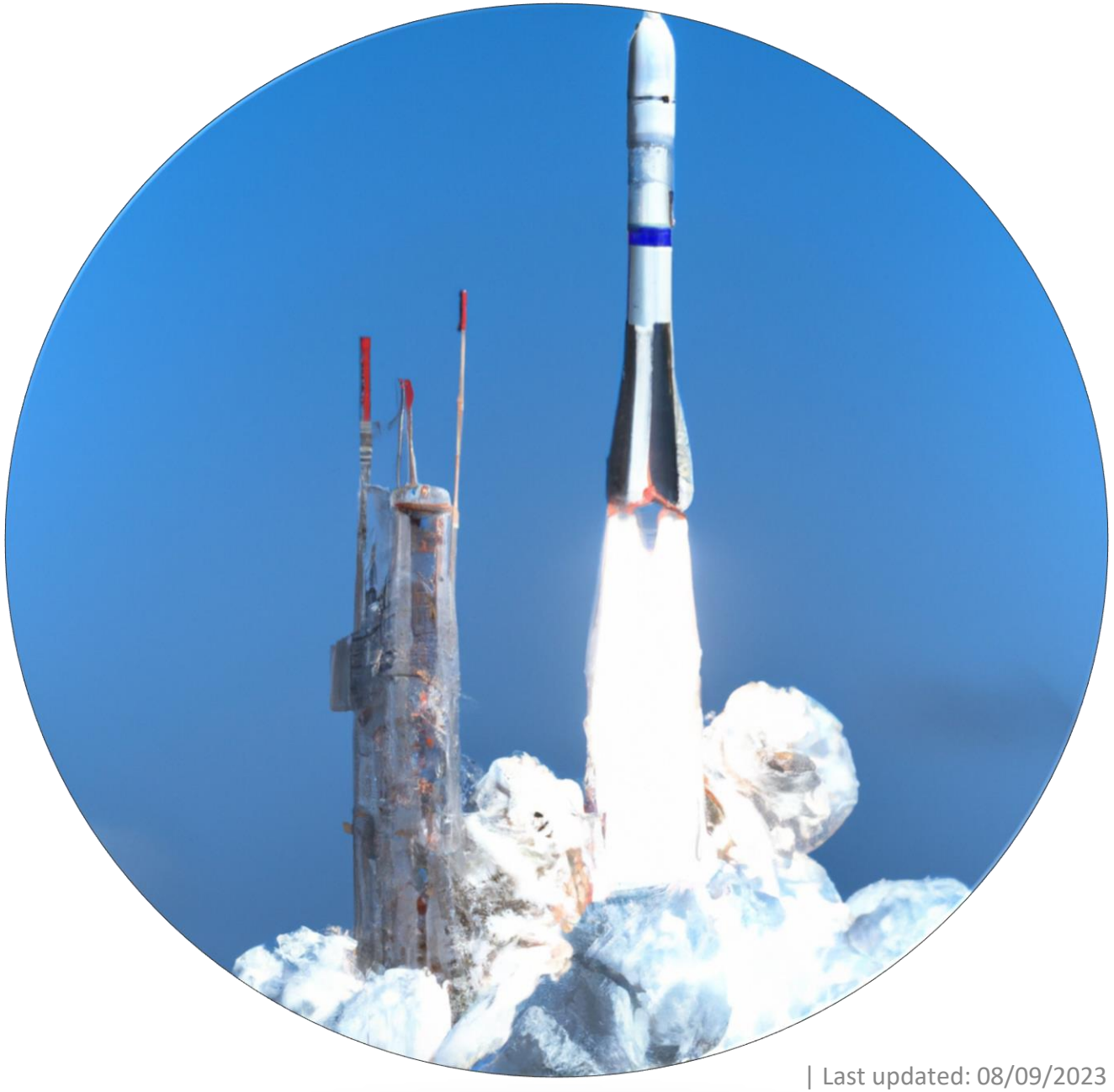
Streamlining system-safety engineering with digital technologies



Software Product Assurance Workshop
European Space Astronomy Centre, Spain
26-28th September 2023

| Last updated: 08/09/2023

Who are we?

ANZEN
SYSTEM SAFETY AND DIGITAL ENGINEERING

The company

- ✓ Spanish SME - Founded in 2019 – ESA BIC Madrid
- ✓ Team of 30 system /RAMS /MBSE engineers

Specialization

- ✓ Complex electronics
- ✓ Safety Critical Systems
- ✓ Autonomous & software defined systems

System, safety and reliability experts

- ✓ Specialization in complying with the highest quality standards for safety/availability critical missions

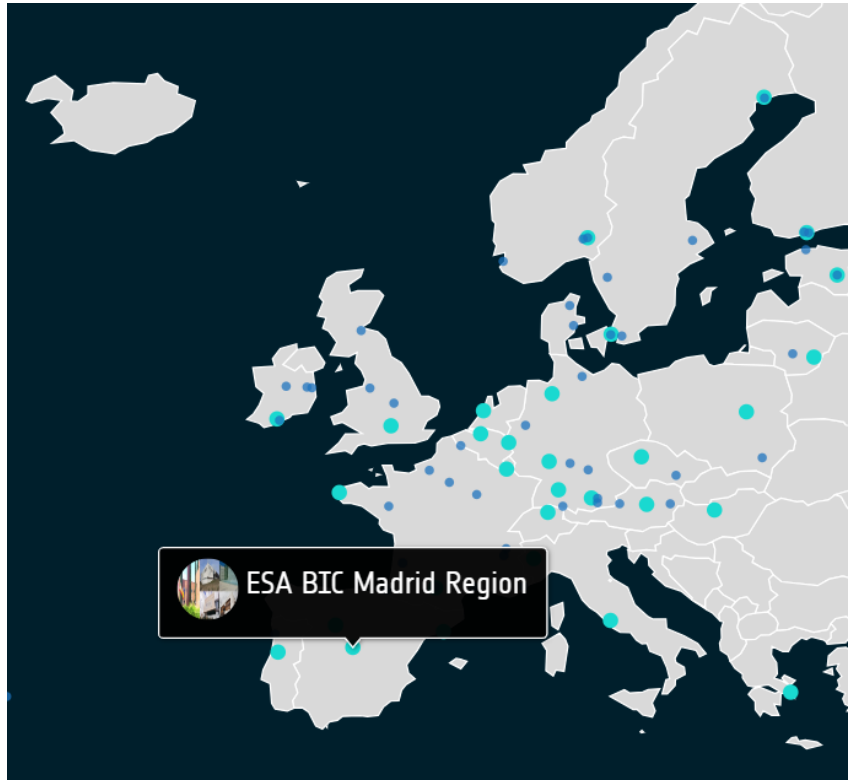
Digitalization of systems engineering

- ✓ Development and extension of model-based software tools for digitalization of the system & safety engineering process

ESA Business Incubation Centre

ANZEN
SYSTEM SAFETY AND DIGITAL ENGINEERING

Network of incubators supporting tech & space start-ups in Europe

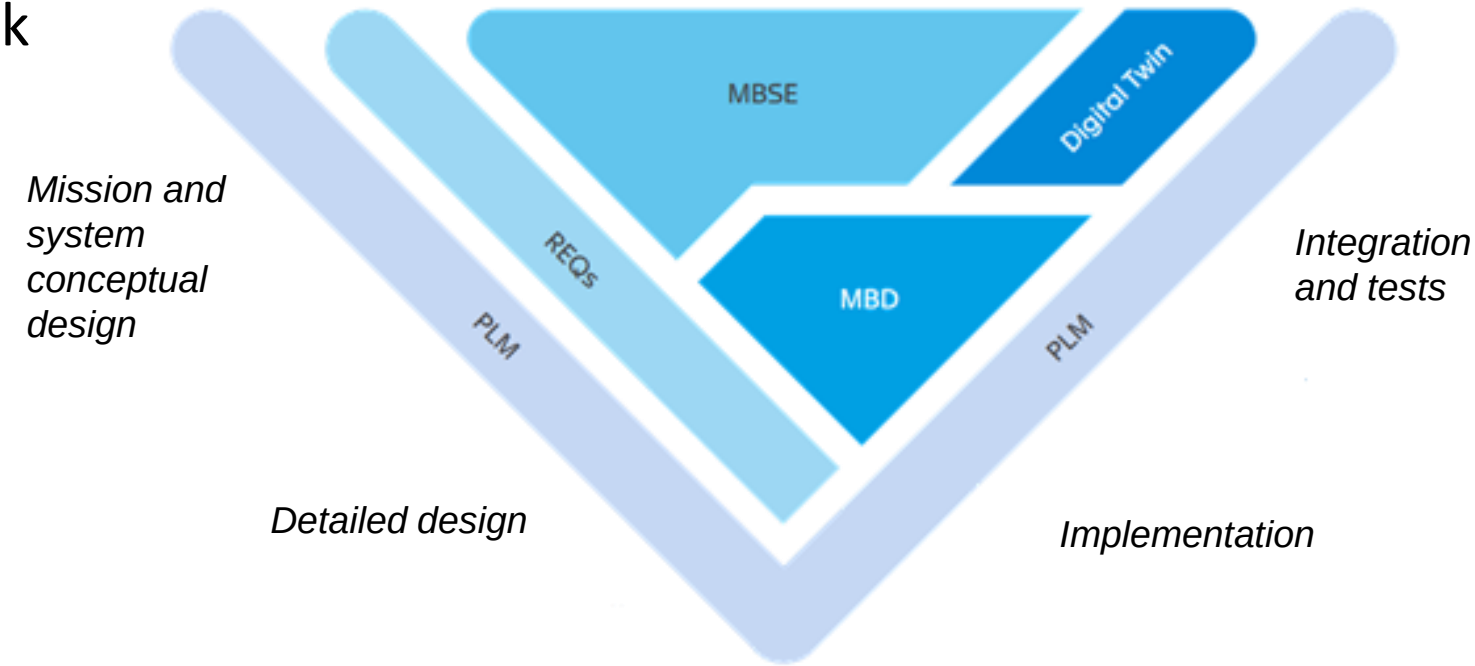


- Partnership between ESA and local institutions to support entrepreneurship
- Initial grant and commercial and technical assistance to launch the company
- Focus on technology transfer from space to other sectors (spin-off) and from other sectors to space (spin-in)
- **Anzen** joined ESA-BIC Madrid in 2019 with the mission of improving **safety & reliability** engineering in the **space** and **advanced air mobility** sectors

