A Process and Data Model for Automotive Safety-Critical Systems Design

hugo.chale-gongora@renault.com
ofaina.taofifenua@renault.com

DRIVE THE CHANGE

Plan

- Introduction
  - Automotive systems, complexity & safety
  - ISO26262 standard overview
- System design process
  - Background, Principles & Process outline
  - Difficulties in process implementation
- Systems & Safety data model
  - Rationale
  - Design of SE and Safety data model
- Conclusions

Automotive systems, complexity & safety

- In a strongly competitive market, carmakers must propose to their customers
  - Innovative, pertinent, reliable, environmental-friendly and safe services
  - … at very competitive costs and time to market
  - … and complying to more and more stringent regulation constraints

- The intensive use of electronics and software technologies is a commonly used solution to face this challenge

- As a consequence
  - The complexity of systems increases
  - Safety analyses by traditional methods become complicated, time-consuming, i.e. costly
  - A particularly delicate issue when dealing with safety-critical systems

ISO26262 overview

- ISO26262 stems from EIC61508
- It covers the functional safety of programmable electric electronic systems on motorized road vehicles
- It defines a system lifecycle, activities to be performed, associated support processes
- It defines a systematic procedure to assess the risks caused by failures of EE components : ASIL quotation
- In “Committee Draft” version today, the international standard should be published on July 2011

Severity	Exposure	Controllability		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Salient aspects of ISO26262

- Its specificities
  - Pondering of the human factor
  - All system functionalities considered *a priori* as safety-related
  - The relationship between car manufacturer and providers is explicitly cited
  - Every normative part depends on the safety integrity level
    - Compliance to the standard will be made and verified in a systematic way
  - Very few guidelines concerning methods and tools to perform the described activities
- The current situation
  - ISO20262 recognized and shared as a state of the art
  - All major actors of the automotive industry participated to the elaboration of the standard
    - Actors are getting ready
    - Source of apprehension?
    - Or an opportunity to improve working methods?

Plan

- Introduction
  - Automotive systems, complexity & safety
  - ISO26262 standard overview
- System design process
  - Background, Principles & Process outline
  - Difficulties in process implementation
- Systems & Safety data model
  - Rationale
  - Design of SE and Safety data model
- Conclusions

