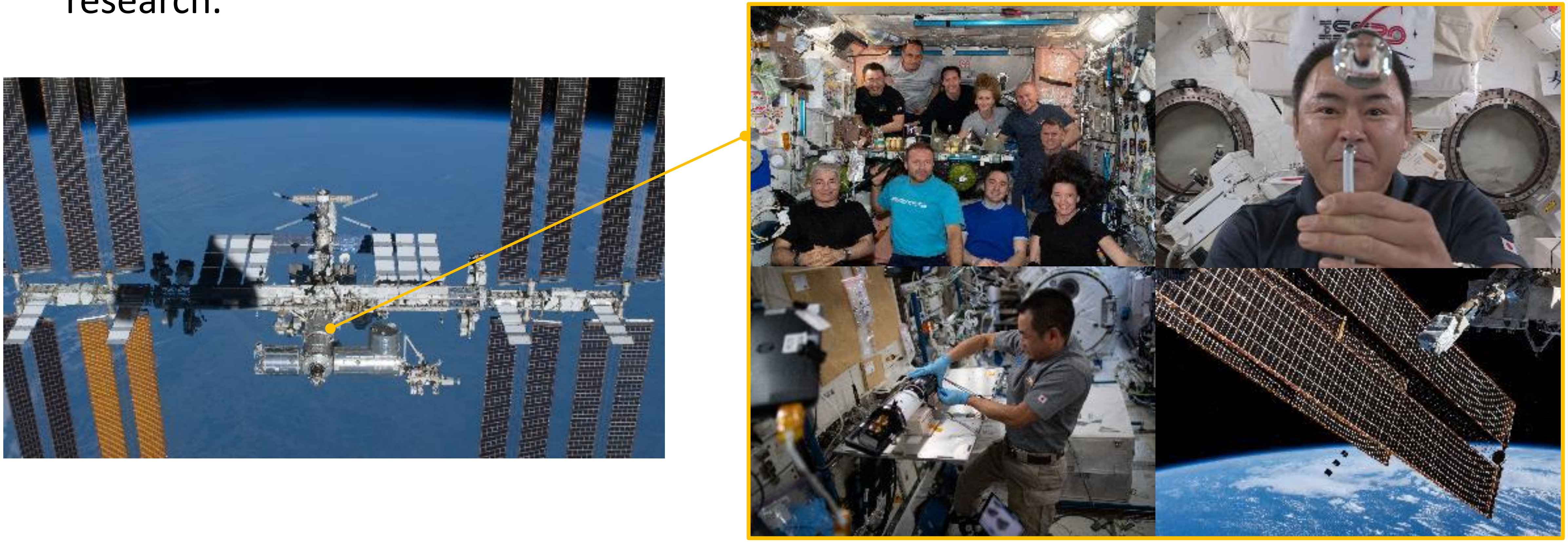
JAXA UNISEC JAPAN University Space Engineering Consortium

United Nations Office for Outer Space Affairs ★ Japan Aerospace Exploration Agency
Kibo CUBE

What is the safety review?

Environment for the International Space Station (ISS)

- The ISS is a unique scientific platform on orbit and has habitable elements.
- Several crews remain on the ISS at all times to conduct various experiments and research.

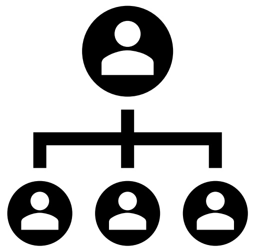


©JAXA/NASA

What is the safety review?

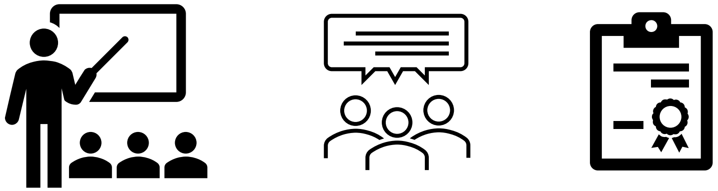
Significance of System Safety

◆ As a participating member of the ISS program, Japan is responsible for ensuring the safety of our mission under the overall responsibility of NASA.



◆ JAXA is responsible for guaranteeing the safety of the Japan Experiment Module (JEM, also called Kibo), the Visiting Vehicle, and other payloads.

◆ The JAXA Safety Review Panel, chaired by the Director of Human Space Safety and Mission Assurance Office under the Safety Review Board, will review human systems, including experimental payloads.



What is the safety review?

Basic policy for human safety design

Human space development is a history of struggles.

People build and operate things to avoid accidents, but accidents still happen.

<u>There is no such thing as "absolutely safe" .</u>

- **It must always be assumed that there is risk.**
- **It is important to <u>manage and minimize</u> it.**

What is the basic policy for human safety design?

Basic policy

◆ According to the System Safety Standard and the Safety Review Process Requirements, risks will be minimized as much as possible by managing hazards.

(1) Target of safety assurance

The ISS is a system where human beings live for extended periods of time, and safety must be ensured in order to prevent death or injury to the crew or loss of a spacecraft.

(2) How to ensure safety

All hazards will be identified and controlled, and the risks of remaining hazards will be evaluated.

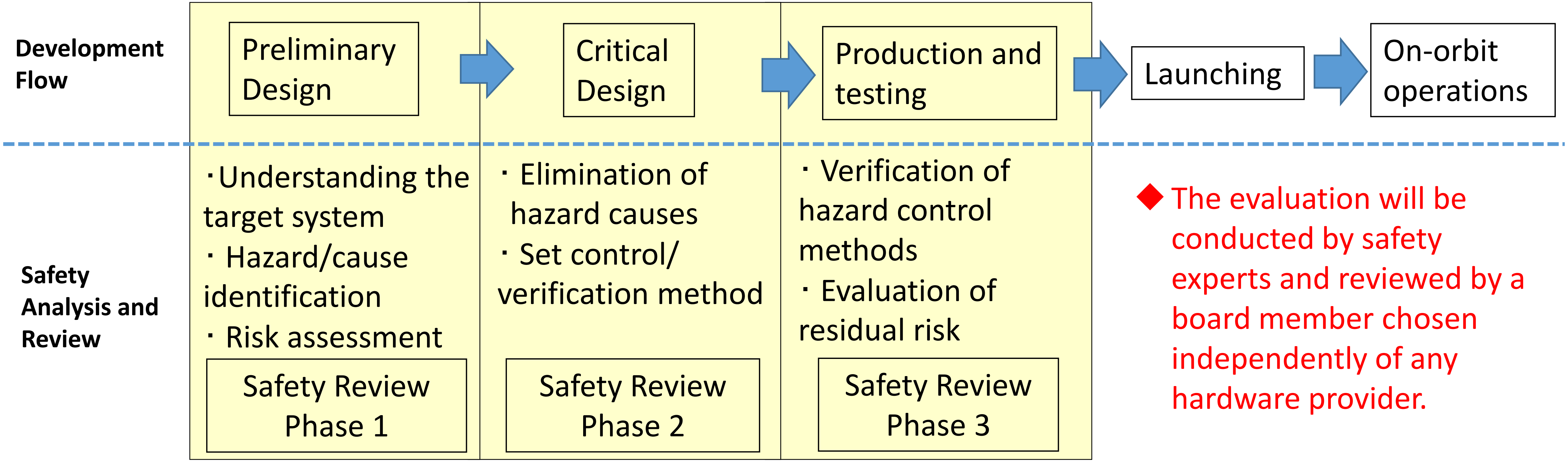
(3) Consideration of the special nature of human activities

Any of Kibo systems shall be designed to protect a crew and to conserve safety related device.

