Dependability Case for Open Systems Lifecycle

Yutaka Matsuno

CVS, AIST, Japan

yutaka.matsuno@aist.go.jp

Contents

- Use cases of Dependability Case (D-Case) in DEOS project
  - Expressing Dependability of DEOS elemental technologies
  - Experiments of Writing D-Case
- Ongoing Works
  - Managing D-Case in every lifecycle phase
    - Cooperating with the system
  - Guideline for writing AC
- D-Case as a medium for showing evidences

All works are collaboration of all DEOS teams

Contents

- Use cases of Dependability Case (D-Case) in DEOS project
  - Expressing Dependability of DEOS elemental technologies
  - Experiment of Writing D-Cases
- Ongoing Works
  - Managing D-Case in every lifecycle phase
    - Cooperating with the system
  - Guideline for writing AC
- D-Case as a medium for showing evidences

Background of introducing Assurance Case

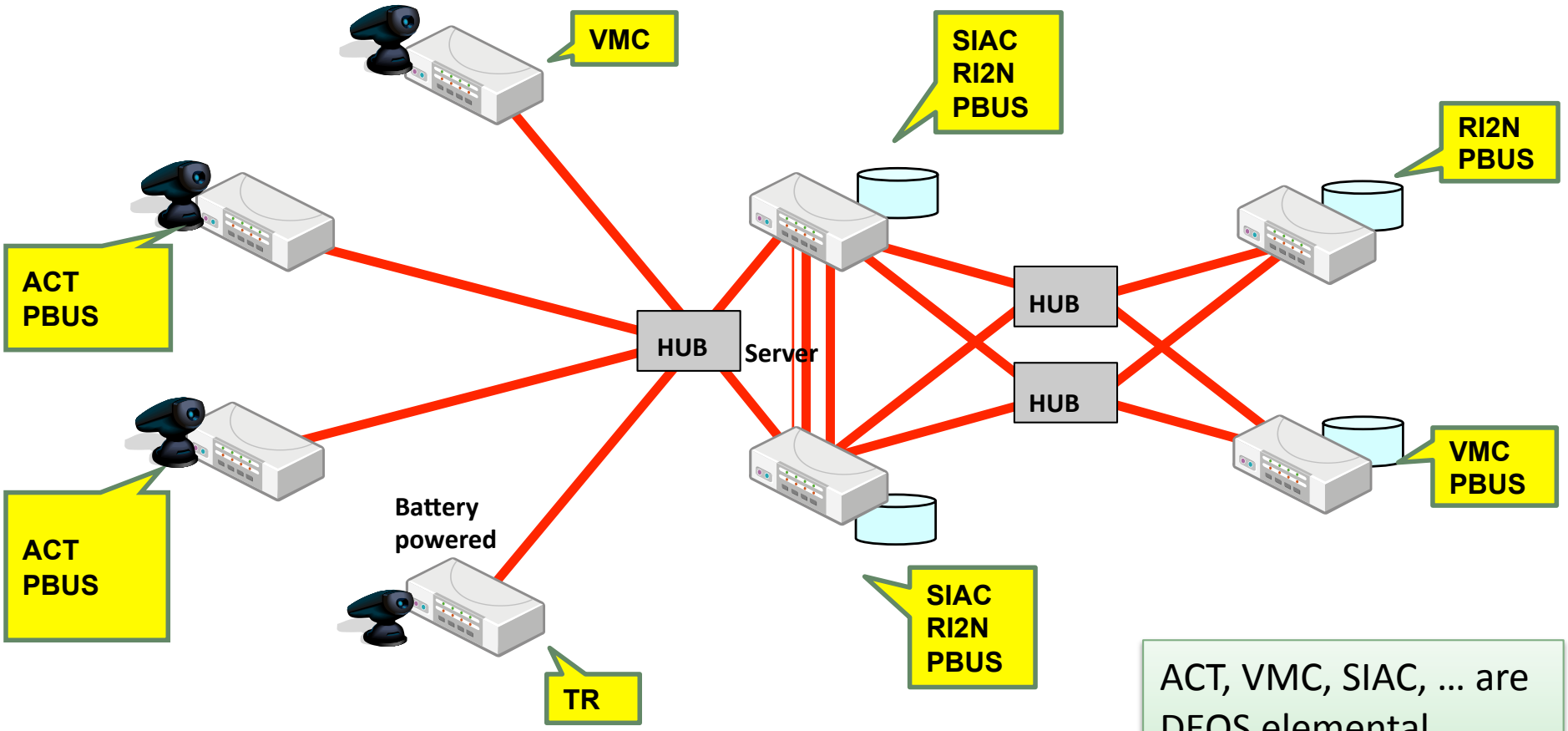
- AIST team is focused on risk communication and assurance case

- For mid-term evaluation of DEOS (2009.9.4), there were two problems:
  - DEOS teams could not explain clearly how their elemental technologies are dependable
  - DEOS teams could not summarize their discussions on dependability
- To solve these two problems, we introduced assurance case and it become “D-Case”

