Definition of a Model Based Mission Assurance Methodology

Software Product Assurance Workshop 2023

Clement Puybareau

TEC-QQS YGT 2022-2023

27/09/2023

INTRODUCTION

- **Clement Puybareau**
- TEC-QQS YGT at ESA ESTEC

- Supervisor: **Isabelle Conway**

- Part of a trilateral NASA-ESA-JAXA MBMA Task Force

WHAT TO EXPECT?

- Technical deep-dive

- Overview of the MBMA methodology and the core concepts built so far
- Example through simple SysML project
- Observations, lessons learned and future work/prospect
- Communicate the philosophy of our work

WHAT IS MBSE?

- **MBSE = M**odel **B**ased **S**ystem **E**ngineering

- "*formalized application of modelling to support system requirements, design, analysis, verification and validation activities*" - INCOSE-TP-2004-004-02, Sep 2007
- *"[MBSE] uses modelling techniques to look at the space system as a whole, with all of the subsystems and individual parts considered while they are all worked on separately by specialist teams"* – What is MBSE?, TEC Directorate

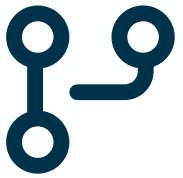
WHAT IS MBSE?

- **MBSE = M**odel **B**ased **S**ystem **E**ngineering

Describe your system with diagrams instead of words

WHAT IS MBSE?

- Going from a text-based approach to a model-based approach brings numerous advantages:



