How to model faults on SW architectural level: an approach to ISO26262 SW safety analysis

Automotive SPIN Italia
11° Automotive Software Workshop
07/11/2012
Milan, Italy

ResilTech
Technologies for Resilience

RESILTECH

*Tech*niques and *Tech*nologies for *Resil*ience

- **Company**
  - SRL born in late 2007
  - Founded by
    - university researchers expert in resilient computing and
    - specialists in the industrial field of Verification and Validation (V&V) of critical systems
- **Mission**

  «To provide **engineering consulting and design services** to companies and public bodies mainly for, but not limited to, the field of **resilient systems and infrastructures**»

- **Research**
  - Strong relations with both universities and research institutes
  - Activities on FP7 projects
  - Artemis

SEVENTH FRAMEWORK PROGRAMME

ISTITUTO DI SCIENZA E TECNOLOGIE DELL'INFORMAZIONE "A. FAEDO"

ISTI-CNR (Pisa-italy)

Università degli Studi di Firenze (Florence-Italy)

- **Automotive Working groups**
  - ISO SC3/WG16 for ISO26262 ("Road vehicles - Functional safety")
  - AUTOSAR Phase III
    - WP 1.3 – Safety

AUTOSAR AUTOMOTIVE OPEN SYSTEM ARCHITECTURE

- **Automotive Certification**
  - Partnership with TUV-SGS for functional safety certifications

SGS SGS TÜV SAAR

SW Safety Analysis: ISO26262 - WG16 activities

- London meeting (June 2013)
  - Big discussion on common understanding of concept of Safety Analysis at SW level,
  - particularly on the concepts of SW faults and differences between SW and HW approaches, for instance related to FMEA-like methods of analysis.
  - Outcomes of the meeting were
    - different understandings are present,
    - It is important to provide some kind of clear guidance on application
- and next steps
  - Official SW sub group to be created under guidance of Part 6 responsible (UK).
  - Possibilities for guidelines to be included in first revision of ISO26262 or PAS document to be created.

ResilTech
Technologies for Resilience

SW “faults” issue 1/3

- To run safety analysis we often starts from the concept of fault.
- We basically need to understand/model what could be wrong before “fixing” it.
- In relation to SW Safety Analysis, then, the concept of SW “faults” is a key one.
- For instance this is relevant to judge the efficiency of a safety mechanism.
  - “Safety mechanisms can be specified to cover both issues associated with random hardware failures as well as **software faults**” – *ISO26262:2011-Part6*.
- Anyway sharing the understanding of what a SW fault represents could be a challenging task.

SW “faults” issue 2/3

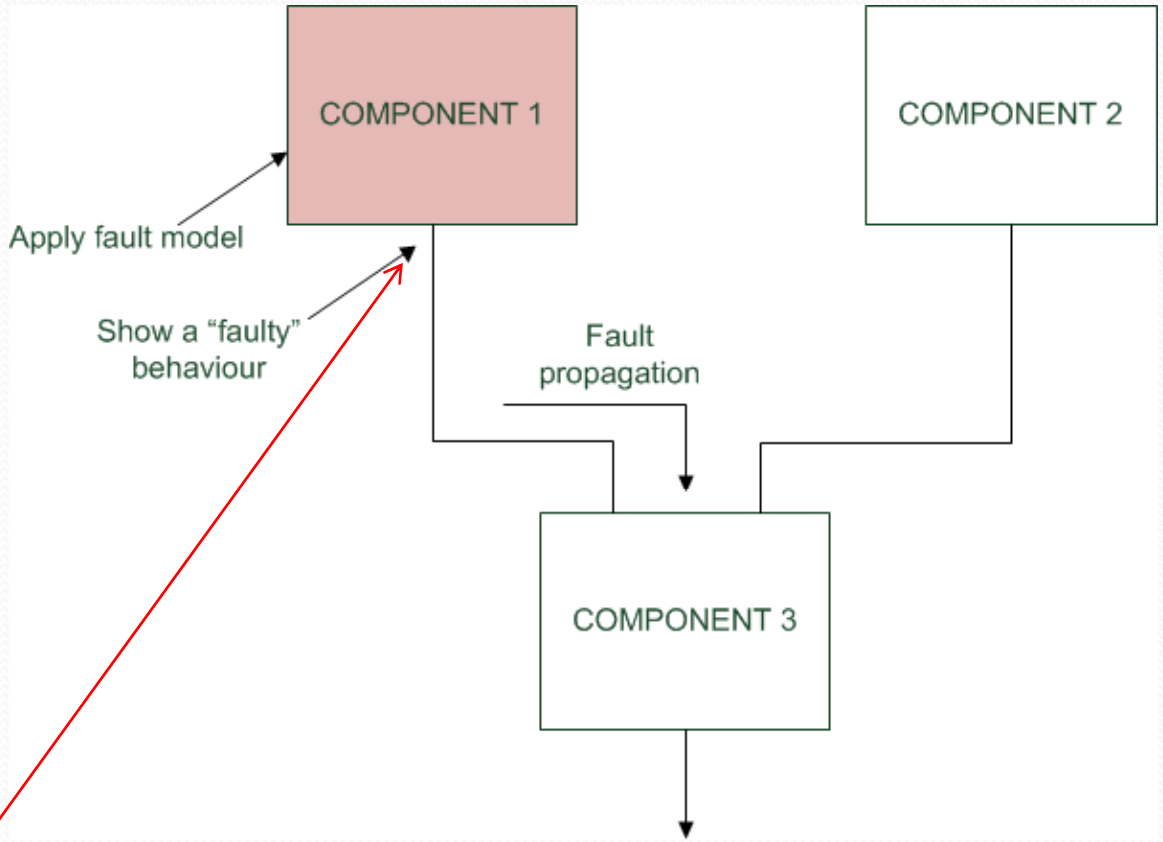
- SW faults can be linked to many aspects but mainly related to
  - Incorrent/missing requirements
  - Incorrect implementation
- In order to “validate” the SW architecture it is key to study how these faults
  - originate
  - propagate
  - affect the behavior of the SW and eventually impact the Safety Requirement
- Main practical issue is then how to “instantiate” the single fault.