D-Case

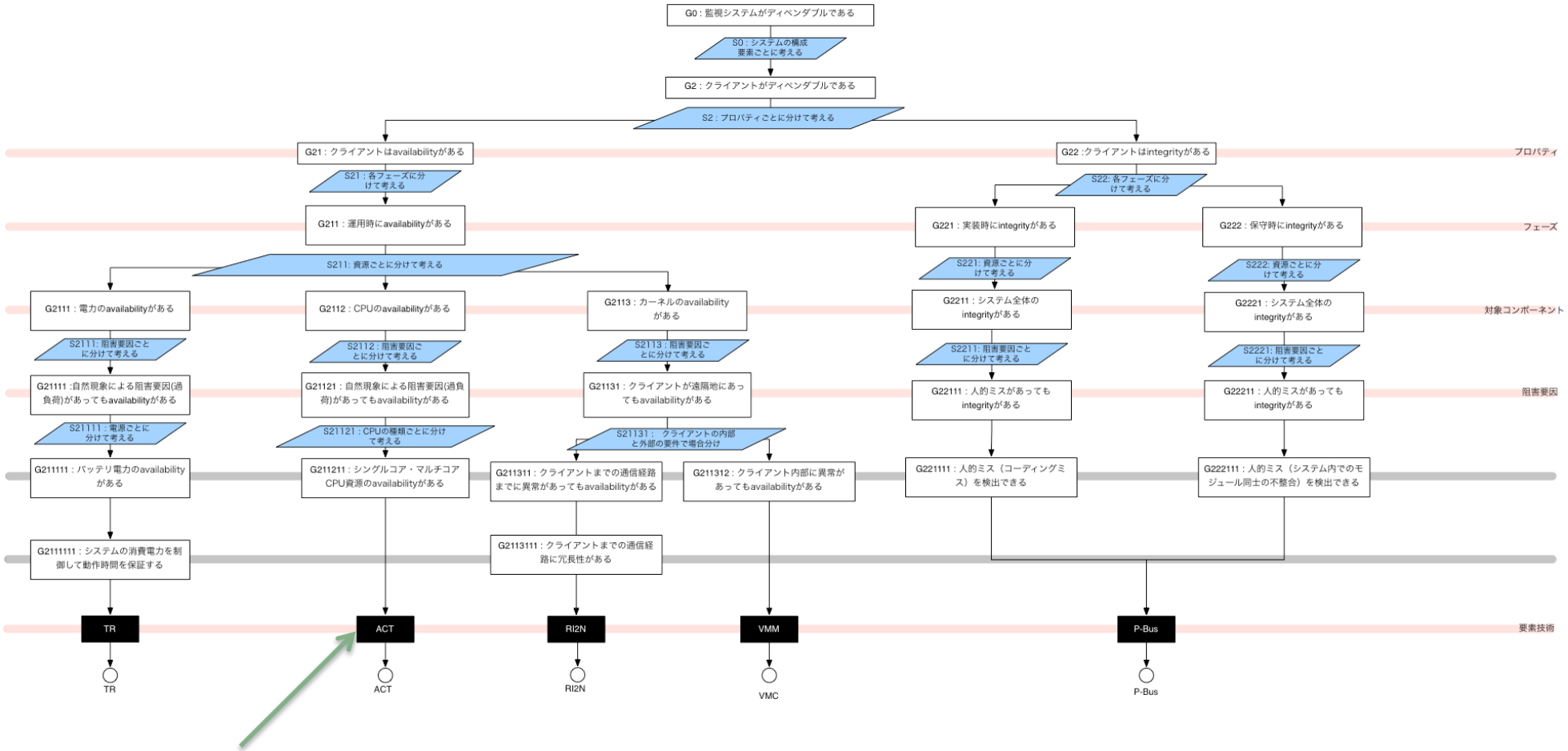
- Dependability Case is an instance of Assurance Case
- D-Case is a new Dependability Case being developed in DEOS project
  - Synchronize with system (not just human arguments, as Kimio's demo)
  - Editor (started in January 2010)

Camera Surveillance Demo System in 9.4 mid-term DEOS evaluation



ACT, VMC, SIAC, … are DEOS elemental technologies

D-Case of
Camera Surveillance Demo System

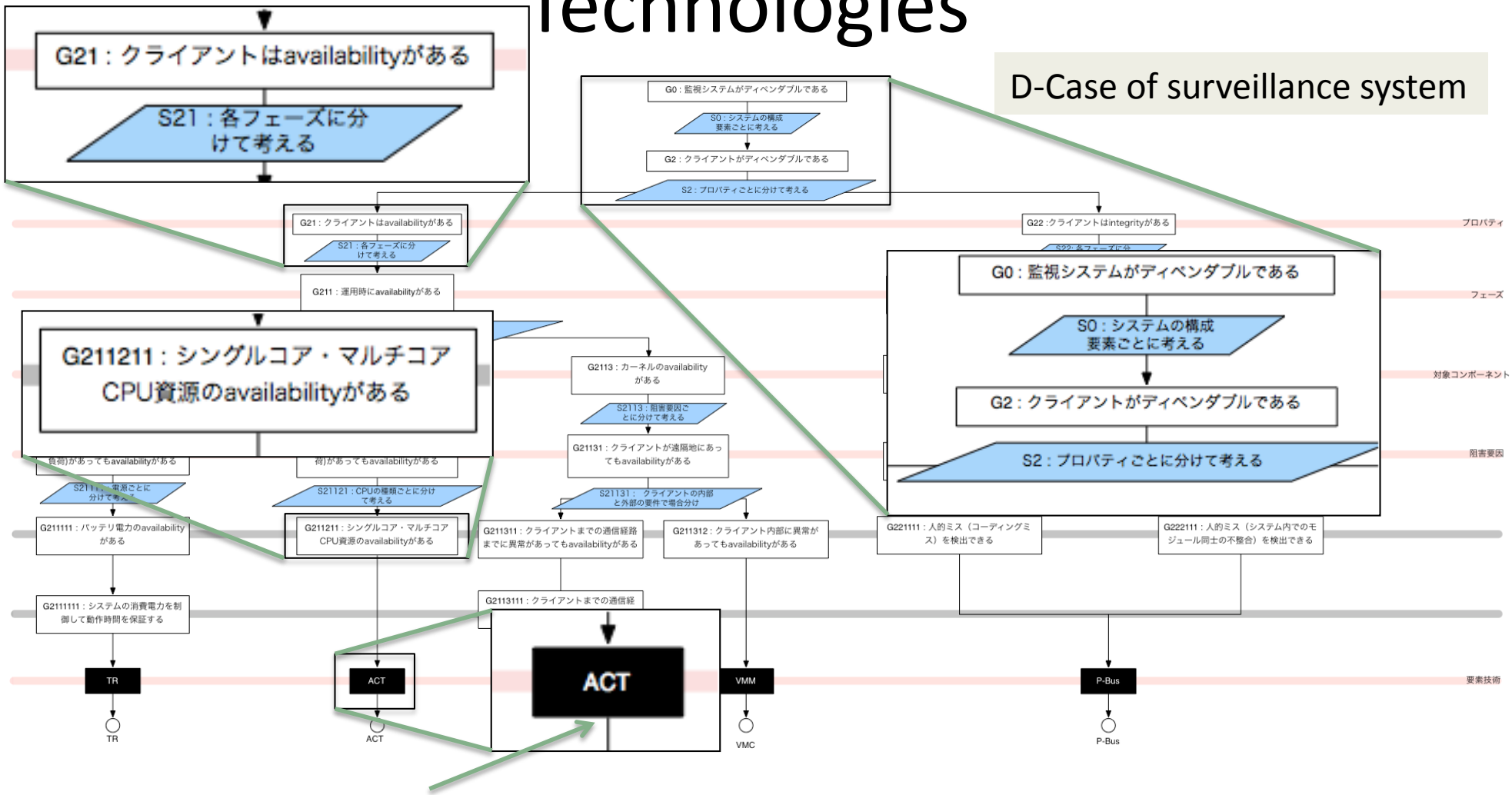


Elemental Technology Node

A kind of node we added to original Goal Structuring Notation (Tim Kelly, 1998)

