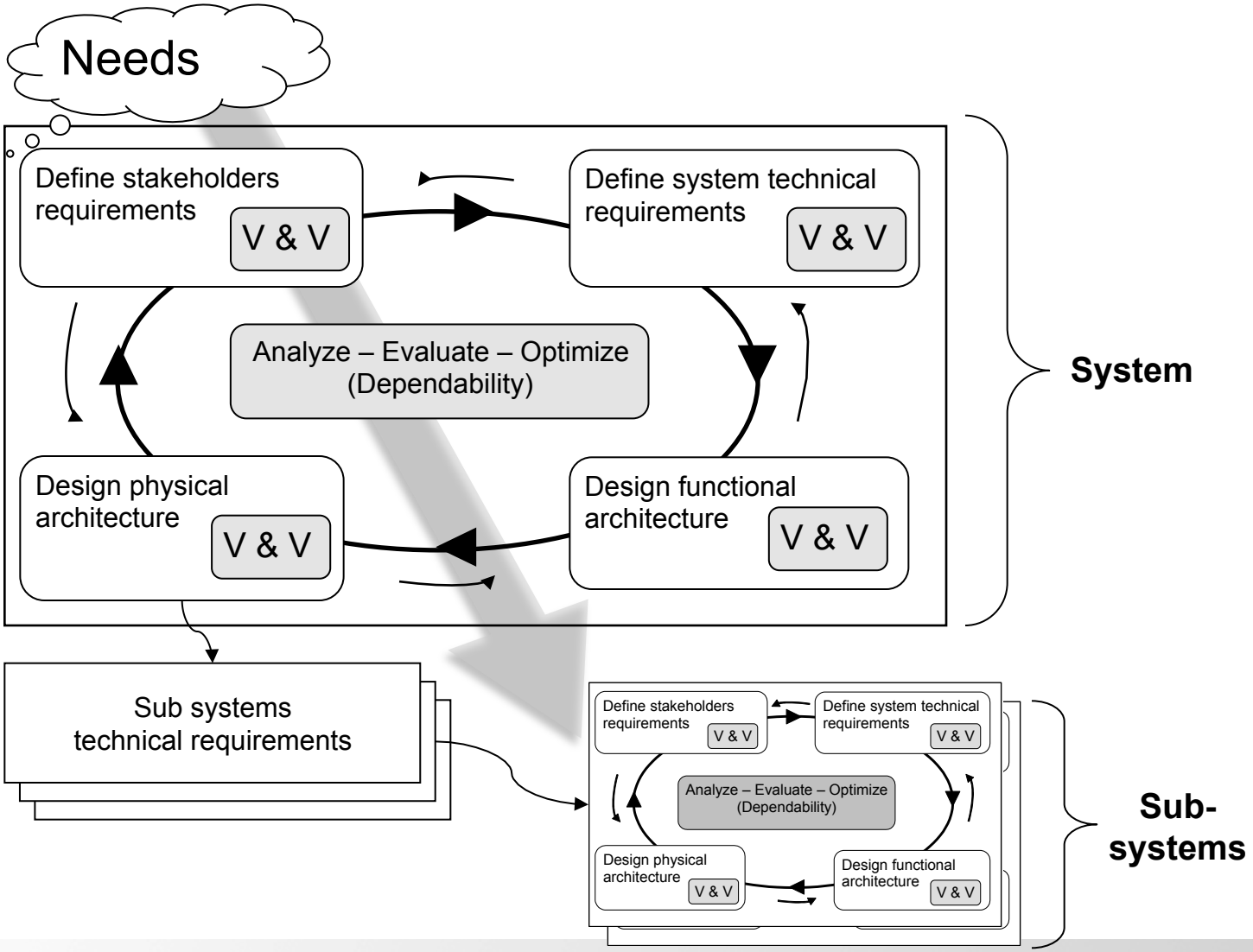
Reducing the Gap Between Formal and Informal Worlds in Automotive Safety-Critical Systems

HUGO CHALÉ, **OFAINA TAOFIFENUA**, THIERRY GAUDRÉ, ALEXANDRA TOPA
RENAULT

NICOLE LÉVY
LABORATOIRE CEDRIC, CNAM

JEAN-LOUIS BOULANGER
CERTIFER

Current Design Process at Renault



Problems of the Current Process

- System stakeholders and actors from different professional fields have their own languages
- “Misunderstanding is the most frequent form of communication between people”, Peter Benary
- **Consistency** problems
  - documents and models in English and French
  - communication omission or misinterpreted
  - inter-domain and inter models consistency problem
  - **Lack of traceability**