ResilTech
Technologies for Resilience

SW “faults” issue 3/3

- In line with the standard requirements and then focusing on
  - the architectural level
  - and the design phase
- a possible solution is
  - to focus more on the fault “effect”
  - and then to adopt a fault model.
  - Follow this reasoning a proper level of granularity is a SW component within a more complex SW architecture.
  - Then the fault models are “applied” to the SW component.

Analysis method



- In relation to the safety analysis method this approach can be mapped to an HAZOP-like approach where
  - The analysis keywords represent component level fault model as, for instance, *"corrupted value of signal x on the component output"*

How to model – Which technology 1/2

- The analysis can be run on a model of the SW architecture because
  - it is necessary to drive the architectural definition and “validation” of specified safety mechanisms and as such
  - it has to be applied on an (early) design stage
- But can a model express enough information to support this study?
- Or rather which model can be suitable?
- In this context somehow modeling behavior in addition to the SW structure is essential.
- Also having an executable model would allow to adopt a tool-supported analysis that is important to analyze complex systems.

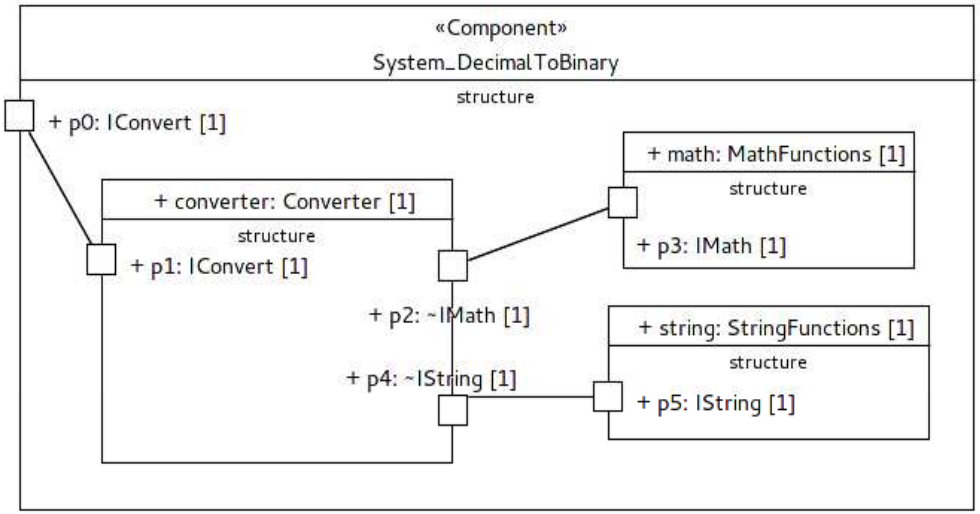
How to model – Which technology 2/2

- **Foundational UML** (**fUML**) is an executable subset of standard UML that can be used to define, in an operational style, the structural and behavioral semantics of systems.
- Anyway graphical modeling notations are not good for detailed programming.
  - The **Action Language for fUML** (**Alf**) standard specifies a textual action language with fUML semantics.

