



Toward Practical Use of Assurance Cases: Definitions, Methods, and Tools.

Nihon University

Yutaka Matsuno

matsuno.yutaka@nihon-u.ac.jp



Contents

- D-Case Project – Assurance Case Project in Japan
- AC Working Library in Japan
- Tool
- Concluding Remarks



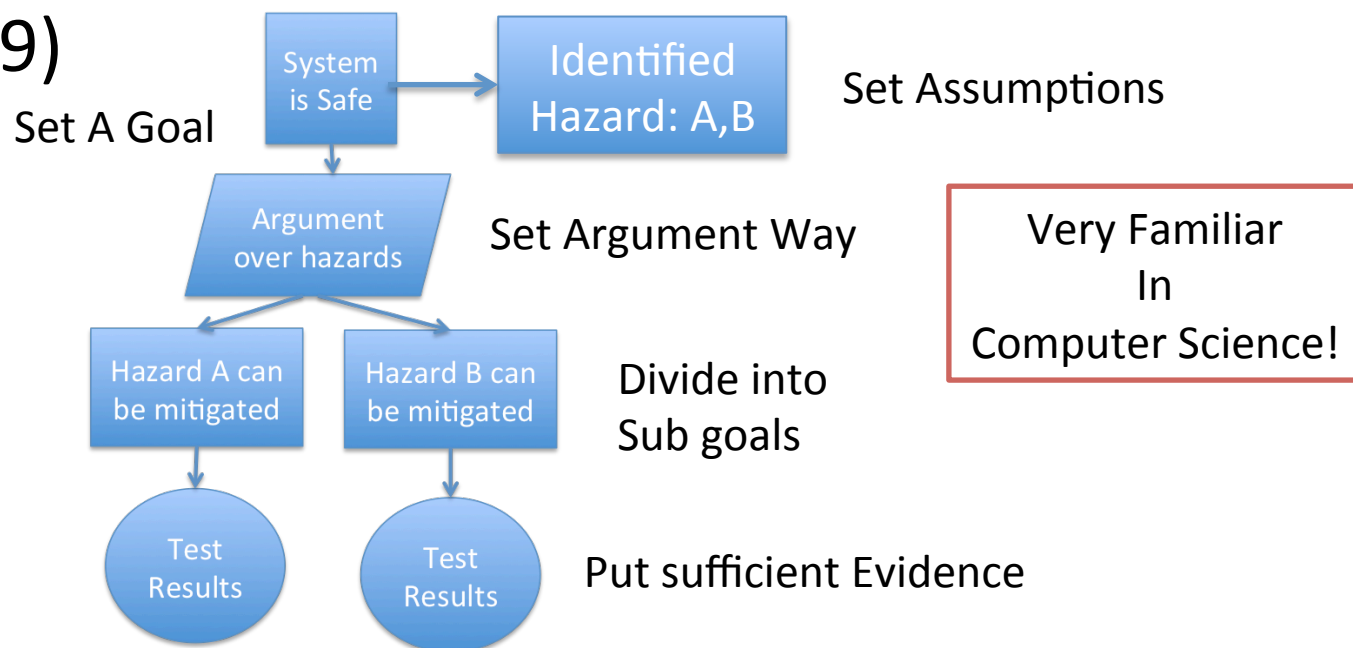
D-Case Project

- Assurance Case Project in DEOS (Dependable Embedded Operating System) project funded by Japan Science and Technology Agency (2010-2015)
 - D: Dependability
- DEOS Consortium D-Case Working Group
 - Nihon U、Nagoya U、Fuji Xerox、Naist、Tokyo U、Denso Create、Change Vision、Mitsubishi、Aizu U、...



Assurance Cases

- Recognized after serious incidents such as Piper Alpha (1989)



- Wrote AC in GSN for a demo system (2009)
 - Japanese Industry Expected AC as a common language inside and between companies



Challenges of AC

- When, who write and evaluate?
- Claim and argument structure setting
 - System is acceptably safe, dependable,...
 - Argument over lifecycle phases, system structure?
- Granularity、Size
 - Write reliability of a resister?
 - System becomes huge → AC becomes huge?