Outline

ATICA
Digital engineering for complex systems

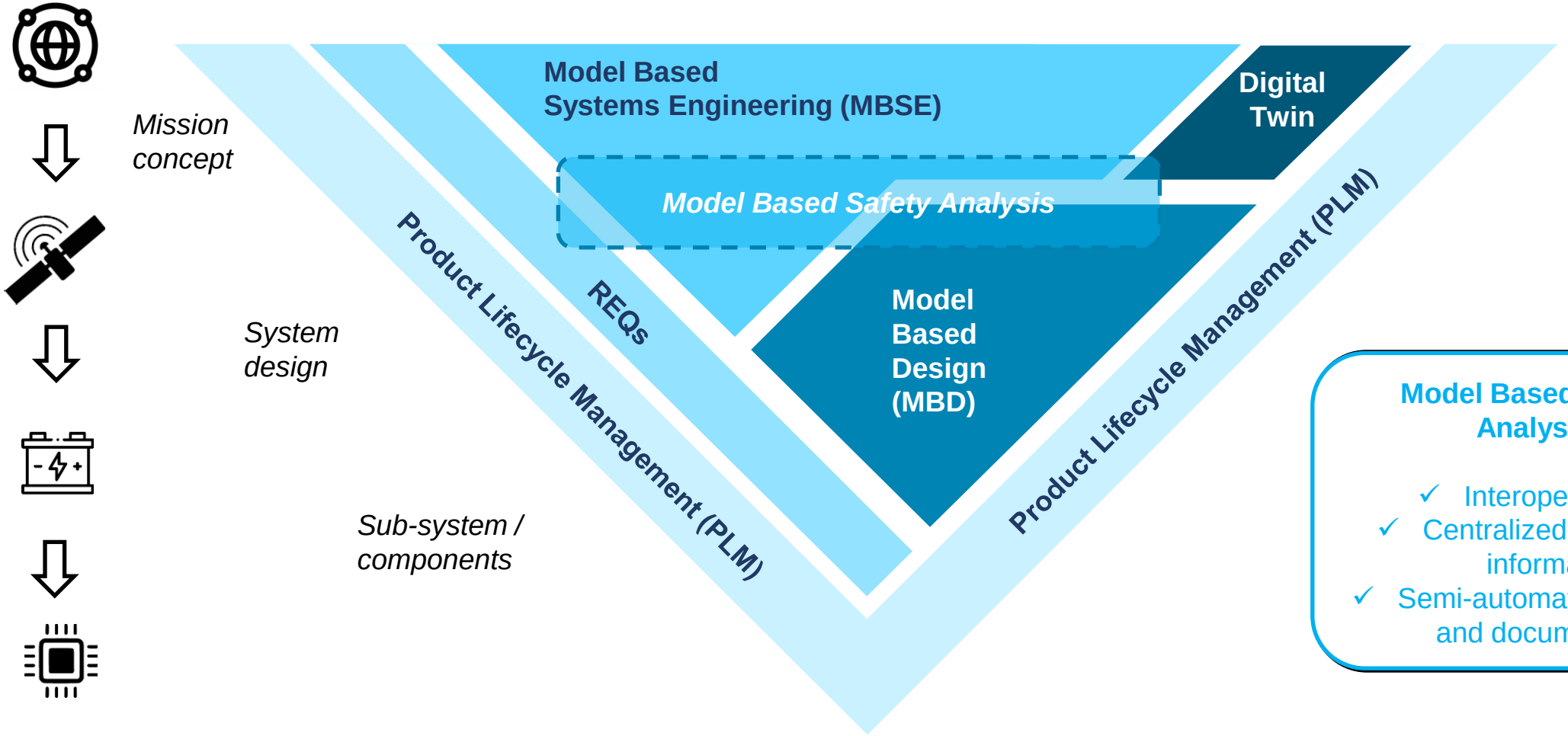
- Introduction to digital engineering
  - The systems engineering process
  - Framework and tools
- Safety and dependability analysis
- Wrap-up and future work



The systems engineering process

ATICA
Digital engineering for complex systems

Use of digital tools to support the systems engineering process



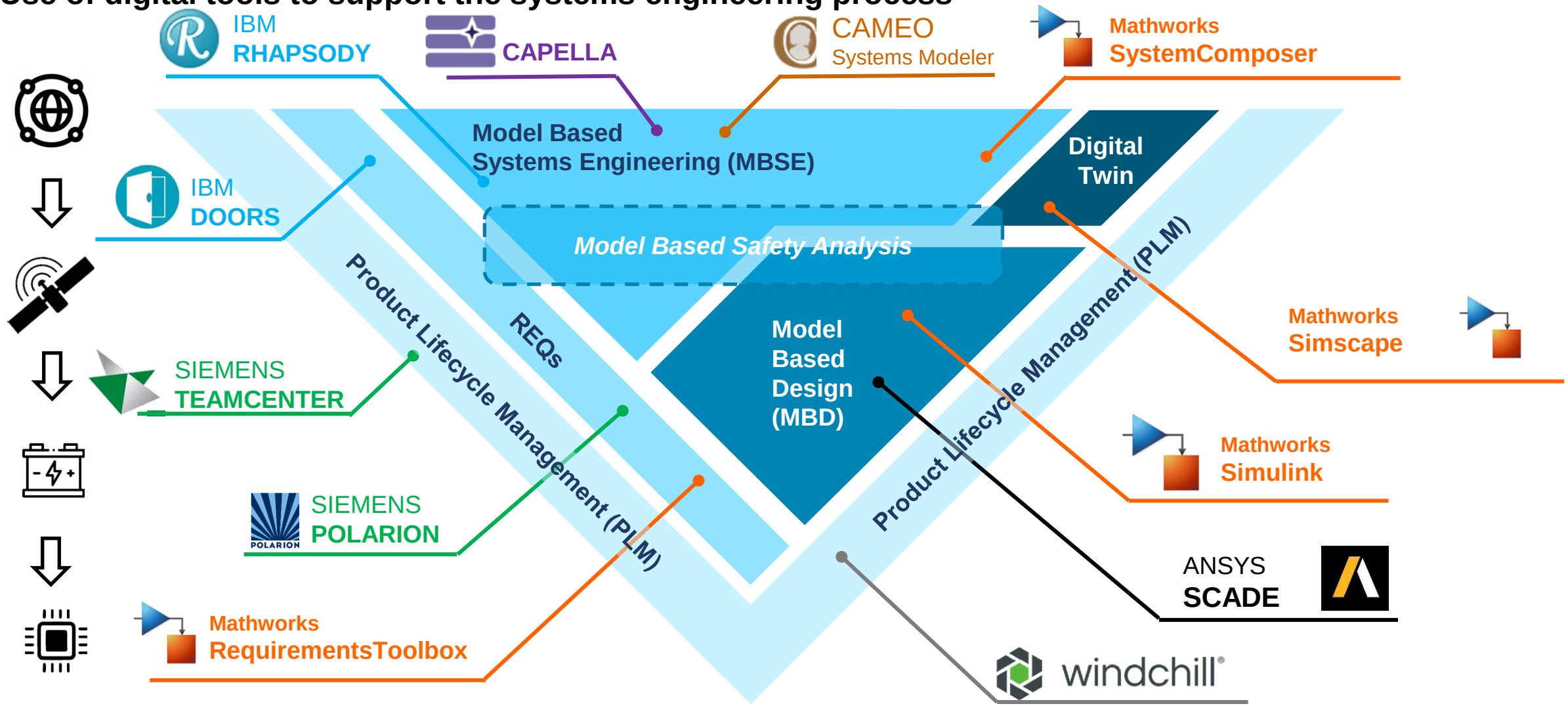
Model Based Safety Analysis

- ✓ Interoperability
- ✓ Centralized source of information
- ✓ Semi-automated analysis and documentation

Framework and tools

ATICA
Digital engineering for complex systems

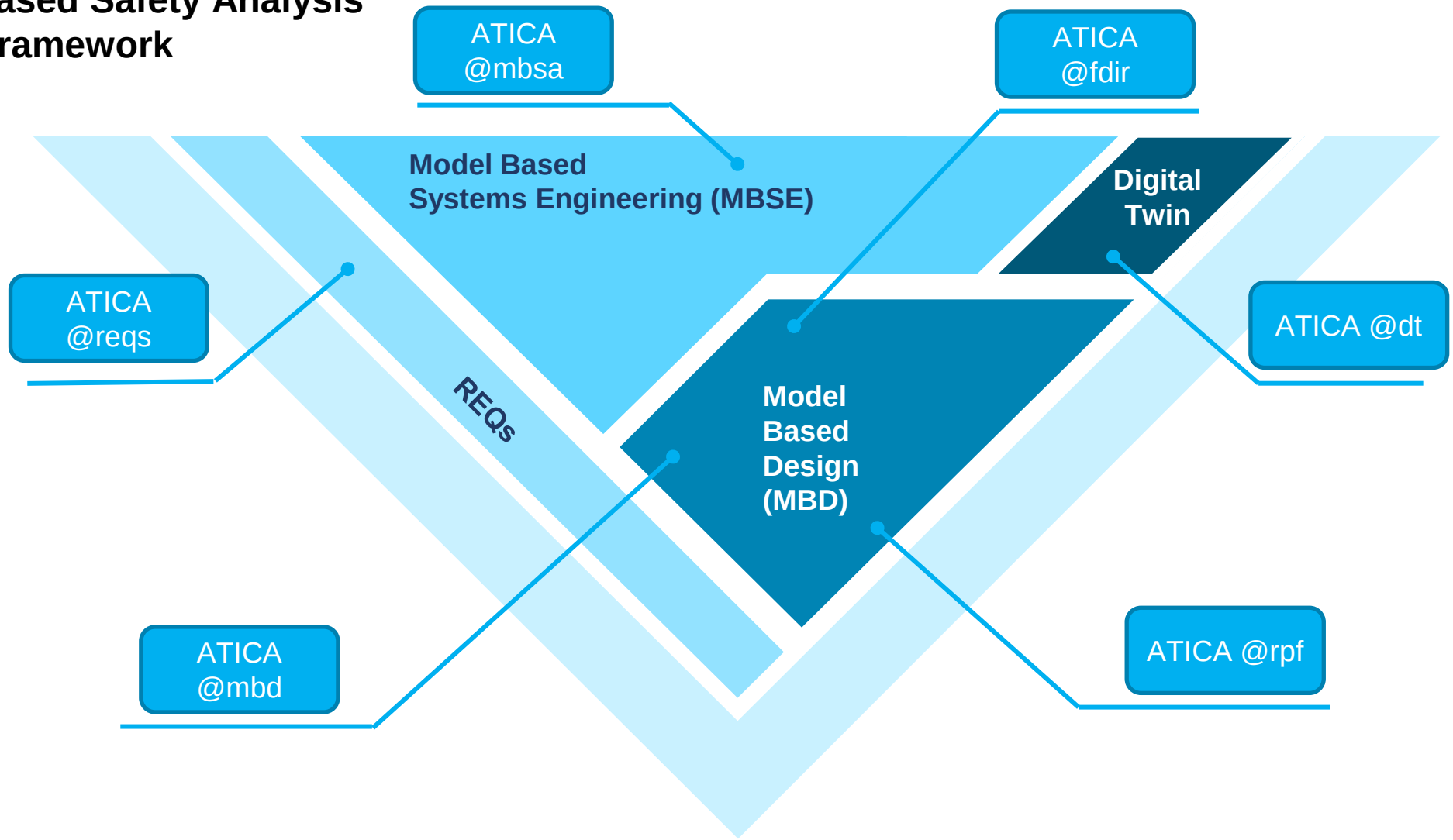
Use of digital tools to support the systems engineering process