UML package	*Included in fUML?*
Modeling of structure	
Classes	yes
Components	no
Composite Structures	no
Deployments	no
Modeling of behavior	
Actions	yes
Activities	yes
Common Behaviors	yes
Interactions	no
State Machines	no
Use Cases	no

Structural views are essential, then it is key to bridge the gap related to the missing views.

Model transformation



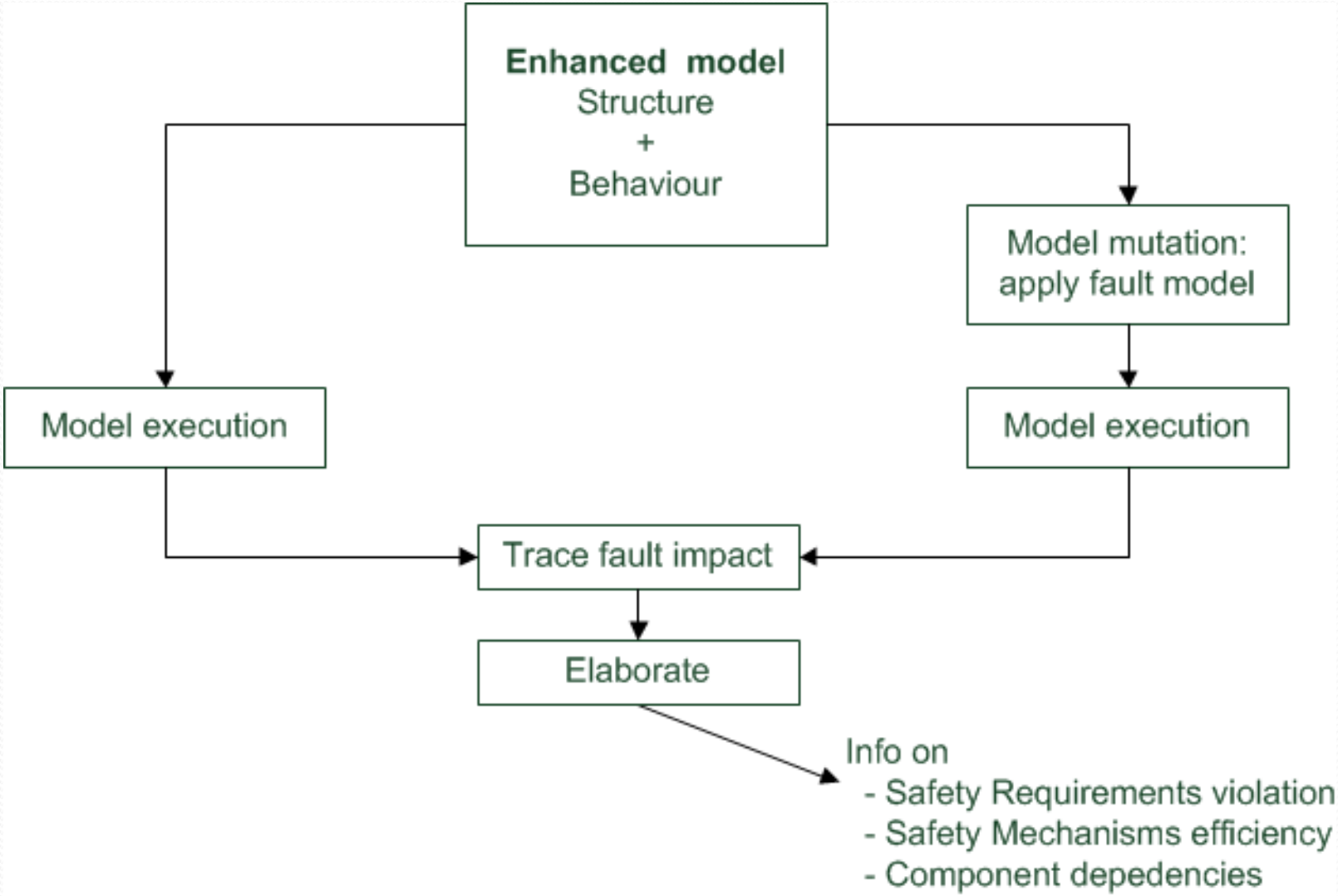
+

The behaviour of the operations provided by each component is described in fUML/ALF separately

An fUML/ALF executable model of the whole SW architecture

ResilTech
Technologies for Resilience

Model execution



ResilTech
Technologies for Resilience

Conclusions

- Main benefits
  - A clear procedure to perform the analysis is present
  - Results are reproducible
  - It is “easy” to compare different architectural solutions
  - It is possible to integrate within the SW development flow
- Main drawback
  - Effort in the model definition is necessary
    - More details are defined more the accuracy of the analysis benefits

Thanks for your attention!

francesco.rossi@resiltech.com