Other Issues

- Upcoming of **ISO 26262** standard requiring rigorous development processes
  - ISO 26262 standard : Road Vehicles - Functional Safety

- Transition towards Model Based Systems Engineering
  - formal and informal models
  - produce and control the global model of the system

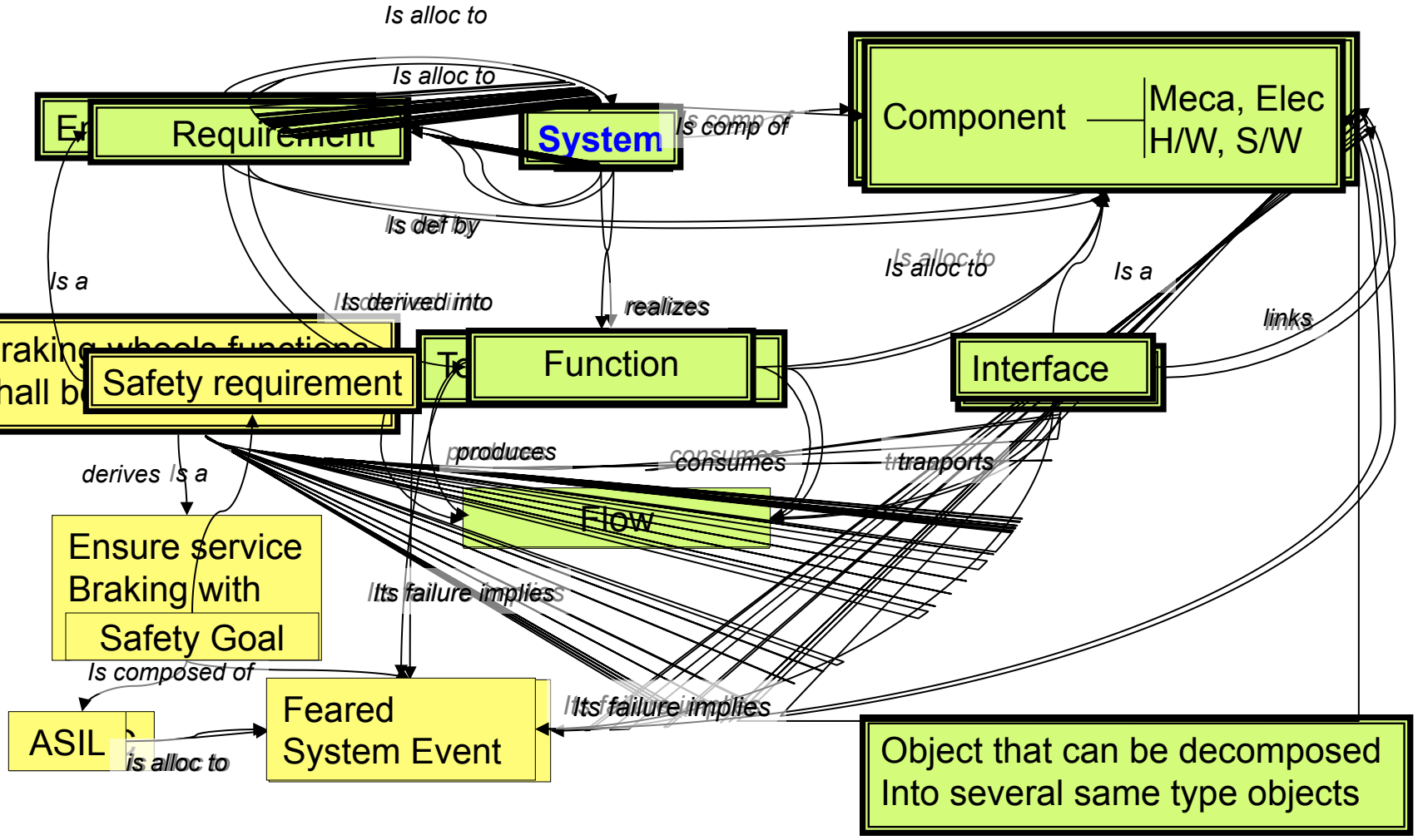
Ontology centric design process

- **Our approach:** define **ontologies**
  to formalize concepts and knowledge of
  - systems engineering
  - functional safety
  - automotive domain

