Formal Methods Outside the Mother Land (or BeVelopment?)

Aryldo G. Russo Jr

AeS Group

RIAB – Eindhoven 3/11/09

Agenda

- Introduction
- Past experiences
- Deploy Associate
- DA Project
- Future work

Introduction

- 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).

Introduction

- 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…)

Past experiences

- 2 examples
- Signaling system
- Door control system

Past experiences – Signaling system

- The new project was based on a previous one.
- The task consisted in implementing new functions and then revalidating all the system (about 4900 POs, 85% proved automaticaly)
- The changes were applied in the abstract model, and after that they were reflected in the refinements and implementation.
- New proof obligations were generated and the affected older ones were reapplied.

Past experiences – Signaling system

•No failures where detected after the deployment of the system.

•The associated costs in this development were less than in a traditional process as:

- •there were no needs of maintenance changes
- •the necessary time dedicated to testing was really short.

•But this job was performed by a company that has been using formal methods for a long time.

Past experiences – Door system

- Verify the consistency of a door system specification.
- RODIN was used as a proof of concept.
- The objective was to help the door system manufacturer to rewrite the specification based on the result of the verification of the formal model.
- The natural language specification is more than 100 pages long, and the needed information is spread out over all this specification.

Past experiences – Door system

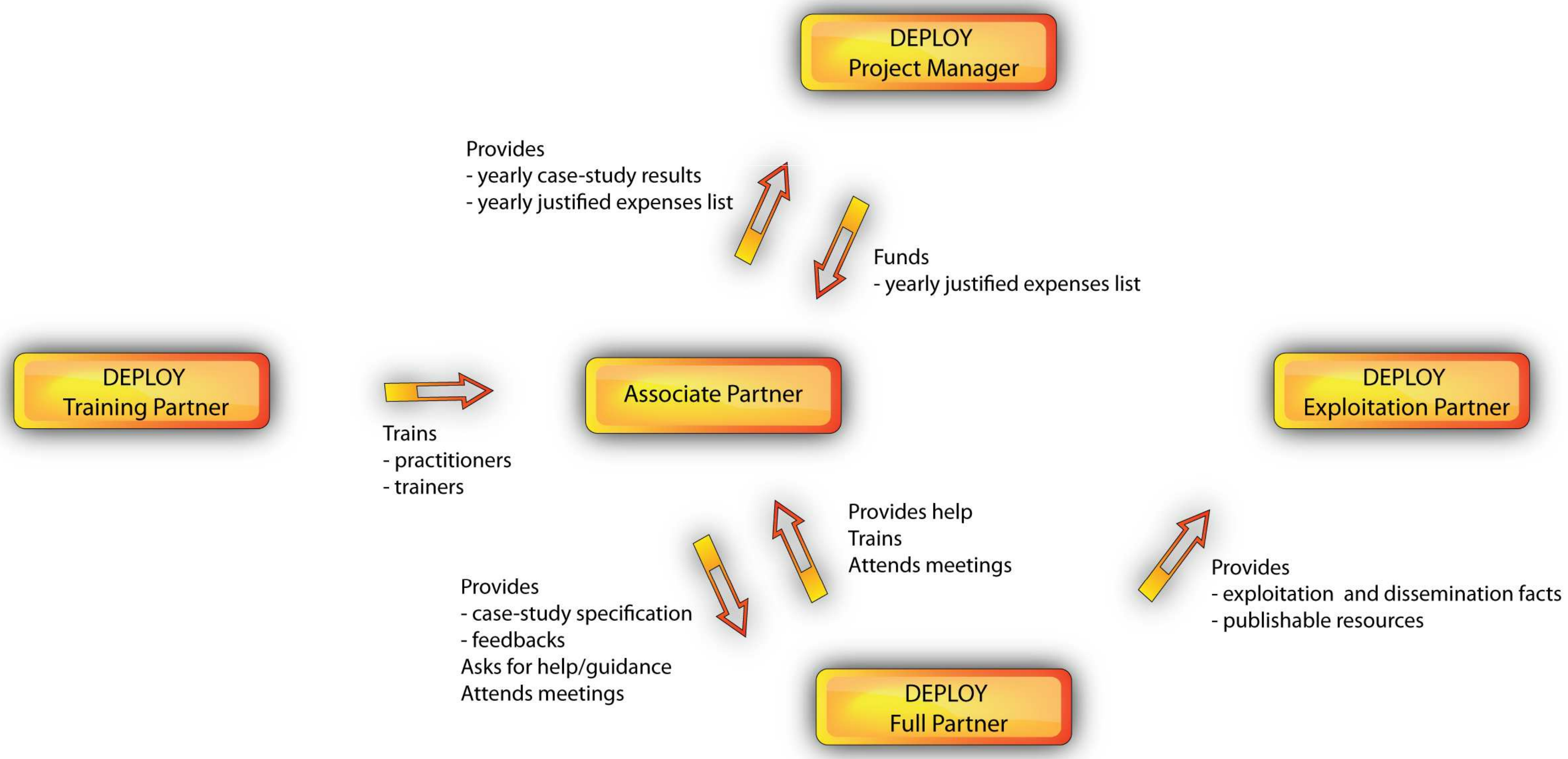
- This simple example helped to present the formal method benefits, stating the impossibility to introduce ambiguities and contradictions.
- The objective now is:
  - Try to represent the complete specification of one train sub-system
  - Reformulate the natural language specification in a better representation.
  - Pointing out the items that need to be revised to create a more consistent specification.