Dependability of Elemental Technologies

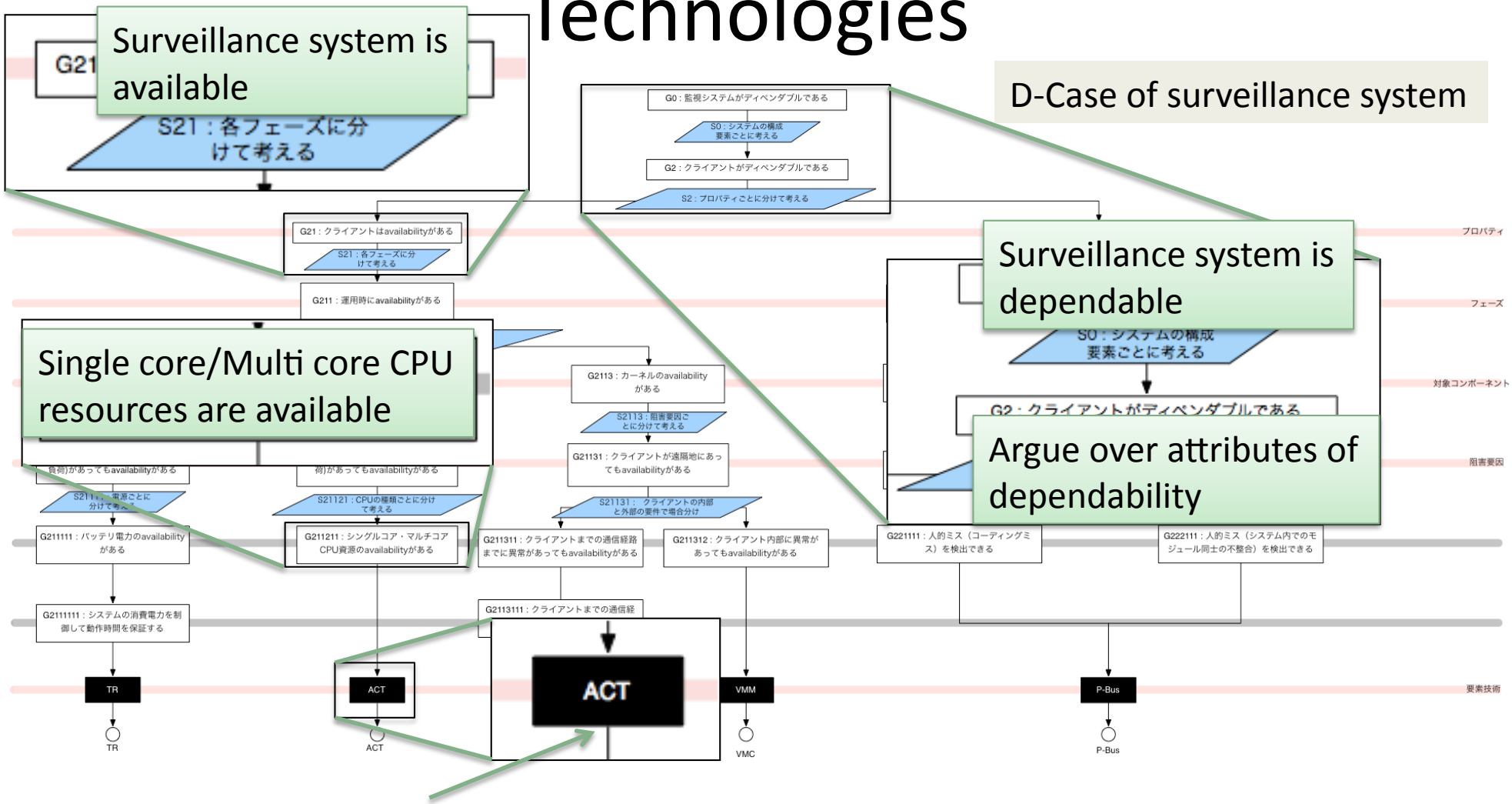
D-Case of surveillance system



Elemental Technology Node

A kind of node we added to original Goal Structuring Notation (Tim Kelly, 1998)

