Architecture Framework for Spacecraft Computer Control Safety System

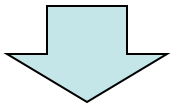
Seiko Shirasaka
shirasaka@sdm.keio.ac.jp
KEIO University

Contents

- Backgound
- Experiece
- Design Process from Experience
- Architecture Framework Development
  - Development Process
  - Process Identification
  - View/Viewpoint Identification
- Architecture Views Example

Background

- Crew are continuously stay on board (The space station).
- Manned/unmanned spacecraft developments are increasing in the world.
  - Upgrade of existing spacecrafts
  - New visiting vehicles (Dragon:Space-X, Cygnus:Orbital Science)
  - Commercial manned vehicles
- However, there is no architecture framework to support the design of spacecraft computer control safety system.



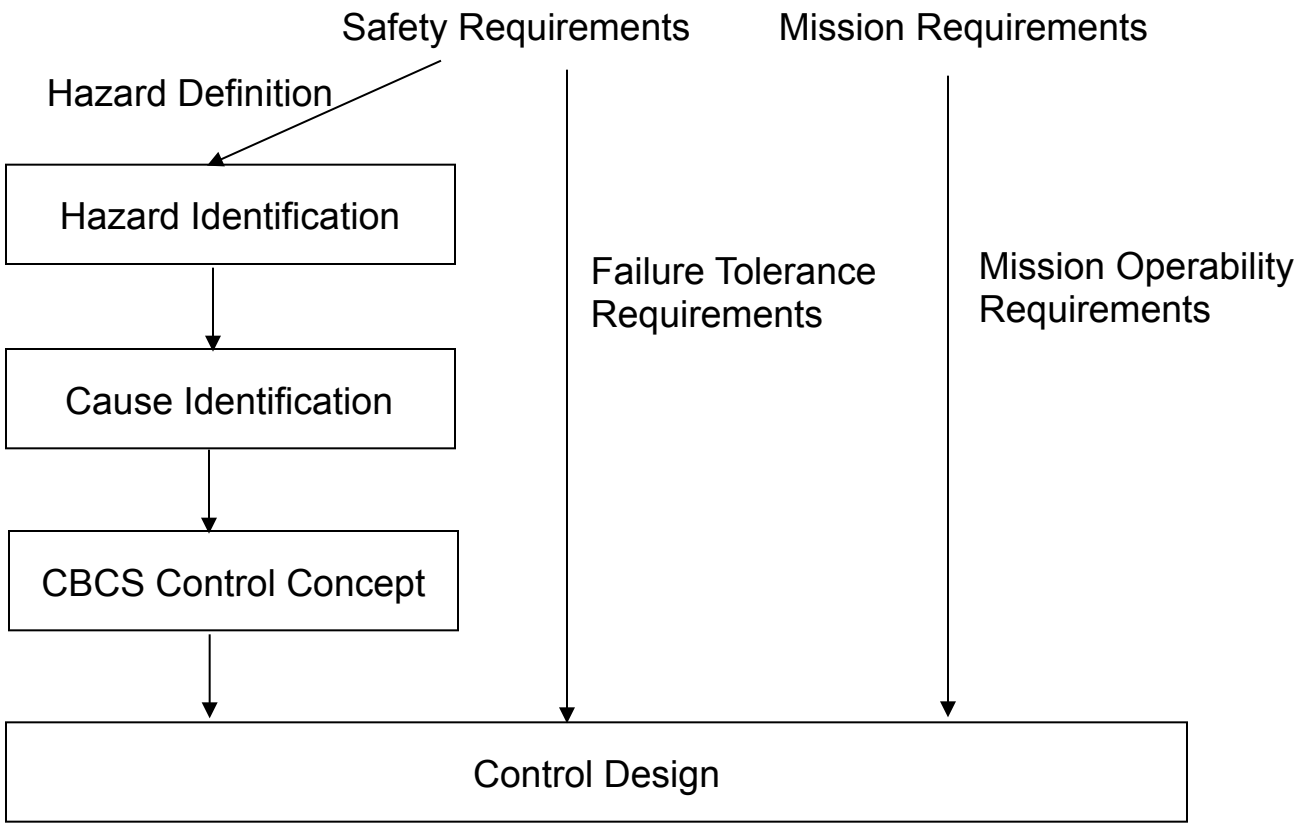
- I tried to make the architecture framework for spacecraft computer control safety system.

Experience

- Spacecraft Computer Control Safety System Design
  - HTV (H-II Transfer Vehicle)
  - Length:10m, Diamiter:4.4m, Weight:16.5 ton (Cargo 6ton)
  - HTV-1 was launched on September 11, 2009.
  - HTV-1 arrived at ISS (International Space Station) and was captured by the robotic arm on September 18, 2009.
  - After more than 40 days attached operation, HTV-1 was unberthed from the ISS and released by the robotic arm on October 31, 2009.
  - HTV-1 has reentered the atmosphere on November 2.

