A Model-Based Safe-by-Design Approach with IP Reuse for Automotive Applications

ICSEA 2020

Morayo Adedjouma, Nataliya Yakymets
{name.surname}@cea.fr
Université Paris-Saclay
Institut CEA LIST
Département Ingénierie Logiciels et Systèmes
Laboratoire Conception de Systèmes Embarqués et Autonomes (LSEA)

SHORT RESUME

Morayo Adedjouma, PhD

CEA Research Engineer, Safety expert, Project manager

- 2008/2012: System Safety Engineer in automotive domain
- 2012: PhD in Computer Science
- 2012/2015: Research associate & Fellow at University of Luxembourg (LU), McMaster University (CA)
- 2015/-: Member of Design of autonomous and embedded cyber physical systems lab at CEA LIST since 2015

Research interests:

- Model-driven engineering, process and system engineering
- Dependability/safety, assurance and certification of cyber physical systems
- Natural Language Processing and text semantic analysis, machine learning

Current projects: Trustworthy AI, dynamic risk management, Evolutionary certification for critical systems

OUTLINE

- **Model-based and reuse paradigms**
- **Our approach**
  - Co-engineering system and safety
  - Reuse
  - Modelling framework
- **Tool support**
- **Evaluation**
- **Conclusions: findings, limitations, perspectives**

MODEL-BASED AND REUSE PARADIGMS

Reuse and Model-based as promising paradigms for system development promise

- **Reuse paradigm**
  - Integrate in several engineering domains with code, software & hardware component libraries, CASE tools, etc.
  - Support by standards through architecture modularity (SeOOC, IMA),
- **Model-based paradigm**
  - Propose flexible and expressive semantics for easy and common understanding
  - Also use in several engineering domains an align with standards recommendations

Both show benefits to save development effort and costs and to increase the quality of system/software

MODEL-BASED AND REUSE PARADIGMS

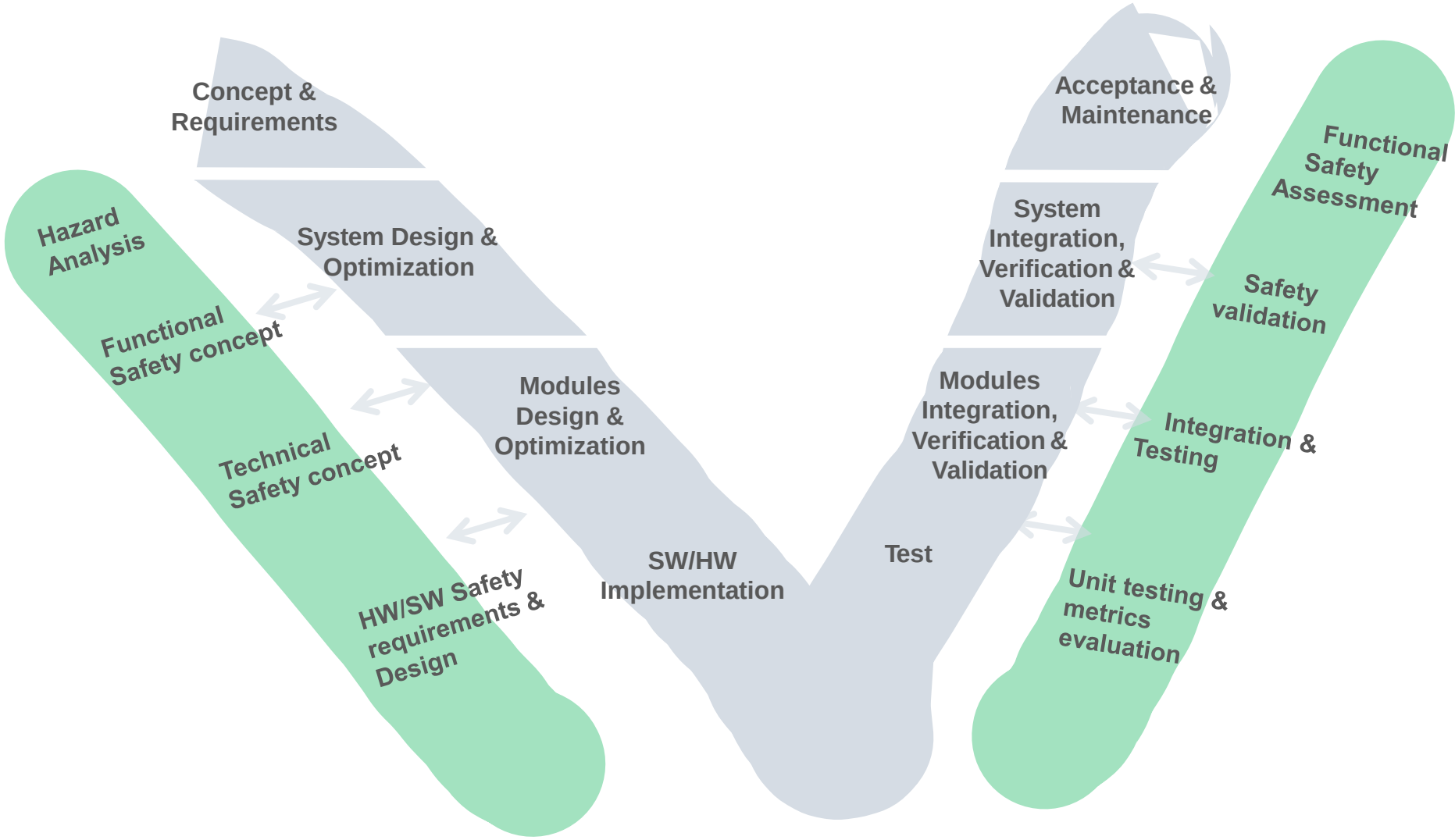
- **Paradigms suffer of limits for large scale critical system**
  - No so many open data approaches existing to achieve interoperability and reuse of data
  - No strong integration between model-based system engineering and RAMS analysis
  - No trivial to support reuse of safety assets due to their context-dependent nature
  - Tool support for both approaches are not well integrated