Dependability of Elemental Technologies



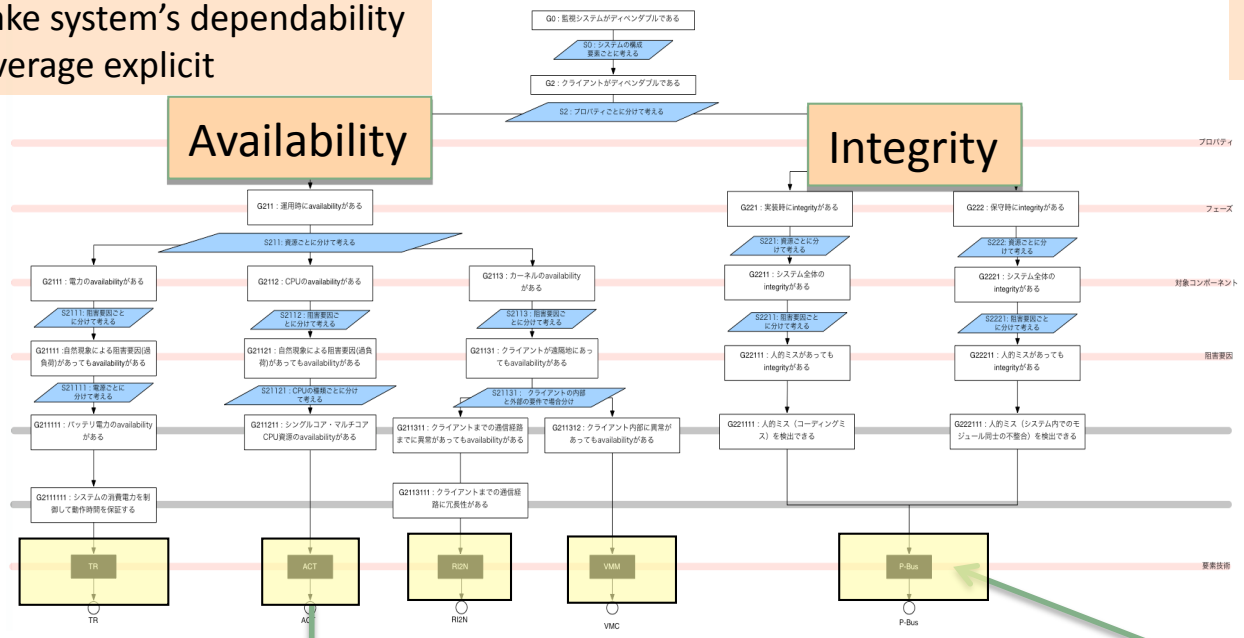
Elemental Technology Node

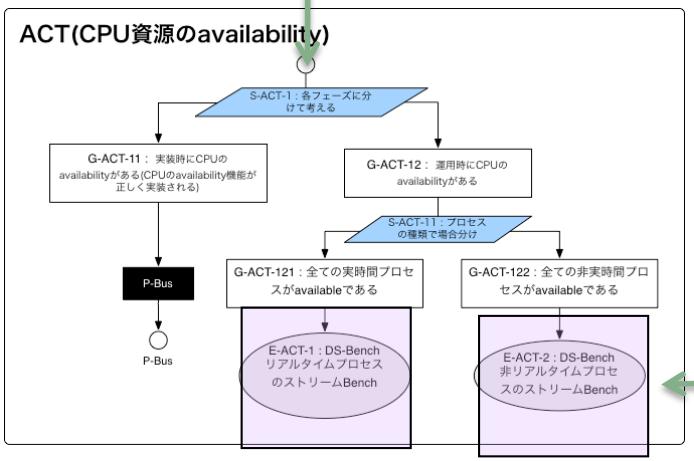
A kind of node we added to original Goal Structuring Notation (Tim Kelly, 1998)

Summarizing Dependability Discussions

Make system's dependability coverage explicit

Argue according to the qualitative metrics





"Metrics"
Set of qualitative metrics for evaluating systems

"Configuration"
Set of combination of elemental technologies in specific environments

Set of elemental technologies for the given goal

Quantitative Evidence

"DS-Bench" Benchmarks

Collaboration with Metrics 1/3

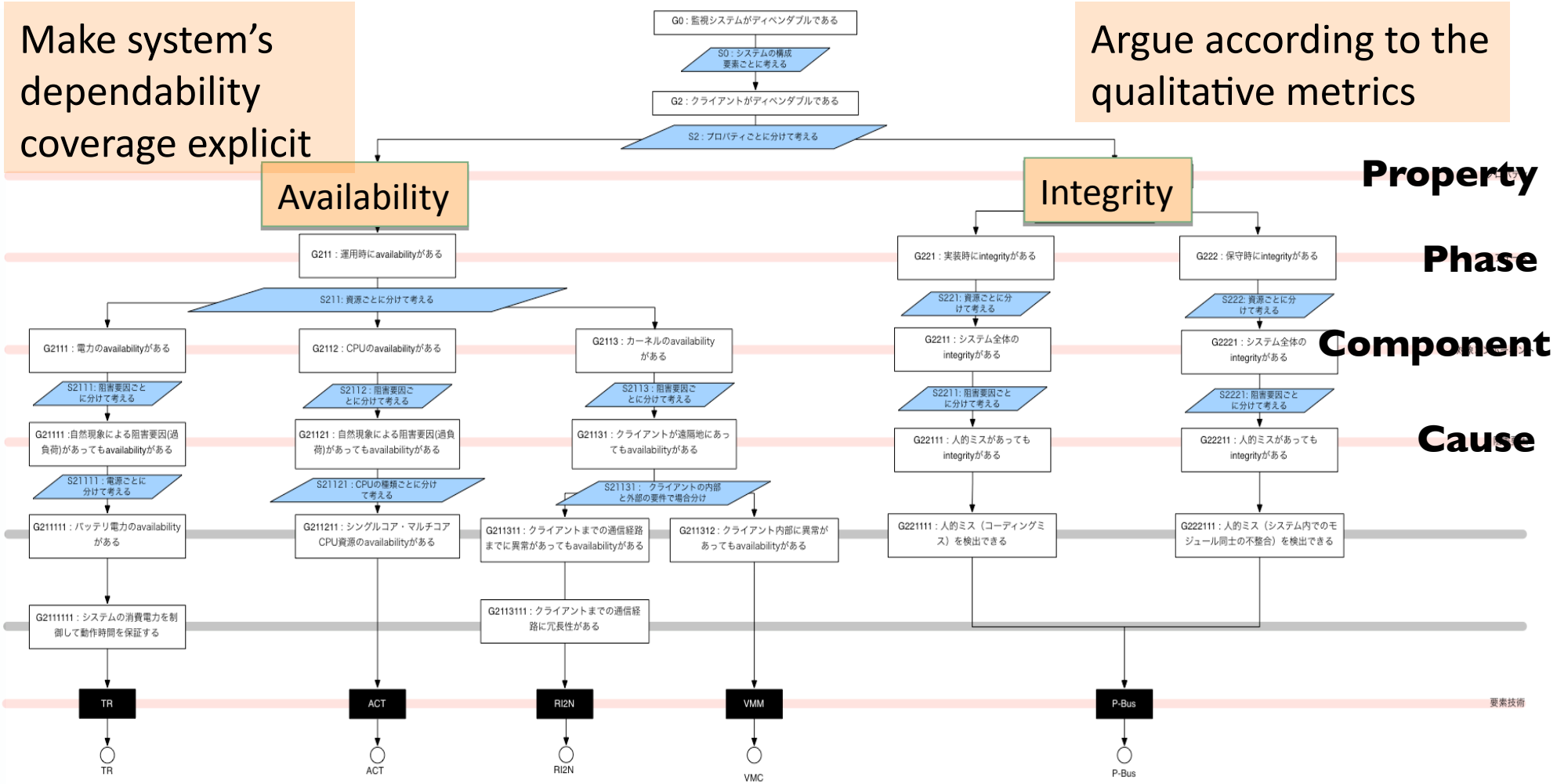
- Argue according to the qualitative metrics for OS

