Potpourri of what?

(A bit more than) One year in a DA’s life

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

AeS Group

Natal 8/11/10

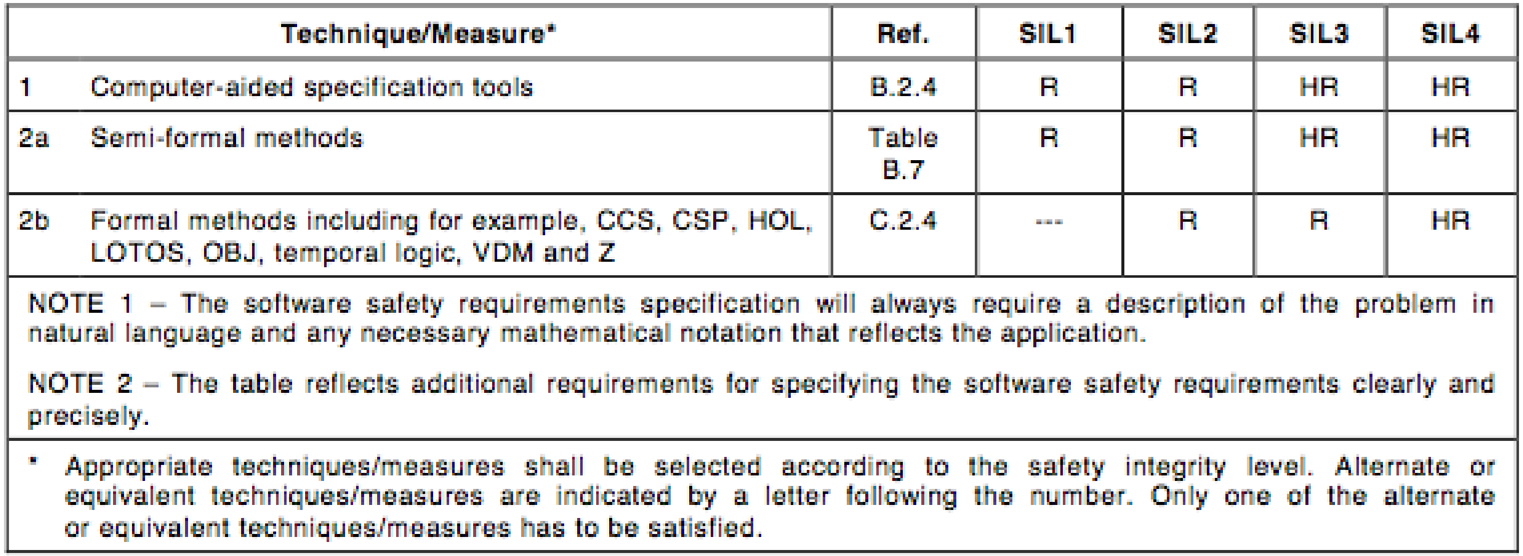
Agenda

- 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.

•We were recognized one of the best consultant in LATAM.

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
- Can we do better – change the way to vital verification

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

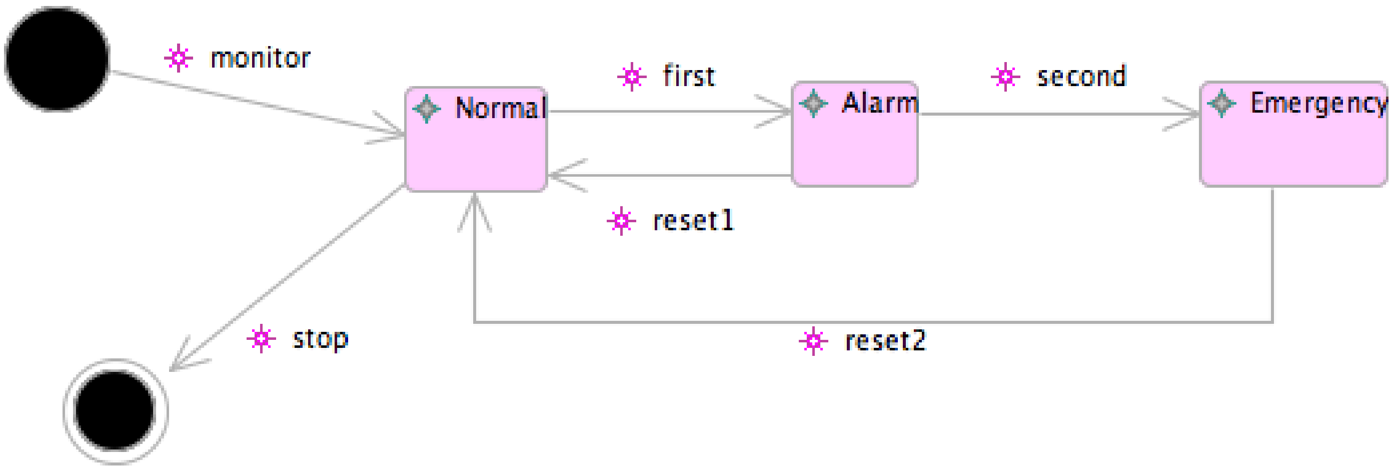
- The pilot project for DA program
- Small system with only few NL requirements
- Modeled in UML-B (only the abstract portion)

Lost & Found in Requirements - A Formal Help

- A small system that's used to stop the train when the operator is not possible any more to apply protection actions. This system is called "dead man control" and the basic requirements are: (the full requirements elicitation is also part of this research)
  - 1. if the train is in automatic mode, the dead man control must be disabled
  - 2. if the train is in manual mode, the dead man control must be enabled
  - 3. in manual mode the operator must push the control button each X seconds
  - 4. after X seconds, if the operator have not pressed the button the system must provide an alarm sound
  - 5. after X seconds after the alarm activation, if the operator has not pressed the button the system must stop the train
  - 6. in any time the operator press the button, the system must go back to the normal situation.