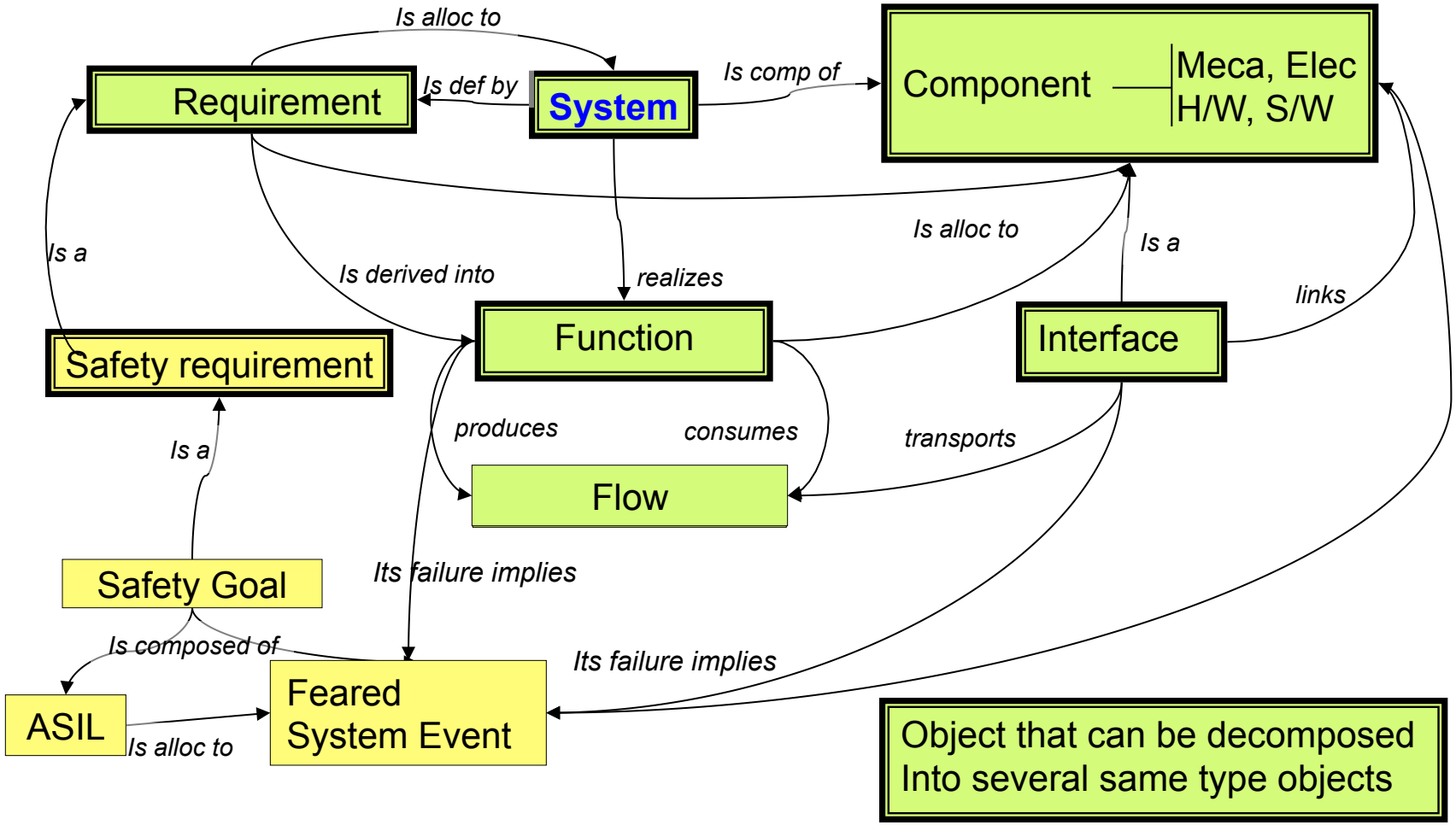
➔ Establish logical consistency
  - of the whole design process,
  - including transformations