Single Source of Truth (**SSoT**) + Easier traceability/versioning

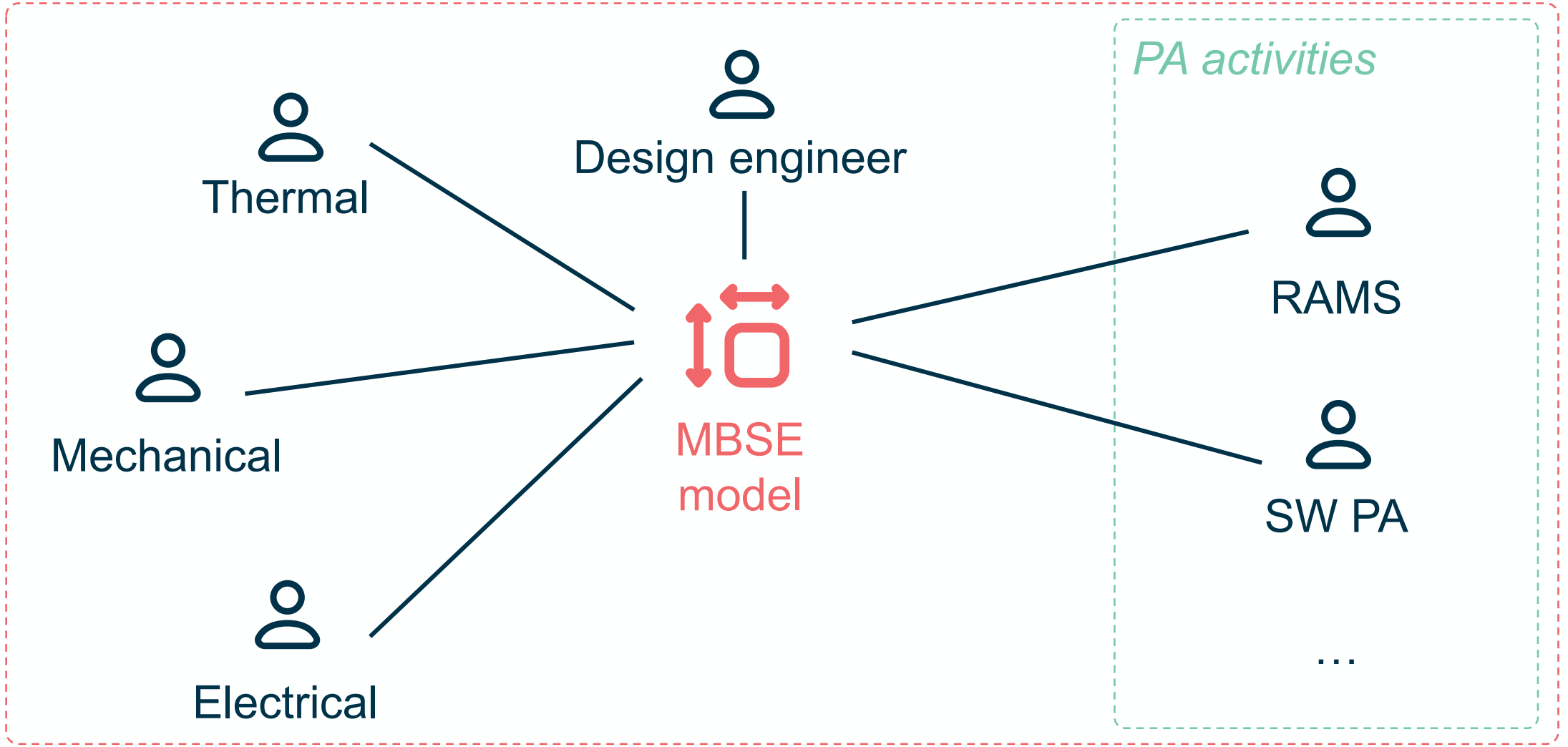
Access to **automation** & auto-coding

