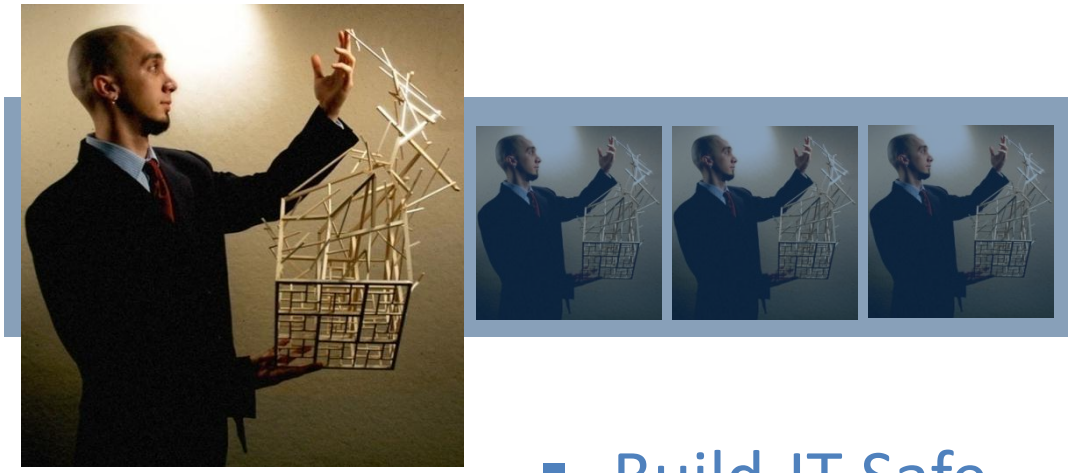
ALL4TEC - Etudes & Conseil

MBSAW 2012 : Build-IT Safe Project

Franck Sadmi – 11&12th September 2012

The Build-IT Safe project is supported by European Community FEDER-2007-2013

Contents



- Build-IT Safe
  - Project
  - Partners
  - Organisation
  - Roadmap
- Description of the tool
- Demo
- Questions / Next steps

The Build-IT Safe project (1/2)

- The problematic
  - Safety Analyses are necessary when developing critical systems
  - The cost of those activities must be reduced
  - Safety analyses must be more reliable than they are today (still often done at the hand) & more maintainable

- Title of the project
  - The main goal of the Build-IT Safe project is to propose a Demonstrator of a tool that will help make FMEA (Failure Mode and Effects Analysis) easier.
  - This tool will be automotive oriented and will offer automobile & equipment manufacturers appropriate support to make compliance with ISO 26262 easier (for the development of critical ECU's).

The Build-IT Safe project (2/2)

- The concerned parts of the ISO 26262
  - Part 3 : the tool will simplify the execution of those tasks : « hazard analysis and risk assessment » and « functional safety concept »,
  - Parts 4, 5, 6 : the approach is generic and the tool will be adapted to the architecture & design of the system (Part 4), hardware (Part 5) and software (Part 6).

- This project is financed by FEDER (ERDF: European Regional Development Fund)

Partners

Beginning of the project	May 2011
End of the project	May 2013

Project leader

ALL4TEC ETUDES & CONSEIL	Frédérique Vallée Franck Sadmi	ALL4TEC is a French-based company specialized in Process improvement, Safety engineering, System engineering and Testing of complex embedded systems.

Partners

GIE REGIENOV Recherche Innovation RENAULT	Youssef Laarouchi	RENAULT - Embedded Software Competency Group
cea list	Agnès Lanusse	the CEA LIST Institute focuses its research activities on developing innovative technologies for smart and complex systems.
FAAR industry	Adil Alif	FAAR Industry® specialized in the development and production of embedded electronic control systems for land and marine vehicles.

