Session 5
Evidence and Assessment II

From Fault Injection-based Assessment to Dependability Benchmarking: A 4-Way Street or a Long and Winding Road? , Jean Arlat, LAAS-CNRS.

Developing and evaluating critical software for space systems, Lothar Winzer, ESA/ESTEC

Jean Arlat

- Fault Injection – two main uses
  - Assessment of a single system (coverage, recovery time, etc.
  - Benchmarking (comparison of systems, mechanisms, etc)
- Historic overview – many techniques
  - Hardware based, software based, radiation,
  - Simulation at different abstraction levels
- FI serves as a complement to modelling, field failure data collection, etc.
- Farm – Faults, Activations, Readouts - > Measures
- Partial assessment
  - No info about fault rate.
- Coverage estimation
  - Coverage factor – introduced by Carter et al. in 1969

Jean Arlat (2)

- Coverage estimation
  - Impact of observation time
  - Time-dependent vs Asymptotic coverage
- Sampling the fault-activation space
  - Simple sampling vs stratified sampling
  - How to select meaningful faults? (Mirek)
- Benchmarking
  - Need for agreement on the FARM attributes and FI interface
- Future needs and issues
  - Work on faultload representativeness
  - Fault collapsing techniques
  - Security – attacks and vulnerability

Lothar Winzer (1)

- Do's and Dont's in evaluation of critical software
- Examples of major failures of space missions
- Achievements – Processes in place
  - Software process assessment and improvement
    - SPICE for space
    - 30 assessements over 6 or 7 years
  - Evaluation for re-use of software from previous missions
    - Suppliers sometimes think re-validation is too heavy
  - Third party assessment
    - ESA standard, used in all lifecycle phases

Lothar Winzer (2)

- Work in progress
  - Software Quality Modeling and Metrication
    - Past effort: 80 metrics: too many
    - New effort: fewer metrics
    - User involvement in metrics definitions? (John M)
    - Consideration of operability ?(Michel)
      - No(?)
    - Who gets the blame if anything goes wrong? (Roy)
      - Translate into lessons learnt
  - Use of COTS SW & OSS in Critical Functions
  - Model based Validation of RAMS Requirements

- Less successful areas
  - RAMS at Software Level
  - “Certification” of Software Products
  - Risk Management using Process Assessment Results

Lothar Winzer (3)

- Things not in the list
  - Software Reliability Modelling
  - N-version programming
- Discussion
  - What about the inadequacies? (Roy)
    - Lothar: Time and Money is the problem
  - Problem of testing at the end of the lifecycle.
  - How to validate metrics
    - Lothar: Use commercial metrics tools.

Session 4
Evidence and Assessment I

Challenges on safety Evaluation in Future rail and Air Transportation Systems, Joao Batista Camargo, USP, Brazil

Railway Safety Assessment Processes: the past, the present and possible future challenges, Federico Caruso, RINA, Italy

Joao Batista Camargo

- Comparison of standards
  - Meta standard (IEC 61508)
    Human factors

ISO26262 - Methods and measures for system integration

Methods and measures		According to req.	ASIL			
			A	B	C	D
1	Requirements-based tests[a]	7.4.3.2	++	++	++	++
2	Back-to-back tests[b]	7.4.3.2	o	+	+	++
3	Tests of external interfaces[c]	7.4.3.2	+	++	++	++
4	Interface consistency check[d]	7.4.3.2	+	++	++	++
5	Tests of internal interfaces[e]	7.4.3.2	+	++	++	++
6	Communication tests[f]	7.4.3.2	++	++	++	++
7	Tests of interaction/communication[g]	7.4.3.2	++	++	++	++
8	Fault injection tests[h]	7.4.3.2	+	+	++	++
9	Error guessing tests[i]	7.4.3.2	+	+	++	++
10	Tests derived from field experience[j]	7.4.3.2	o	+	+	++
11	Resource usage tests[k]	7.4.3.2	o	+	+	++
12	Performance tests[l]	7.4.3.2	o	+	+	++
13	Stress tests[m]	7.4.3.2	o	+	+	++
14	Tests for interference resistance/robustness and under certain environmental conditions[n]	7.4.3.2	++	++	++	++

Federico Caruso

- History
  - From ropes to FPGAs
- SIL 4 always required
- ALARP
- European consensus
- Validation of Functional Requirements
- Discussion