MODEL-BASED SAFE-BY-DESIGN WITH IP REUSE METHOD

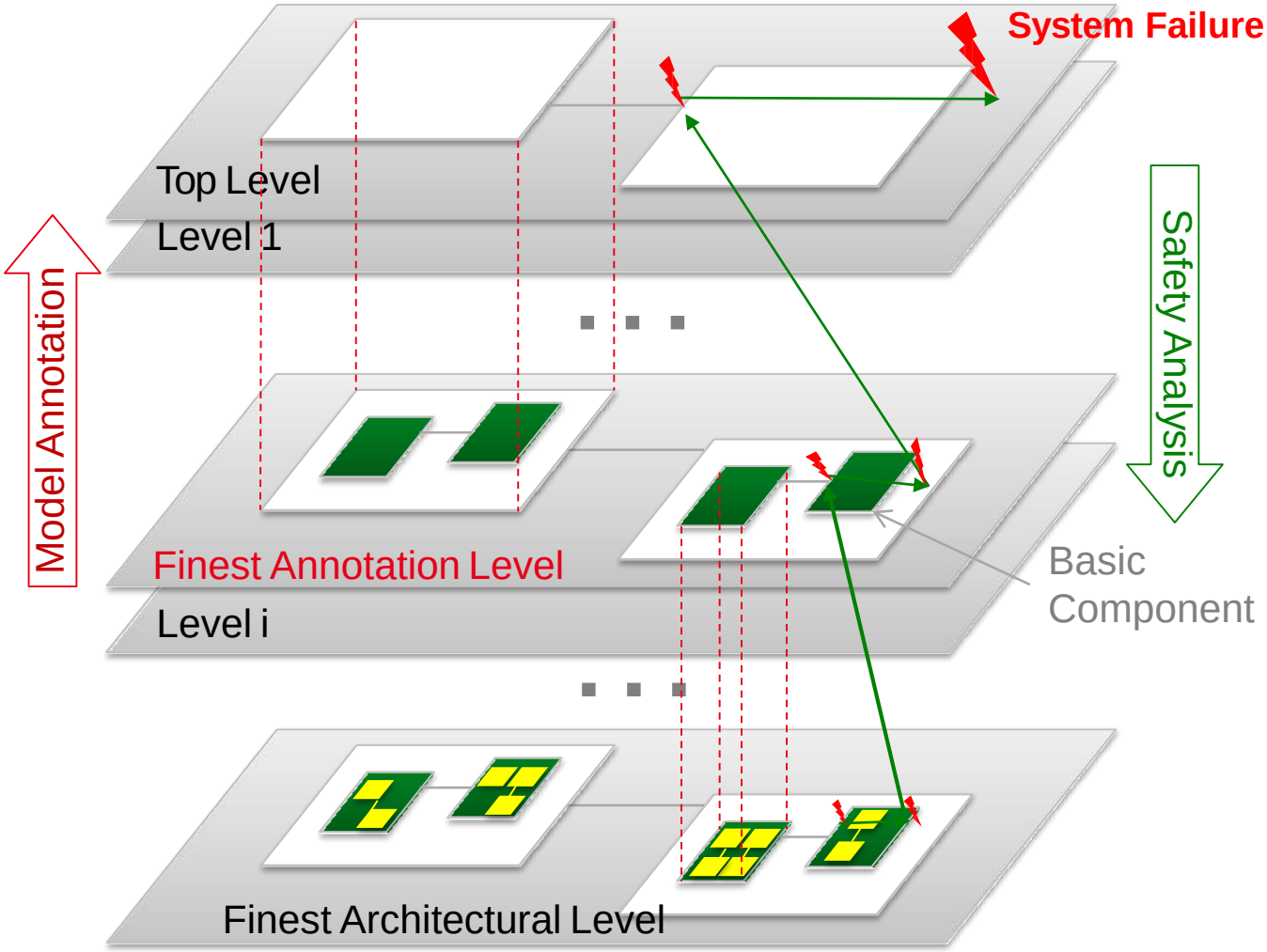
- Methodology
  1. Develop a co-engineering methodology to conduct safety assessment and system development process
     - Synchronize the processes through the requirements and output workproducts of activities
  2. Combine top-down approach of system design with Bottom-Up approach of system implementation by storing and reusing safety artefacts and component IP cores
  3. Use a unified modeling environment to ease traceability and reuse management
- We develop the methodology over the ISO26262 reference development model, requirements and recommendations for compliance