Improved communication between stakeholders…
If they speak the same language

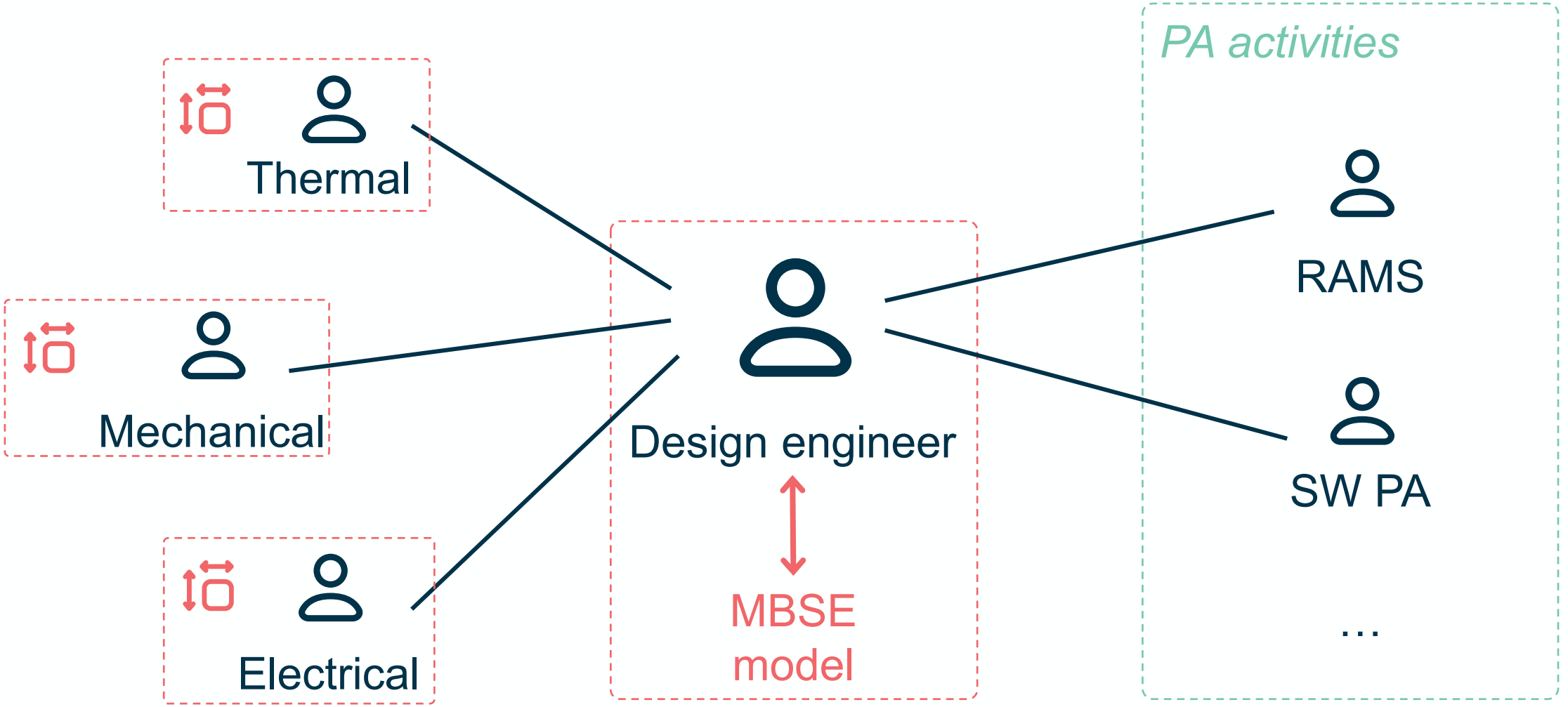
WHAT IS MBSE?