Framework and tools

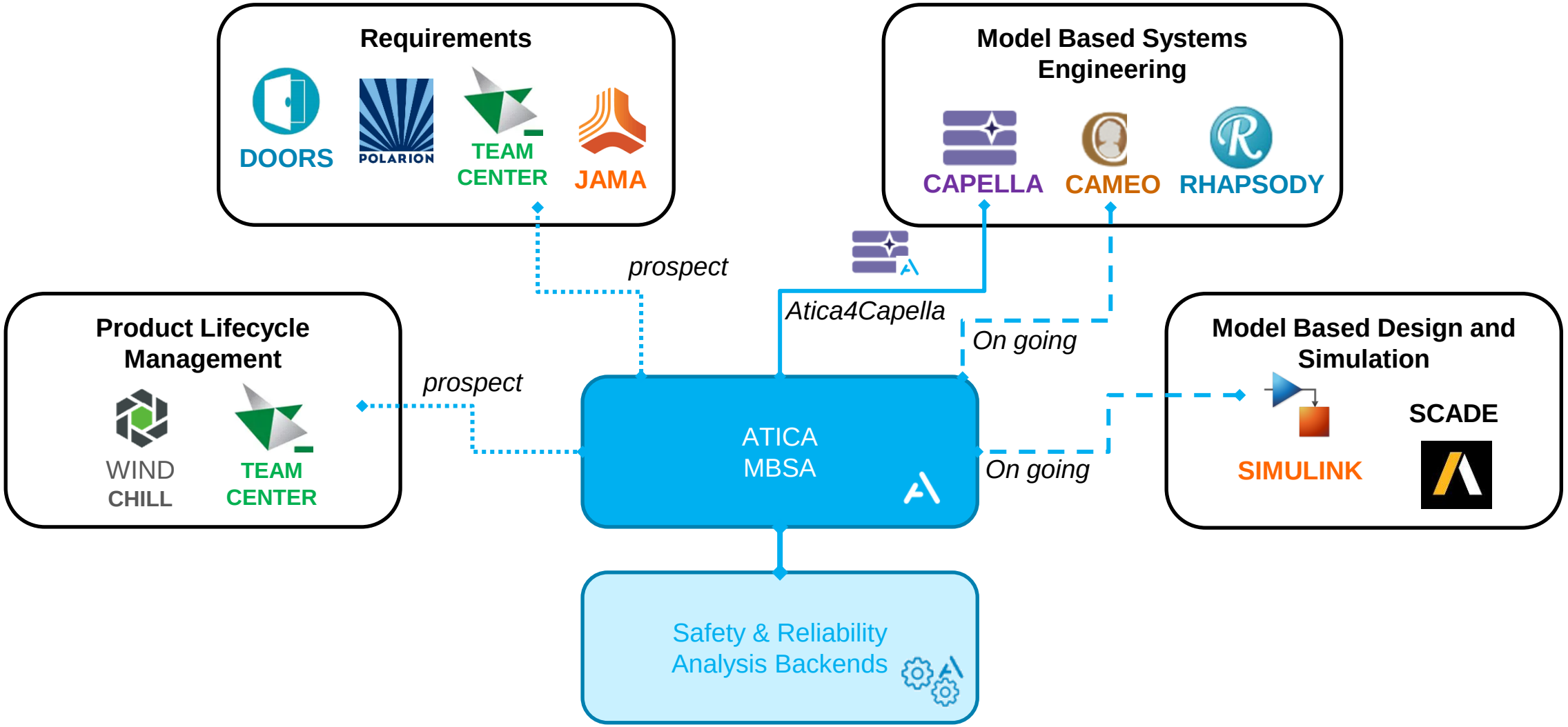
ATICA
Digital engineering for complex systems

Model Based Safety Analysis
ATICA Framework



ATICA Model Based Safety Analysis

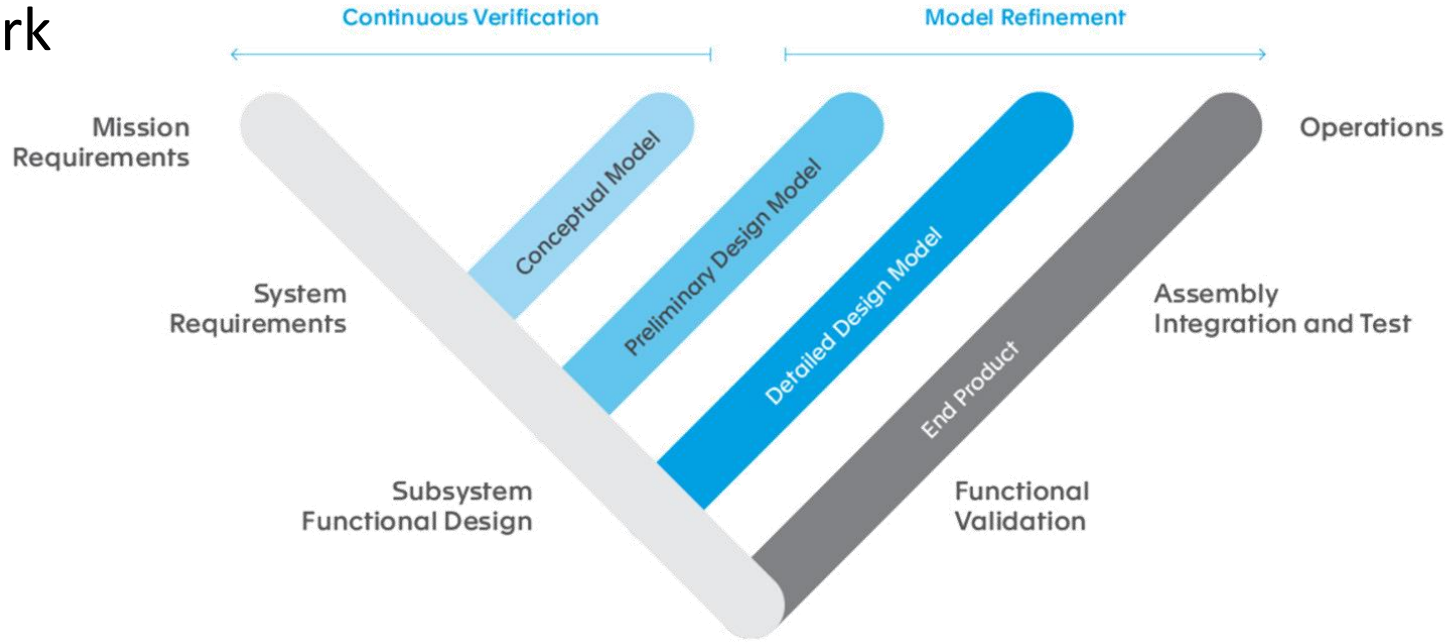
ATICA
Digital engineering for complex systems



Outline

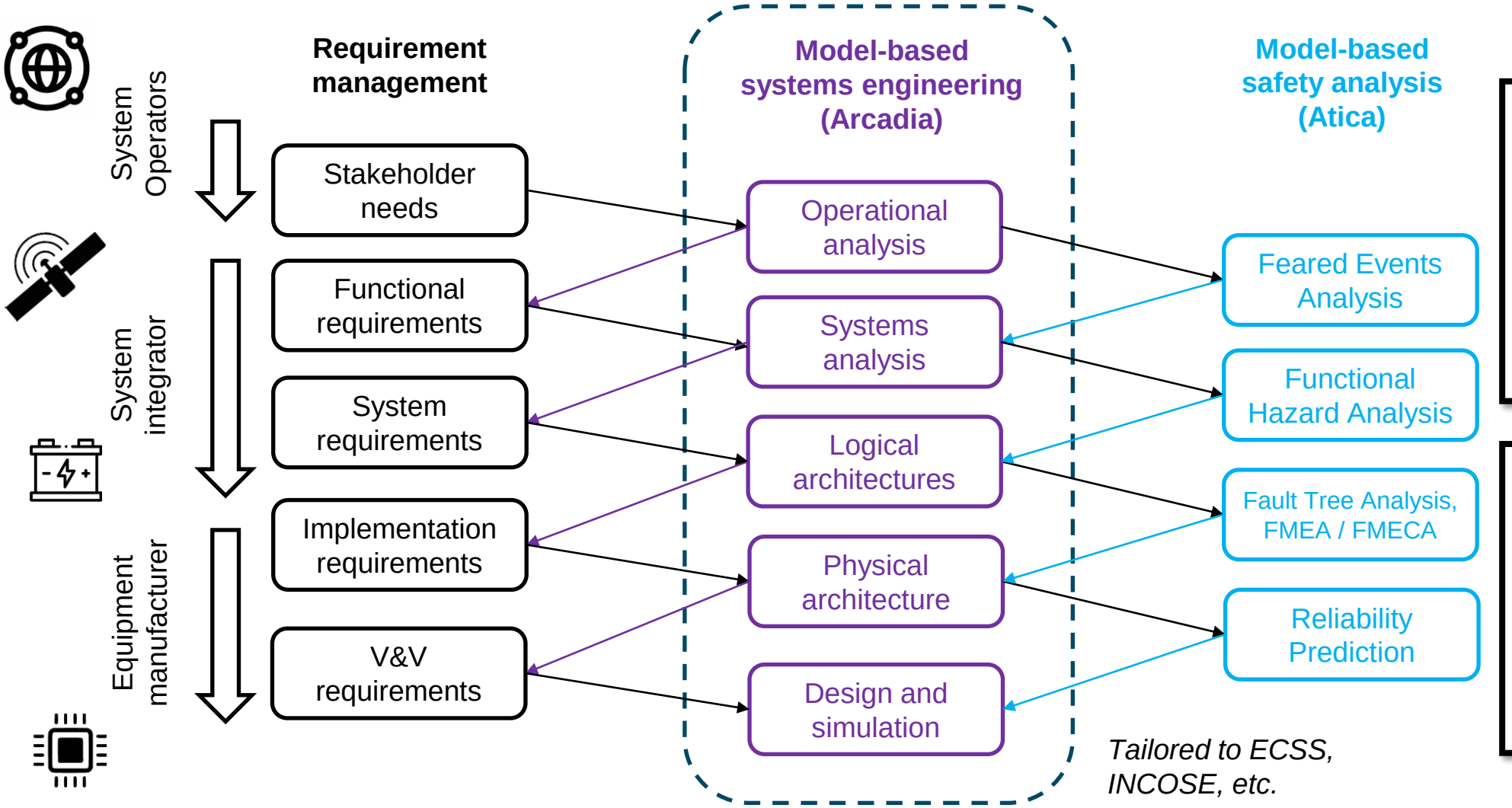
ATICA
Digital engineering for complex systems

- Introduction to digital engineering
- Safety and dependability analysis
  - Model-based systems engineering and RAMS
  - Systems analysis
  - Logical and physical architectures
- Wrap-up and future work