Most challenges were unsolved,
so we started D-Case Project



Contents

- D-Case Project – Assurance Case Project in Japan
- **AC Working Library in Japan**
- Tool
- Concluding Remarks



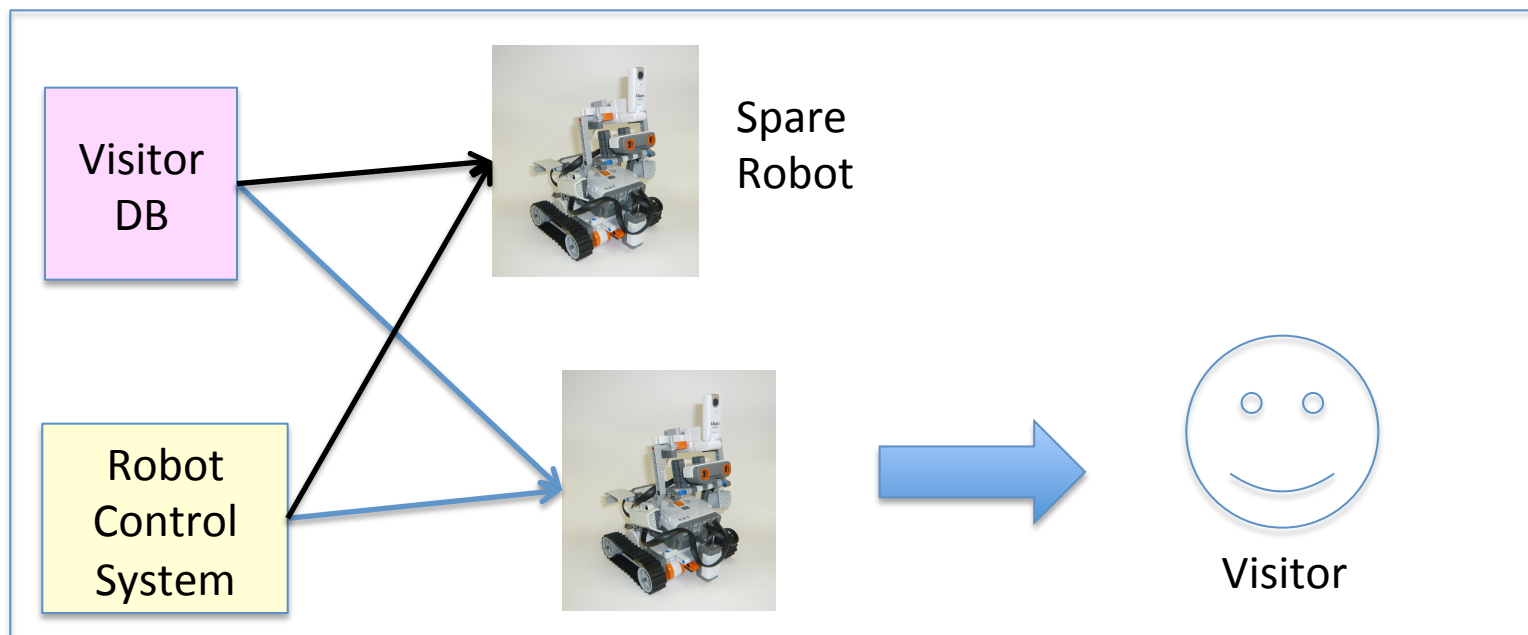
AC working library in Japan

- Over 50 ACs in GSN since 2010, www.dcase.jp
- Size
 - 10 - 200 nodes, Ave. 63.5 (SD: 47)
 - 2 - 6 Depth, Ave. 4.1 (SD: 1.03)
- Contents
 - Fault Tolerance AC
 - DEOS Demo System
 - System Safety, Dependability AC
 - ISO26262, Automotive, Micro Satellite,
 - Situational AC (Specific Context, Stakeholders, Goal)
 - Mitsubishi Elect., Denso Create, Fuji Xerox, ...



AC 1: Reception Robot Fault Tolerant (2010)

- Prepare a spare robot, and implement Fail-Over mechanism. By Fail-Over, in most cases, visitor only needs to wait 10 seconds when a failure occurs. In worst case (both robots are unavailable), visitor must wait 5 minutes.
- Goal ``Robot recovers from failures within acceptable time''





Top Level

Context:C_1

- Reception Service is delivered by a camera robot consisting of Camera component and Robot component.
- There are a redundant pair of camera robots: Primary Camera Robot and Backup Camera Robot.
- Acceptable time limit for recovery is 10 seconds when Backup Camera Robot is functioning, otherwise 5 minutes.

Goal:G_1

Reception Service recovers from failures within the acceptable time limit

Strategy:S_1

Argument across failure detection and recovery action

Effective for Explicitly Presenting FT mechanism

Risk Analysis Results

Context:C_2

To detect a failure is to monitor for it and to alert Maintenance Personnel when it occurs.

Goal:G_2

Service failures are detected when they occur.