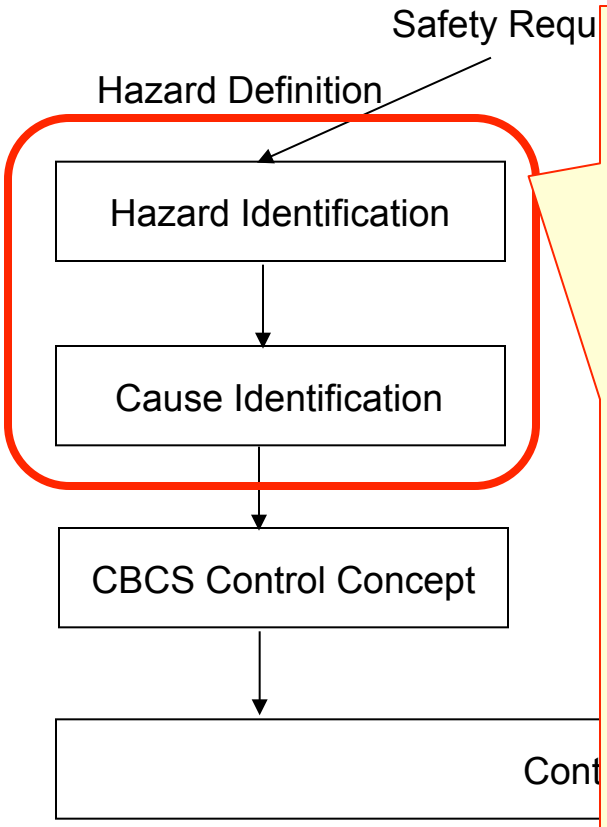
Design Process

- Safety design followed NASA requirement.



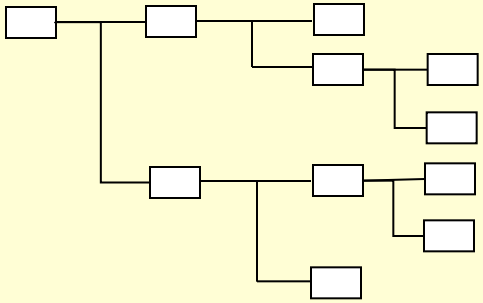
Design Process

- Safety design followed NASA requirement.



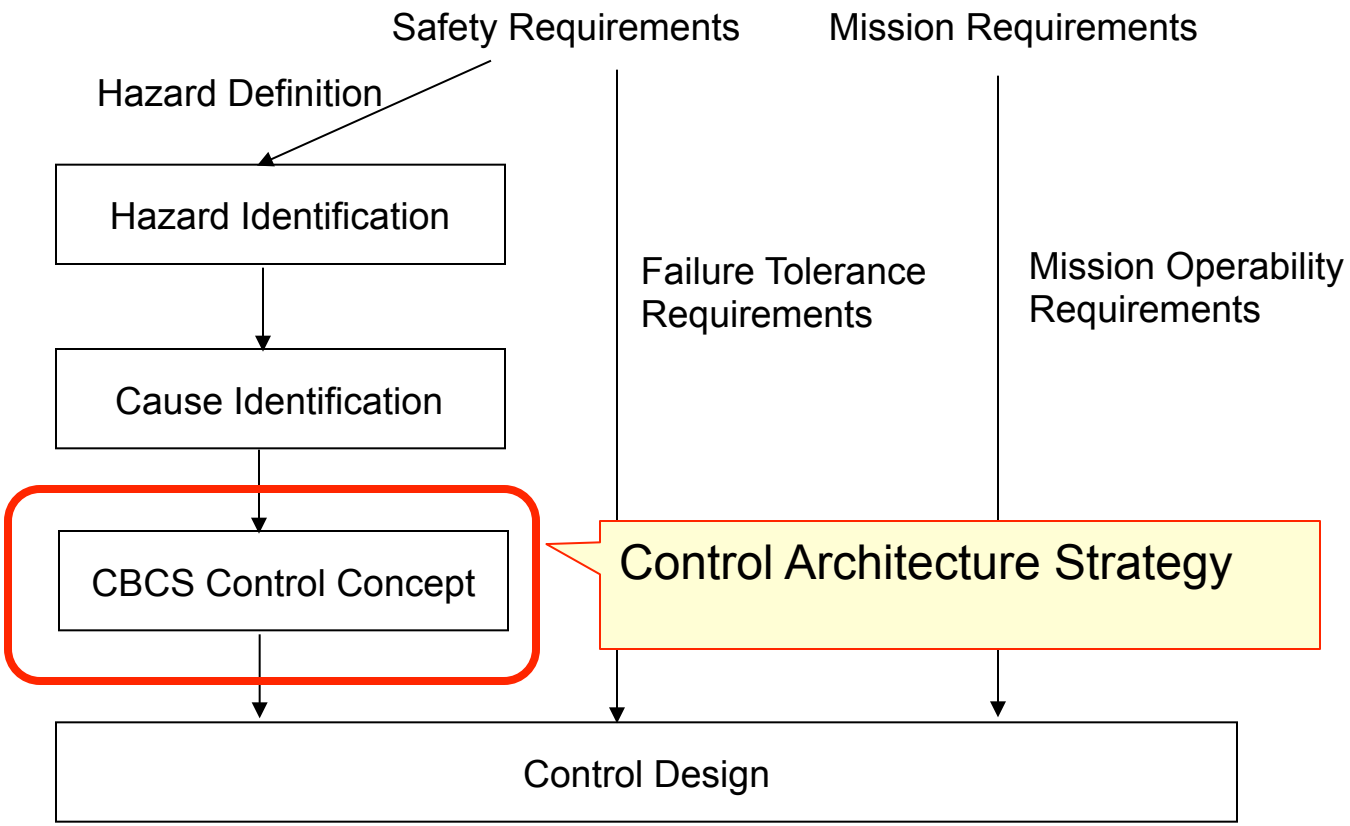
Hazard:
Critical Hazard
- Non-disabling personnel injury
- loss of a major ISS element Function
Catastrophic Hazard:
- Fatal personnel injury
- Loss of ISS

