Measuring Dependability as Mean Failure Cost

Ali Mili, NJIT
Frederick Sheldon, ORNL
CSIIRW, May 2007

Motivation

MTTF of System S with respect to specification R is M: mean time to next failure to satisfy R.

Two implicit assumptions:

- Independence wrt Subspecification. R is a monolith. Failing any requirement.
- Independence wrt Stakeholder. All stakeholders have the same stake in failure free operation.

Motivation

Distinction between

- Reliability: failure with respect to low stake requirements.
- Safety: failure with respect to high stake requirements.
- Security: failure with respect to security requirements.

Necessary distinctions?

Proposal

Wish List

- Varies according to which requirement is violated.
- Varies by stakeholder.
- Continuum of failure costs.
- Captures requirements dependencies (subsumptions, redundancies).
- Integrated measure of failure cost, regardless of source.

Tentative formulation

- Mean Time To Failure:

$$MTTF = \sum_{T>0} T \times P(t = T).$$

- Mean Failure Cost:

$$MFC(\sigma) = \coprod_{R_i} P(\overline{S \text{ õõ} R_i}) \times C(\overline{S \quad R_i}, \sigma),$$

Must be heavily qualified. Not really a sum.

Decision Support

- MTTF: Go iff

$$\frac{OpTime}{MTTF} \times FailCost << Benefit.$$

- MFC: Go iff

$$MFC << ServiceValue.$$

Quantification Infrastructure

- MTTF: Probability distribution of failure.
- MFC:
  - Probability distribution of failure with respect to various sub-specifications. Depends on sub-spec, and on V&V effort.
  - Cost matrix, stakeholder vs sub-specification.

Difficulty: sub-specifications overlap. Decompositions vary by stakeholder. MFC is a sum only for orthogonal sub-specifications.

Quantification Infrastructure: An Example

	SubSp1	SubSp2	SubSp3	SubSp4	SubSp5
StHld1					
StHld1			Cost		
StHld1					
StHld1					
StHld1					

Flight Control System, Stakeholders

- Pilot
- Passenger
- Aviation authorities (FAA)
- Environmental organization
- Airport area residents
- CEO, airline
- CEO, aircraft manufacturer
- CEO, insurance company

Flight Control System, Requirements

Requirements (naïve). User driven decomposition ≠ V&V decomposition ≠ Designer decomposition

- Smooth ride
- Adherence to flight vector
- Timeliness
- Fuel efficiency
- Noise pollution standards
- Responsiveness to AP setting
- Avoid reversing thrust in mid air
- Avoid stalling conditions

<u>Overlap significantly</u>.

Flight Control System, Stakes

- CEO of Airline, Fuel Efficiency: Bottom Line.
- Passenger, Fuel efficiency: 0.
- CEO of Airline, timeliness: corporate image.
- Passenger, timeliness: scheduling inconvenience.
- Safety requirement, passenger: Life.
- Safety requirement, CEO of airline: corporate image.
- Safety requirement, manufacturer: future sales.
- Safety requirement, insurance company: value of insurance claims.

Quantifying MFC

Key Construct: Requirements Structure.

Requirements Specifications: ordered by refinement. Partial ordering.

Lattice Properties: Semi Lattice. Join exists conditionally (adding requirements). Meet exists unconditionally (common requirements). Universal lower bound. No universal upper bound.

Lattice-like Structure

Specification Structure

- Compound/ Composite Specifications:

$$R = \coprod_{1 \le i \le n} R_i .$$

- Composition is neither unique, nor orthogonal.
- Illustration:

$$\begin{aligned} & 1155 \\ & = 15 \oplus 21 \oplus 33 \oplus 35 \oplus 55 \\ & = 105 \oplus 3 \oplus 11 \oplus 7 \oplus 55 \\ & = 3 \oplus 5 \oplus 7 \oplus 11 . \end{aligned}$$

Computing MFC

- Specification,

$$R = \coprod_{1 \le i \le n} R_i .$$

- Mean Failure Cost, if Ri's are independent:

$$MFC(\sigma) = \sum_{R_i} P(\overline{S \text{ õõ} R_i}) \times C(\overline{S \quad R_i}, \sigma).$$

Requirements Independence

Independent Sub-specifications:

$$R_1 \otimes R_2 = 0.$$

Interpretation: Relatively prime.

Implications

$$P(S \text{ õõõ } (R_1 \oplus R_2)) = P(S \quad R_1) \times P(S \quad R_2).$$

$$C(\overline{S \text{ õõõ } (R_1 \oplus R_2)}) = C(\overline{S \quad R_1}) + C(\overline{S \quad R_2})$$

- Interpretation: being multiple of 11 makes no difference whether number is or is not multiple of 15. Being multiple of 9 makes us more likely to be multiple of 15.

General Case

- Stakeholders know failure costs of arbitrary sub-specifications. Needed: identities that allow us to derive failure costs of independent (orthogonal) sub specs.
  - Refinement Identities,
  - Lattice Identities.
- Probabilities: textbook material.

Cost Identities

- Refinement Ordering:

$$R_1 \sqsubseteq R_2 \Rightarrow C(\overline{S \quad R_1}) \geq C(\overline{S \quad R_2}).$$

- Refinement Lattice:

$$C(\overline{S \quad (R_1 \oplus R_2)}) = C(\overline{S \quad R_1}) + C(\overline{S \quad R_2}) - C(\overline{S \quad (R_1 \otimes R_2)}).$$

Conclusion/ Summary

Mean Failure Cost

- Acknowledges variance in failure cost by stakeholder.
- Acknowledges variance in failure cost by requirement.
- Provides uniform metric for many dimensions of dependability.
- Consistent with spirit of Value Based Software Engineering.

Very speculative; very preliminary. Urgent: sample application.