| 6

SYSTEM & SAFETY CO-ENGINEERING



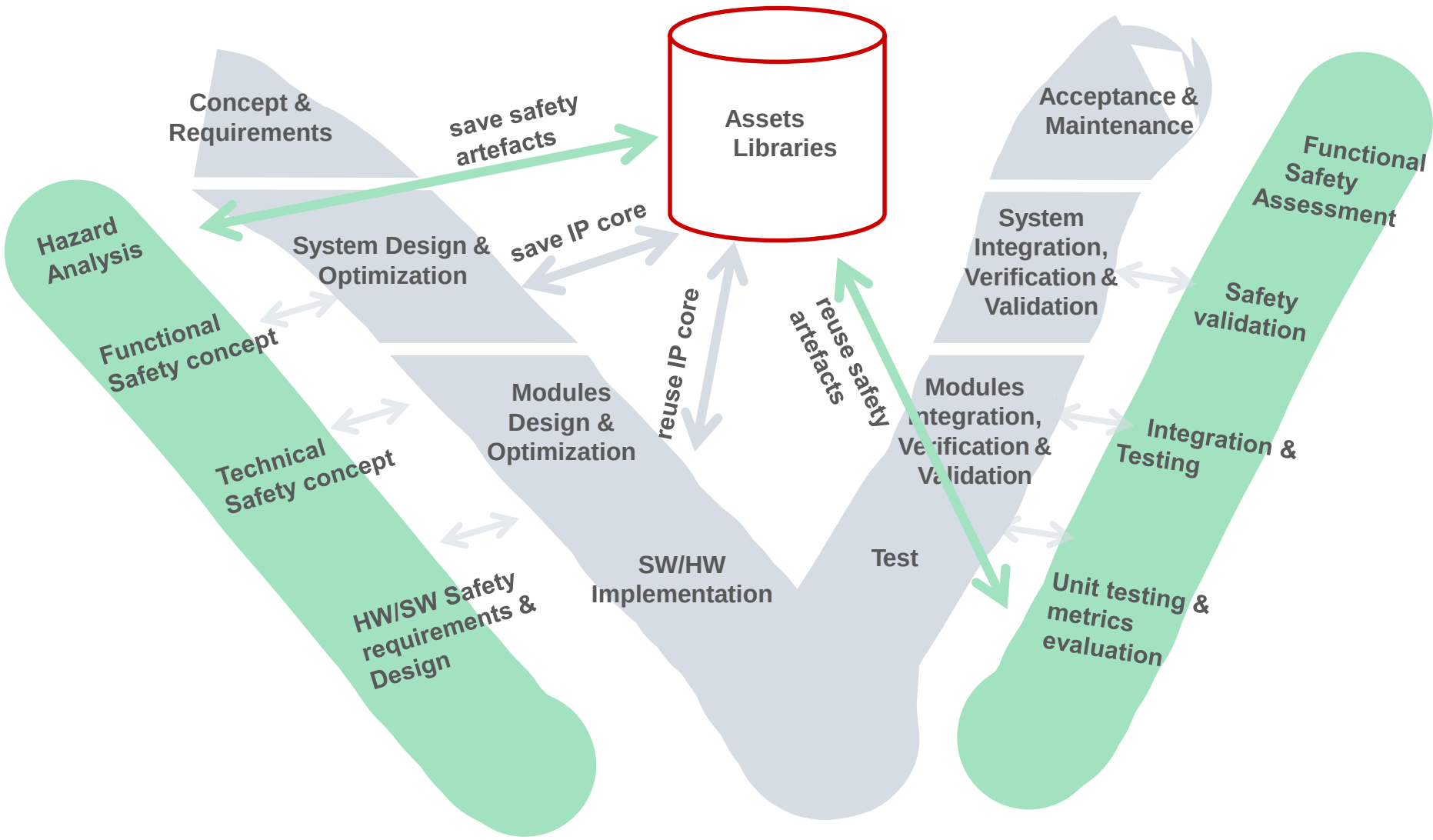
SYSTEM AND SAFETY CO-ENGINEERING



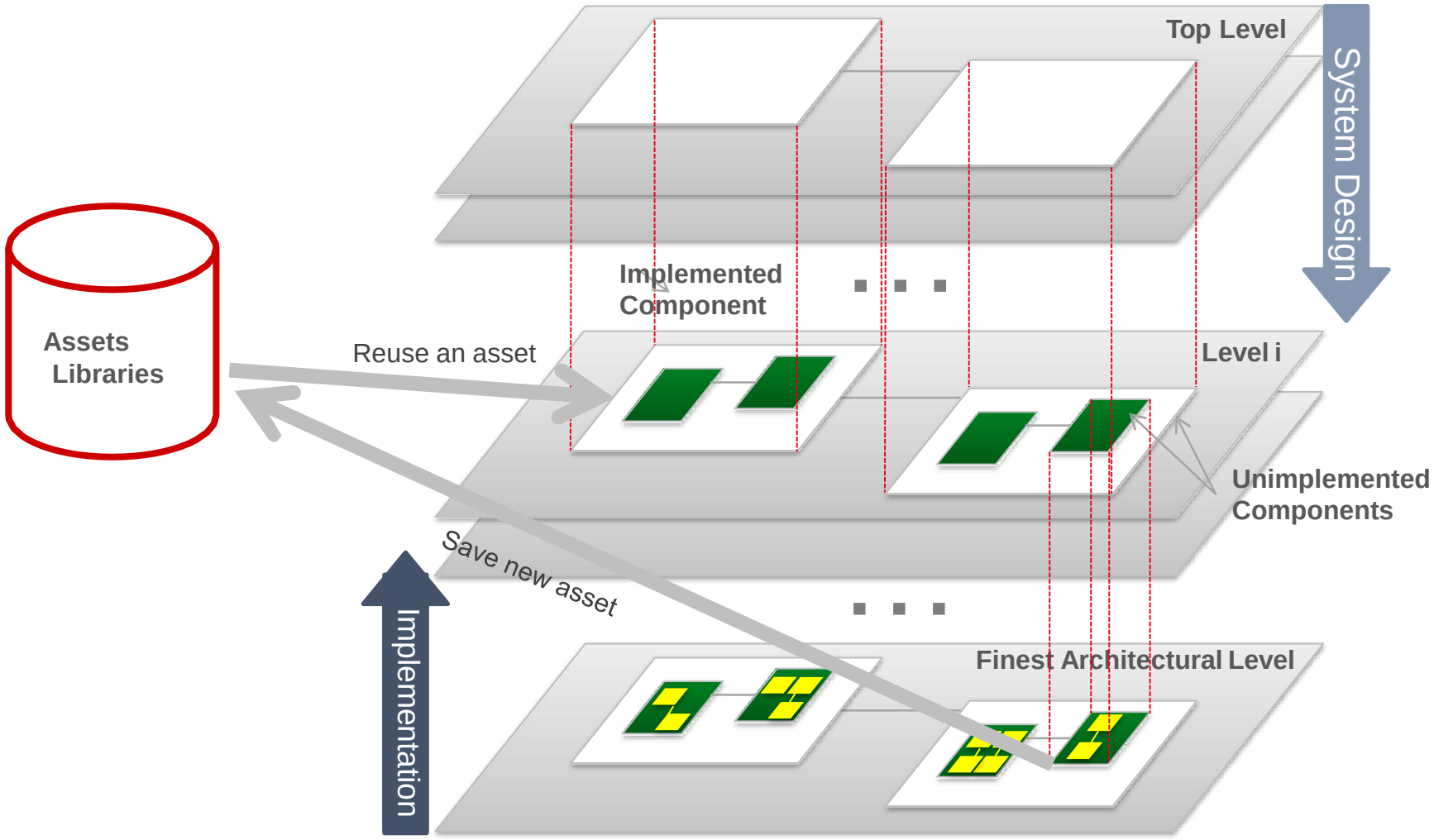
Flexible analysis

- Keep a desired level of precision during safety assessment (SA) process
- Control a complexity of RAMS methods applied
- Reduce time and cost required for SA
- Keep coherence of dysfunctional behavior on different levels
- Ensure unrivalled level of consistency, and traceability of dependability information

