Potpourri of what?

One year in a DA's life

Aryldo G. Russo Jr, Thiago Sousa, Paulo Muniz,
David Deharbe, Haniel Barbosa

AeS Group

Dusseldorf 21/09/09

Agenda

- Introduction
- The AeS Group and Formal Methods
- Ongoing work

Introduction

- Many safety functions that were handled by hardware are now responsibility of the embedded software.
- Formal methods in standards relevant to software safety.
- One of the most widely used is the IEC 61508

Table A.1 – Software safety requirements specification (see 7.2)

	Technique/Measure*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Computer-aided specification tools	B.2.4	R	R	HR	HR
2a	Semi-formal methods	Table B.7	R	R	HR	HR
2b	Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	C.2.4	---	R	R	HR
NOTE 1 – The software safety requirements specification will always require a description of the problem in natural language and any necessary mathematical notation that reflects the application. NOTE 2 – The table reflects additional requirements for specifying the software safety requirements clearly and precisely.						
* Appropriate techniques/measures shall be selected according to the safety integrity level. Alternate or equivalent techniques/measures are indicated by a letter following the number. Only one of the alternate or equivalent techniques/measures has to be satisfied.						

The AeS Group and Formal Methods

- The AeS Group has developed railway sub-systems since 1998.
- Door system became one of the most important in the railway market
- AeS Group has acquired a reputation as a company that has the needed know-how to develop safety critical applications.
- AeS group decided to identify a formal method that would best fit the current CGP SIL 3-level requirements and railway industry standard practices and standards (as is the case of CENELEC EN 50128).

The AeS Group and Formal Methods

- The AeS Group, in 2006, started to provide Safety assessment services
- Since 2006 has participated in more than 10 projects involving formal methods.
- Those projects were related to equipment development, software development, and development process assessment (safety case generation, etc…)
- Only in the last year, AeS has grown around 500% due, in some part, the application of formal modeling.

Ongoing work

- A Methodological WRSPM Approach to a B Formalization in an Industrial Setting
- Lost & Found in Requirements - A Formal Help
- UPside Down, Another way to see the same thing - LADDER to B
- Using the B Formal Method in the process of traditional software development for critical systems
- A UML-based Method for Event-B Refinement

A Methodological WRSPM Approach to a B Formalization in an Industrial Setting

- Systematic approach to understand and organize requirements
- Increase traceability
- The results so far
  - Not possible to implement in B as it is;
  - Not possible to implement in Event B as it is;
  - ?!?!

Lost & Found in Requirements - A Formal Help

- The pilot project for DA program
- Small system with only few NL requirements
- Modeled in UML-B (only the abstract portion)
- Several gaps were found in the NL language spec, that forced clarification with the specialists, and, at the end to rewrite the NL spec
- New attempt now in formalize a safety function for hardware failure detection

UPside Down, Another way to see the same thing - LADDER to B

- A new starting project partially paid by Petrobras
- PLC usage in safety critical applications
- IDE with defined function blocks
- The formalism works behind the scene
- Attempt to use Event B

Using the B Formal Method in the process of traditional software development for critical systems

- A management project
- Set of metrics to compare Formal / Non Formal developments
- Door system case study
- Result: A Comparative Dossier

A UML-based Method for Event-B Refinement

- Incorporate Use Cases, Activity and Sequence Diagrams in UML-B
  - Use Cases for Requirements;
  - Activity for Event-B Refinement;
  - Sequence for Event-B Decomposition
- Get "UML-style" feedback for proof discharge
  - Get understandable feedbacks;
  - Provide alternative ways to fix the UML model

Future work

- Everything!!
- The project is about to start
- We already have (sort of)
  - Annotated use cases (automatic generation of abstract model)
  - Requirement modeling
- RODIN integration in the methodology
- Metrics
- Comparison with other languages

WOBD and SBMF 2010 – Natal – Brazil
8 – 12 - November

Thank You!!

Dusseldorf 21/09/09