Goal:G_3

Reception Service recovers from a detected failure within the time limit

Strategy:S_2

Argument across monitoring and alerting

Strategy:S_3

Argument by cases

Goal:G_5

Maintenance Personnel is alerted when a failure occurs

Goal:G_6

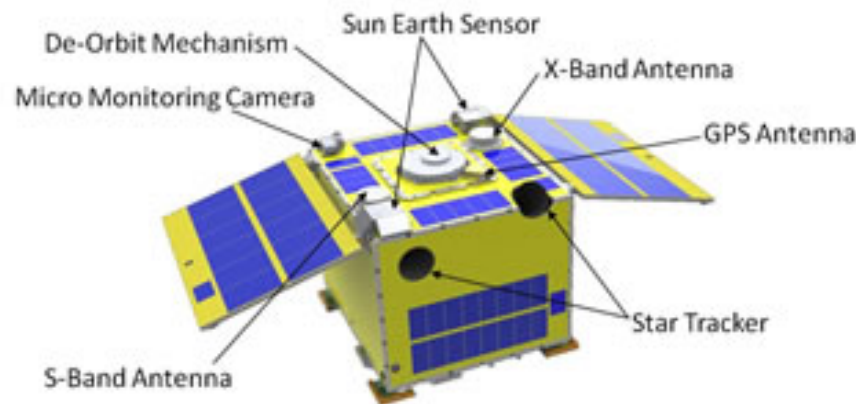
If Backup Camera Robot is functioning, then it resumes Reception Service within 10 seconds.

Fault Tolerance AC



AC 2: Micro Satellite AC (2013)

- “Battery will never die”
- The developer (MS student) himself wrote AC according to the V model development process



<http://park.itc.u-tokyo.ac.jp/nsat/hodo2.html>



Micro Satellite AC

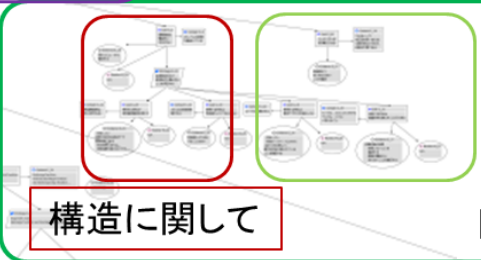
200 nodes,
1 month

System
AC

FTA results are attached
as Evidence



Battery will never die
Defs (Environment, Operation, NASA Req.)



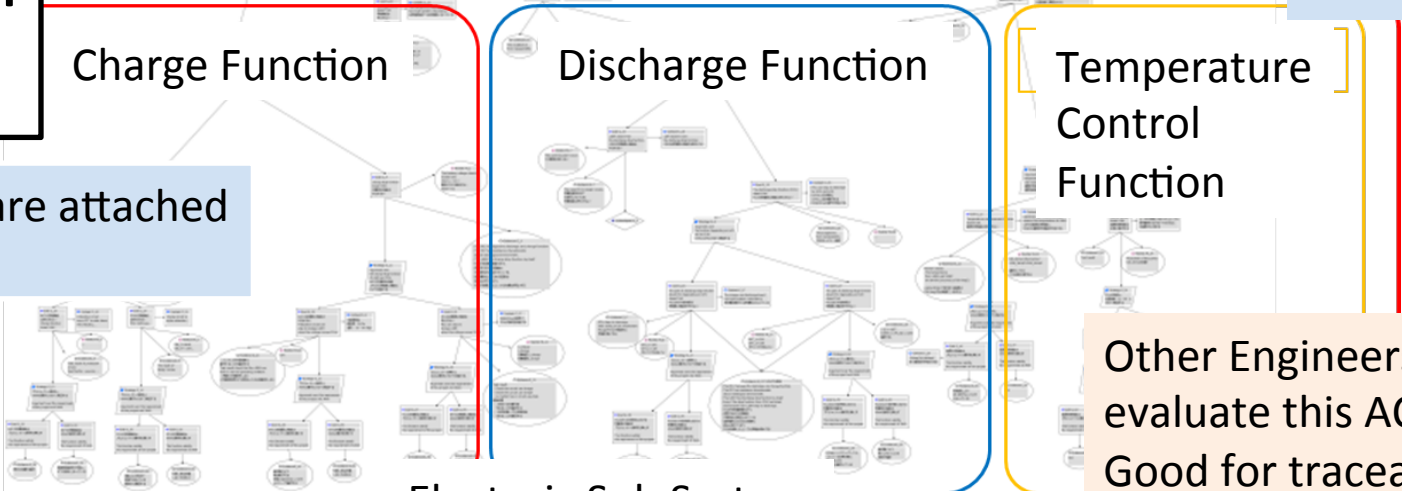
Argument over
Structure based on
V development model