IP CORE AND SAFETY ARTEFCATS REUSE

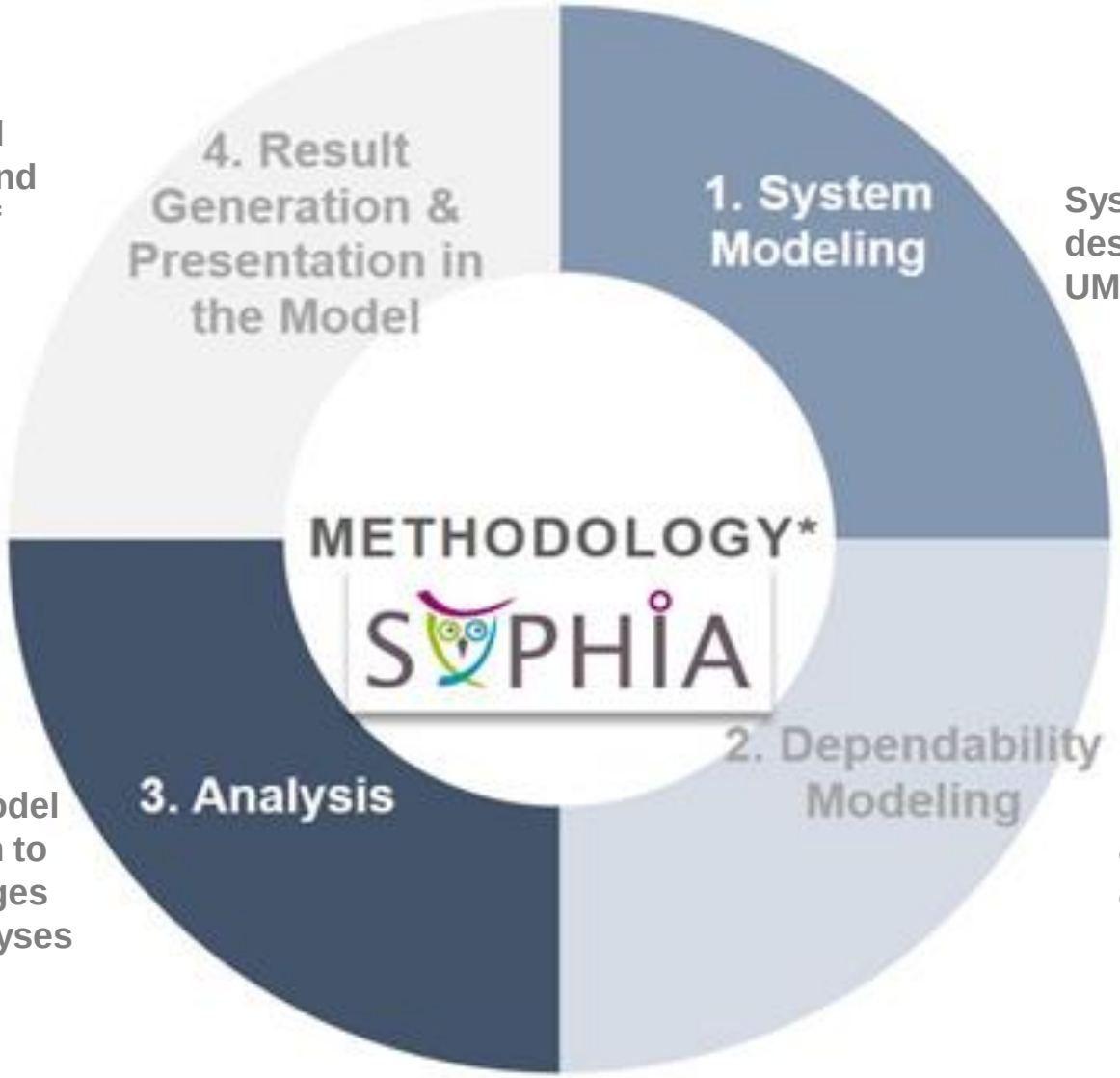


IP CORE AND SAFETY ARTEFCATS REUSE



MODELLING FRAMEWORK

Display critical components and propagation of risks, failures, etc.



System description in UML/SysML

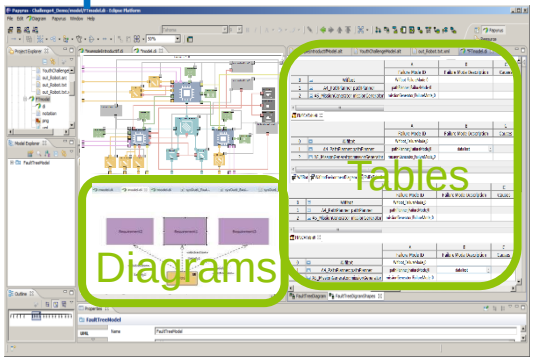
Analyses & model transformation to formal languages for furher analyses