Hazard/Cause Identification
Fault Tree Analysis (FTA)



Design Process

- Safety design followed NASA requirement.



Design Process

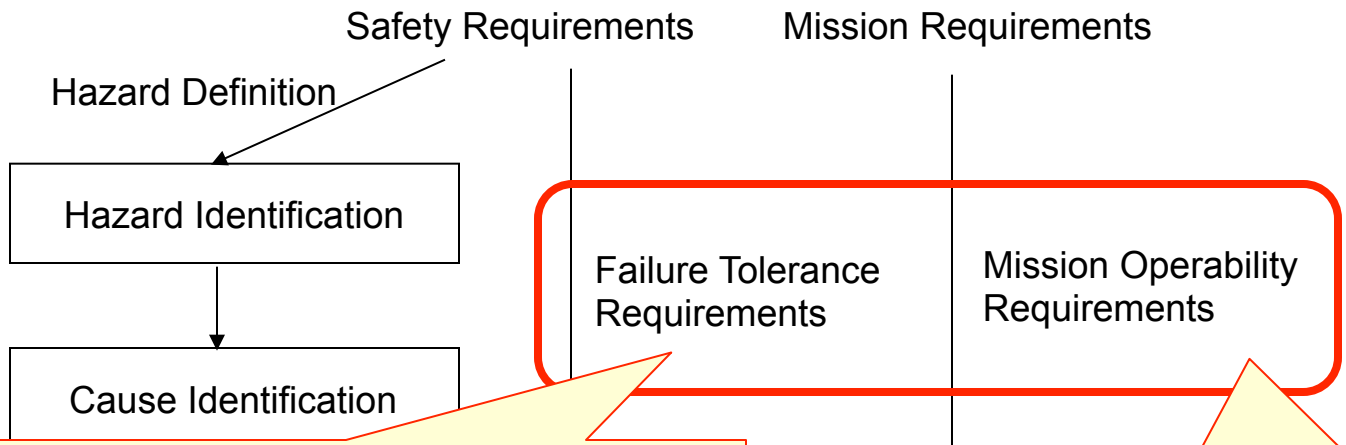
- Computer Based Control System Safety Requirements
  - Must Work Function Requirements
    - In case of Loss of function resulting in hazards
    - Fault Tolerant Approach

  - Must Not Work Function Requirements
    - In case of inadvertent operation resulting in hazards
    - Controlled by Inhibit

  - General Requirement
    - General requirements for a computer or software that is used for hazard control

Design Process

- Safety design followed NASA requirement.



- **Two Fail Safe for Catastrophic Hazard**
  - **Two failures or two operator errors or combination of one failure and one operator error shall not cause hazard.**
- **One Fail Safe for Critical Hazard**
  - **One failure or one operator error shall not cause hazard.**