Organisation

Modeler

Demonstrator to perform safety analysis (FMEA)

Roadmap of the project

- The main steps of the Build-It Safe project
  - Development of a prototype implementing the FMEA principles based on the ALL4TEC methodology
  - Validation of the needs (requirements) by the users (Renault)
  - Specification & Development of a demonstrator interfacing the modelers Papyrus & Matlab/Simulink
  - Training of the actors to the methodology of the demonstrator
  - Test of the demonstrator on 1 or 2 pilot projects
  - Synthesis of all the results of this project on the technical & financial aspects

ALL4TEC FMEA method (1/2)

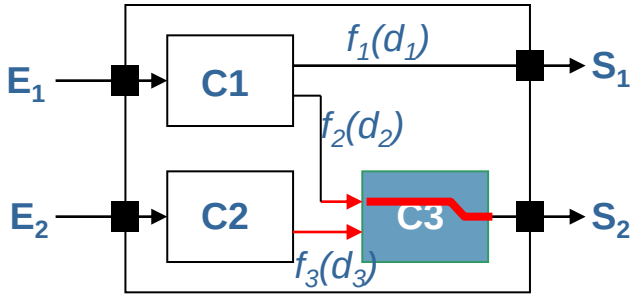
- Structured decomposition all the way down to elementary components (leaves)
- Local analysis on the leaves
  - Taking into account possible barriers
- Global analysis
  - Propagation of elementary failure modes to the specified Feared Event
- Results summarized into a FMEA table and/or a Fault Tree
- When necessary, design is enriched and analysis is done until the expected safety level is obtained:
  - Addition of new barriers

ALL4TEC FMEA method (2/2)

- **Local analysis**

  - Each block is independtly analyzed from others:

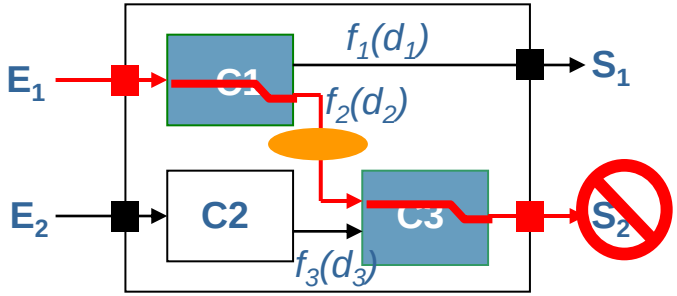
    - Linked outputs failure modes to inputs failure modes for a block (or to the internal failure of the block