➔ If MBSE is so great, why do we not see wider adoption?

HOW IT SHOULD BE...



HOW IT IS...


PA activities
Thermal
Mechanical
Electrical
Design engineer
MBSE model
RAMS
SW PA
...

WHAT IS MBMA?

Observation:

- MBSE methodology and toolset have reached a stable point for System Engineering activities
- Product Assurance activities are not well integrated in the MBSE environment

➔ Need to define a Model Based Mission Assurance Methodology

i.e. defining how PA activities should be done inside a model

WHAT IS MBMA?

End goal of MBMA:

- Allow PA engineers to integrate their activities inside the existing MBSE methodology, unlocking key advantages of the model-based approach

What data to input, and how

Interfaces with other stakeholders

Modelling and extraction toolset

WORK IN PROGRESS

- Guiding principle for the first iteration:

K.I.S.S. ➔ Keep It Simple and Stupid

➔ Don’t change what works

➔ Build on top of what has been done

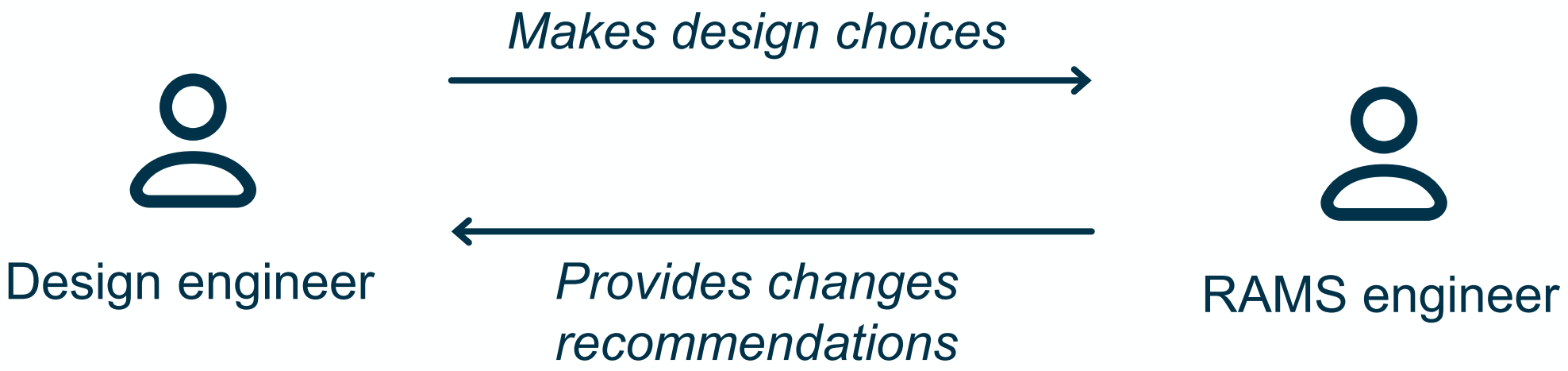
➔ Reduce scope to a minimum

K.I.S.S. ➔ **K**eep **I**t **S**imple and **S**tupid

- Focus on one field: **RAMS engineer** (= Fault management)
- Focus on one specific artefact: **FMEA**
- Put in practice in a simplified environment: **SysML Cubesat demonstrator**

Why choose RAMS?