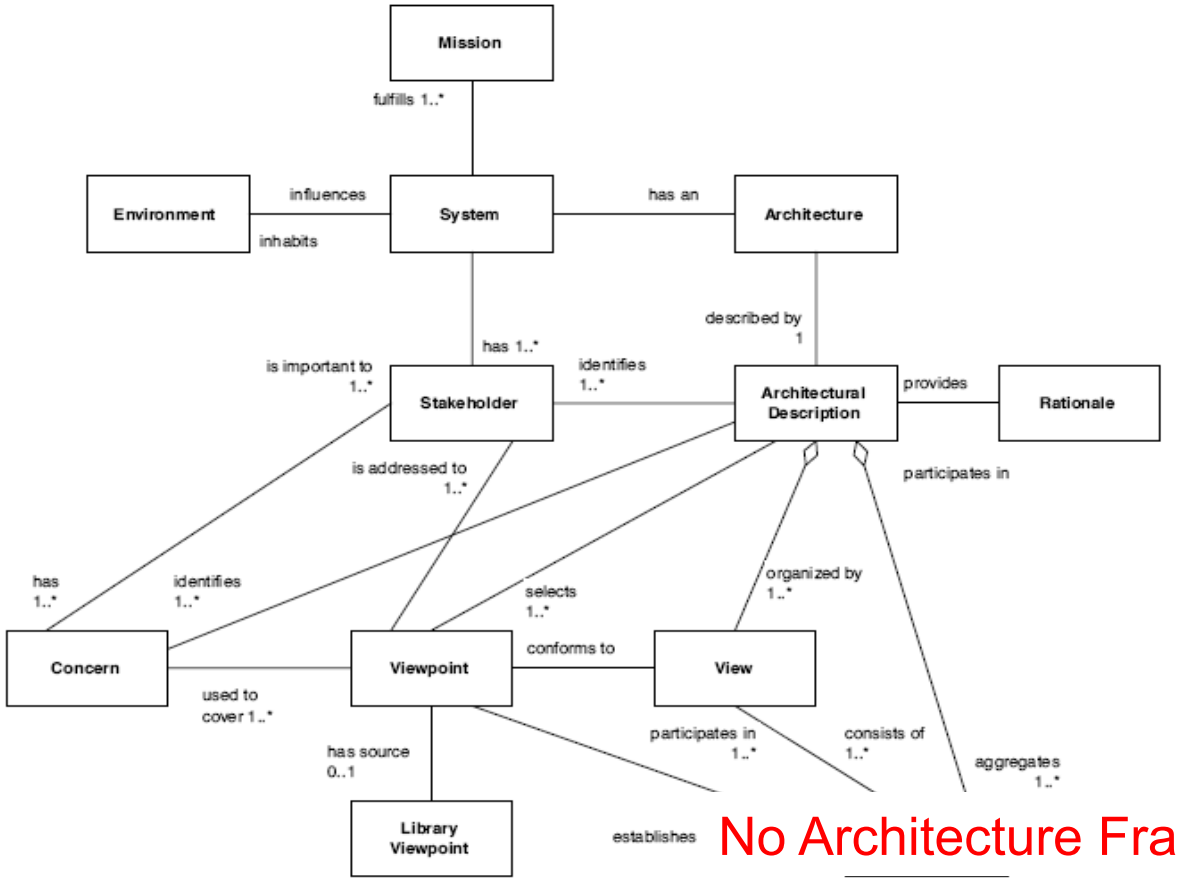
- **One Fail Operative**
  - **After one failure or one operator error, HTV shall continue mission.**

Contents

- Backgound
- Experiece
- Design Process from Experience
- Architecture Framework Development
  - Development Process
  - Process Identification
  - View/Viewpoint Identification
- Architecture Views Example

Architecture Framework

- IEEE1471-2000 Recommended practice for architectural description of software-intensive systems