How to proceed with human safety design?

Relationship between satellite development and safety design

◆Hazards that may loss of the ISS and directly harm crews or indirectly harm crews by damaging safety-related systems should be identified early in the design process.

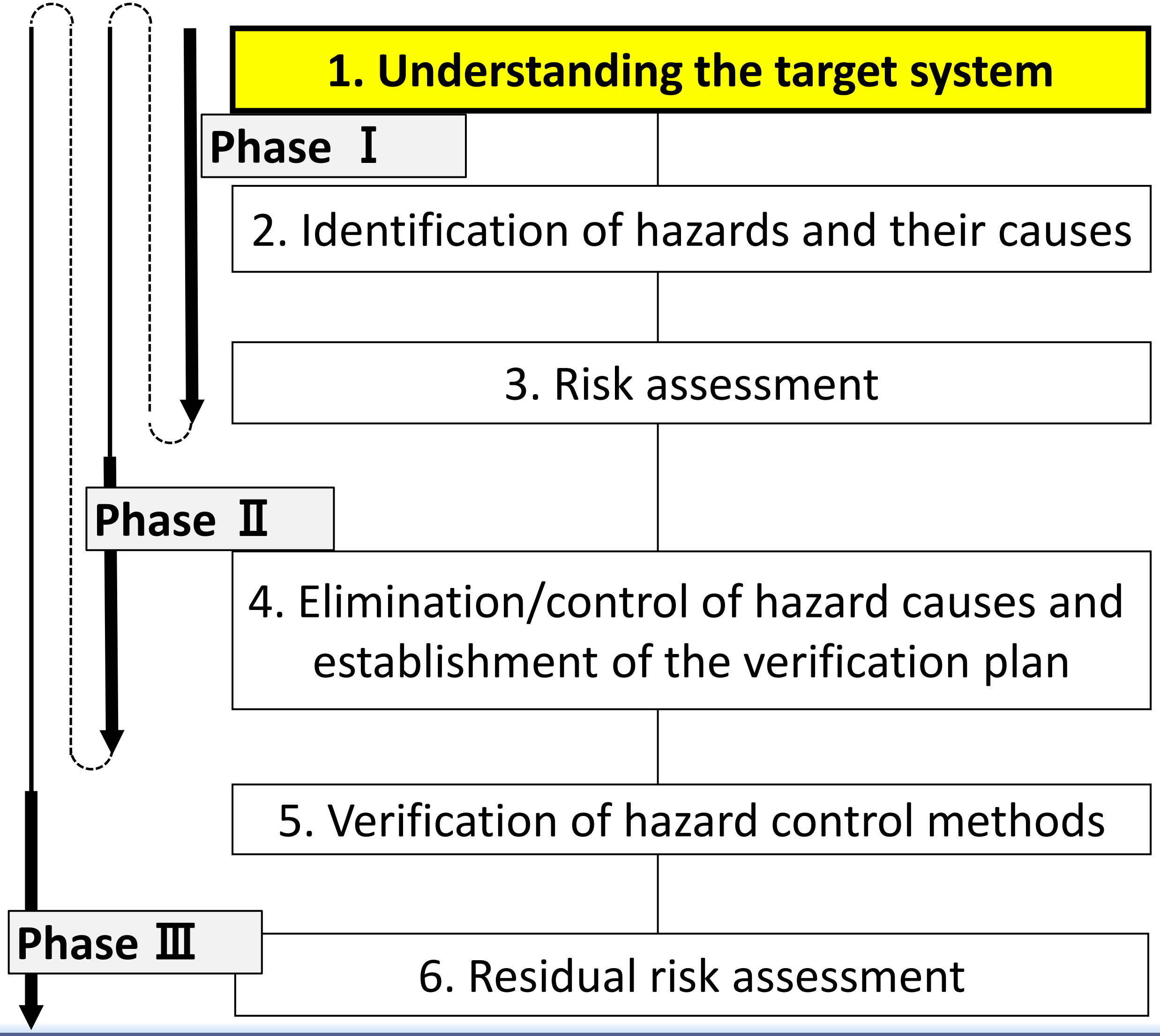


◆The evaluation will be conducted by safety experts and reviewed by a board member chosen independently of any hardware provider.

△Safety verification

Let's try the human safety design analysis for CubeSat!

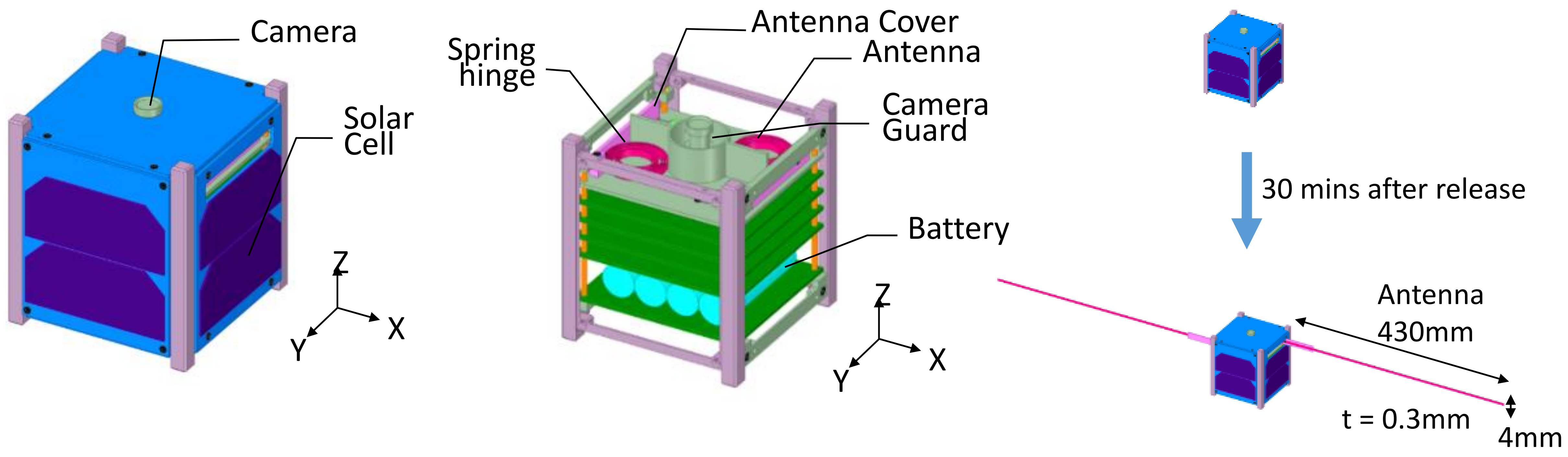
1. Understanding the target system



1. Understanding the target system (1/2)

Understanding the Cubesat

- ◆Become familiar with the external and internal structure of the satellite you have designed.
- ◆Understand the specifications of the components to be installed.
- ◆After the satellite is released, whether the satellite has a configuration change or not.