Dependability annotations application

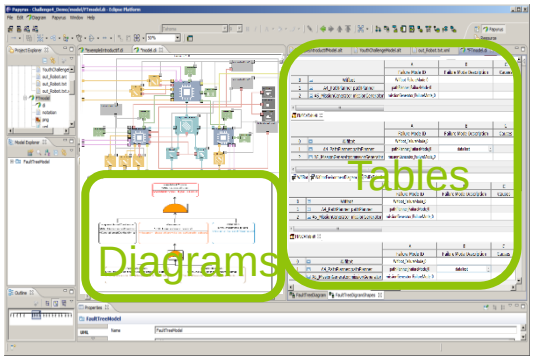
TOOL SUPPORT

SOPHIA TOOL SUITE

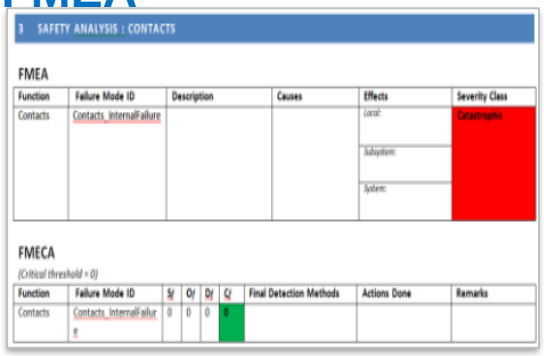
Requirement



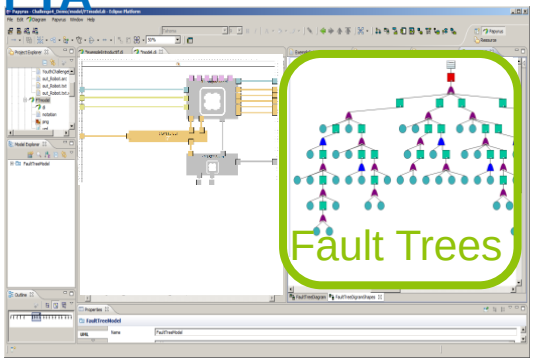
HA



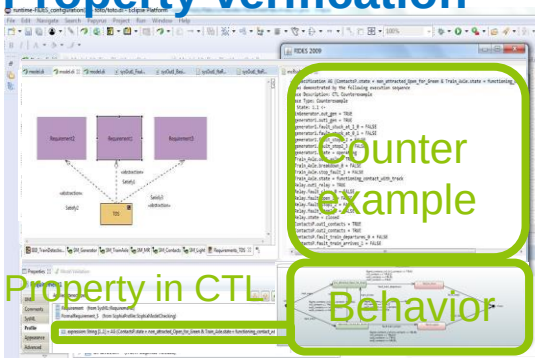
FMEA



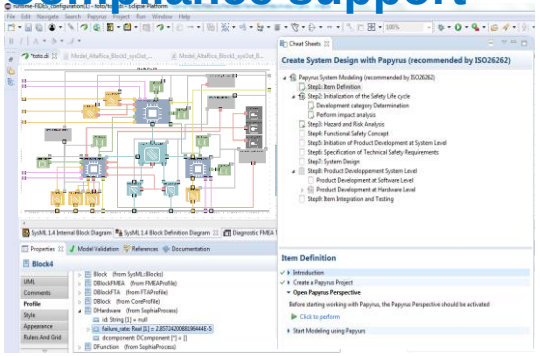