Lost & Found in Requirements - A Formal Help

The UML-B Abstract model



Lost & Found in Requirements - A Formal Help

•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

Can we do better – change the way to vital verification

- A way to help boolean verification
- Not new but still not used in large scale
- Nowadays, it’s done by hand, based on verifier expertise

Can we do better – change the way to vital verification

•What we received – Safety properties :

Bool_0027

No alinhamento de rota, o estabelecimento do perfil de velocidade deve obedecer ao sentido de tráfego estabelecido e as condições da via.

Can we do better – change the way to vital verification

- What we received – Boolean description and equations:

Seleção de Código de Velocidade

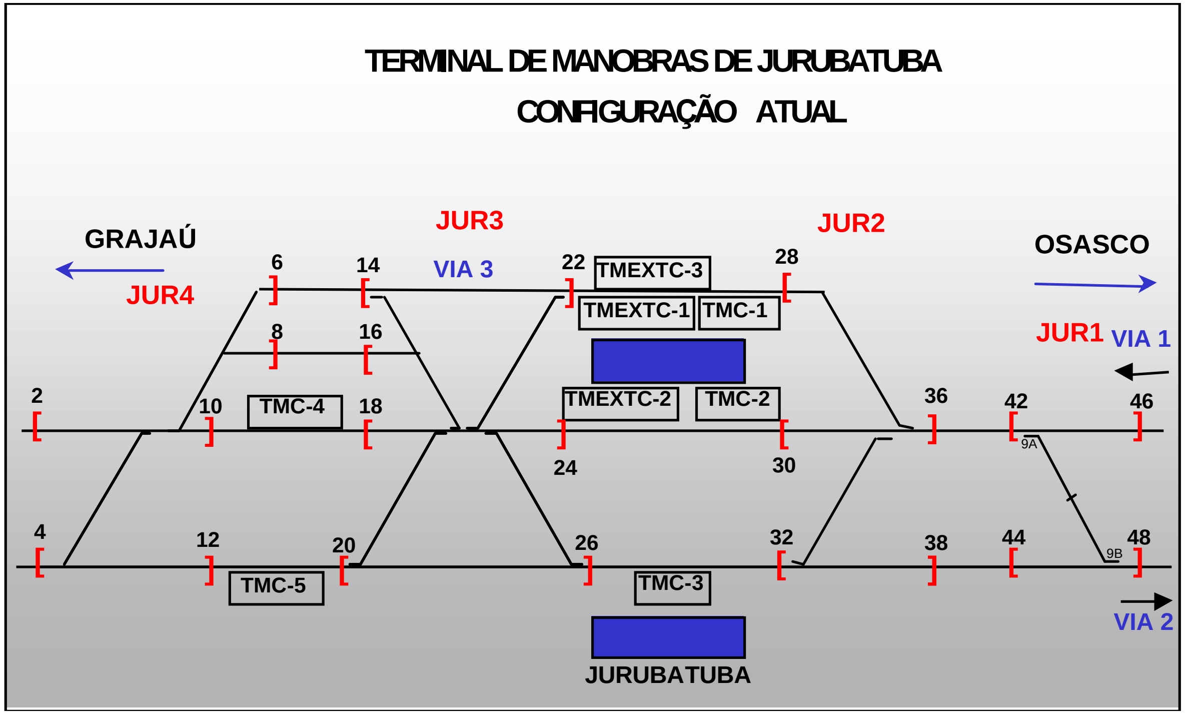
Finalidade:

Selecionar o código de velocidade em cada circuito de via, conforme determinado pelo Plano de Vias Sinalizadas.

Requisitos: **Bool_0001, Bool_0022, Bool_0023, Bool_0024, Bool_0025, Bool_0026, Bool_0027, Bool_0028, Bool_0029, Bool_0032, Bool_0042, Bool_0042, Bool_0043, Bool_0045, Bool_0046, Bool_0047, Bool_0054, Bool_0108, Bool_0113, Bool_0115, Bool_0116 e Bool_0138**

Can we do better – change the way to vital verification

- The Booleans are used to represent track configuration, like:



Can we do better – change the way to vital verification

- 3 big steps (Not necessary in this order)
    - Translate boolean equations to B
    - Collect the safety requirements
    - Formalize the safety requirements
- Begin the real formal verification
- Animate it!!!

Can we do better – change the way to vital verification

- First Boolean translation
  - CODVEL.DTA -> ALSTOM MACHINE

Can we do better – change the way to vital verification

- Collection of safety requirements
- Formalize it

Thank You!!