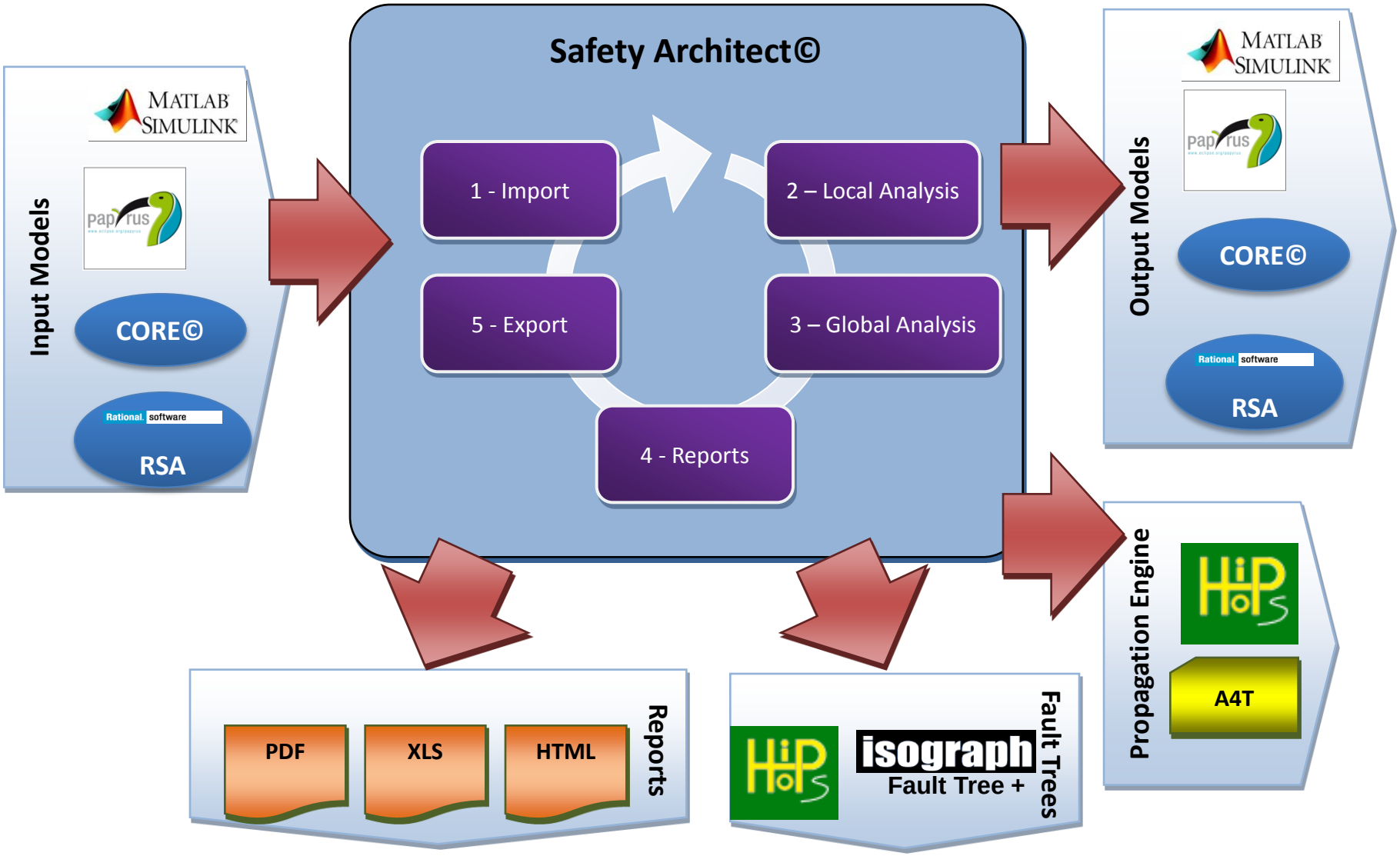
- **Global analysis**

  - Propagate all model failures to output feared events:

    - Identification of all critical paths which lead to each feared event



Overview



Safety Architect ROI

- Average gain on FMEA effort

Hyp. : FMEA effort without Safety Architect = 30 m.days

- If initial FMEA : gain > 15 m.days (50%)
  - Importation of the functional model: > 5 m.days
  - Local analysis automated: 0
  - Global analysis automated : > 5 m.days
  - Ease of reporting: > 5 m.days

- If rework of an existing FMEA: gain > 25 m.days (80%)
  - Importation of the functional model: > 5 m.days
  - Local analysis automated : > 10 m.days
  - Global analysis automated : > 5 m.days
  - Ease of reporting: > 5 m.days

Benefit of the tool

- FMEA automatic generation (all the methodology is driven by tools)
- Model based oriented (better understanding)
- Compliant with usual safety standards such as: ISO/CEI 61508, EN 5012x, ESARRs, ISO 26262 …
- Maintenability increased (model based)

Conclusion / Next Steps

- Prototype has been developed & validated
- Demonstrator is under construction
- Many reflexions have been done or are still in progress:
  - Corrrect use of SysML/UML modelers
  - Improvement of the ALL4TEC FMEA methodology
  - Definition of the components to import / modelize from Matlab/Simulink (interpretation of such constructions as S-functions, Matlab function,…)
  - Inject Safety informations in the modelers
  - Using more than only structural information from the model?
- Great interest & involvement of all the partners in this project