- They need to have an overview of the whole system
- They can affect the design by emitting specific recommendations



FIRST LOOK AT THE METHODOLOGY

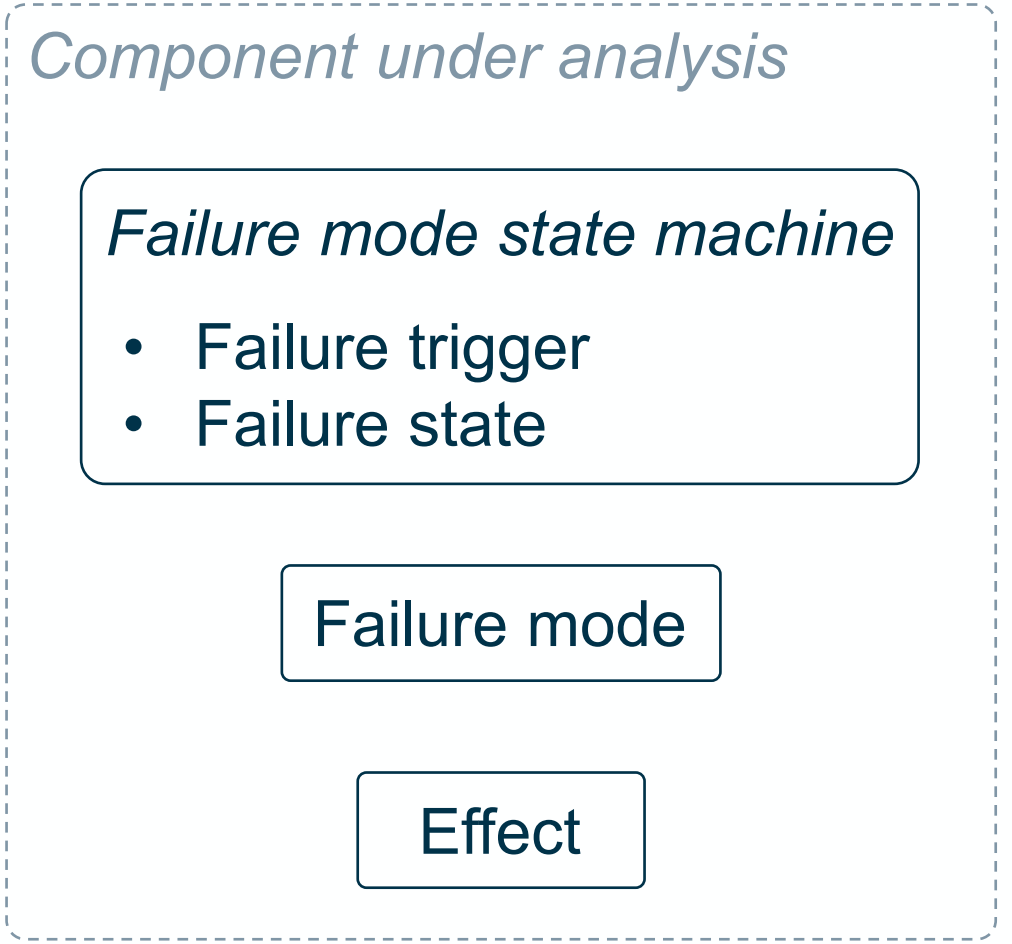
Key questions to answer

- What can go wrong?
- What functionality is damaged/lost?
- Can this affect other components?
- How to mitigate the failure?

FIRST LOOK AT THE METHODOLOGY

Key questions to answer

- What can go wrong?
- What functionality is damaged/lost?
- Can this affect other components?
- How to mitigate the failure?