Phase	**Component**	**Cause**	**Property**
Specification	CPU	Environment	Availability
Design	RAM	Hardware	Reliability
Implementation	File system	Attack	Safety
Test	Communication	Mistake	Integrity
Operation	Input/output		Maintainability
Maintenance	Power supply		
Disposal			

Collaboration with Metrics 2/3

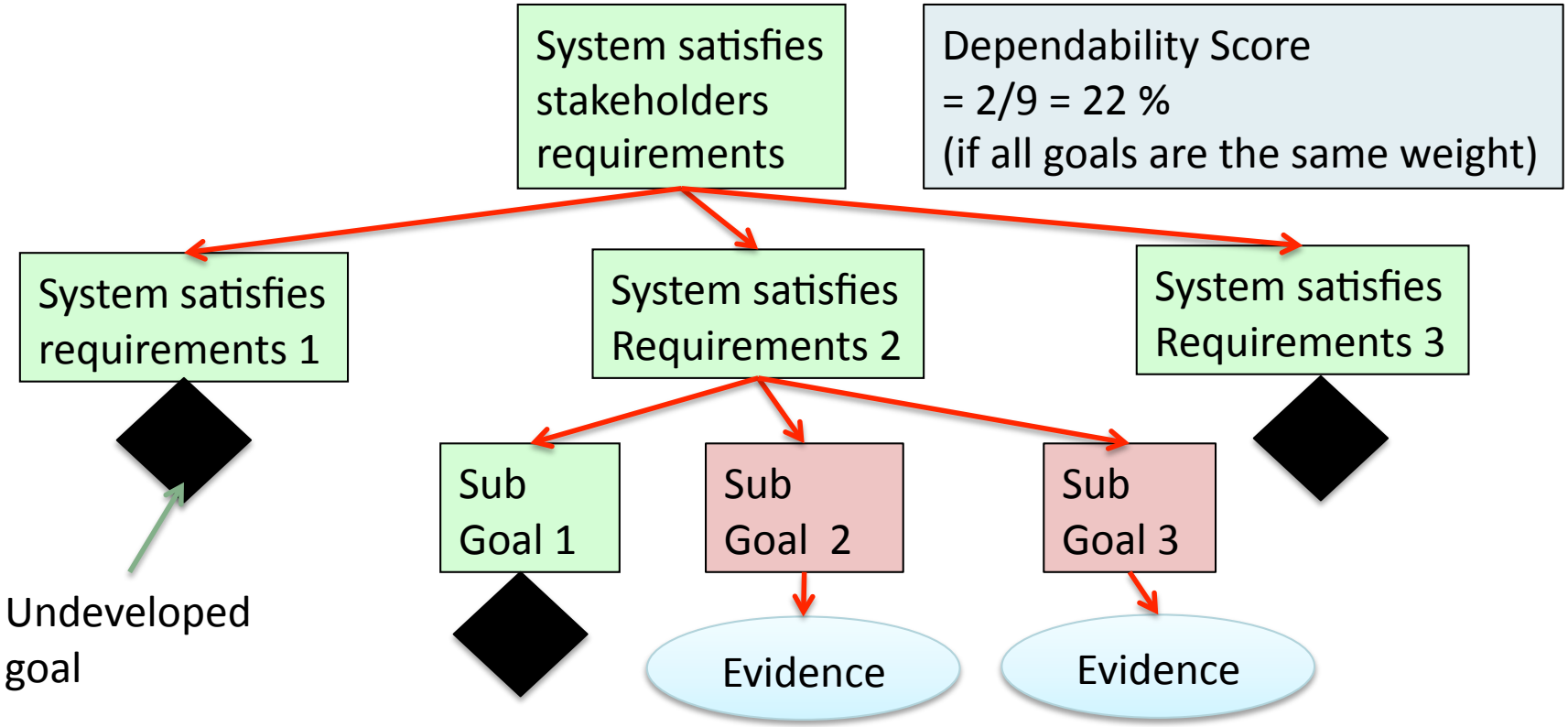
Make system's dependability coverage explicit