MBSE & RAMS framework

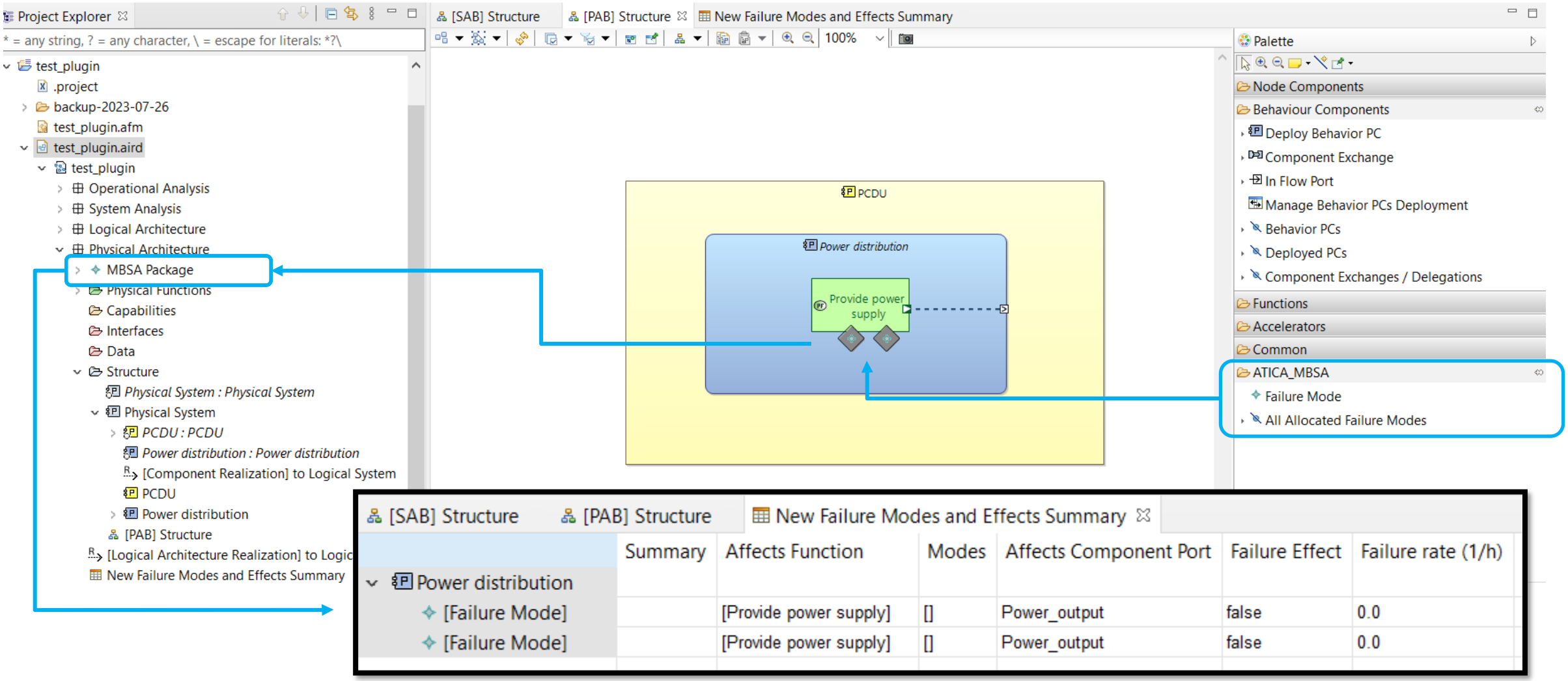
ATICA
Digital engineering for complex systems



Implementation in Capella

ATICA
Digital engineering for complex systems

FMEA & FMES



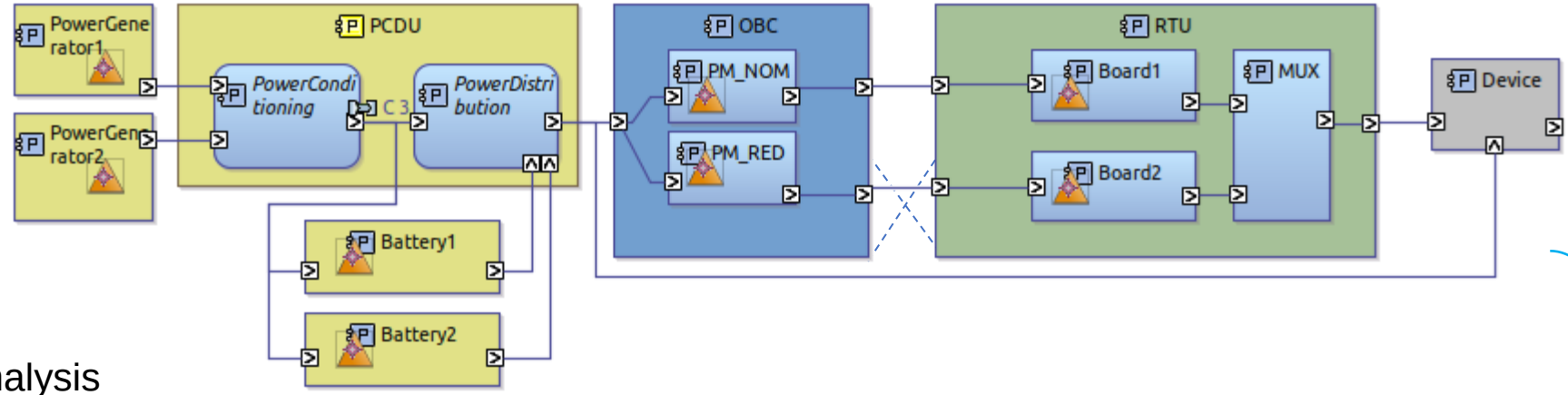
[SAB] Structure | [PAB] Structure | New Failure Modes and Effects Summary

	Summary	Affects Function	Modes	Affects Component Port	Failure Effect	Failure rate (1/h)
Power distribution						
[Failure Mode]		[Provide power supply]	[]	Power_output	false	0.0
[Failure Mode]		[Provide power supply]	[]	Power_output	false	0.0

Implementation in Capella

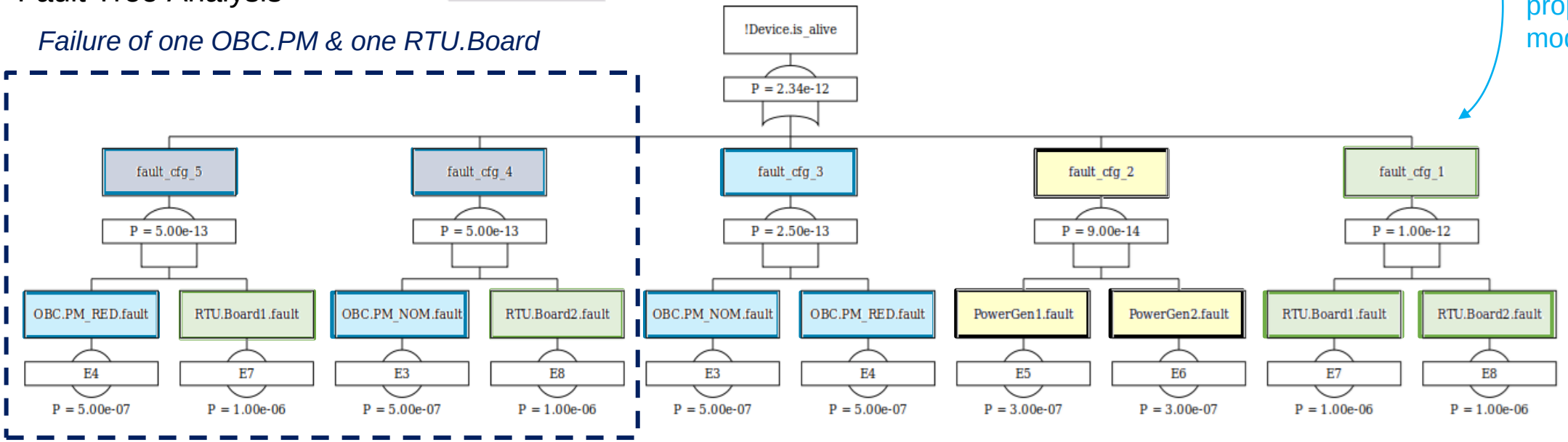
ATICA
Digital engineering for complex systems

