Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

SATURN 2006 Working Session: Strategic Risk Management for Architectures

DRAFT – Work in Progress
This summary is meant to convey preliminary ideas for the purpose of getting feedback. It does not necessarily represent the consensus of the members of the session.

Sponsored by the U.S. Department of Defense

Carnegie Mellon
Software Engineering Institute

Plan for the Workshop

To determine an effective risk management plan for an architecture, you need to answer the following questions:

- How do you plan for risks?
- How do you estimate risk exposure?
- What risk assessment/reduction techniques do you use?
  - For which attributes?
- What are their costs?
- What is their effectiveness (in terms of risk reduction)?
- *How do you know?*

- In this workshop we wanted to elicit the above…

Carnegie Mellon
Software Engineering Institute

Project Attributes

A1: Worst-case Performance (priority inversion, queue overflows)
A2: Availability/Robustness (No single point of failure)
A3: Ease of integration
A4: Usability
A5: Performance (no missed data frames)
A6: Cost
A7: Development Schedule
A8: Portability/Replaceability
A9: Maintainability
A10: Scalability
A11: Testability
A12: Understandability
A13: Resource Utilization
A14: Security

Attribute Assessment Techniques

T1: SAAM	T7: ALMA
T2: ARID	T8: OCTAVE
T3: FRAP	T9: QAW
T4: Model Checking	T10: Markov Modeling
T5: ATAM	T11: CBAM
T6: ALPSM	T12: RMA

Carnegie Mellon
Software Engineering Institute

S(L) and P(L)

Attribute i (Ai)	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14
Loss potential (Ai)	100	90	90	80	60	30	50	20	10	10	60	10	90	60
P_{before}(Ai)	6	5	20	15	20	5	20	10	10	10	30	20	50	40

Cost of Assessments

Cost of assessing Ai with Tj	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14
T1	50	x	10	70	10	x	x	x	x	50	5	x	10	x
T2	100	x	x	100	100	x	x	x	x	x	x	x	x	x
T3	x	x	80	80	80	x	x	x	x	x	x	x	x	x
T4	100	90	x	x	19	x	x	x	x	x	x	x	x	x
T5	70	100	70	70	70	x	x	x	x	x	x	x	x	x
T6	30	30	30	30	30	x	x	x	x	x	x	x	x	x
T7	x	x	x	x	x	5	10	x	5	5	3	x	3	x
T8	x	x	x	x	x	80	70	x	80	80	x	x	x	x
T9	x	x	x	x	x	x	3	10	20	20	20	10	20	10
T10	60	x	x	60	50	40	50	50	50	40	40	20	40	20
T11	60	x	90	60	60	x	x	x	x	50	10	x	10	x
T12	x	x	x	x	x	5	5	10	10	10	10	5	x	x
T13	30	x	x	30	30	x	x	30	x	30	5	x	30	x
T14	100	x	x	100	100	x	x	x	x	100	5	x	100	x

P(L) After Assessment

P_{after}(Ai) using Tj	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14
T1	4	x	15	12	15	x	x	x	x	5	15	x	20	x
T2	6	x	x	13	15	x	x	x	x	x	x	x	x	x
T3	x	x	15	12	13	x	x	x	x	x	x	x	x	x
T4	6	0	x	x	19	x	x	x	x	x	x	x	x	x
T5	6	2	2	13	18	x	x	x	x	x	x	x	x	x
T6	6	2	5	13	19	x	x	x	x	x	x	x	x	x
T7	x	x	x	x	x	2	15	x	8	10	30	x	30	x
T8	x	x	x	x	x	1	10	x	7	9	x	x	x	x
T9	x	x	x	x	x	x	10	4	6	8	25	20	30	30
T10	6	x	x	12	19	3	15	8	8	8	27	20	30	20
T11	3	x	15	5	5	x	x	x	x	5	5	x	5	x
T12	x	x	x	x	x	3	18	9	10	10	30	20	x	x
T13	5	x	x	12	15	x	x	5	x	6	20	x	28	x
T14	3	x	x	3	5	x	x	x	x	5	10	x	20	x

Carnegie Mellon
Software Engineering Institute

The Results

We mainly focused on identifying architectural risk assessment techniques.
We also examined a small amount of cost data.

Carnegie Mellon
Software Engineering Institute

The Results - 2

Security
- Series of characteristics in DoDAF, their security checklist
- ATAM like reviews with scenario generation and analysis only focusing on information assurance
- Boeing - PASM, largely DoD-based checklist style for qualitative security assessment

COTS Assessment
- Assessment techniques for COTS (book by Lewis et al)

Testability
- Scenario-based testing

Project Management
- Time box scheduling
- Scope reduction
- Periodically re-compute cost to complete and time to complete to address schedule and cost risks to see how much more resources are left

Carnegie Mellon
Software Engineering Institute

The Results - 3

Performance

- Boeing – RACM for changing or new technologies.
- Boeing – PAPM for performance and scalability
- Instrumentation
- Modeling Tools, e.g. SLAM-2
- Build executable architectures with stubbed components to look for risks
- Simulation
- Experimenting for performance, scalability

Availability

- Boeing - PAAM for availability analysis.
- Experimenting for availability

Safety

- HazOp, fault-tree analysis, …

Interoperability

- Inspections for measuring interoperability: look at data exchanges

Carnegie Mellon
Software Engineering Institute

The Results - 4

Modifiability
- Checklists for modifiability
- Experimenting for modifiability

Usability
- Rapid application development, GOMS, paper prototypes, visual basic mock-ups

Generic Risk Awareness
- Record assumptions from developers and use them as input to the list of risks.
- Argumentation, structured argument to find the risks – global structuring notation

Carnegie Mellon
Software Engineering Institute

Cost Data

Boeing's ATAM cost data: 730 hours +/- 10-20%
Boeing's own tools: 3-16 person-weeks (depending on project size/scope)
Cherokee's CMMD: 3-5 x cheaper than Boeing and ATAM (!)

Carnegie Mellon
Software Engineering Institute

The Final Result

Proposal: A “center of excellence” for exchanging information regarding techniques, their costs, their effectiveness (in terms of risk reduction).