1. Understanding the target system (2/2)

Understanding overall processes for the satellite deployment

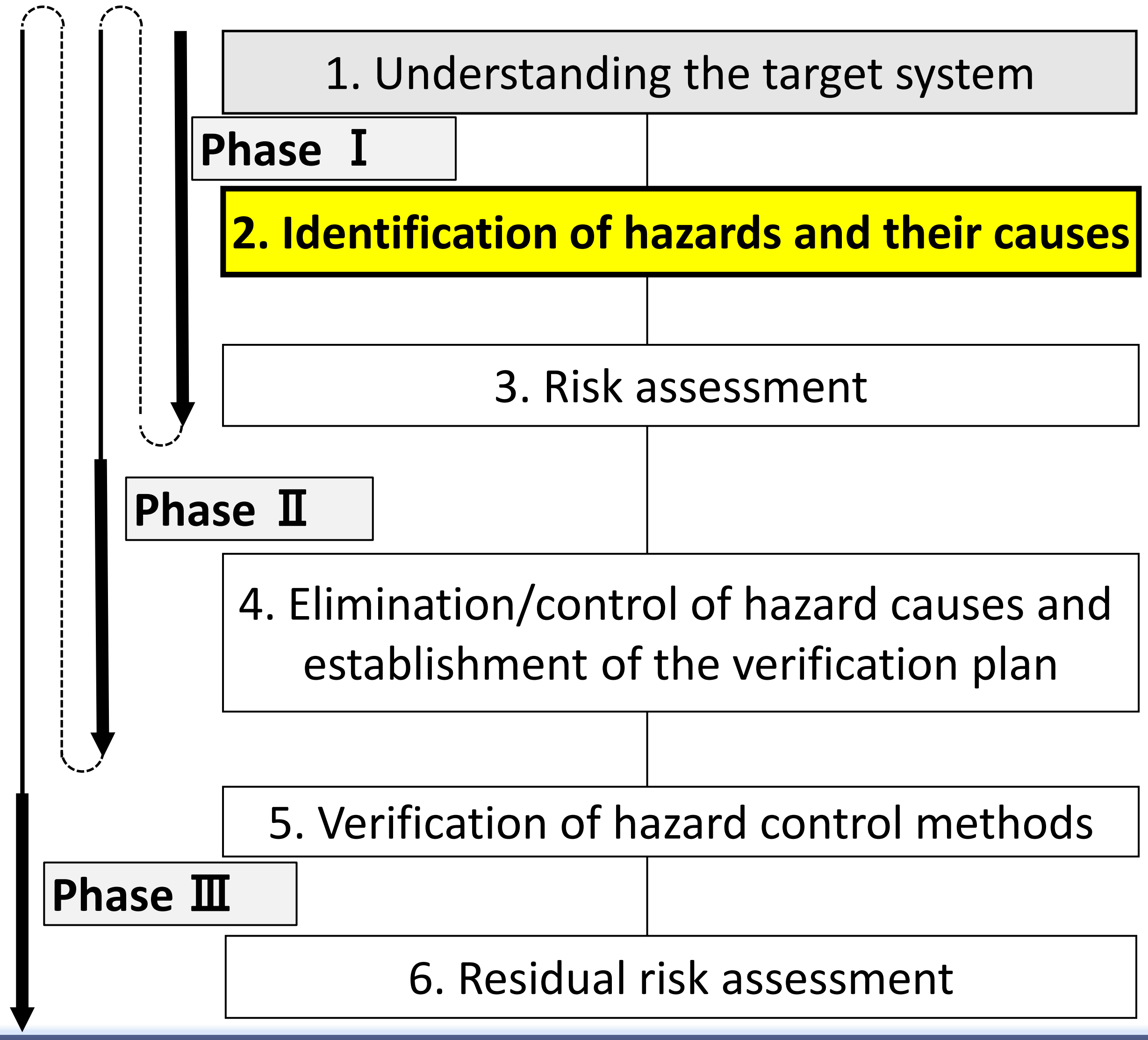
◆The CubeSat is launched to the ISS by a supply shipping vehicle, installed on the Multi-Purpose Experiment Platform (MPEP) in Kibo module, then moved into space by a robot arm and released.

(a) Launch → (b) Inter-Vehicular Activity → (c) Extra-Vehicular Activity → (d) Satellite deployment

→ After deployment, CubeSat begin antenna deployment, propulsion system operation, and so on.

Let's try the human safety design analysis for CubeSat!

2. Identification of hazards and their causes



2.Identification of hazards and their cause (1/5)

What is a “Hazard”?

◆A hazard is defined as "**a condition in which factors causing an accident are apparent or latent**".

◆Hazards can be classified into **two** categories according to their degree of damage.

I. **Catastrophic hazards**
   - A condition that could result in loss of the ISS or fatal injury to crew members.
     ex.) Fire, Depressurization, … etc.

II. **Critical hazards**
   - A condition that may result in damage to the ISS equipment or injury to crew members.

2.Identification of hazards and their cause (2/5)

Standard hazards and Unique hazards

◆There are 14 categories called as “Standard Hazard” to be evaluated.

◆If the hazard cannot be classified as a standard hazard, it should be classified as a unique hazard.