FTA



Property verification



Compliance support



MBSA tool suite aligned with upcoming OMG Safety and Reliability standard

EVALUATION

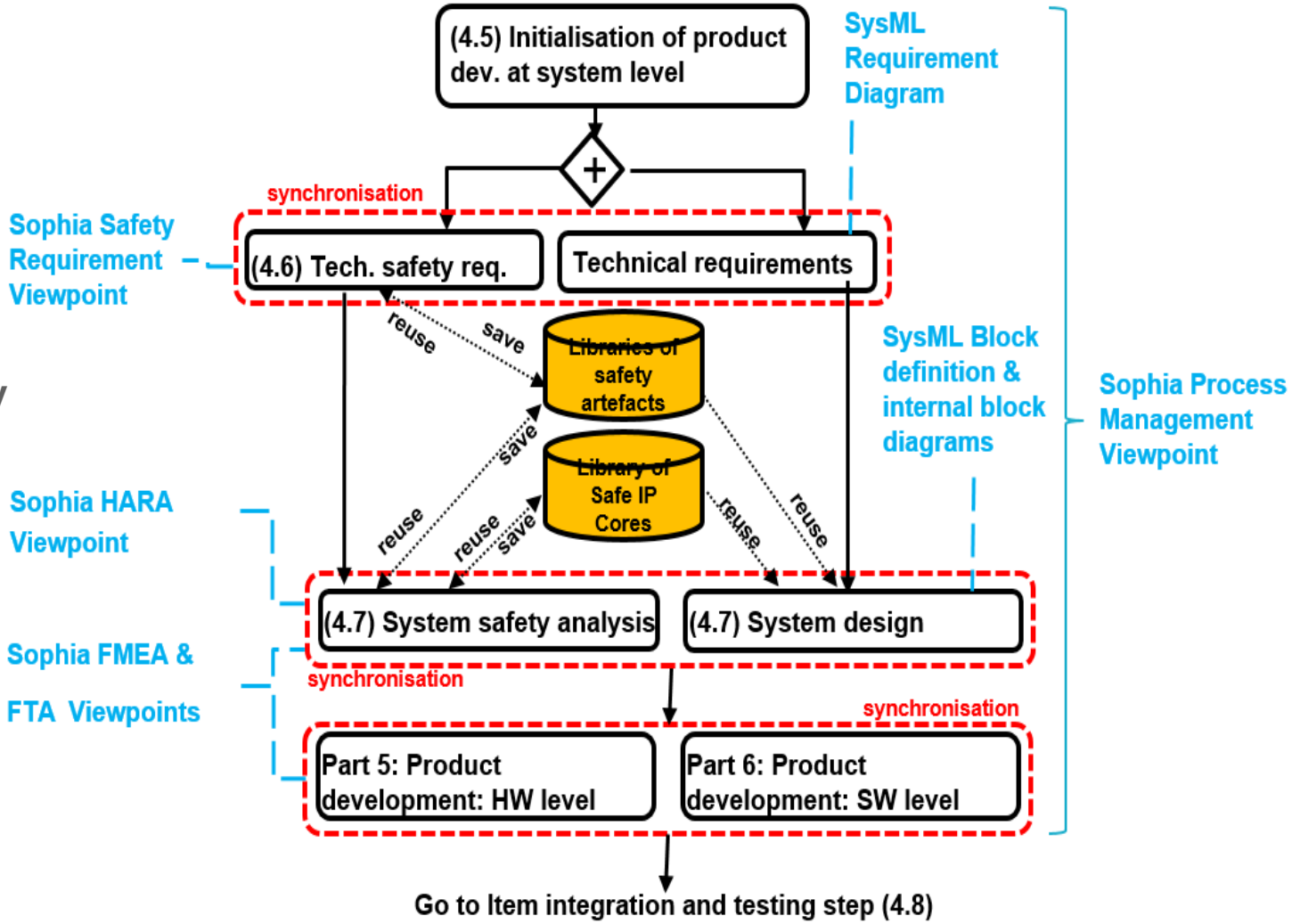
Evaluation procedure and data collection in 2 phase on an Adaptive Cruise Control (ACC)