Argument over
functions

Charge Function

Discharge Function

Temperature
Control
Function



Electroic Sub System

Other Engineers
evaluate this AC is
Good for traceability and
explanation



AC 3: for Mitsubishi Simulator (2014)

Simulator for
Setting relative order
Of parameters

Relative ordering
Of simulation parameters
Can be done

Explicitly show that
There are experts
knowledge

Argument with and
without Experts
knowledge

Experts knowledge
documents

Relative ordering
Can be done in the
Condition when
Experts knowledge
exists

Relative ordering
Can be done in the
Condition when
Experts knowledge
Does not exist

<https://www.ipa.go.jp/files/000046465.pdf>



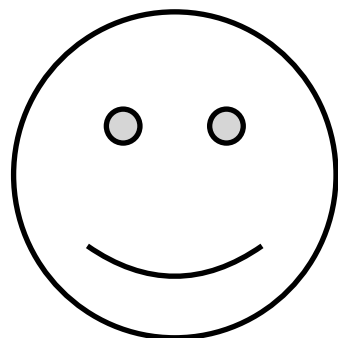
Simple Observation

- System AC
 - General Goal: System is safe, secure, ...
 - Typical Arguments (Argument over sub systems,...)
 - FTA, FMEA results as contexts and evidence
 - Huge Cost -> Automation and Verification Needed
- Situational AC
 - Specific Goal: “Relative Ordering of Simulation Parameters can be done”
 - Situation Dependent Arguments, 20~ nodes
 - Low Cost



Situational AC

Mitsubishi Case

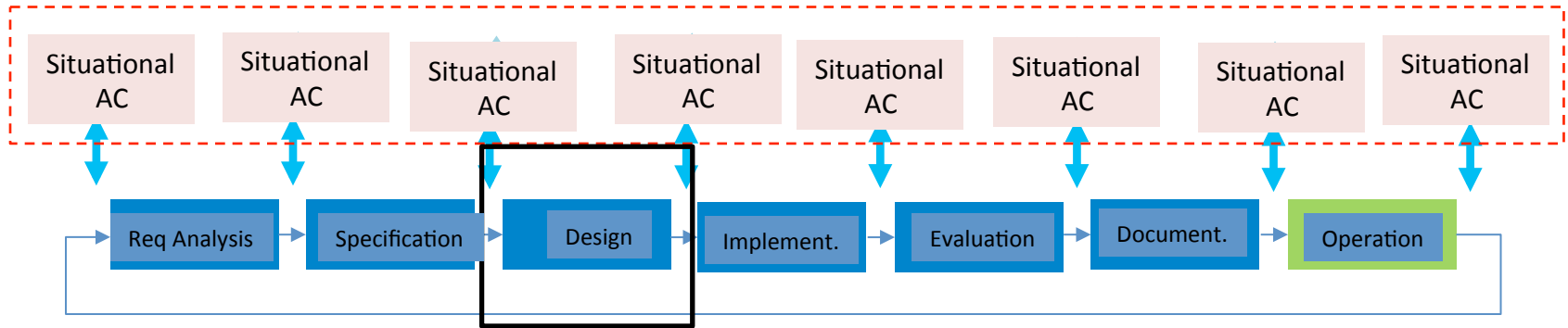


Designer

Relative Ordering of Simulation parameters Can be done



Expert





Answers for AC challenges?

- When, who write and evaluate?
 - In a situation, by Stakeholders in which assumption, culture may be different
 - Ex. Automotive and Supplier Companies in design phase
- Goal, Argument Structure
 - Specific (not necessarily directly related to safety, security, ...) and understandable for all stakeholders
- Granularity, Size
 - At most 20 nodes (in GSN), within a Power Point slide



Tool (DSN 2014 paper)

- Design and Implement GSN tool
(D-Case Editor, www.dcase.jp)
 - Formalize GSN community Standard using Functional Programming Language Techniques
 - Pattern (parameter, loop, choice, multiplicity) and Module System

Design and implementation, and then verification



Concluding Remarks

- Dependability is Consensus Building
 - Assurance Case is a method for that
- System AC (huge cost, automation and verification required) and Situational AC (lightweight, practical)



Concluding Remarks

- DEOS Consortium
 - www.deos.or.jp
- D-Case Working Group
 - www.dcase.jp
 - Started writing Situational AC with Japanese Automotive companies
- D-Case Certification Scheme started in 2015.6
 - D-Case Syntax (Based on DSN2014 paper)
[Astah/GSN](#) Certified!
 - D-Case Syllabus [Denso Create](#) Certified!



D-Case
Project
Logo