D-RisQ

SOFTWARE SYSTEMS

Changing the way the world thinks about software systems

Theorem Proving Conference Cambridge

9/10 December 2013

Sub-Topic 1

Standards Relationships

Nick Tudor: njt@drisq.com

ToRs – Stream 1

- Relationship with existing industry standards and guidelines used by certification authorities such as RTCA DO-178C, ISO26262, ...
- "Packaging" of TP results for submission to certification authorities, i.e., specific guidance for how certification authorities should expect verification results obtained by means of TP should be recorded and delivered as part of the “certification package”.

DO-178C – DO-333

- Now recognised by both FAA and EASA
  - NB still requires some test
- DO-333 sets out FM Objectives that align with DO-178C test based Objectives
  - Planning, QA, CC and Cert liaison in DO-178C
- Text relating to Tables FMA2-A7 (ie verification) has:
  - New, modified/additional text
  - Tables FMA2-7 have new FM specific Objectives
  - Table FMA7 has completely replaced equivalent DO-178C

The Main Formal Challenges - 1

- Within DO333 the formal method should be correctly defined and justified
  - This is an ‘Objective’ repeated for HLR, LLR, source code, coverage
- These are the related ‘Activities’:
- All notations used for *formal analysis* should be verified to have precise, unambiguous, mathematically defined syntax and semantics, that is, they are *formal notations*
- The soundness of each *formal analysis* method should be justified. A sound method never asserts that a *property* is true when it may not be true
- All assumptions related to each *formal analysis* should be described and justified, for example, those assumptions associated with the target computer or about the data range limits

D-RisQ
SOFTWARE SYSTEMS

2 More FM Objectives for DO-333

- Objective: Formal analysis cases and procedures are correct
    - Covers Objectives for HLR, LLR & Source code
    - Assumptions are correct
    - Procedures and cases were accurately developed
- Objective: Formal analysis results are correct
    - Means discrepancies are explained

D-RisQ
SOFTWARE SYSTEMS

Final [& Crucial] FM Objective

- Objective: Formalization is correct
  - This means that the translation to the formal representation has to be justified
  - Note this is a unique objective within the DO-178 suite of documents!
  - review or analysis should be used to demonstrate that the formal statement is a ‘conservative representation’ of the informal requirement.
- Note: If the gap between an informal statement of the requirement and its embodiment in a formal notation is too large, then this may be difficult to review. The preciseness of formal notations is only an advantage when they maintain fidelity to the intent of the informal requirement

ISO26262

- Has indirect and direct reference to the use of FM
  - Specific reference in Part 6 (Software)
  - Implicit use can be found in Part 4 (Architecture)
- FM are ‘Recommended’ not ‘Highly Recommended’
  - Means their use has to be justified over ‘Highly Recommended’ techniques
- Similar approach in other related standards
  - IEC61508, EN50128
  - NB North Europe now expects FM ie they are HR

Relevance to ISO26262-4

7.4.3 Measures for the avoidance of systematic failures

Table 1 — System design analysis

Methods		ASIL			
		A	B	C	D
1	Deductive analysis [a]	o	+	++	++
2	Inductive analysis [b]	++	++	++	++

[a] Deductive analysis methods include FTA, reliability block diagrams

[b] Inductive analysis methods include FMEA, ETA, Markov modelling

NOTE 1 The purpose of these analyses is to assist in specifying the design. At this stage, qualitative analyses are likely to be appropriate and sufficient. Quantitative analyses can be performed if appropriate.

NOTE 2 The analysis is conducted at an appropriate level of detail.

A Formal approach can support system and architecture analysis

More Relevance to ISO26262-4

7.4.8.1 System design shall be verified for compliance and completeness with regard to the technical safety concept. In this aim, the methods and measures in Table 2 shall be considered.

Table 2 — System design verification

Methods		ASIL			
		A	B	C	D
1a	System design inspection [a]	+	++	++	++
1b	System design walkthrough [a]	++	+	o	o
2a	Simulation [b]	+	+	++	++
2b	System prototyping and vehicle tests [b]	+	+	++	++
3	Safety analyses [c]	see Table 1			

[a] Methods 1a and 1b serve as check of complete and correct detailing and implementation of the technical safety requirements into system design

[b] Methods 2a and 2b can be used advantageously as a fault injection technique

[c] For conducting safety analyses, see ISO 26262-9: —, Clause 8.

A Formal approach can support system and architecture verification

Relevance to ISO26262-6

- Table 1 – Enforcement of coding, design, etc
- Table 2 –Verification of requirements
- Tables 3 -7 – Notations, principles for software architecture design, error detection, etc
- Table 8 - 11 – Unit design notations, design, implementation and verification
- This is not an exhaustive or definitive list….

‘Packaging’

- There is no specific guidance on what needs to be presented in terms of ‘results’
  - Nor justification, soundness, etc
- Tool qualification probably helps
  - See DO330
  - Some related guidance in ISO26262
- Question therefore is what constitutes ‘suitable evidence’ and how should it be presented…and to whom?

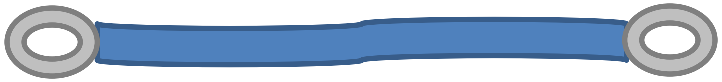
Example [safe/secure] Systems

Context of Use - Identified

Vulnerabilities Identified

User Manual Available

‘Qualified for Use’



What could possibly go wrong…?

D-RisQ

SOFTWARE SYSTEMS

Changing the way the world thinks about software systems