- **Case study:** a **R**egenerative **C**ombi-**B**rake system

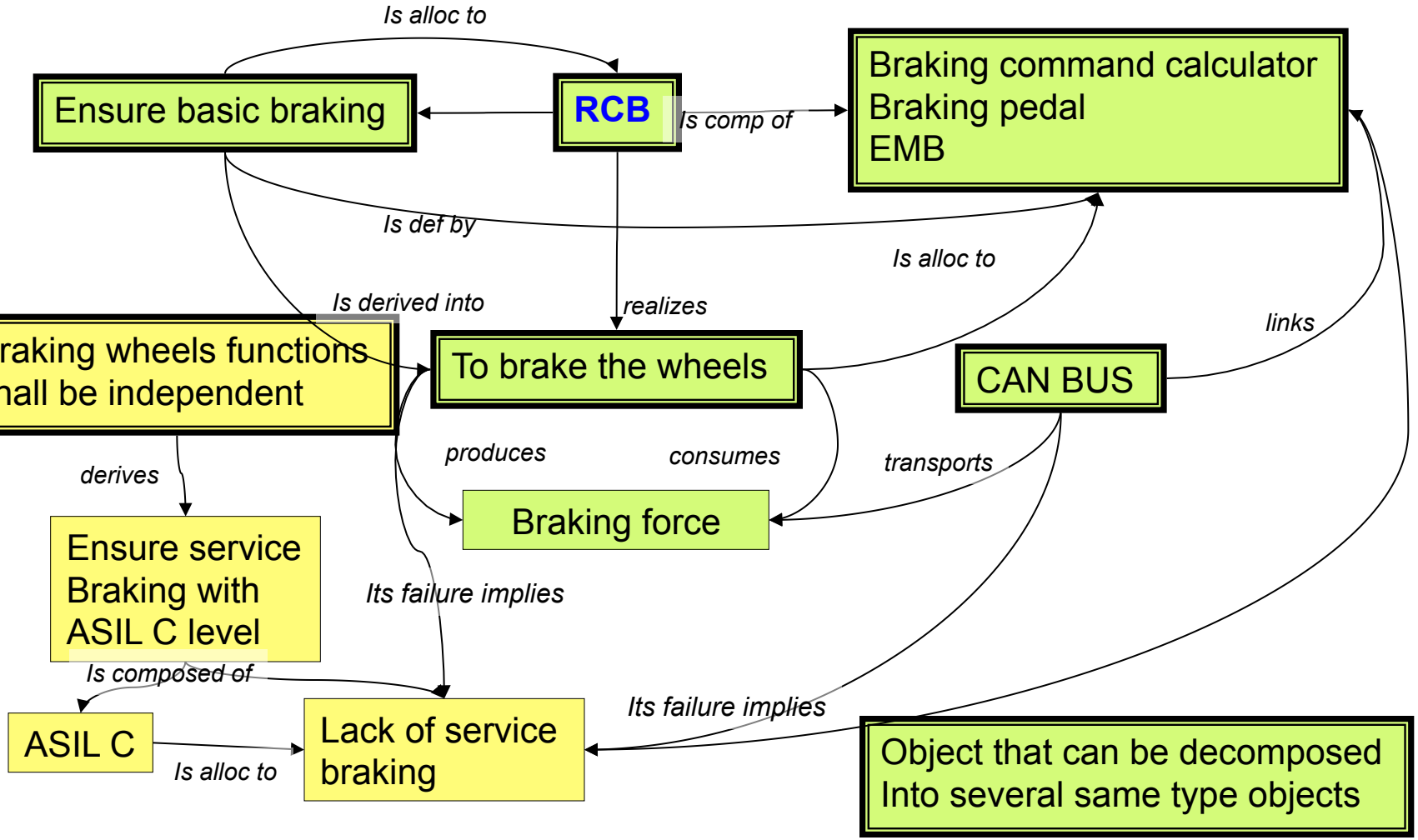