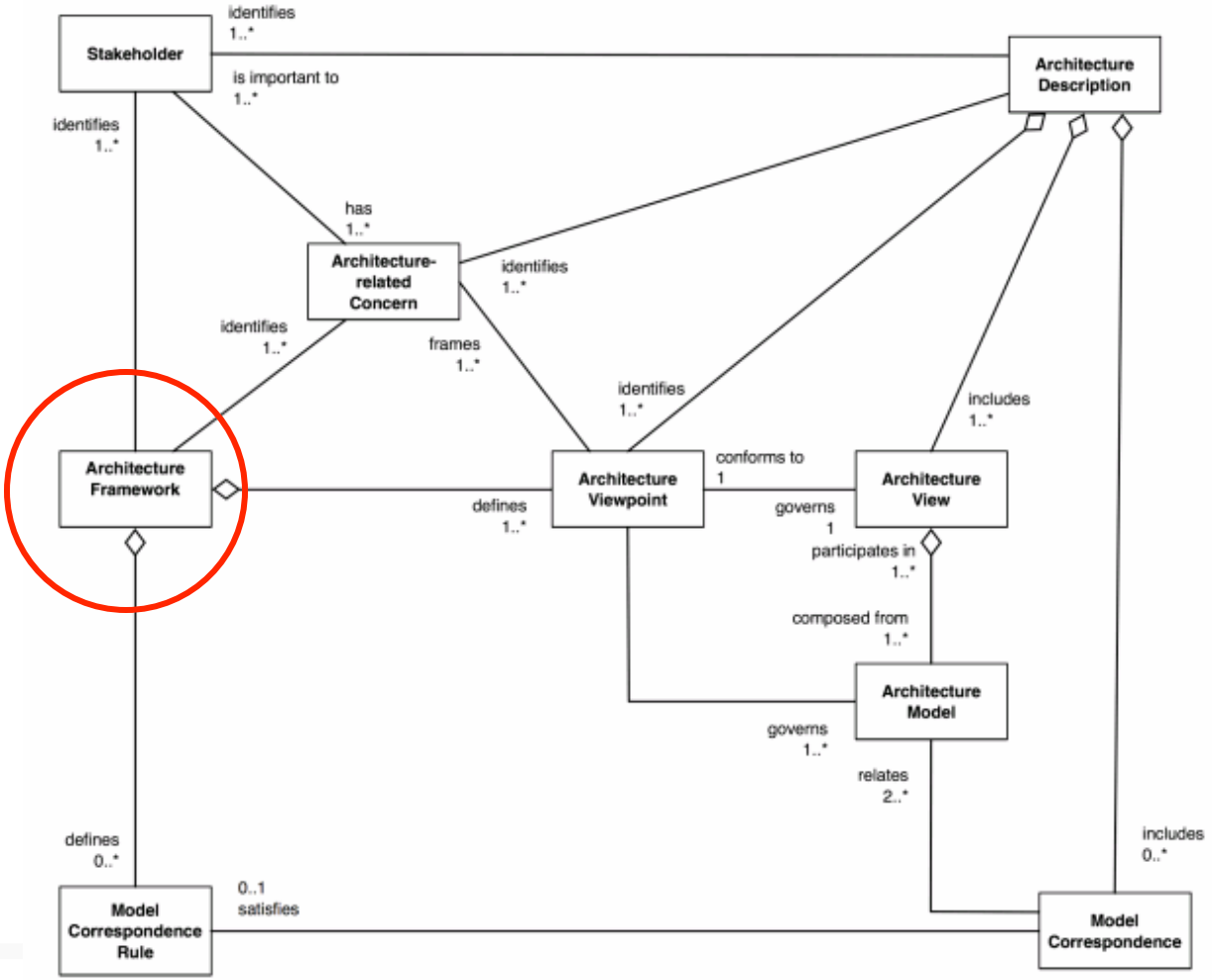


No Architecture Framework

Architecture Framework

- Next IEEE1471/ ISO/IEC 42010 (Draft)

  Systems and Software engineering – Architecture Description



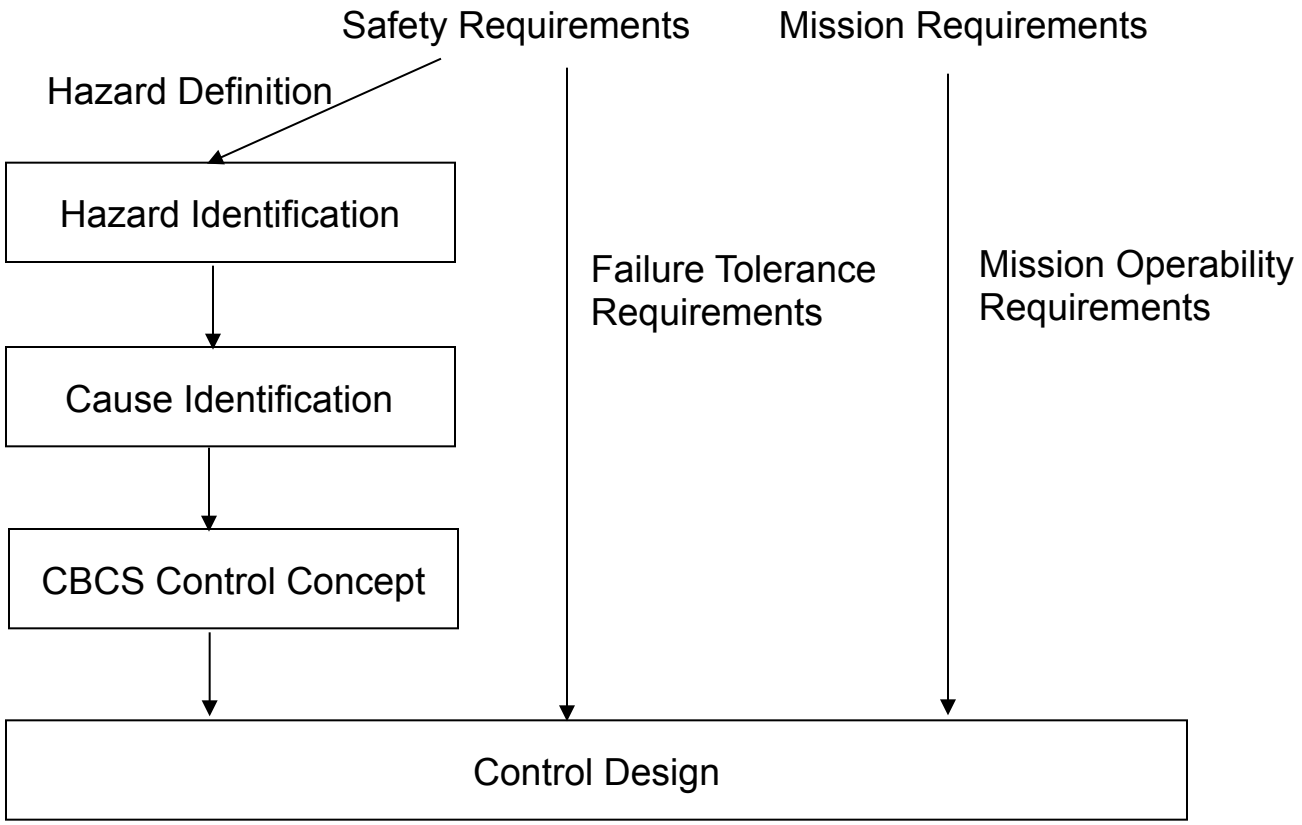
Development Process

- The way to develop the Architecture Framework.