Standard Hazards

1. Flammable Material
2. Material Off-gassing
3. Dust, Toxic or Biological Hazardous Materia
4. Sharp Particles
5. Exposure to mechanical hazards and translation path obstructions
6. Exposure to Touch Temperature Exceedances
7. Exposure to Light Amplification by Stimulated Emission of Radiation and/or Incoherent Electromagnetic Radiation Emissions.
8. Exposure to Noise Limit Exceedances
9. Injury/Damage as a Result of Improperly Bonded and Grounded Equipment
10. Injury/Damage as a Result of Improper Power Distribution Circuitry and Circuit Protection Devices
11. Mating and Demating of Energized Connector
12. Non-Ionizing Radiation Interference
13. Injury/Damage as a result of Rotating Equipment Failure
14. Injury/Damage as a result of Sealed Container Failure

Typical Unique Hazards

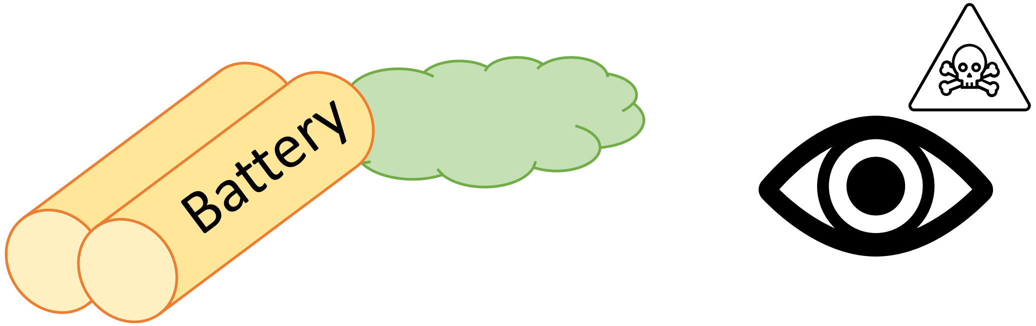
- Leakage of electrolyte or rupture of battery
- A collision of the deployed CubeSat with structure failure against the ISS structure
- A collision of the CubeSat with inadvertent deployable part against the ISS structure
- Others…

2.Identification of hazards and their cause (3/5)

Leakage of electrolyte or rupture of battery

[Hazard]
Leakage of electrolyte or battery rupture can lead to contamination, corrosion, injury to ISS crew, or damage to other equipment on ISS.

[Causes]
1. Battery cell internal short
2. Cell/battery external short
3. Overcharging of battery
4. Over-discharging of battery
5. Thermal Extremes

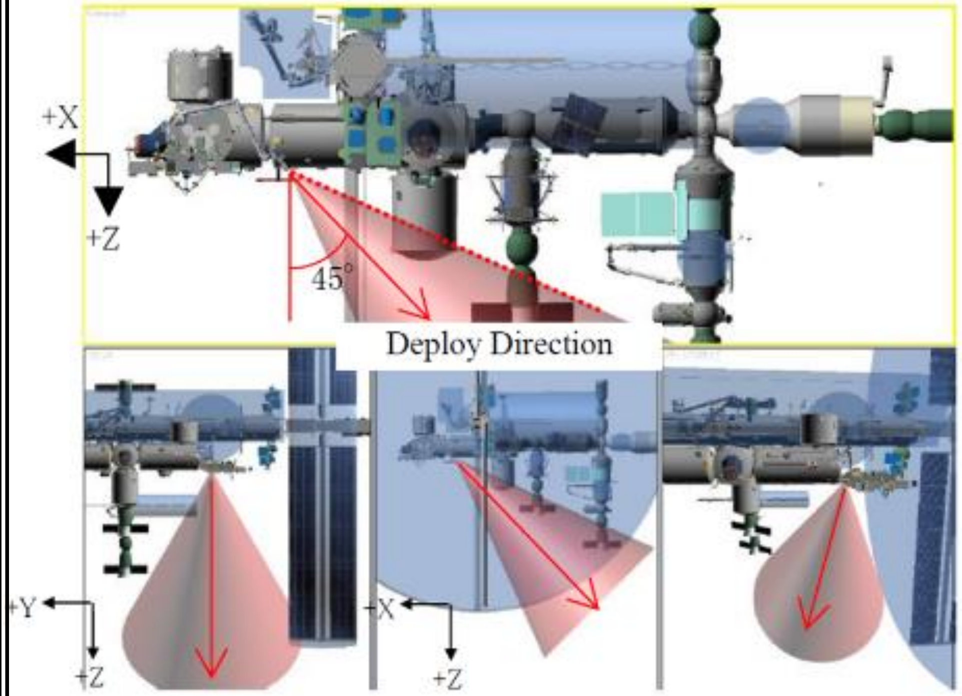


2.Identification of hazards and their cause (4/5)

A collision of the deployed CubeSat with structure failure against the ISS structure

[Hazard]
After a satellite is deployed, there is a risk of collision with the ISS because the deployment direction can be shifted by contact with the satellite and the J-SSOD Satellite Install Case.

[Causes]
1. Inadequate structural strength for launch, in-orbit load and depressurization.
2. Improper material selection and processing, including use of corrosion-sensitive materials.
3. Material fatigue or propagation of inherent cracks or internal flaws.
4. Use of sub-standard materials
5. Loosening of fasteners during launch and during orbit
6. Improper manufacturing and/or assembly



2.Identification of hazards and their cause (5/5)

A collision of the CubeSat with inadvertent deployable part against the ISS structure

[Hazard]

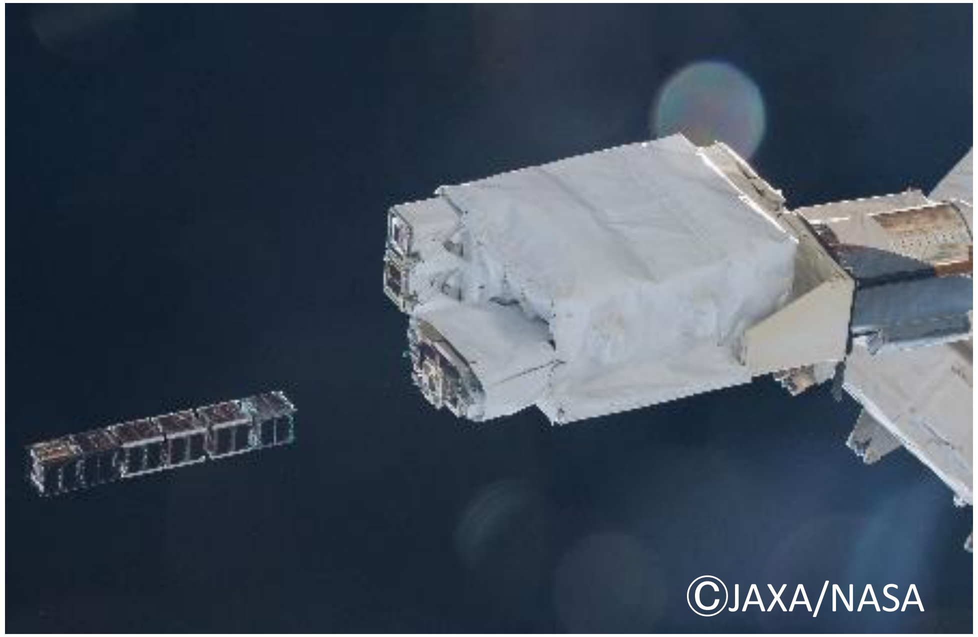
◆ Inadvertent deployment of antenna inside J-SSOD can cause collision with ISS structure.

◆ Inappropriate design and/or manufacturing of the satellite may lead to incorrect satellite deployment from J-SSOD.