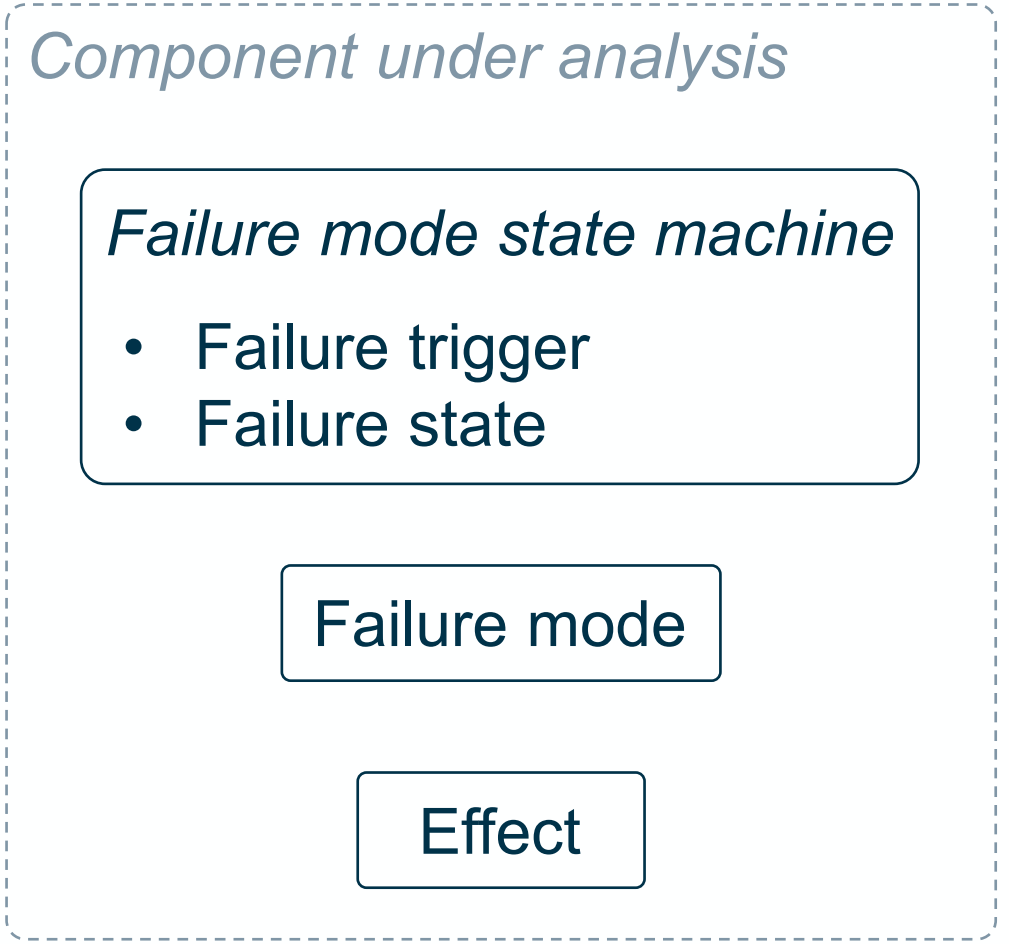


FIRST LOOK AT THE METHODOLOGY

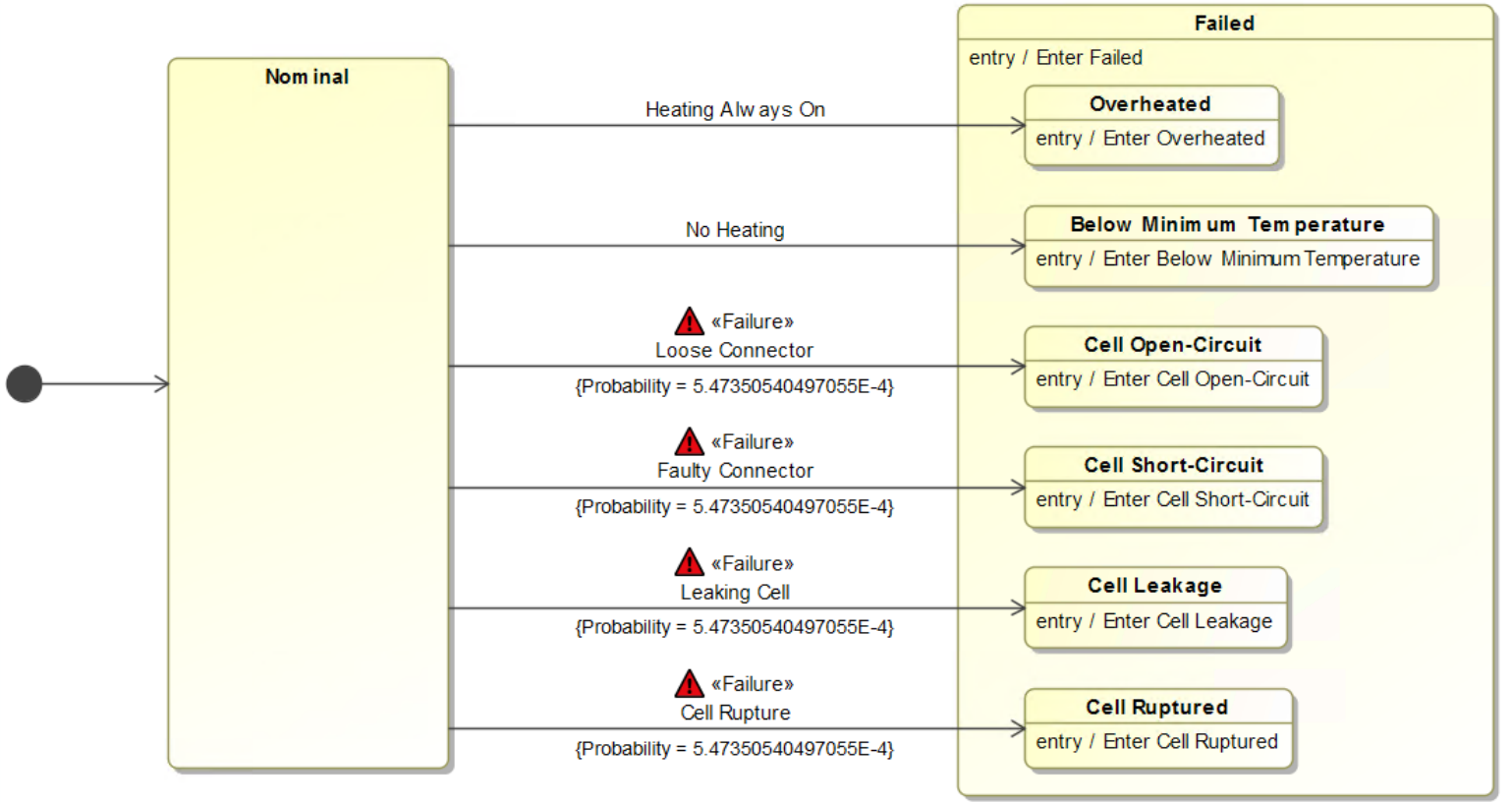
- Elements shown here are MBSE components