1. Process Identification
2. View/Viewpoint Identification/Clarification
3. Architecture Framework Development

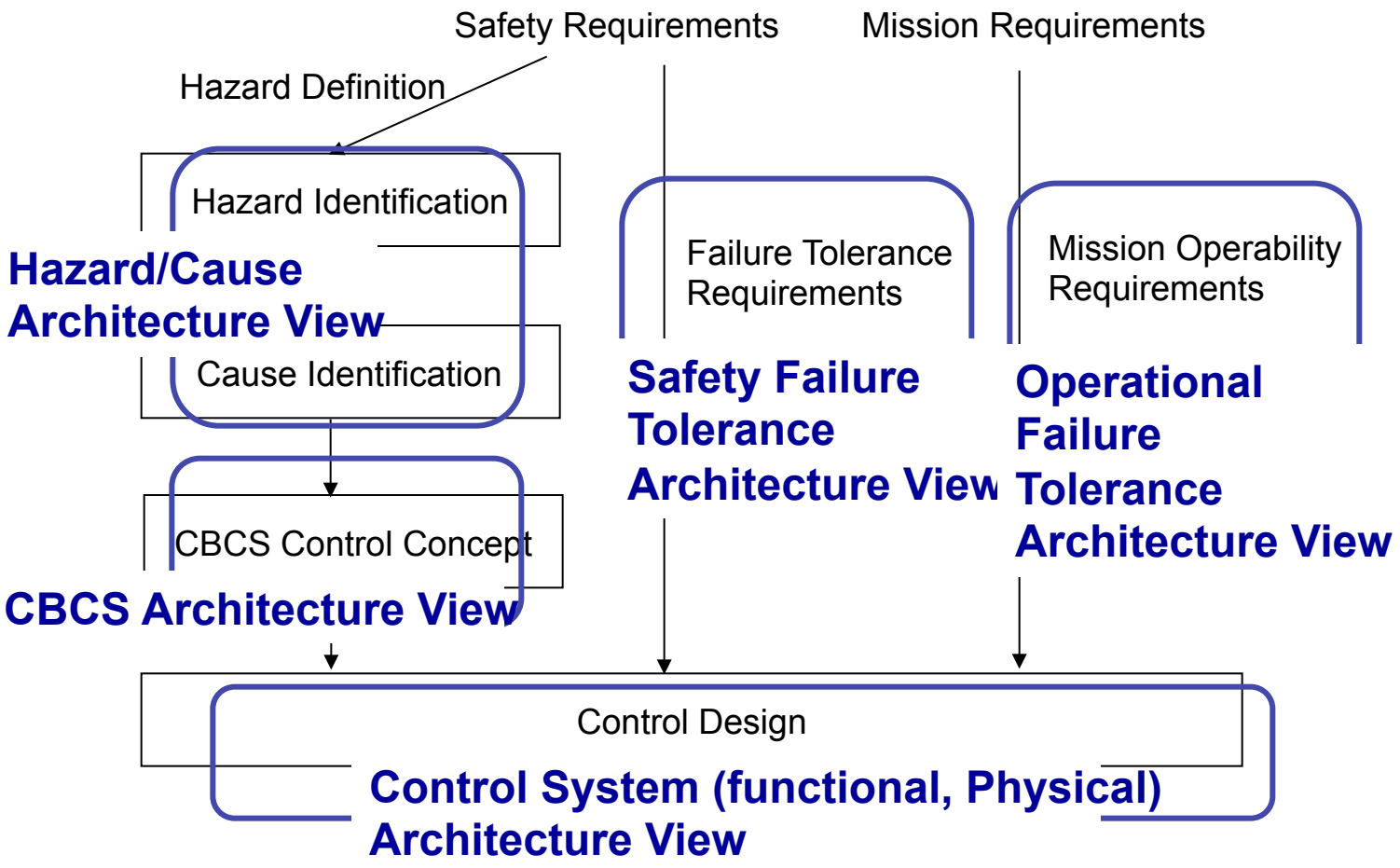
Process Identification

- Spacecraft Computer Control Safety System Design Process



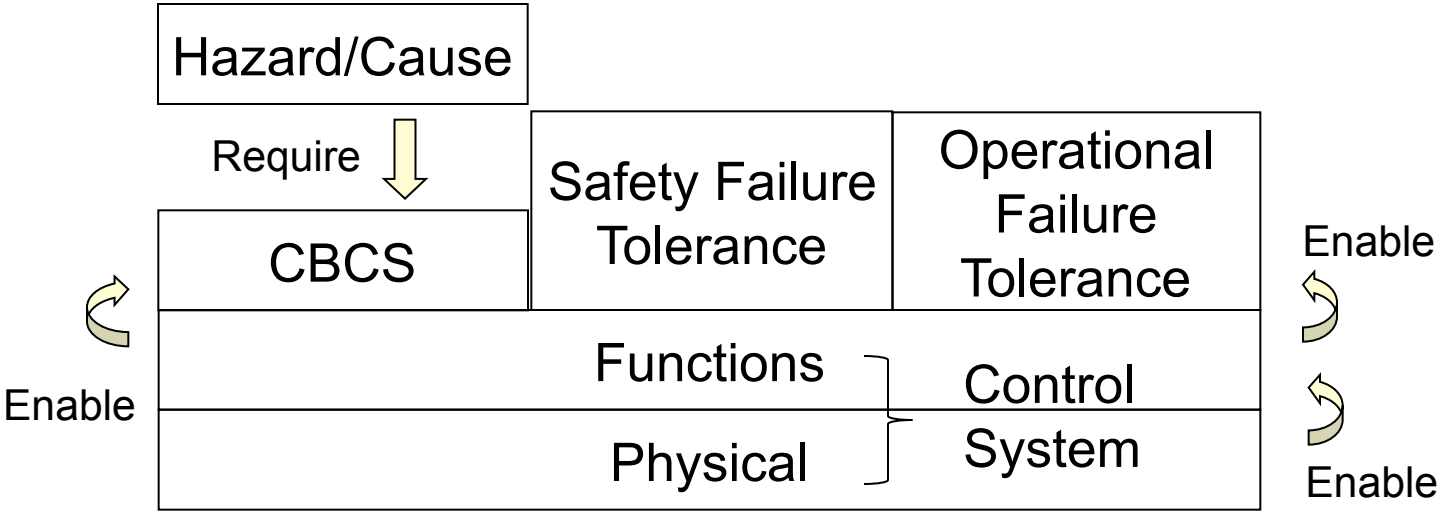
View Identification

- Identified Views in accordance with the design process



Viewpoint Identification/Clarification

- Identified viewpoints and viewpoint architecture in accordance with the views



Architecture Framework Development

- According to next IEEE1471, an architecture framework shall include:
  - the identification of one or more concerns;
  - the identification of one or more stakeholders having those concerns;
  - one or more architecture viewpoints which frame those concerns;
  - zero or more model correspondence rules.

Architecture Framework Development

- . Concern and Stakeholder
  - Safety engineers have several concerns which related to the architecture.
    - The first concern is that what is a hazard and what causes the hazard.
    - The second concern is CBCS controls.
    - The third concern is safety failure tolerance.
  - System architect's concerns are;
    - safety failure tolerance,
    - operational failure tolerance.
  - Customers or users concerns are;
    - hazards,
    - operational failure tolerance,
    - functionality.

Architecture Framework Development

- Viewpoints
  - Hazard / Cause viewpoint

Concerns framed by the viewpoint	Hazard and its cause identification
Model types used in this viewpoint	Fault Tree Analysis (FTA)
Notation;	Node, and / or connector and lines
Source	Not applicable

  - CBCS viewpoint

Concerns framed by the viewpoint	CBCS concept to control hazard cause