- **First phase: Develop an ACC focusing on compliance with Part 3 (Concept level), Part 4 (System level) and Part 5 (HW level) of ISO 26262**
  - We do system description including requirements, functional and system architecture;
  - We perform required safety assessment using HARA, FMEA, FTA tool from Sophia
  - We store in repositories IP cores and safety artefacts
- **Second Phase: Considering some changes in the requirements of the ACC to lower the criticality**
  - We apply our methodology after an impact analysis
  - We review selected activities to review focusing on Part 4 (System level) still using Sophia tool suite
  - We reuse some assets collected from the first phase

USED CO-ENGINEERING AND REUSE METHOD

Key points:

- Parallelize system development and safety development
- Save and reuse of IP cores and safety artefacts
- Development in model-based environment
- Follow the ISO2626 workflow



FINDINGS

- **MDE approach facilitates integration of RAMS techniques into the engineering process**
  - Own RAMS dedicated models BUT consistent & aligned with system architecture models

- **Uniform modeling environment avoid open data and interoperability issues**
  - Smooth traceability across lifecycle
  - Build a system optimized for time, performance, cost

- **Usage of reusable assets to lower system development effort & cost, and improve system quality**
  - Reuse of design artefacts and safety artefacts
  - Reduce design defects by reusing already validated components/architectures

- **Co-engineering method system and safety development**
  - Align with standards recommendations
  - Ease compliance evidence collection for compliance/qualification

LIMITATIONS AND PERSPECTIVES

- **Limitations**
  - Building reusable repositories takes time
    - Expect correct populated libraries several iterations on several projects
    - saving cost, time is not immediate
  - Expertise is not embedded in the tool nor in the methodology but needed for a coherent and correct reuse strategy
    - What artefacts to save for reuse? What justification and information should be attached to a reusable assets
  - Need a method to measure the level of reusability and to estimate the impact of dependability properties on reusable artefacts
- **Perspectives**
  - Integration with FIDES reliability prediction database to consolidate/extend the reusable assets repositories with standardized safe component (IP core)
  - Adoption of contract-based approach to enforce reuse correctness

Morayo Adedjouma, PhD
Research Engineer

Université Paris-Saclay
Institut CEA LIST
Département Ingénierie Logiciels et Systèmes (DILS)
Morayo. Adedjouma@cea.fr
www-list.cea.fr