Argue according to the qualitative metrics



Collaboration with Metrics 3/3

- Metrics for Open System = Degree of how accountability is achieved



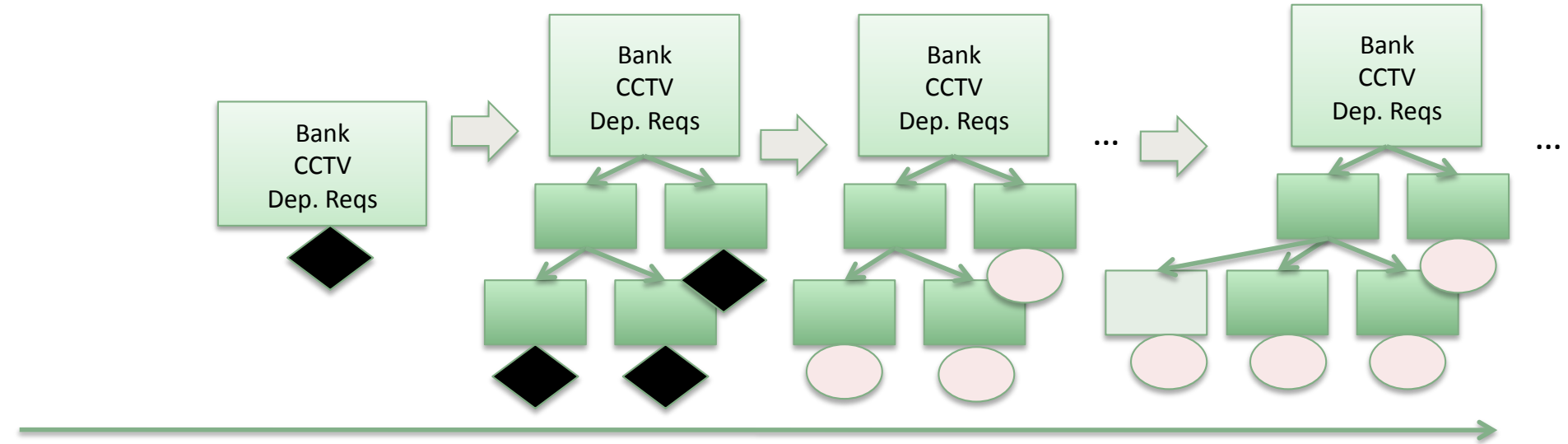
Contents

- Use cases of Dependability Case (D-Case) in DEOS project
  - Expressing Dependability of DEOS elemental technologies by D-Case
  - Experiments of writing D-Case
- Ongoing Works
  - Managing D-Case in every lifecycle phase
    - Cooperating with the system
  - Guideline for writing AC
- D-Case as a medium for showing evidences

Writing D-Case for Bank ATM surveillance system

- To consider how to write D-Case, we take bank ATM surveillance system as an example
  - Services
    - ATM surveillance and waiting people surveillance
  - Requirements
    - Real time ATM surveillance and storing movies in high resolution(30fps, 1.3mega pixel)
    - Real time waiting people surveillance and storing movies in high resolution (30fps, 1.3 mega pixel)
    - 99.999% reliability
    - High resolution face detection
  - Stakeholders
    - Bank, Development Company, Security Company