System and Safety ontology



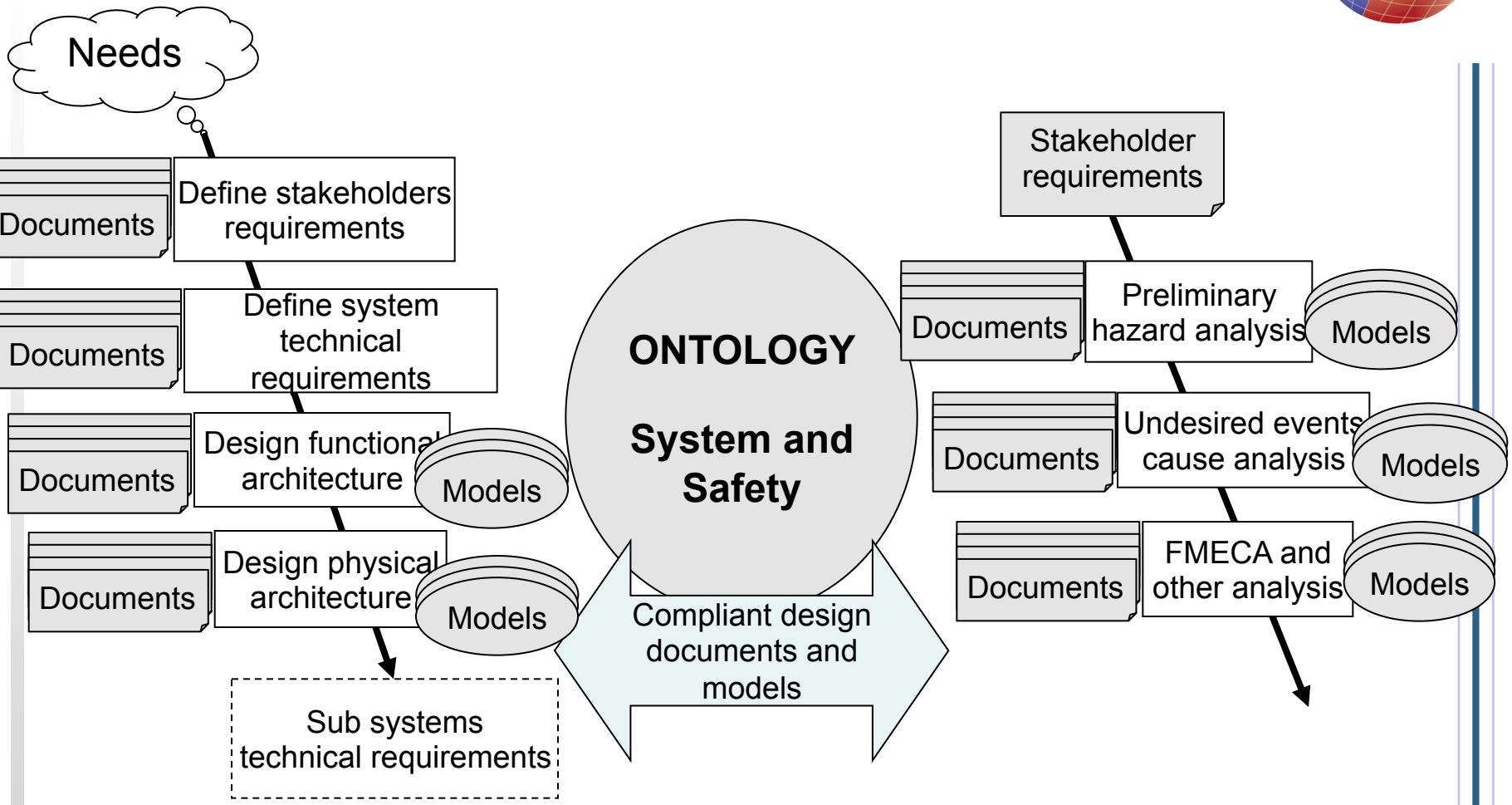
System and Safety ontology: Conceptual level