✓ Extended system model: logical architecture + failure specifications



✓ Fault Tree Analysis

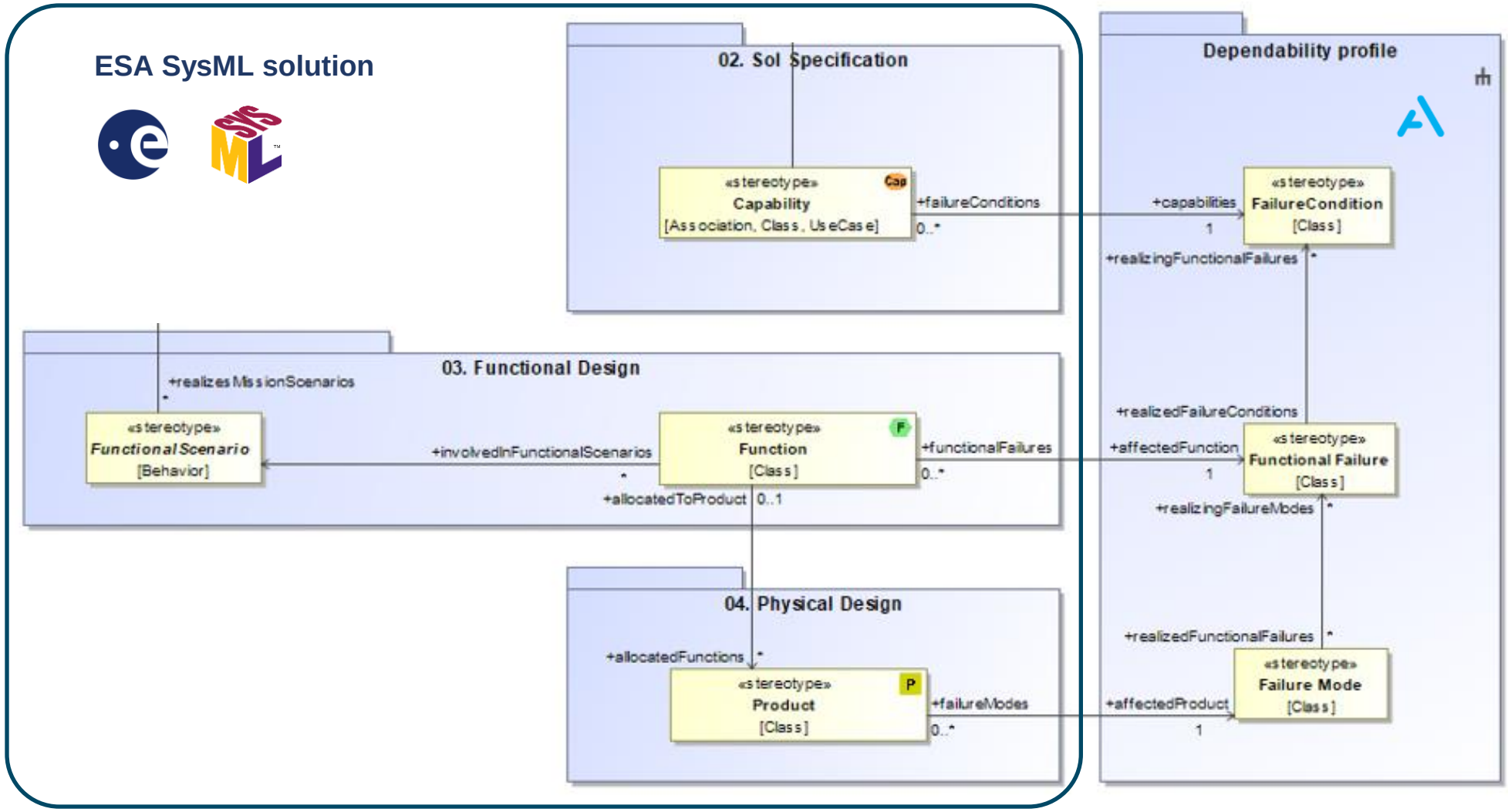
Failure of one OBC.PM & one RTU.Board



Failure propagation model

Adaptation to ESA SysML Solution

ATICA
Digital engineering for complex systems

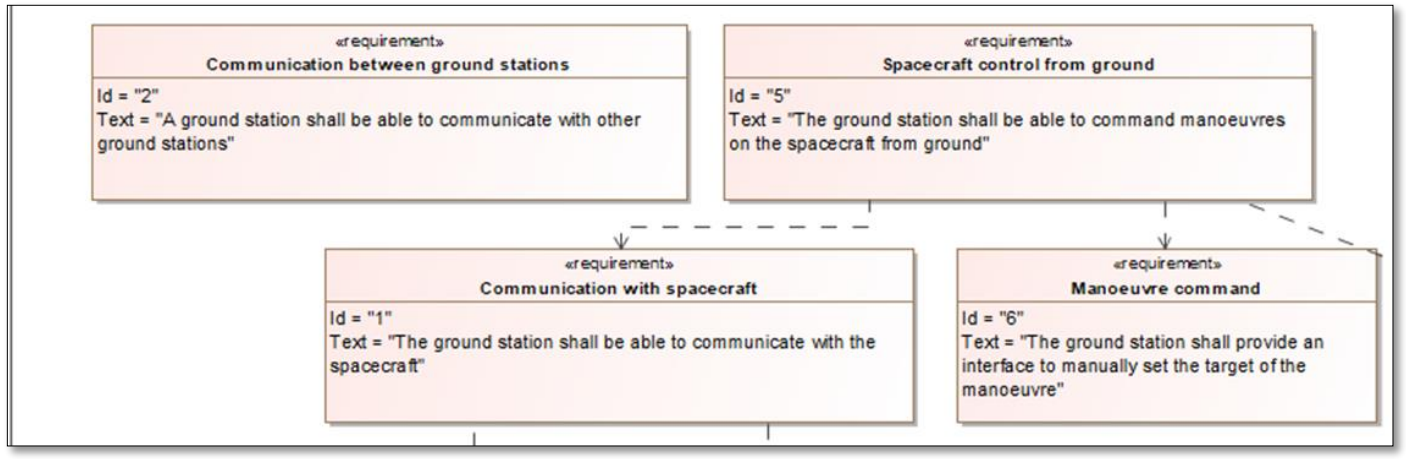


ATICA
Model-based safety & dependability profile

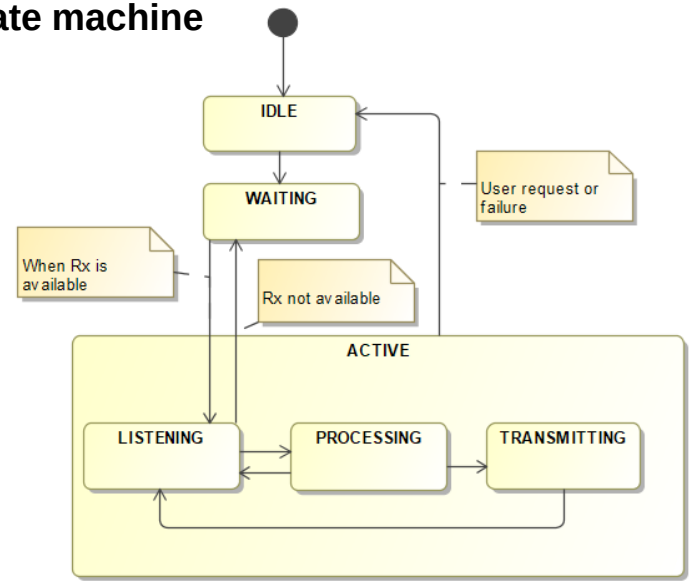
Implementation in Cameo

ATICA
Digital engineering for complex systems

Requirement diagram

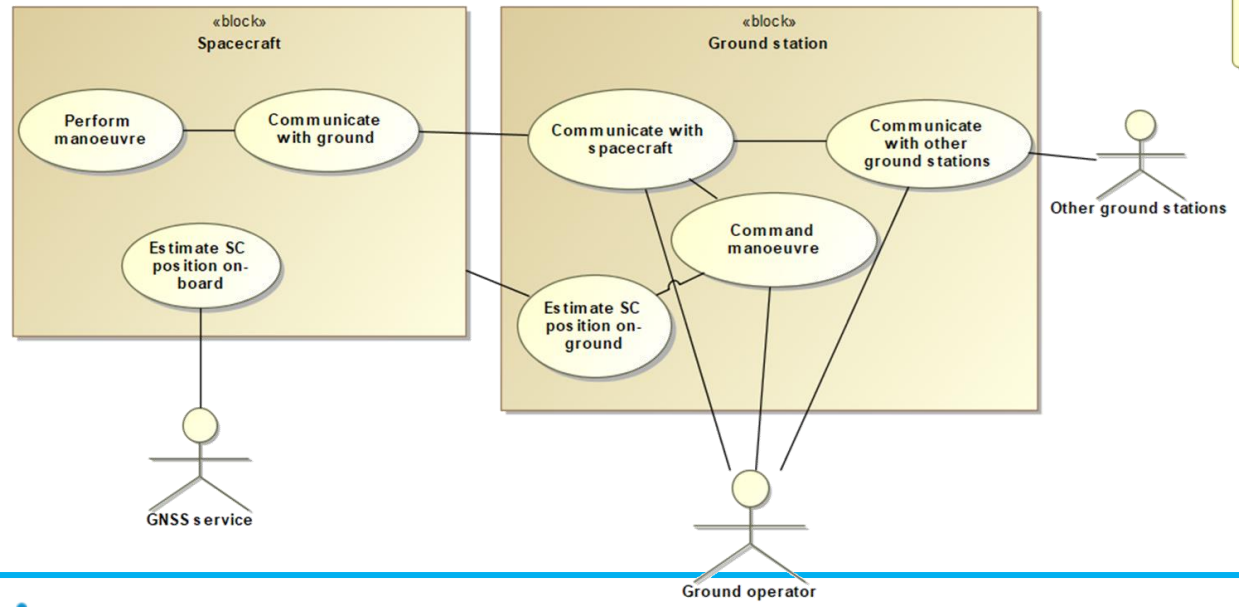


State machine



Behavior diagrams

- Use case
- Activity diagrams
- Sequence diagrams
- …

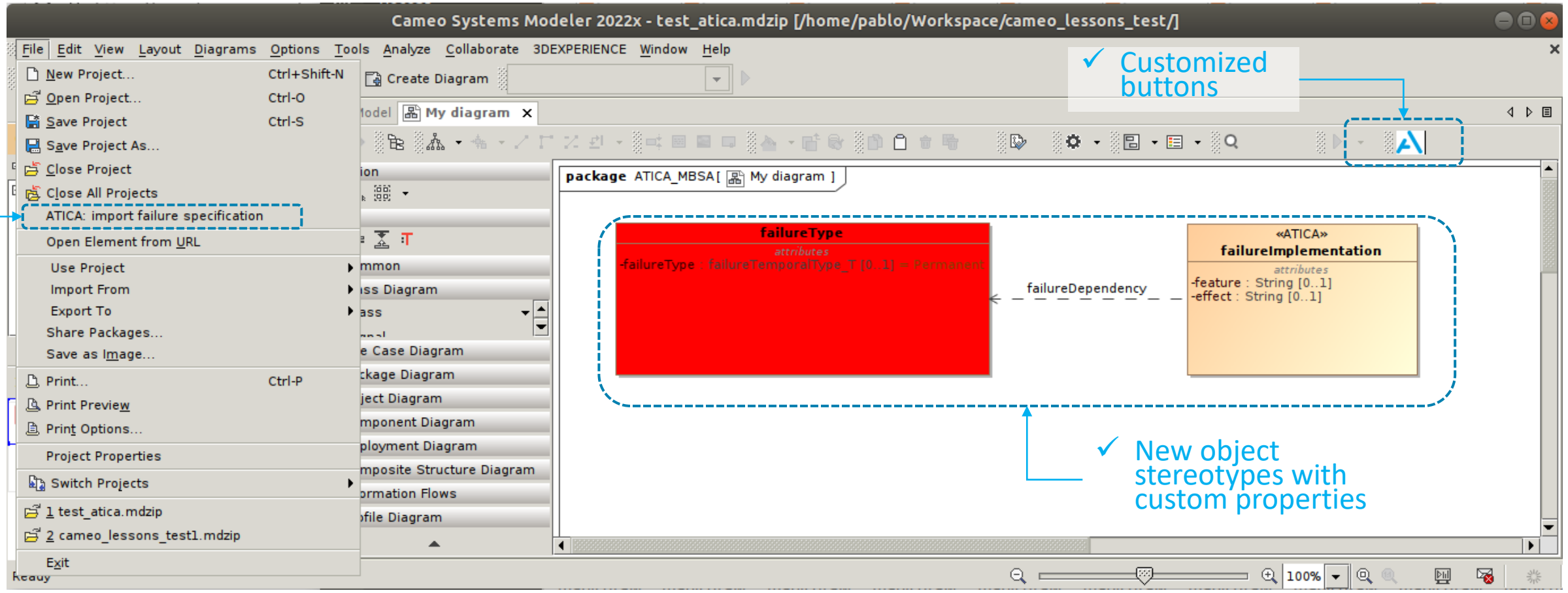


Support to RAMS analysis

- Feared Events Analysis
- Functional Hazard Analysis

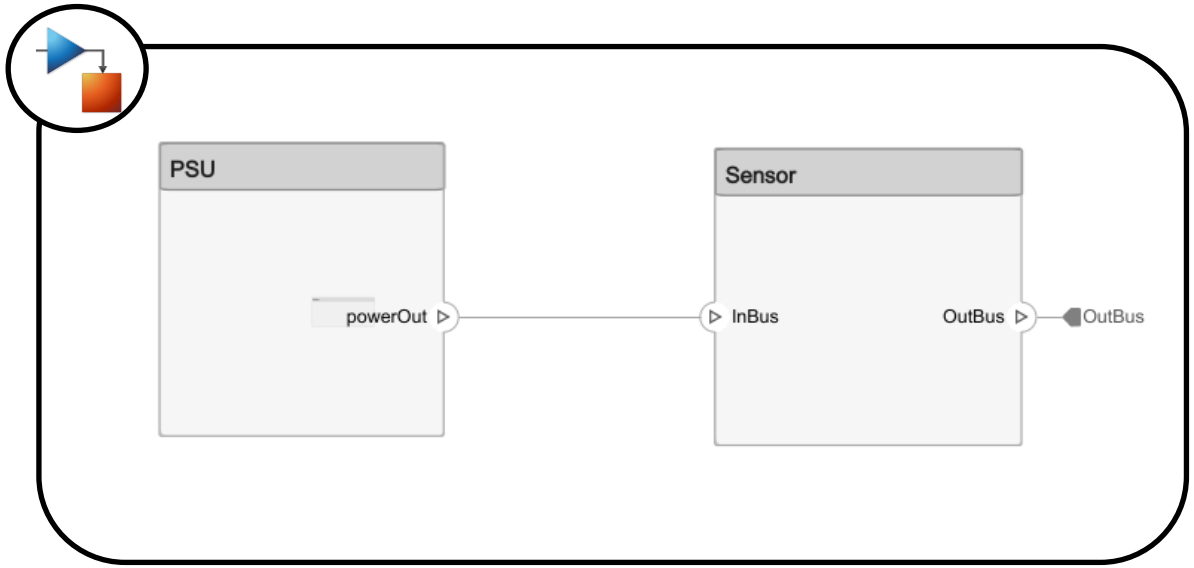
Implementation in Cameo

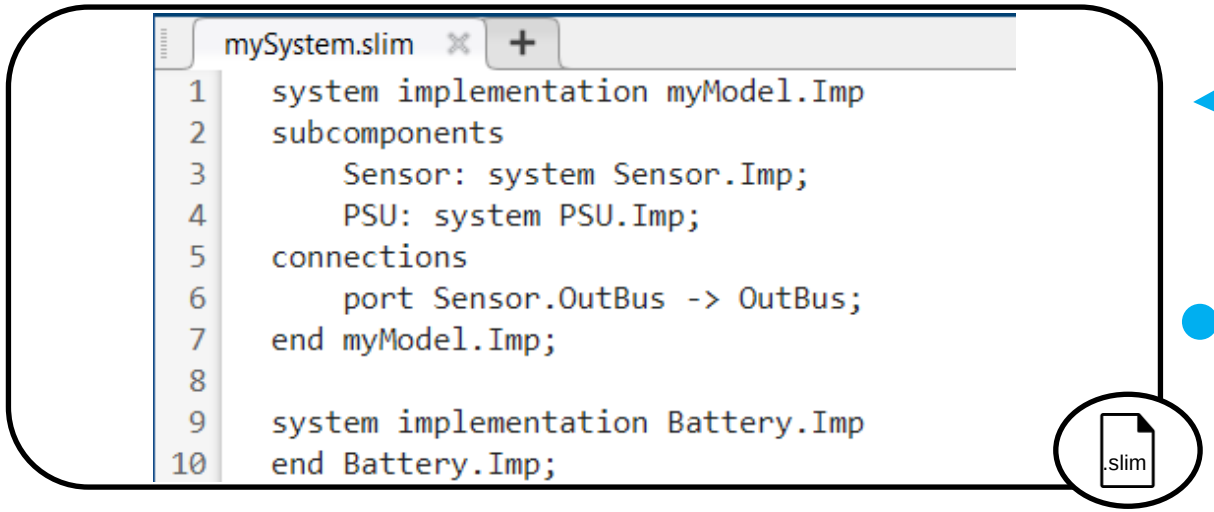
ATICA
Digital engineering for complex systems



From models to formal specification

ATICA
Digital engineering for complex systems





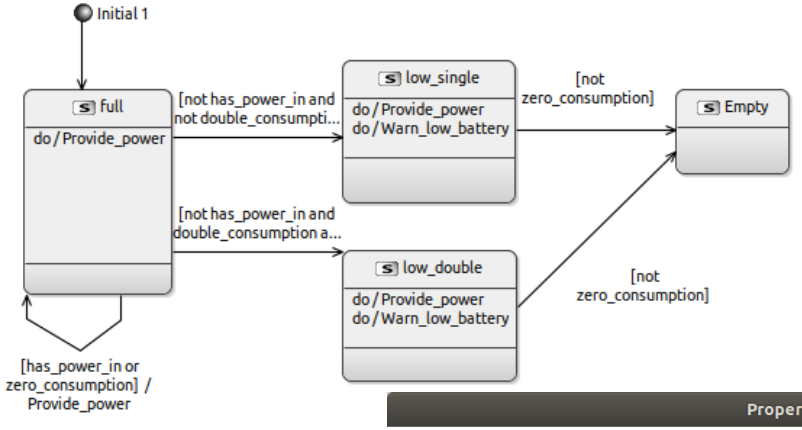
Model parser:
SysML (System Composer)
to SLIM/AADL (TASTE/COMPASS)

Analysis backends
FMEA
Reliability Block Diagrams (RBD)
Fault tree analysis (COMPASS)
Model checking (COMPASS)

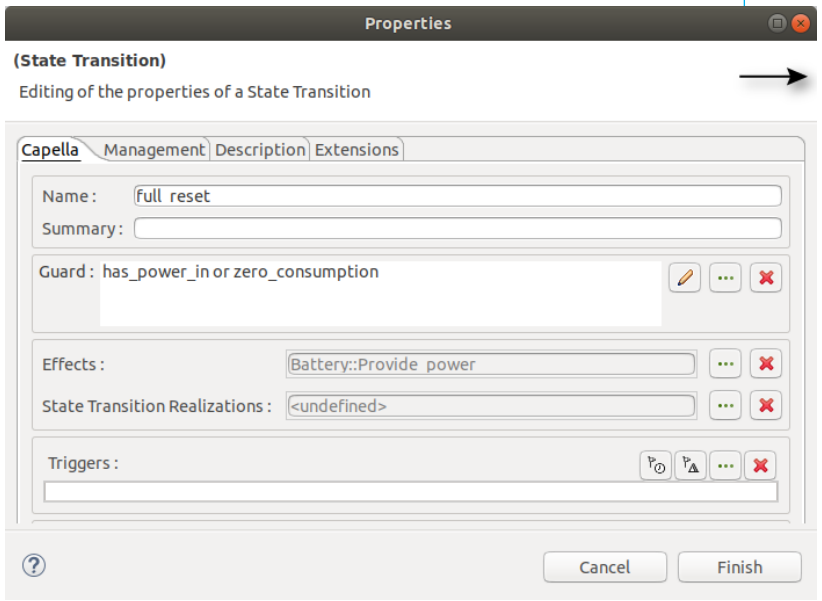
From models to formal specification

ATICA
Digital engineering for complex systems

Modelling viewpoint



Transition specification



Guard

Effects

Triggers

AADL/SLIM file

```
system implementation Battery.Imp
  states
    full: initial state;
    low_single: state;
    Empty: state;
    low_double: state;
  transitions
    full -[ when not has_power_in and not double
            then has_power_out := true; low := t