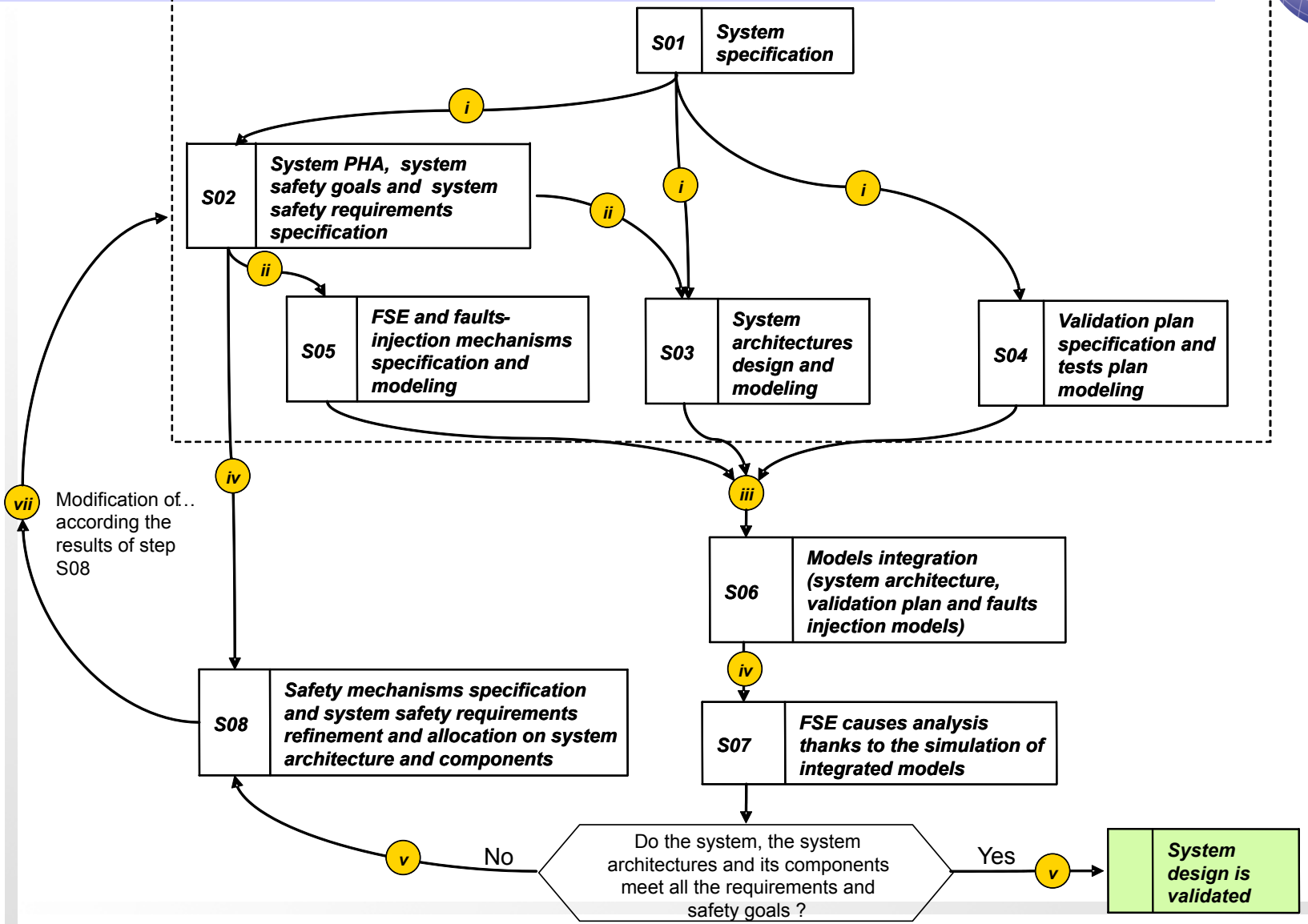
System design process: background

- SE process at Renault
  - Based on ISO/IEC 15288 (and its French equivalent NF Z 67-288)
    - Technical Processes
  - Applied partially from the vehicle system level
    - Customer services and other non-functional vehicle characteristics
    - Refined and allocated to vehicle sub-systems
- Safety management process
  - First Preliminary Hazard Analyses at vehicle level on each customer service
    - Vehicle level Feared Customer Events (FCE) and ASIL quotation
  - FCEs with the higher quotation are managed at corporate level for consistency and completeness
  - FCEs are updated based on the analyses (PHA, FMECA) carried out on technical solution or when introducing new technologies or services

Principles of the system design process

- Integrate safety aspects early in the system design process
  - Perform safety analyses not only on the final solution
  - Make system designers take “naturally” into account safety requirements
- Adopt a “customer-driven” approach to design and V&V activities
  - Safety-related aspects of the design are linked to the expected system service
- Proposed method
  - Implement and validate safety requirements first and foremost on the functional architecture
    - Avoid performing changes once most of design choices and critical decisions have been made
  - Model-based design process & tool-supported risk analyses
    - Combining an architecture description tool and exhaustive simulation of system architecture models

System design process outline



Difficulties in process implementation

- The creation and verification of the different objects of the process is time-consuming and troublesome
- Misunderstanding problems
  - Two different concepts designated by the same name
  - The same concept being referred by different names
- **The origin of these problems**
  - Lack of **semantic consistency** between the different models

Plan

- Introduction
  - Automotive systems, complexity & safety
  - ISO26262 standard overview
- System design process
  - Background, Principles & Process outline
  - Difficulties in process implementation
- **Systems & Safety data model**
  - Rationale
  - Design of SE and Safety data model
- Conclusions

Rationale

- Why make a data model as an **ontology** ?

- Definition:

  “An ontology is a formal, explicit specification of a shared conceptualization” (Studer 1998)

