IMT Mines Alès
École Mines-Télécom

axone

TITLE :
TRANSFORMATION & SIMULATION OF ARCHITECTURE MODELS FOR DEPENDABILITY ANALYSES OF COMPLEX SYSTEMS

ROLF MIEMBA MAKITA

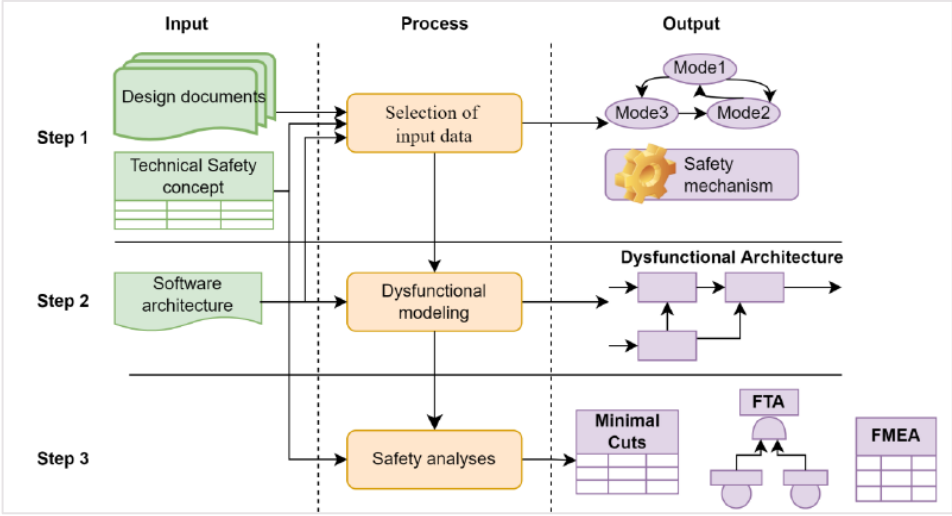
SUPERVISORS :

GREGORY ZACHAREWICZ
FRANCOIS TROUSSET

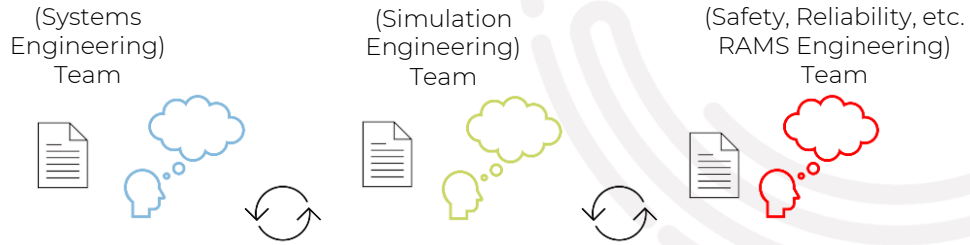
ISSUE AT STAKE

Engineering Critical Infrastructure Systems(CIS): Projects involving several stakeholders working together with specific engineering objectives

- MBSA approaches are not used at ealier stages of systems development.
- There is a lack of a comprehensive model-based approach to manage critical aspects (dependability) of complex systems
- There is a lack of interoperability between the engineering processes.
- There is a lack of conceptual alignment between model-based approaches



A typical MBSA Process from (Sirgabsou et al., 2022)



Systems are characterized by 4 main properties (Avižienis, et al., 2004):

- functionality,
- performance,
- Dependability (RAMS),
- cost

Functionality defines what the system is intended to do and described by the **functional specification** in terms of functionality and performance. Dependability and cost have **separate specifications** (Avižienis, et al., 2004).

- It necessary to define a model-based approach to dependability engineering.
- It could be helpful to directly use system model architectures to perform dependability analysis and simulations on systems
- It could be helpful to define a conceptual modelling methodology of dependability analysis at system level.

SOLUTION

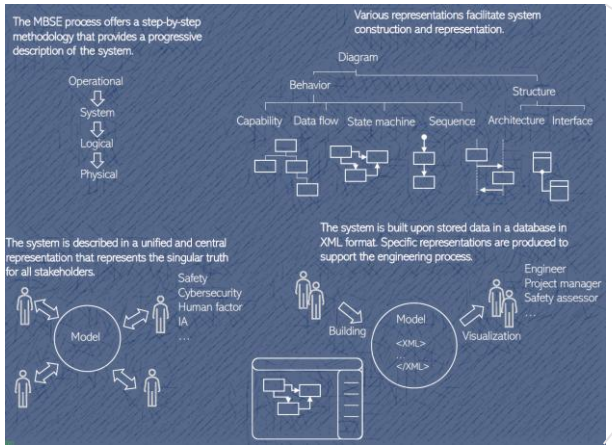
Definition of a Unified Engineering Framework (UEF) implementing model-based approaches :

- ❑ Model-Based Systems Engineering (MBSE)
- ❑ Model-Based Dependability Engineering (MBxA)
- ❑ Model-Based Simulation Engineering (MBS)

The UEF aims at transforming MBSE models into MBxA Models and use them as conceptual models for MBS.

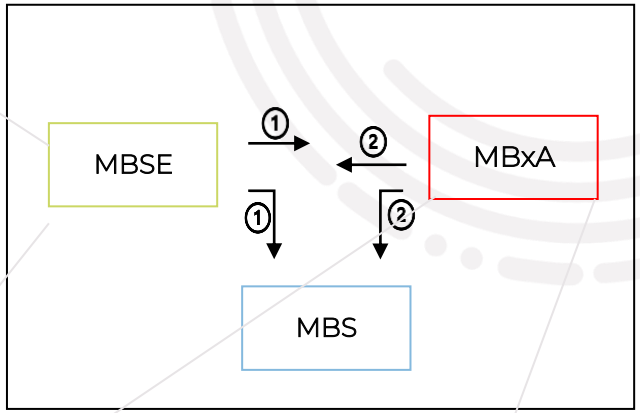
The framework enables interoperability of engineering disciplines using a model transformation methodology and modelling patterns considering architecture views of system :

- ❑ Operational View
- ❑ Functional/Dysfunctional View
- ❑ Logical View
- ❑ Physical View



- ❑ Consistent Models
- ❑ Verifiable Models
- ❑ Valid Models
- ❑ Traceable Models
- ❑ Documentable Models

UEF Framework



x_A: Reliability Modelling

x_B: Availability Modelling

x_C: Maintainability Modelling

x_D: Safety Modelling

USE CASE

Critical Infrastructure System of Interest :
a Spent Fuel Pool system

MBSE

Operational Analysis

MBxA

MBSA

Safety Analysis

MBRA

Reliability Analysis

MBSE Methodology

Example of Method : Arcadia

Technique : Profile, Mode, States Modelling at Operational Level

MBxA Methodology

Example of Methods : Phased-Mission Analysis, Reachability Analysis

Technique : Petri-Nets Technique