[Cause]

Inadvertently deployment of the CubeSat antenna before satellite deployment

1. Sticking due to inadvertent deployment inside J-SSOD or striking adjacent satellites.
2. Inappropriate design or manufacture of the satellite.



Let's try the human safety design analysis for CubeSat!

3. Risk assessment

1. Understanding the target system

Phase Ⅰ

2. Identification of hazards and their causes

3. Risk assessment

Phase Ⅱ

4. Elimination/control of hazard causes and establishment of the verification plan

5. Verification of hazard control methods

Phase Ⅲ

6. Residual risk assessment

3.Risk assessment (1/2)

Classification of risks

◆ Risks are classified into 4 damage levels and the 5 likelihood of occurrence.

Level of damage	Terms	Potential loss
I	Catastrophic	Death of the ISS crew Loss of the ISS
II	Critical	Severe damage to ISS crew Severe damage to the ISS
III	Marginal	Minor damage to ISS crew Minor damage to ISS
IV	Negligible	Damage that does not affect the ISS crew Damage that does not affect the ISS

Likelihood of occurrence	Frequency
A	Frequent/ Likely to occur immediately
B	Probable/ Probably will occur in time
C	Occasional/ May occur in time
D	Remote/ Unlikely to occur
E	Improbable/ Improbable to occur

3.Risk assessment (2/2)

Risk assessment and elimination

◆ Assess risk by combining the level of damage and the likelihood of occurrence.

Reduce the likelihood of occurrence →

Prevention of damage ↓

		Likelihood of occurrence				
		A frequently	B occasionally	C infrequently	D only rarely	E nearly never
Level of damage	I Catastrophic	red	red	red	yellow	green
	II Critical	red	red	yellow	green	green
	III Marginal	red	yellow	green	green	green
	IV Negligible	green	green	green	green	green

Distinguished as unacceptable risk

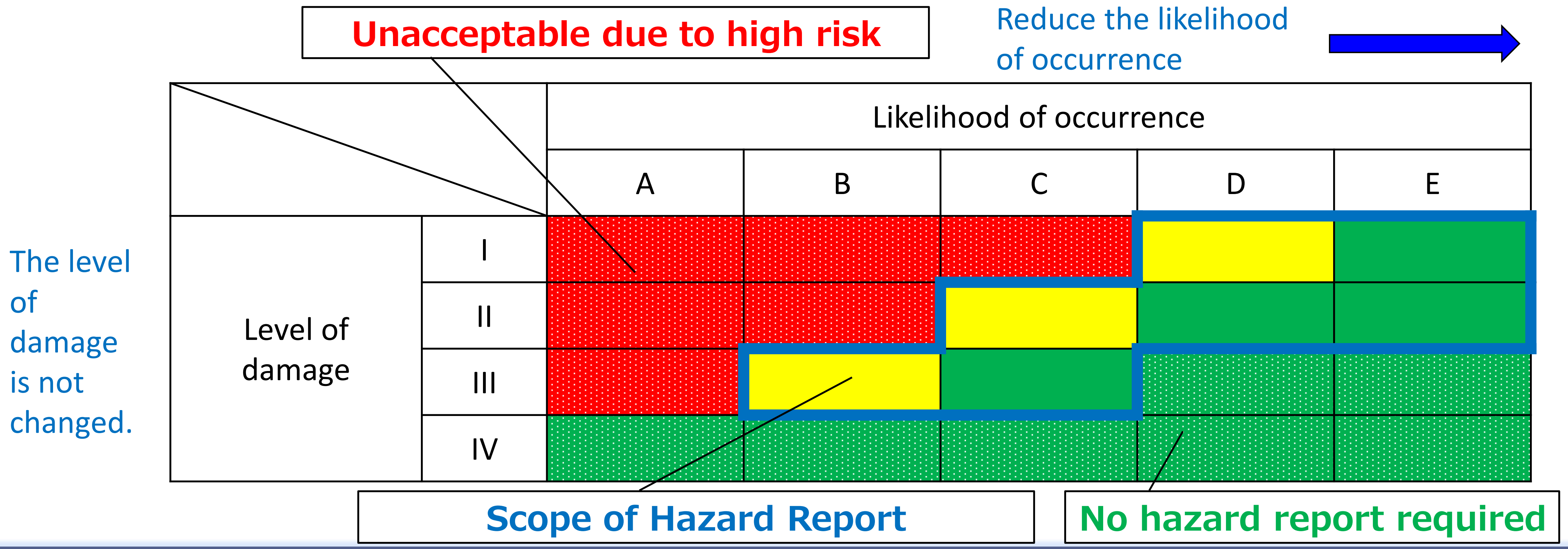
Requiring an acceptable/unacceptable decision

Acceptable risk

3.Risk assessment (3/3)