D-Case in Lifecycle



Requirement Analysis Phase

Development Phase

Test Phase

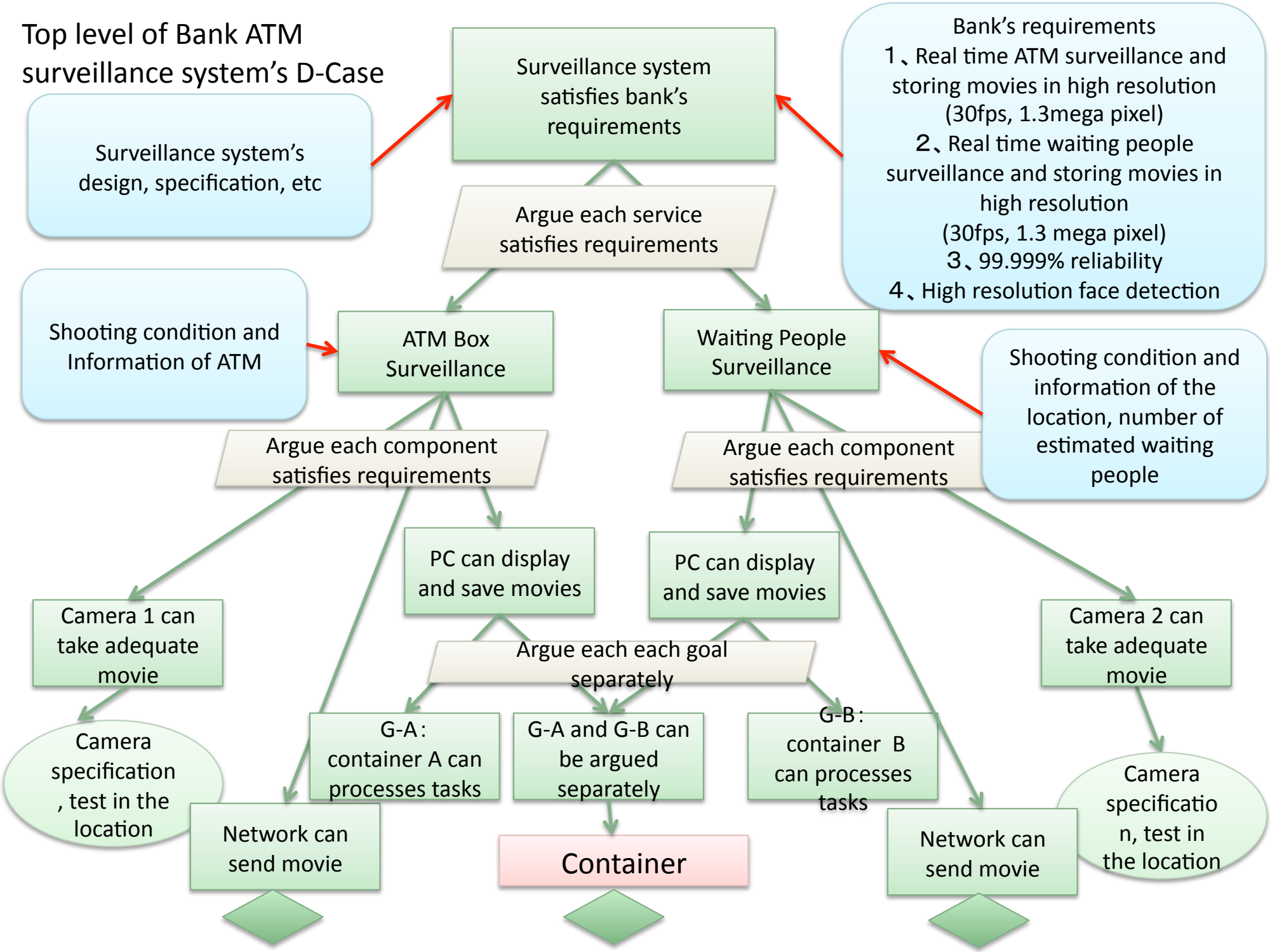
Operational Phase

Stakeholder

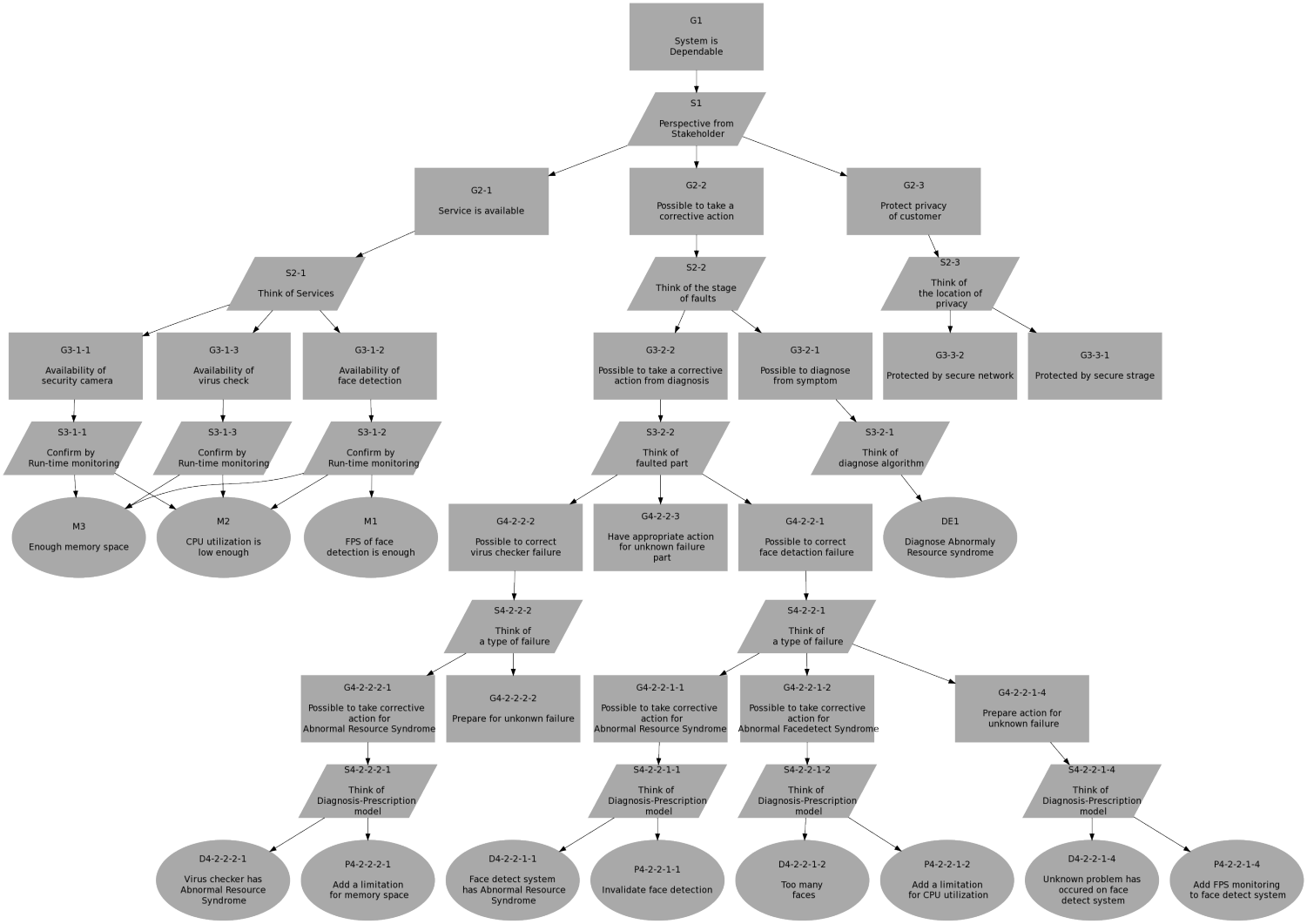
Bank

Development company

Security Company


Top level of Bank ATM surveillance system's D-Case
Surveillance system satisfies bank's requirements
Surveillance system's design, specification, etc
Bank's requirements
1、Real time ATM surveillance and storing movies in high resolution (30fps, 1.3mega pixel)
2、Real time waiting people surveillance and storing movies in high resolution (30fps, 1.3 mega pixel)
3、99.999% reliability
4、High resolution face detection
Argue each service satisfies requirements
Shooting condition and Information of ATM
ATM Box Surveillance
Waiting People Surveillance
Shooting condition and information of the location, number of estimated waiting people
Argue each component satisfies requirements
Argue each component satisfies requirements
PC can display and save movies
PC can display and save movies
Camera 1 can take adequate movie
Camera 2 can take adequate movie
Argue each each goal separately
Camera specification , test in the location
G-A : container A can processes tasks
G-A and G-B can be argued separately
G-B : container B can processes tasks
Camera specificatio n, test in the location
Network can send movie
Container
Network can send movie

Yet another D-Case of Bank ATM surveillance system (Kimio Kuramitsu)



Issues

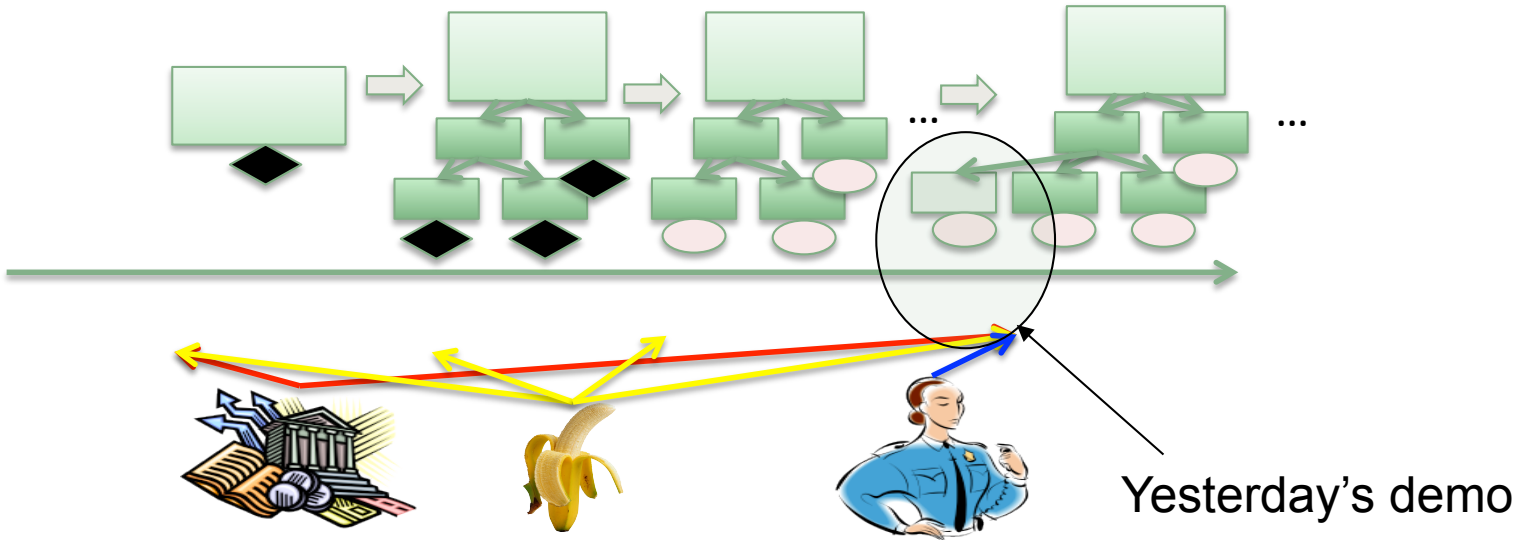
- When writing D-Case, we need to consider
  - Lifecycle
  - Stakeholder
- Some DEOS members wrote their own D-Cases of Bank ATM surveillance system
  - It was hard to make agreement to choose one D-Case