Model types used in this viewpoint	MWF: Functional flow block diagram (FFBD) Or system function diagram (SV-4) MNWF: Inhibit allocation diagram
Notation;	MWF : follow FFBD or SV-4 MNWF : Ad hoc
Source	SV-4 : derived from DoDAF format Others : Not applicable

Architecture Framework Development

- Safety failure tolerance viewpoint

Concerns framed by the viewpoint	Number of failure to be controlled safely for each hazard level
Model types used in this viewpoint	Table of hazard level and failure number
Notation;	Ad hoc
Source	Not applicable

- Operational failure tolerance viewpoint

Concerns framed by the viewpoint	Number of failure to be controlled operatively with the definition of "operability".
Model types used in this viewpoint	Failure number and text
Notation;	Ad hoc
Source	Not applicable

- Control system viewpoint

Concerns framed by the viewpoint	Functional and physical architecture
Model types used in this viewpoint	System architecture diagram
Notation;	Node, and / or connector and lines
Source	Not applicable

Contents

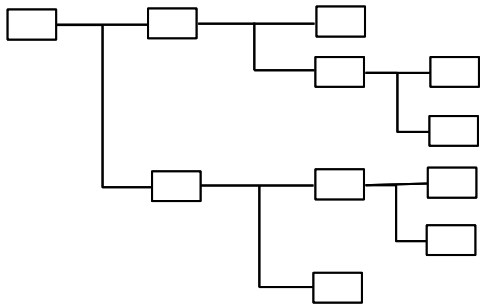
- Backgound
- Experiece
- Design Process from Experience
- Architecture Framework Development
  - Development Process
  - Process Identification
  - View/Viewpoint Identification
- Architecture Views Example

Architecture Views Example

- According to the next IEEE1471, the architecture view includes;
  a. a version identifier;
  b. overview information as specified by the organization or project;
  c. configuration control information as specified by the organization or project;
  d. architecture models addressing all of the concerns framed by its governing viewpoint and covering the whole system from that viewpoint;
  e. recording of any known issues within a view with respect to its governing viewpoint.
- I follow the annex C to develop example.