    low_single -[ when not zero_consumption
            then  ]-> Empty;
    full -[ when has_power_in or zero_consumptic
            then has_power_out := true ]-> full;
    full -[ when not has_power_in and double_cor
            then has_power_out := true; low := t
end Battery.Imp;
```

Transition condition specification
[*trigger* when *guard* then *effect*]

Implemented features:

- ✓ Mode/state declaration
- ✓ Mode/state transition
- ✓ Mode/state transition criteria (guard) and effects

Outline

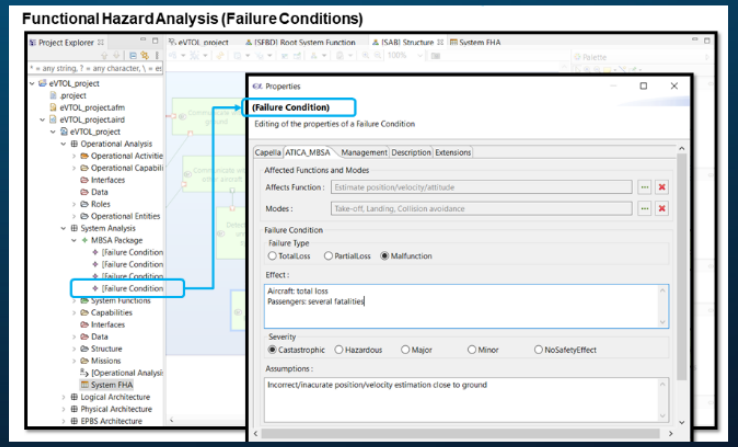
ATICA
Digital engineering for complex systems

- Introduction to digital engineering
- Safety and dependability analysis
- Wrap-up and future work

\ ANZEN \ Download

ATICA4Capella

ATICA4CAPELLA is a model based safety analysis (MBSA) plugin that extends Capella functionalities and allows to perform safety and reliability analysis directly from the system models.



Download Atica4Capella READ MORE

Wrap-up and future work

ATICA
Digital engineering for complex systems

Key takeaways

- ✓ ATICA is a model-based safety and dependability analysis framework
- ✓ ATICA could be adapted to multiple MBSE frameworks and modeling methodologies

ATICA simplifies the job of systems and software architects by providing a consistent **framework** covering from conceptual design up to hardware & software implementation

Wrap-up and future work

ATICA
Digital engineering for complex systems

Future work

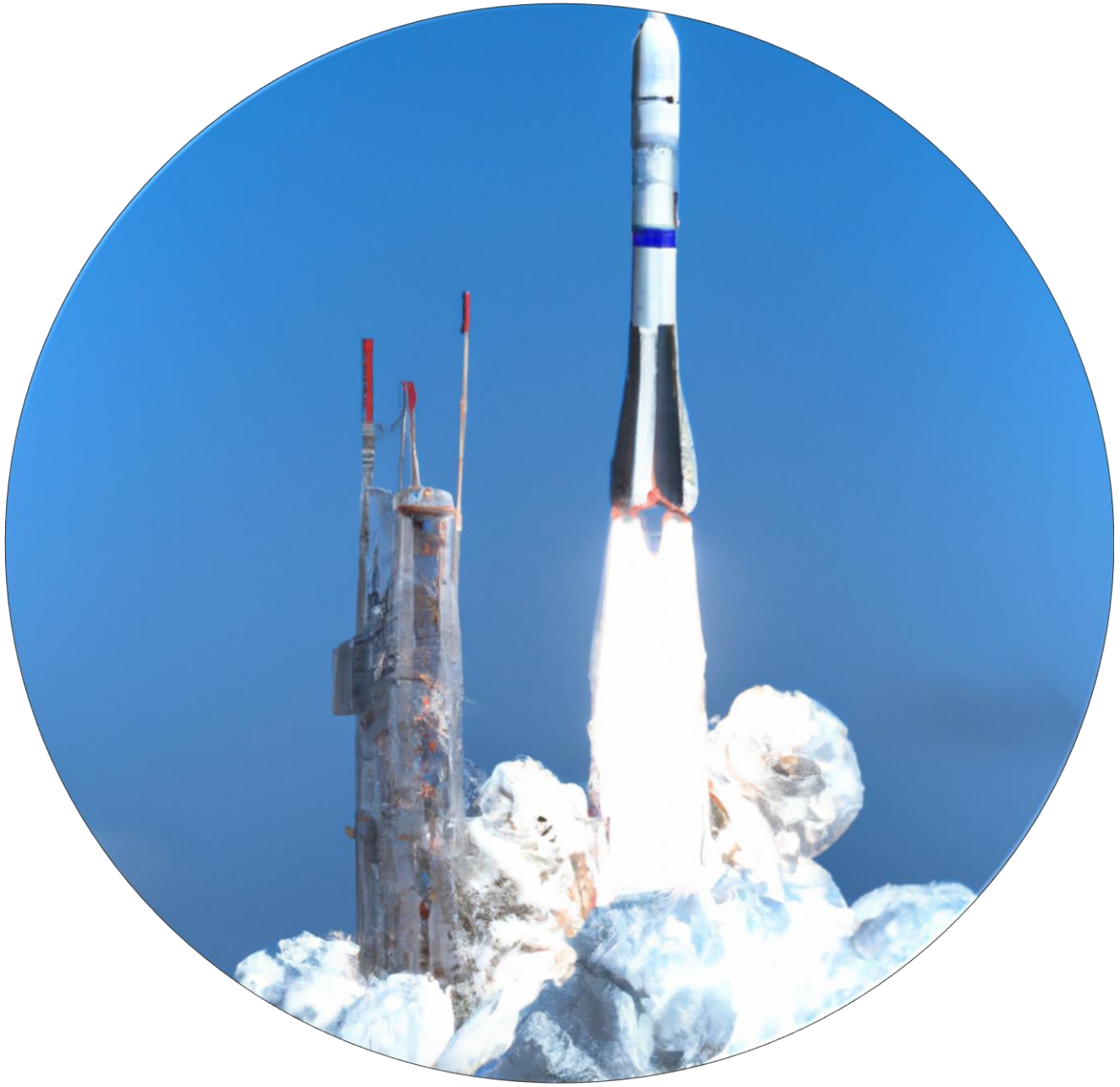
- ✓ Consolidate the framework and extend its functionalities towards software engineering
  - ✓ Hardware and Software Integration Analysis (HSIA)
  - ✓ System correctness (model checking and formal analysis)
  - ✓ Dynamic and autonomous systems (FDIR)