System and Safety ontology: System level



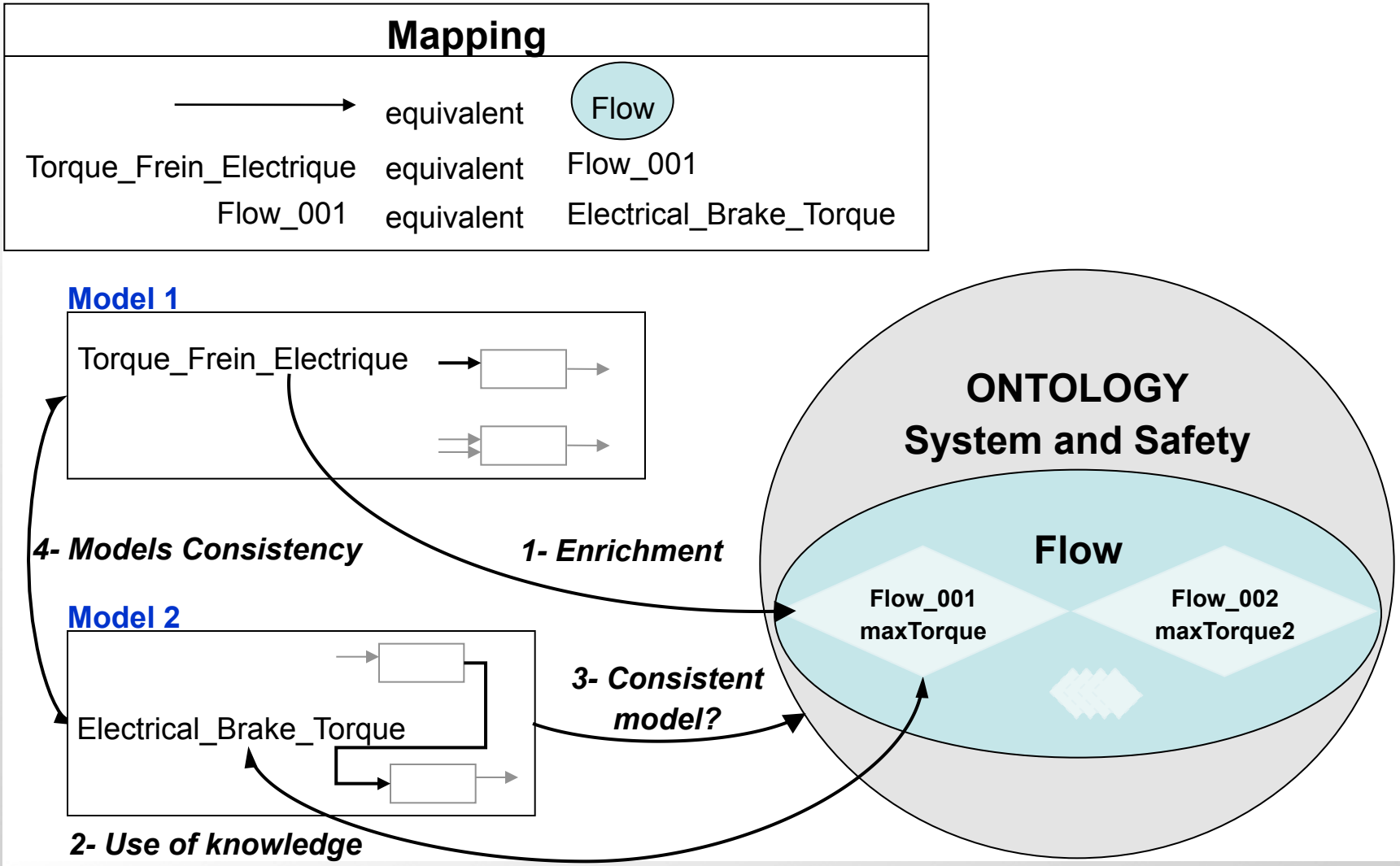
Ontology Centric Design Process



System Design

Safety analysis

Ontology as a reference model



Ontology Centric Design Process

- Ontology to **describe in a formal and explicit way**
  - **Concepts** of a domain and their **relations**
  - **Instances** (of concepts and relations)

- System and safety ontology as **reference model** of
  - Systems engineering and functional safety domains
  - The system under development

- **Verify and validate**
  - the compliance,
  - the completeness and
  - the consistency

  of **all the documents and models**

Model-Driven Engineering

- Create different models of a system
- at different abstraction levels
- in order to achieve an architectural separation of concerns
- use transformations to produce the desired implementation