Deploy Associate – What?

•The main goal is to ensure broad dissemination of the results of the project (tools, methodology, documents, etc.) by:

- •experimenting on new case-studies, possibly from domains not yet addressed by the DEPLOY project
- •ensuring that adequate training is delivered to the *DA personnel in charge of the case –study,*
- •*collect feedback (metrics, models, conclusions, etc.) from DA, in order to improve project deliverables and to demonstrate the extent to which they are applicable to industry.*

Deploy Associate – Structure



DEPLOY
Project Manager

Provides
- yearly case-study results
- yearly justified expenses list

Funds
- yearly justified expenses list

DEPLOY
Training Partner

Trains
- practitioners
- trainers

Associate Partner

DEPLOY
Exploitation Partner

Provides help
Trains
Attends meetings

Provides
- case-study specification
- feedbacks
Asks for help/guidance
Attends meetings

Provides
- exploitation and dissemination facts
- publishable resources

DEPLOY
Full Partner

DA Project - BeVelopment

- Creation of a structured development process based on formal methods
- This structured development process must:
  - be able to be used by small companies but with the possibility to scale for the bigger ones;
  - be cost effective in terms to, at least, not increase the development costs;
  - be adherent to the current standards in the railway field;
  - and be able to be used by people with no strong mathematical knowledge

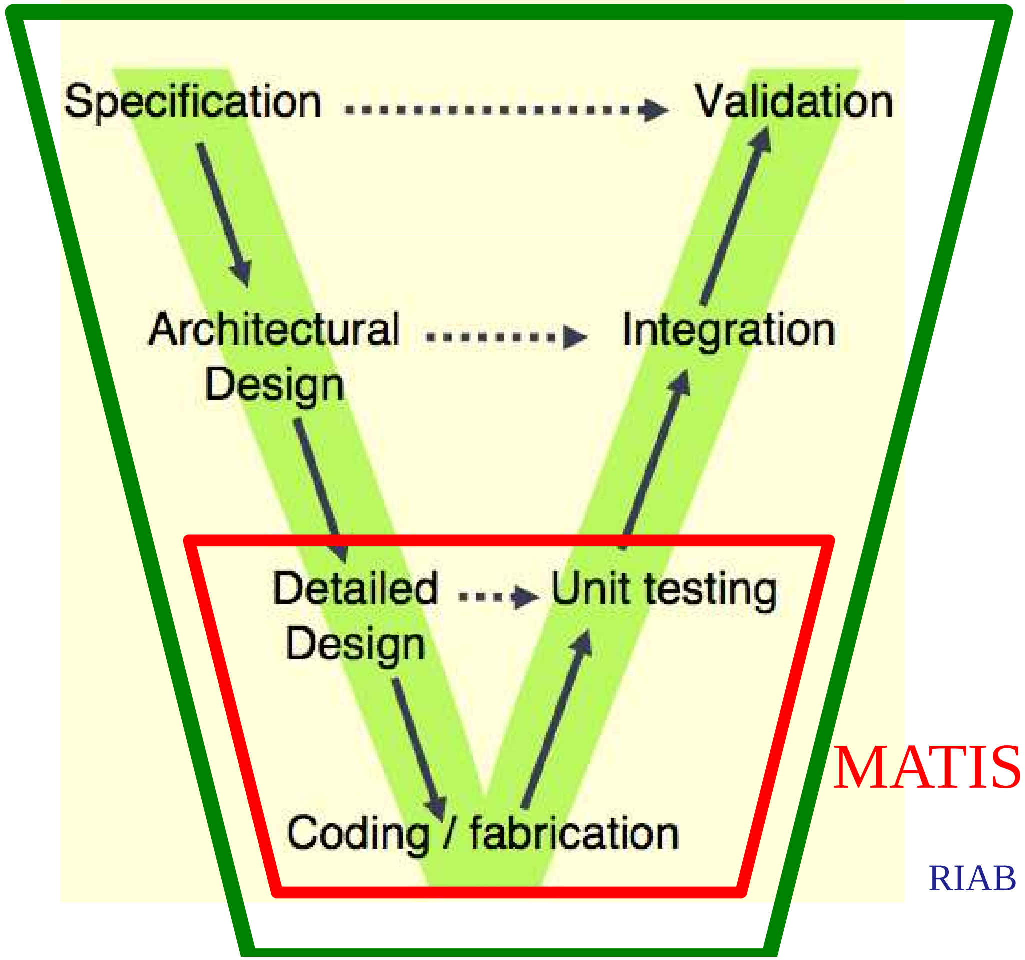
DA Project – Pilot project

- 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.

DA Project – Project details

- The main objective of this project is to create a useful methodology to be used during the development life cycle of safety critical systems, as follow:
    - A development life cycle *framework*. This framework must define what are the phases in this life cycle, and what are the inputs and outputs of these phases
    - 2. Techniques (or languages, tools, etc...), one of the expected results is the identification of what method and related tools would be suitable.
    - 3. A utilization (or application) method to state the steps that are necessary to succesfully achieve the objectives to avoid ”try and error” experiences.
    - 4. A methodology itself, needs to be a guide that state what intermediate tasks are needed in order to an output of a previous phase could be used as input of the next one.

Related work



Specification → Validation

Architectural Design → Integration

Detailed Design → Unit testing

Coding / fabrication

BeVelopment

MATISSE

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

Thank You!!