ANZEN

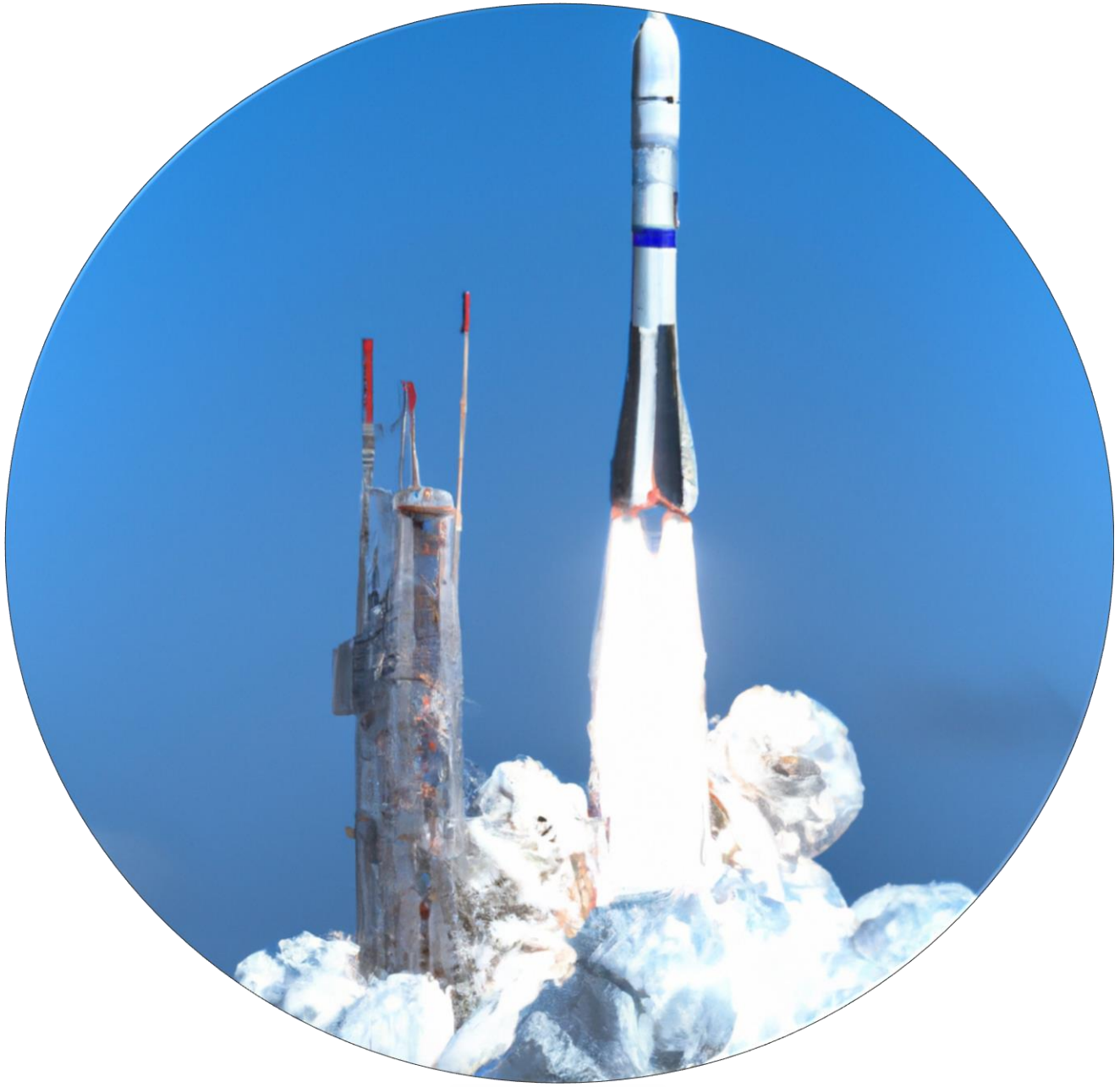
SYSTEM SAFETY AND DIGITAL ENGINEERING

Pablo Lopez Negro
Head of Innovation
pablolopez@anzenengineering.com

María Alonso López
PA & RAMS Lead
mariaalonso@anzenengineering.com



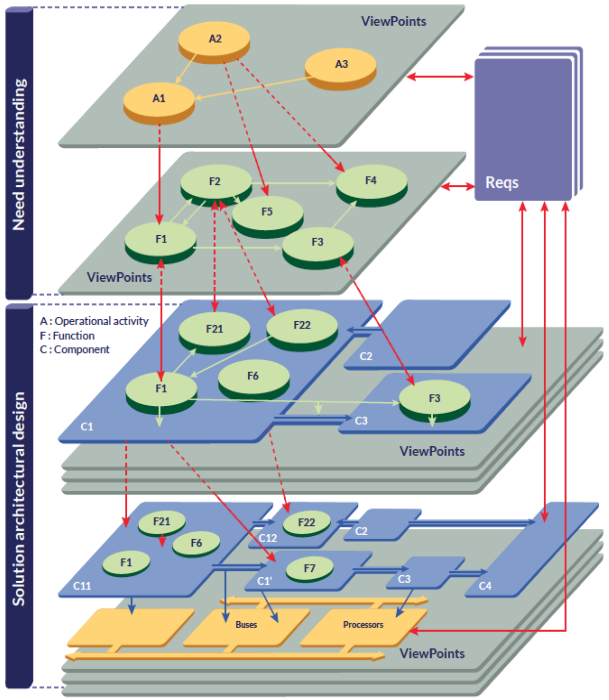
Backup slides



Model-Based Systems Engineering

ATICA
Digital engineering for complex systems

CAPELLA / ARCADIA - MBSE Framework



Operational Analysis
What the users of the system need to accomplish

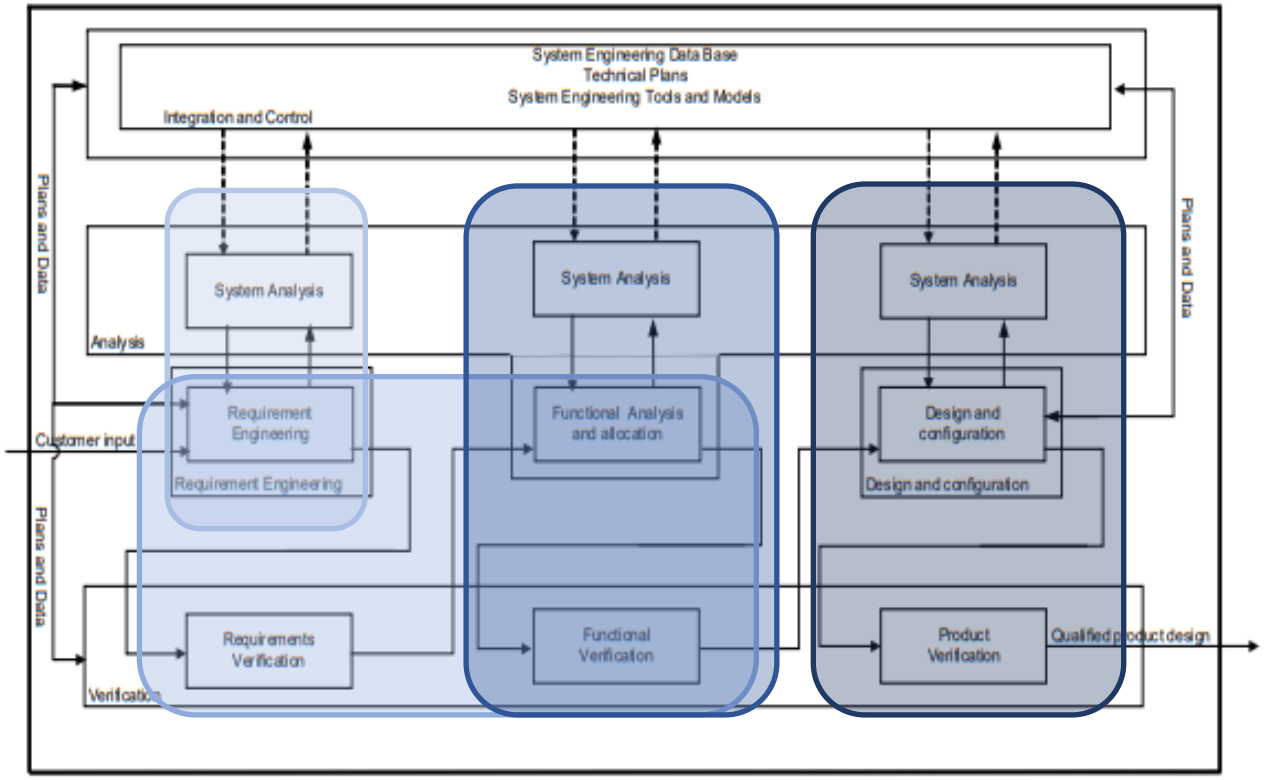
Functional & Non Functional Need
What the system has to accomplish for the users