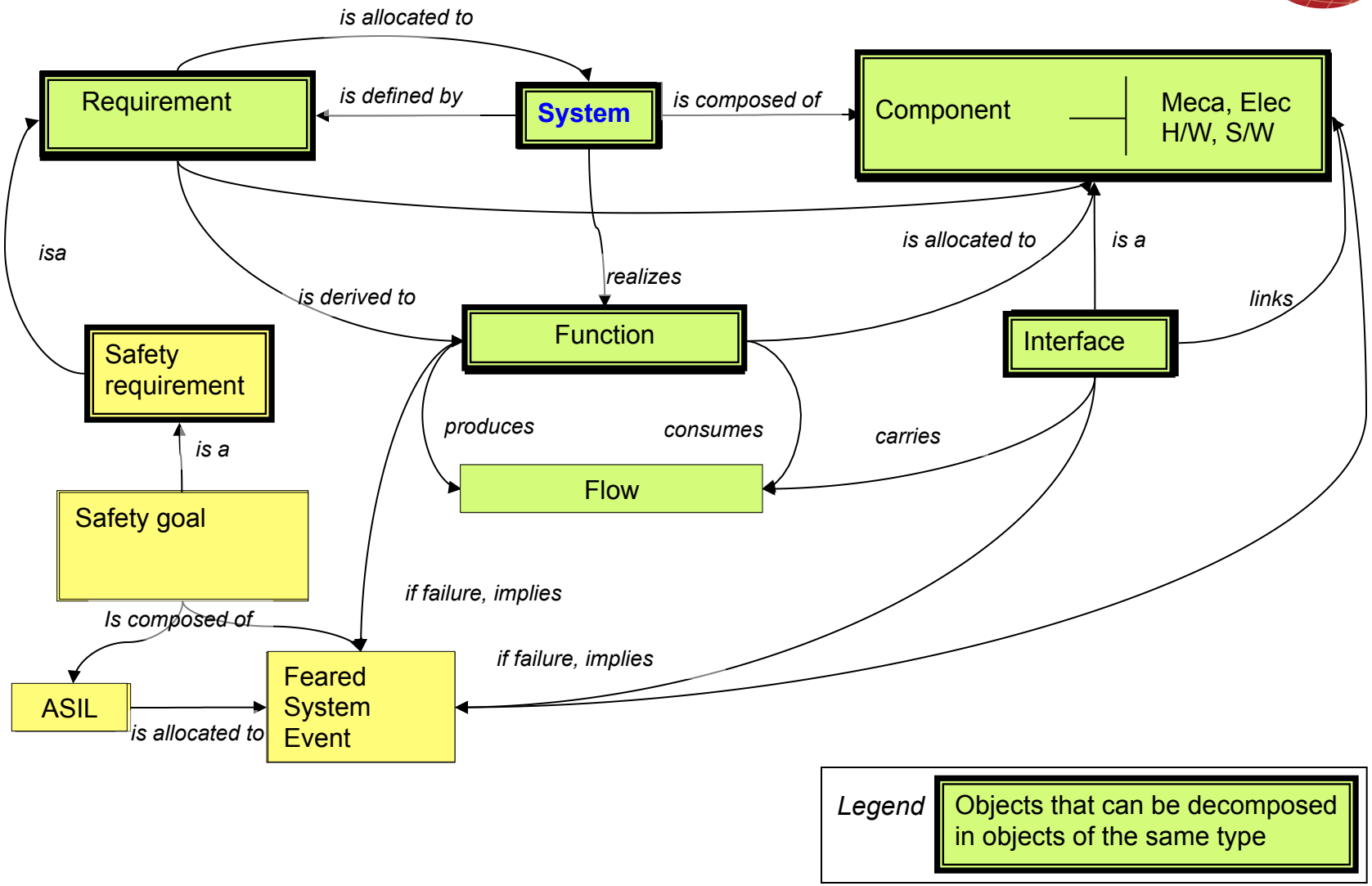
- Ontology compared to usual data model
  - More explicit representations for semantic relationships
  - Generic and task independent
  - Favors reusability, shareability, portability and interoperability

  “Reusability and reliability are system engineering benefits that derive from the use of ontologies” (Ushold 1995)

Rationale (2)

- A system and safety “light-weight” ontology
- Expected benefits
  - Help identify opportunities for front-loading of activities
    - Consistency checks
    - Verification of / compliance to rules
    - Assisted reasoning
  - Inter-disciplinary analyzes
  - Pointers to demonstrate compliance with ISO 26262
  - Data model template to be implemented in the development process

Design of the data model



Plan

- Introduction
  - Automotive systems, complexity & safety
  - ISO26262 standard overview
- System design process
  - Background, Principles & Process outline
  - Difficulties in process implementation
- Systems & Safety data model
  - Rationale
  - Design of SE and Safety data model
- Conclusions

Conclusions

- Open issues
  - Ontology engineering
    - Reaching a consensus
    - Manage ontology changes
  - Ontology language

- Perspectives
  - Place the ontology at the heart of the design & verification activities
  - Further develop the ontology
  - Architecture design and V&V
    - Integrate architecture optimization methods in the model-based approach
  - Formal methods
    - Model-checking (under way)

Thank you!

Questions, comments?