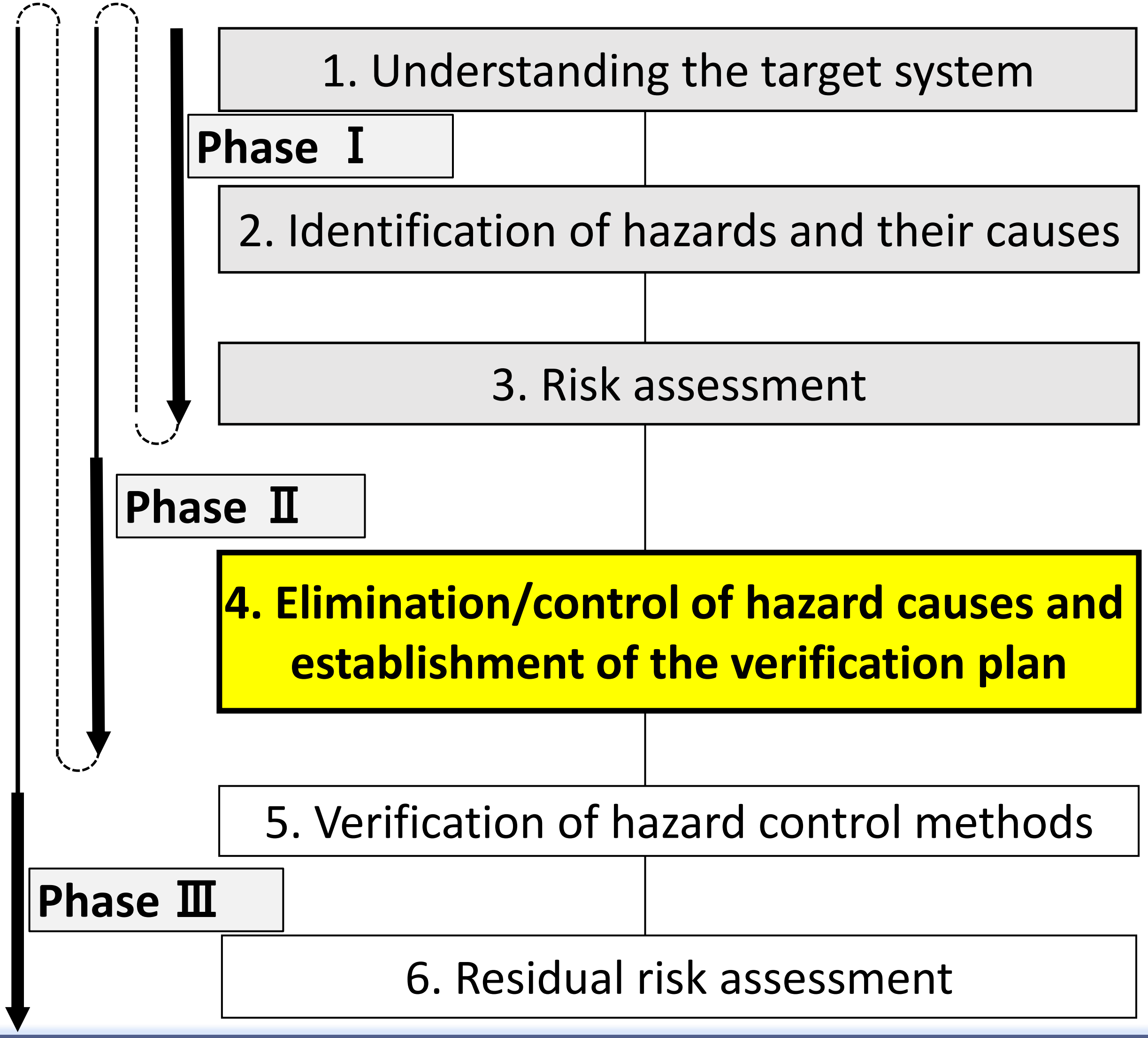
Hazard control

- Identify those hazards that could not be "eliminated" as "residual risks".
- "Hazard control" aims to reduce the likelihood of a hazard occurring.
- Hazard control methods should be verifiable, and "hazard reports" should be used to determine the acceptability of risks.



Let's try the human safety design analysis for CubeSat!

4. Elimination/control of hazard causes and establishment of the verification plan



Hazard control method (1/4)

1. Hazard cause removal
   The first priority response is to eliminate the root cause of the hazard by design.

2. Hazard control
   If a hazard cannot be eliminated, measures should be taken, such as
   by designing the most effective way to reduce potential human and material losses.

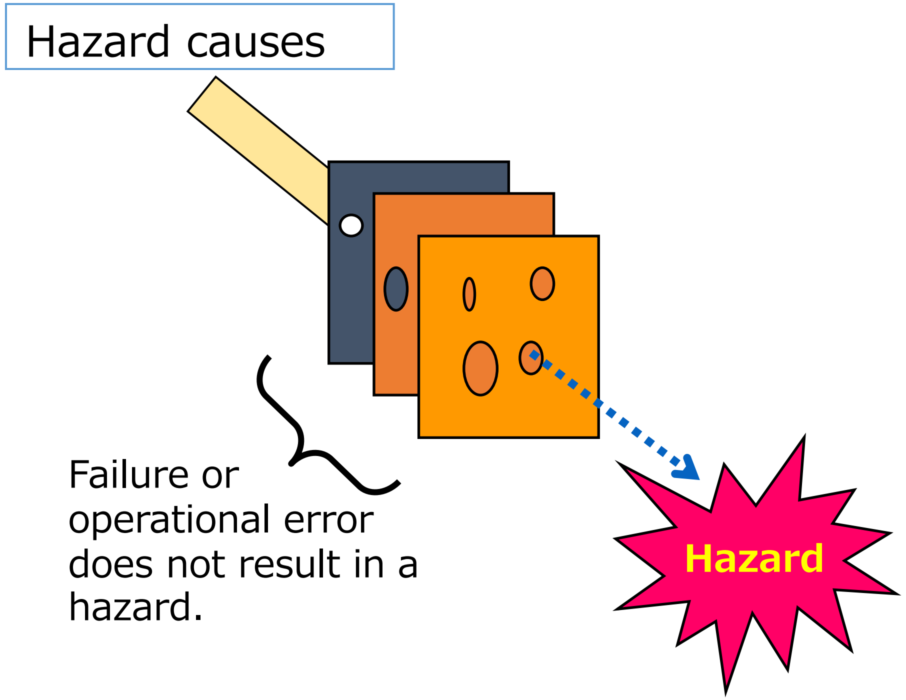
Reduce the likelihood and extent of damage to an acceptable level by controlling the hazard.

I. Fault-tolerant design
II. Design for minimum risk
III. Safety devices
IV. Alarm and emergency equipment
V. Operational procedures

Hazard control method (2/4)

I. Fault-tolerant design

- ☐Design methodology to provide independent hazard protection functions (Designed not to cause any safety problems in case of breakage)
- ☐Install an energy shut-off device (inhibit) if unintended operation is expected due to malfunction.



The allowable number of failures depends on the level of damage.

- **In the case of <u>catastrophic hazard</u>**
  - ➢ Measures must be taken to prevent accidents (loss of ISS, fatal personnel injury, etc.) in the event of two failures, two mishaps, or one failure and one mishap occurring simultaneously.
- **In the case of <u>critical hazard</u>**
  - ➢ Measures must be taken to ensure that a single failure or mishap does not result in an accident (damage to ISS equipment or injury to crew members).

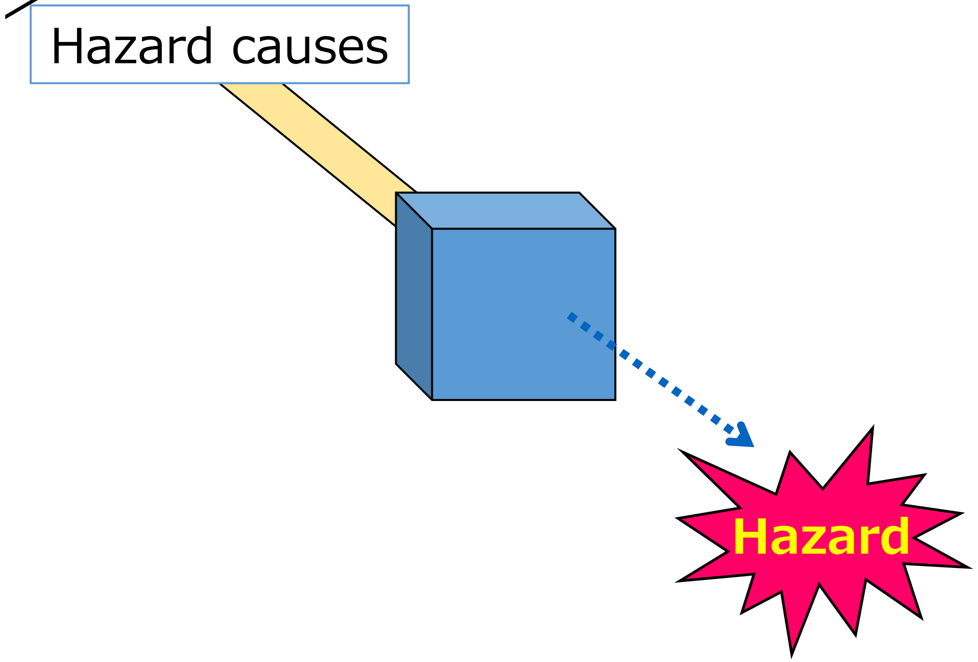
Hazard control method (3/4)

II. Design for Minimum Risk

- ☐ Design methodology for minimizing the risk of hazard occurrence by ensuring adequate design margins.
  Example: Pressure vessel with sufficient design margin (for pressure system failure), etc.