Contents

- Use cases of Dependability Case (D-Case) in DEOS project
  - Expressing Dependability of DEOS elemental technologies
  - Experiments of writing D-Case
- Ongoing Works
  - Managing D-Case in every lifecycle phase
    - Cooperating with the system
  - Guideline for writing AC
- D-Case as a medium for showing evidences

Ongoing Works

- Managing D-Cases in every lifecycle phase
  - Cooperating with system (not just human argument)

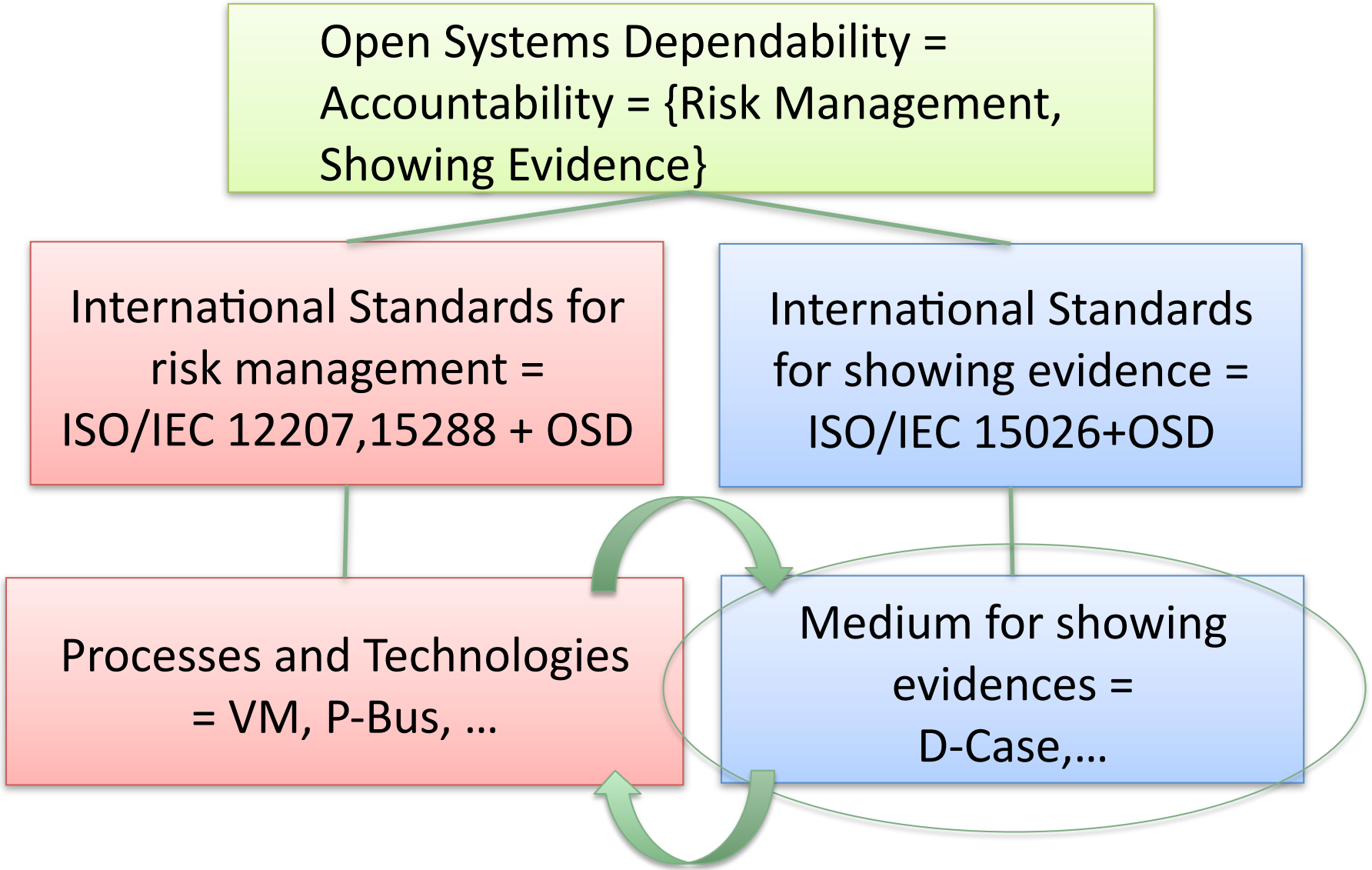


- Guideline for writing D-Case
  - Standardization -> ISO 15026

Contents

- Use cases of Dependability Case (D-Case) in DEOS project
  - Expressing Dependability of DEOS elemental technologies by D-Case
  - Experiments of writing D-Case
- Ongoing Works
  - Managing D-Case in every lifecycle phase
    - Cooperating with the system
  - Guideline for writing AC
- D-Case as a medium for showing evidences

D-Case as a medium for showing evidences



Summary

- Use cases of Dependability Case (D-Case) in DEOS project
- Ongoing works
  - Managing D-Case in every lifecycle phase
    - Cooperating with the System
  - Guideline for writing AC
- D-Case as a medium for showing evidences