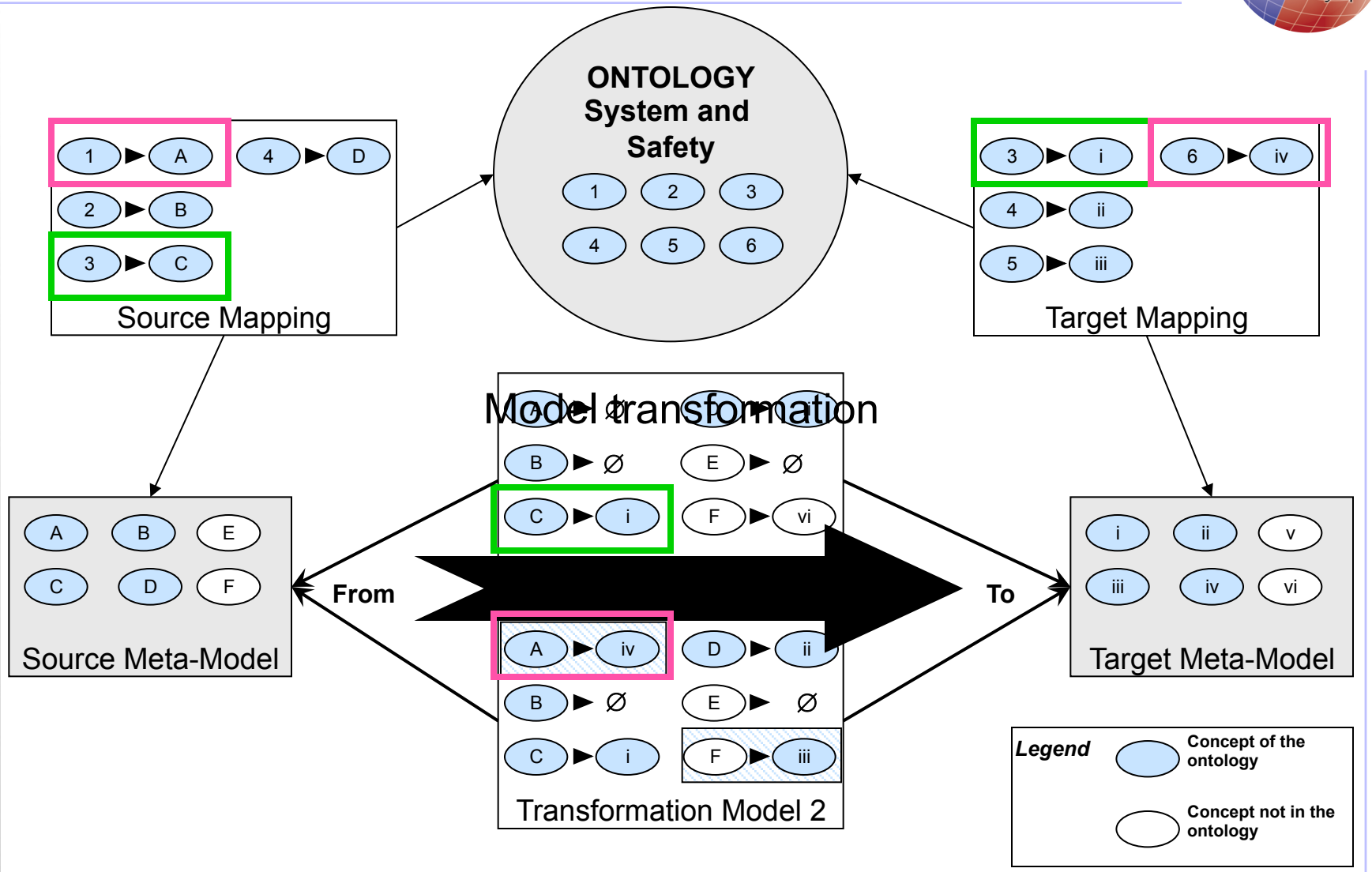
(10-20% efficiency gain is expected …)

Model transformation

- Principle
  - Input model transformed into output model
  - Capitalize on existing models to implement other models

- Need to choose appropriate and efficient transformations covering the process

Evaluation of model transformation



Evaluation of Model Transformation

- The ontology as reference model of
  - The domain
  - The system
  - The ISO 26262 safety standard

- Mapping different languages concepts to the ontology

- Be able to validate consistency !!!

Implementation of the Ontology and First Results

- The ontology is realized with Protégé 3.4.4
  - + plug-in "Semantic Web Rule Language" (SWRL)
  - + an interface with the rule engine Jess
  - ~ 100 classes (concepts)
  - > 100 properties (relations)
- The ontology is realized with Protégé 3.4.4
  - + plug-in "Semantic Web Rule Language" (SWRL)
  - ~ 70 functional requirements at system level
  - + an interface with the rule engine Jess
    - ~ 100 classes (concepts)

Conclusion

This paper: ongoing initiatives at Renault

- Introduce formal descriptions in SE design process
- Define a system and safety ontology
  - integrating the ISO 26262 standard concepts (functional safety of systems) with SE design process concepts

This paper: ongoing initiatives at Renault

- Introduce formal descriptions in SE design process comply with the ontology.
- Define a system and safety ontology

Ongoing and future work

Use ontology relations for:

- traceability between all system data (requirements, functions, components…)
- completeness of the global model
- ASIL propagation
- Integrate several formal languages

- traceability between all system data (requirements, functions, components…)
- completeness of the global model
- ASIL propagation

Thank you!

Questions, comments?