Logical Architecture
How the system will work to fulfill expectations

Physical Architecture
How the system will be developed and built

tailoring

ECSS-E-ST-10C Rev1 – System Engineering General Requirements



Model-Based Systems Engineering

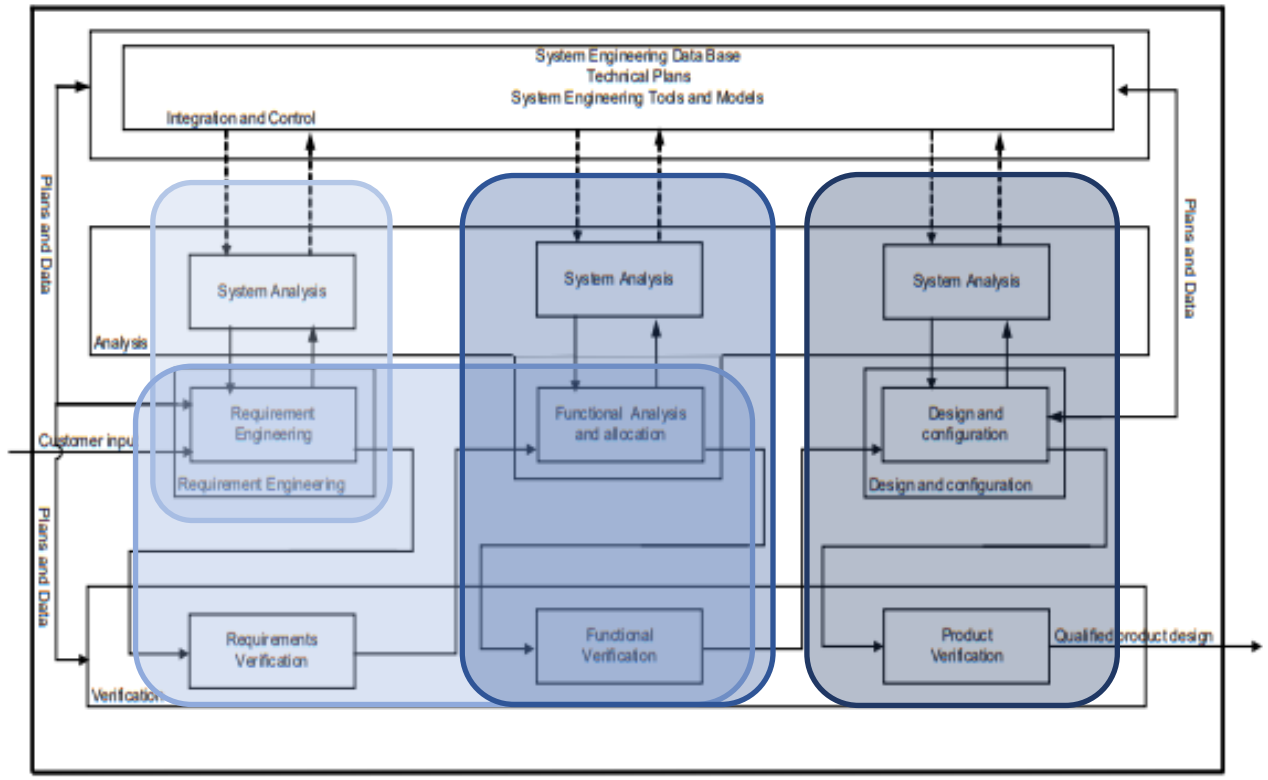
ATICA
Digital engineering for complex systems

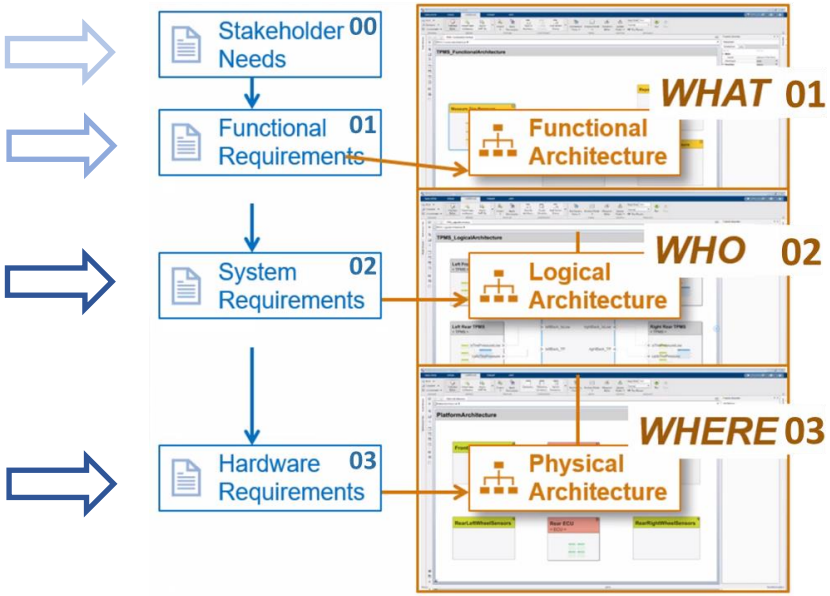
Adaptation to MBSE frameworks

tailoring

Mathworks
SystemComposer (SysML)

ECSS-E-ST-10C Rev1 – System Engineering General Requirements



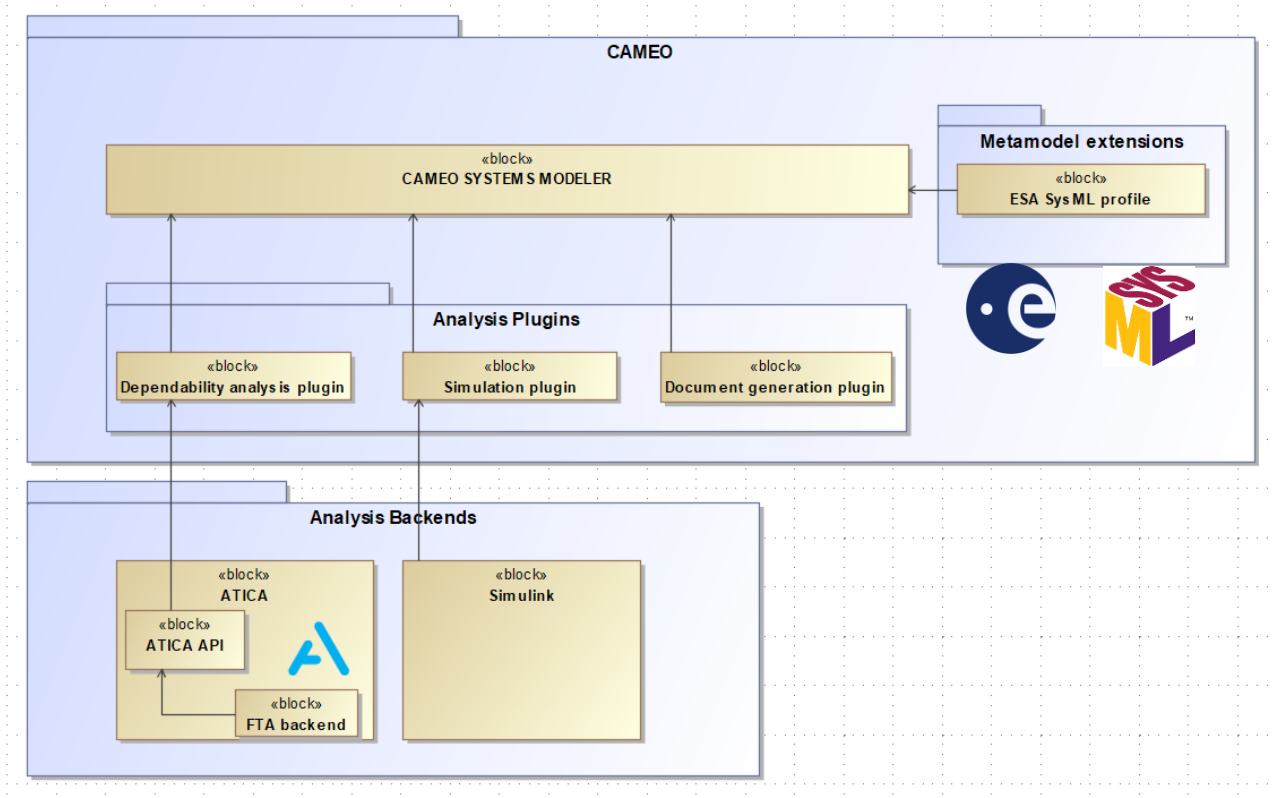


Model-Based Systems Engineering

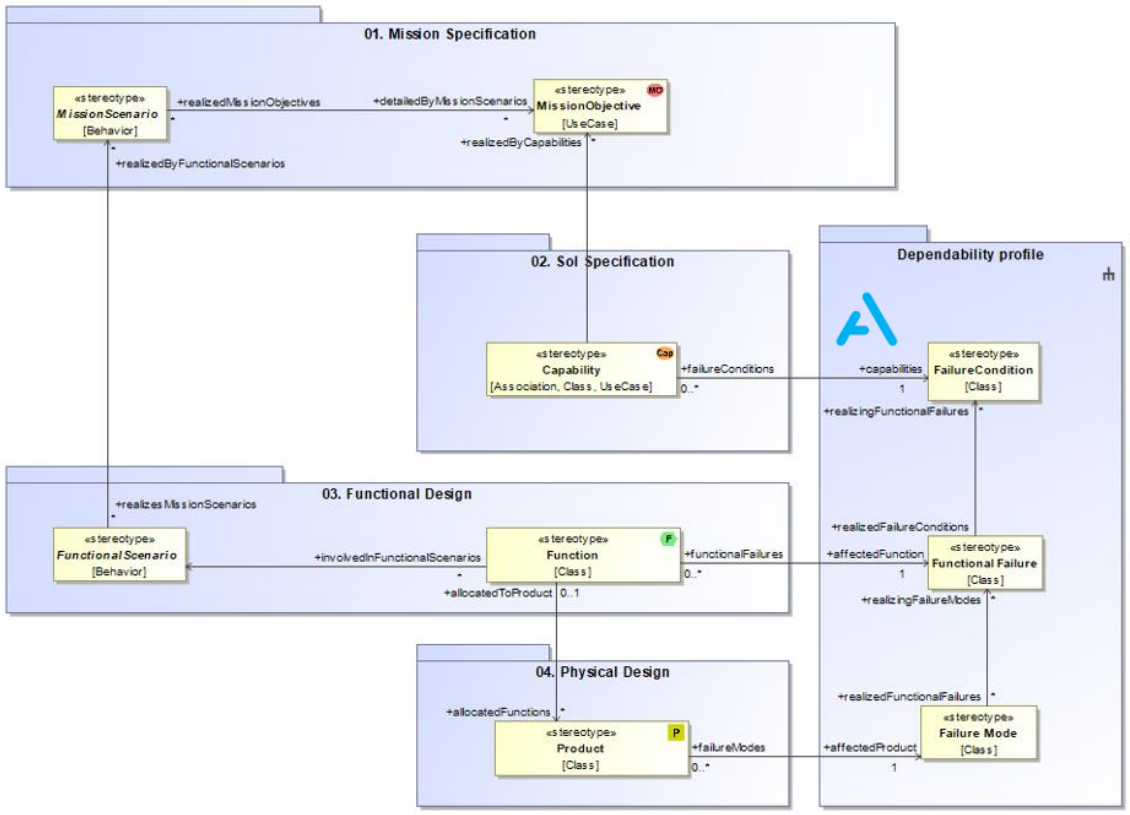
ATICA
Digital engineering for complex systems

Adaptation to MBSE frameworks

Software architecture



System-Safety metamodel



Model-based
safety & dependability profile

Implementation in Capella

Digital engineering for complex systems