＜ Areas of application for Design for Minimum Risk ＞

- Structure
- Pressure vessel
- Pressure piping and fittings
- Pyrotechnics
- Safety-critical mechanisms (mechanisms)
- Material compatibility
- Flammability



Hazard control method (4/4)

III. Safety devices

- Measures to minimize the impact of damage in the event of an anomaly.
  Example: For pressure vessels, design to leak before breaking.

IV. Alarm and emergency equipment

- Correct and timely detection of hazardous conditions, notification of flight crew or ground crew, and preparation of appropriate emergency procedures after detection.
  Examples: Installation of fire detection systems, fire extinguishers, portable oxygen masks.

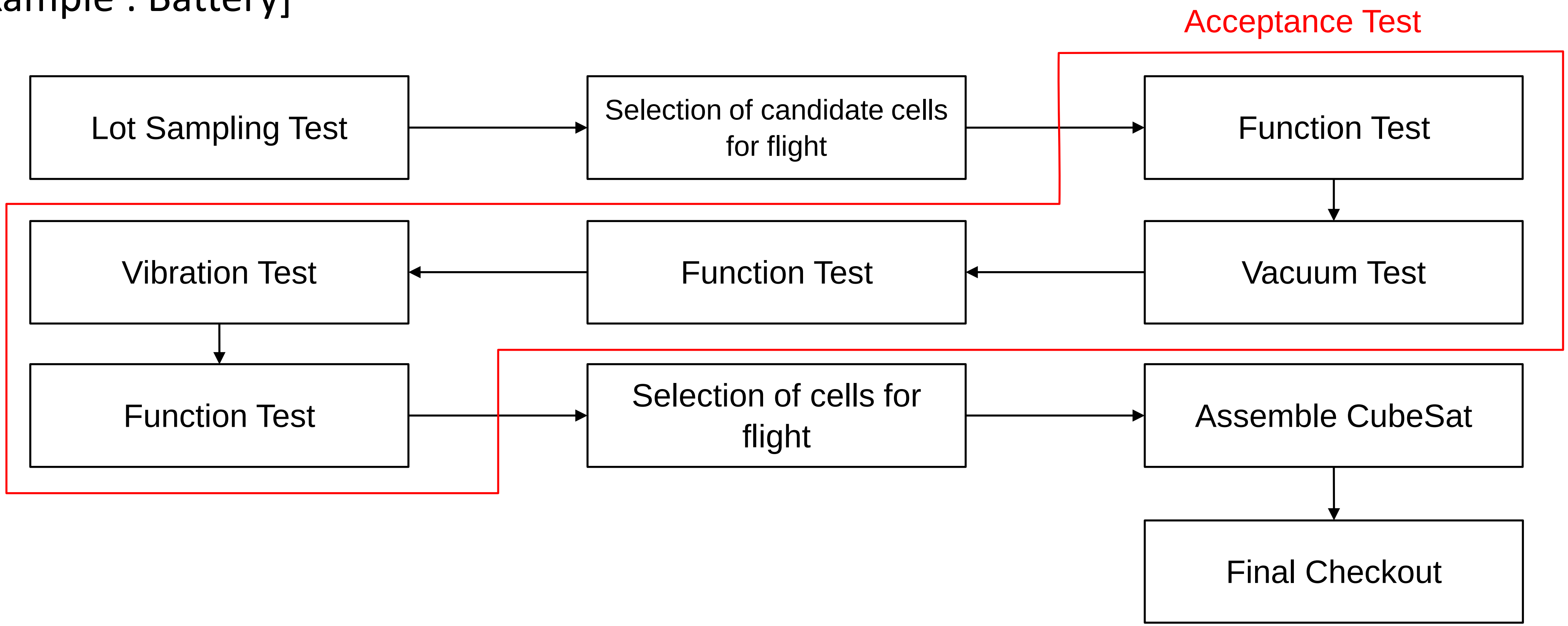
V. Operational procedures

- Avoid hazardous situations through operational procedures when they cannot be dealt with by design.
  Example: Turn off the satellite power switch before deployment to avoid electric shock.

Establishment of the verification plan

◆Establishment of the verification methods such as analysis and testing, when to implement, how to do it, and criteria.

[Example : Battery]



Let's try the human safety design for CubeSat!

5. Verification of hazard control methods

1. Understanding the target system

Phase Ⅰ

2. Identification of hazards and their causes

3. Risk assessment

Phase Ⅱ

4. Elimination/control of hazard causes and establishment of the verification plan

5. Verification of hazard control methods

Phase Ⅲ

6. Residual risk assessment

5.Verification of hazard control methods

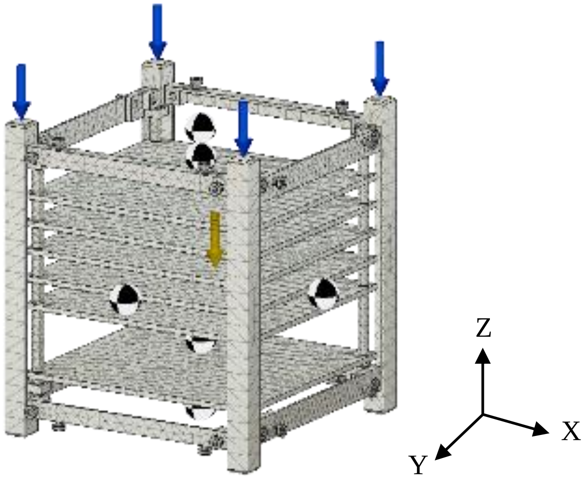
Verification method

◆ Validate the developed flight model according to your verification method and procedure approved by safety review.