Architecture Views

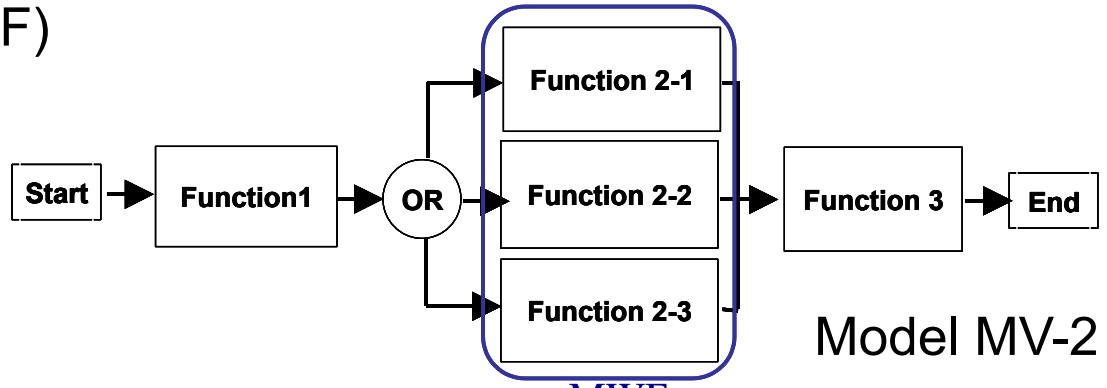
- Hazard / Cause view.
  - Unique identifier: V-1
  - Overview: This view shows the hazards and their causes.
  - Configuration information: Version 1.0
  - Model name (identifier): The hazards and the causes identification diagram model (MV-1)
  - Model type: Fault Tree Analysis.



Model MV-1

Architecture Views

- CBCS view.
  - Unique identifier: V-2
  - Overview: This view shows the CBCS control concept (MWF or MNWF). In case of MWF, the functional structure to realize MWF is shown. And in case of MNWF, inhibit allocation and the inhibit control path are shown.
  - Configuration information: Version 1.0
  - Model name (identifier): The CBCS control concept model (MV-2)
  - Model type: Functional flow diagram (MWF) or data flow diagram (MNWF)



Model MV-2

Architecture Views

- Safety failure tolerance view
  - Unique identifier: V-3
  - Overview: This view shows how many failure shall be controlled with respect to hazard level.
  - Configuration information: Version 1.0
  - Model name (identifier): The safety failure tolerance model (MV-3)
  - Model type: hazard level and failure tolerance requirement spreadsheet.

Hazard Level	Failure Tolerance Req.
Catastrophic Hazard	Two failure tolerance
Critical Hazard	One failure tolerance

Model MV-3

Architecture Views

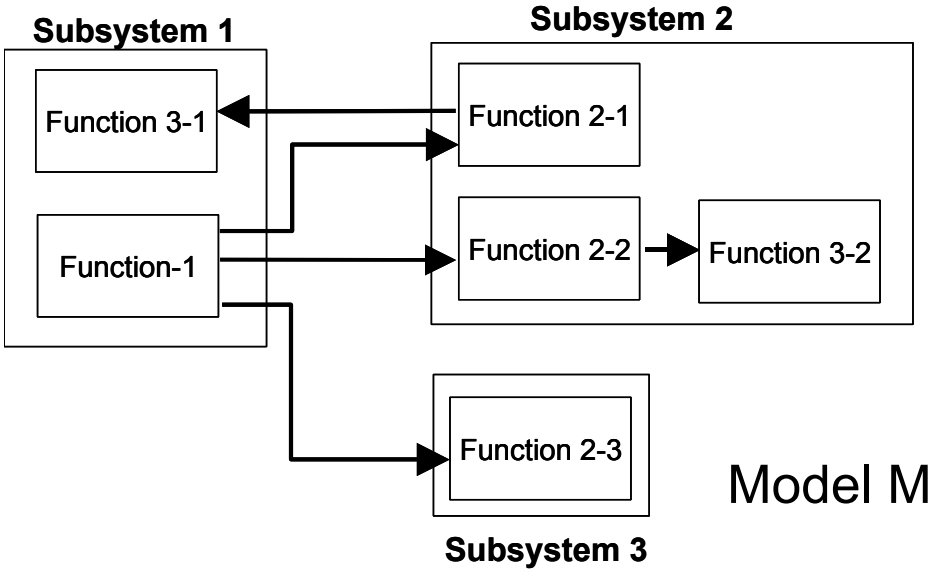
- Operational failure tolerance view
  - Unique identifier: V-4
  - Overview: This view shows how many failures shall be considered to continue a mission.
  - Model name (identifier): The operational failure tolerance model (MV-4)
  - Model type: operational failure tolerance requirement spreadsheet.

Operation	Failure Tolerance Req.
Data collection	Two failure tolerance
Auto targeting	One failure tolerance

Model MV-4

Architecture Views

- Control System view
  - Unique identifier: V-5
  - Overview: This view shows that what function is allocated to which subsystem.
  - Configuration information: Version 1.0
  - Model name (identifier): The control system model (MV-5)
  - Model type: system flow diagram.



Model MV-5

Conclusion

- I tried to development of architecture framework for spacecraft computer control safety system based on the experience of real spacecraft safety design.
- The standard was very helpful to develop the architecture framework.
- I have to evaluate this framework whether it is useful for real design or not by applying it to the design.