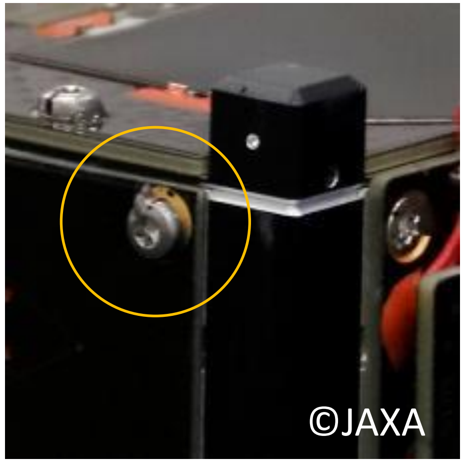
1. **Test**: Confirm that the product or operation meets the required specifications under typical environment and operation.
2. **Analysis**: Estimate by calculation, simulation, etc.
3. **Inspection**: Confirm for immediate determination by visual observation and measurement.
4. **Demonstrate**: Confirm that the design can be used in practical applications

1. Test

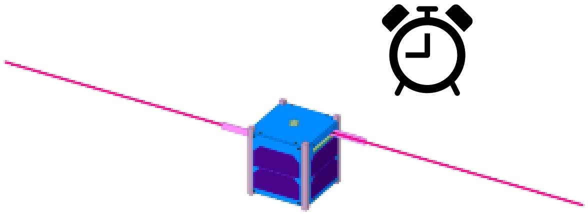
2. Analysis



3. Inspection



4. Demonstration

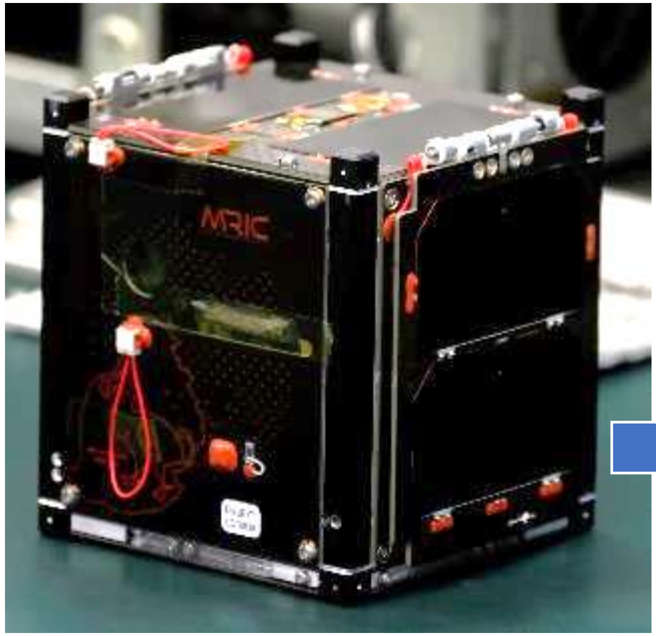


Antenna deployment test by using a timer

5.Verification of hazard control methods

Management by safety verification tracking log

- Verification is typically to be completed before the satellite is handed over to JAXA.
- Final verification is to be performed just before the satellite is integrated and managed in the Safety Verification Tracking Log (SVTL).



Let's try the human safety design for CubeSat!

6. Residual risk assessment

1. Understanding the target system

Phase Ⅰ

2. Identification of hazards and their causes

3. Risk assessment

Phase Ⅱ

4. Elimination/control of hazard causes and establishment of the verification plan

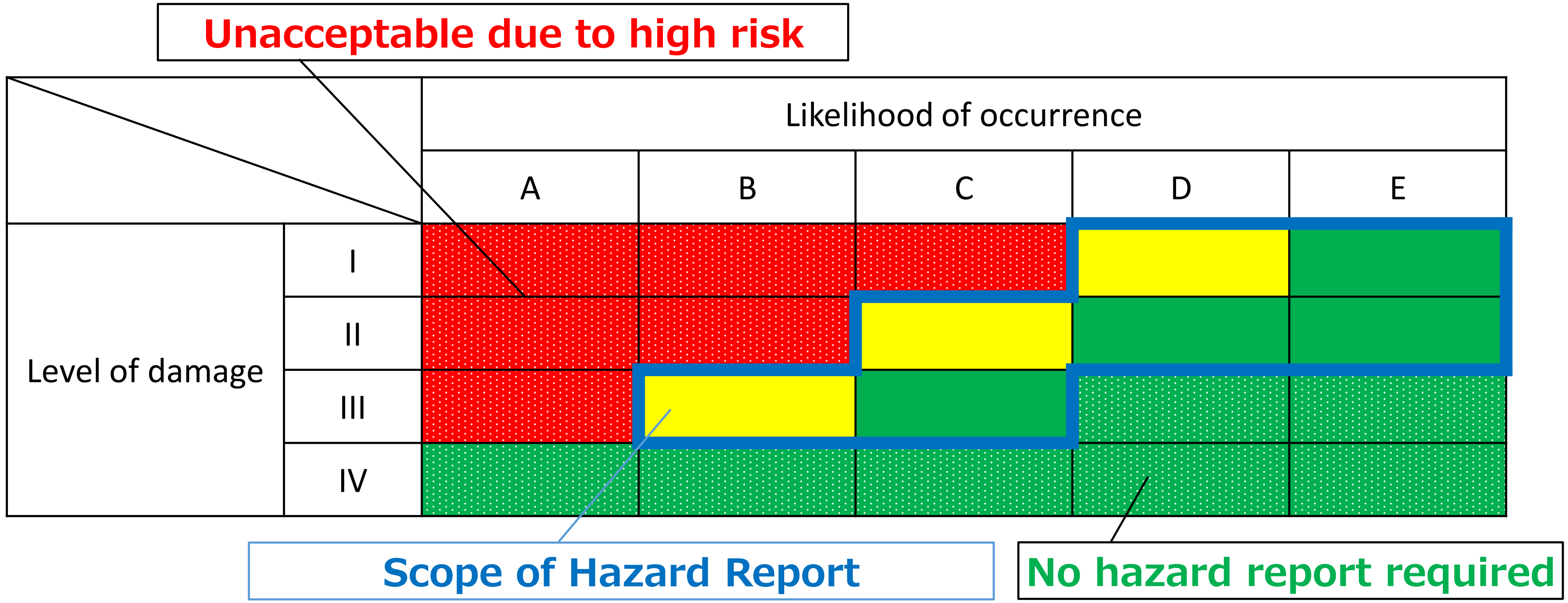
5. Verification of hazard control methods

Phase Ⅲ

6. Residual risk assessment

6.Residual risk assessment

◆Check again for any remaining risks to the developed CubeSat.
◆If they are all in the green area, you have completed the safety design.



Summary

- The hazard identifies loss of crew or space station functions as the most critical event, and safety design, assessment and reviews are conducted by investigating the causes of the event.

- According to the System Safety Standard and the Safety Review Process Requirements, risks will be minimized by managing hazards. The satellite provider shall be conducted safety design analysis.

Is your satellite ready to Launch?

[Disclaimer]
The views and opinions expressed in this presentation are those of the authors and do not necessarily reflect those of the United Nations.