  ➔ **Does not follow** ECSS terminology

- Separate analysis ensures data mapping with Q-ST-30-02C



EXAMPLE: BATTERY COMPONENT



Component under analysis

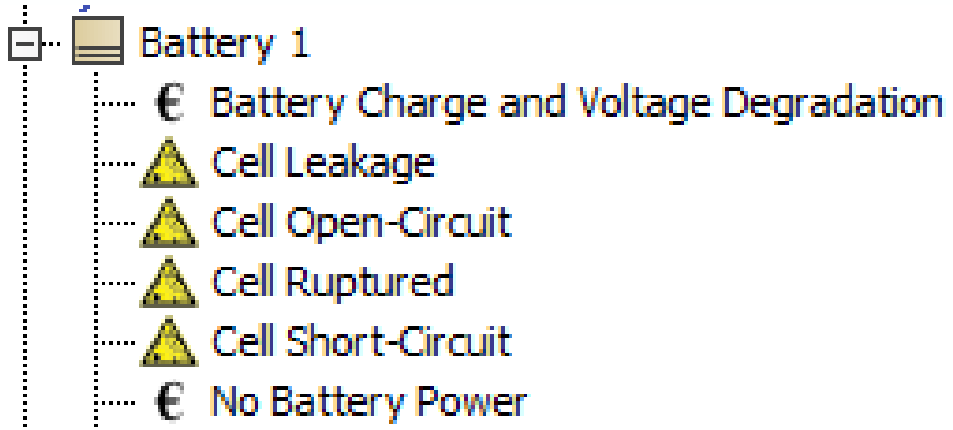
Failure mode state machine

- Failure trigger
- Failure state

Failure mode

Effect

EXAMPLE: BATTERY COMPONENT



- Data placeholders + elements to point to
- SIGNAL stereotypes

Component under analysis

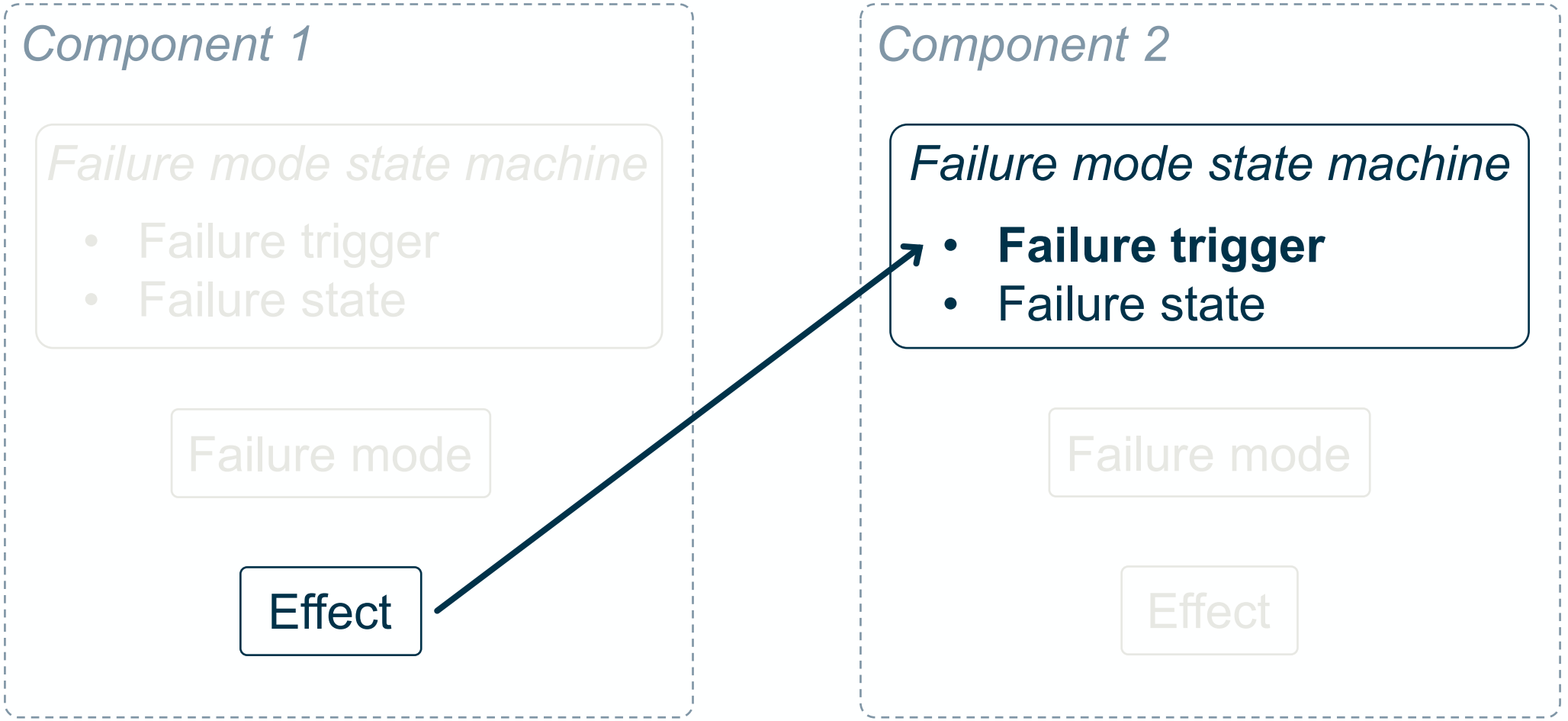
Failure mode state machine

- Failure trigger
- Failure state

Failure mode

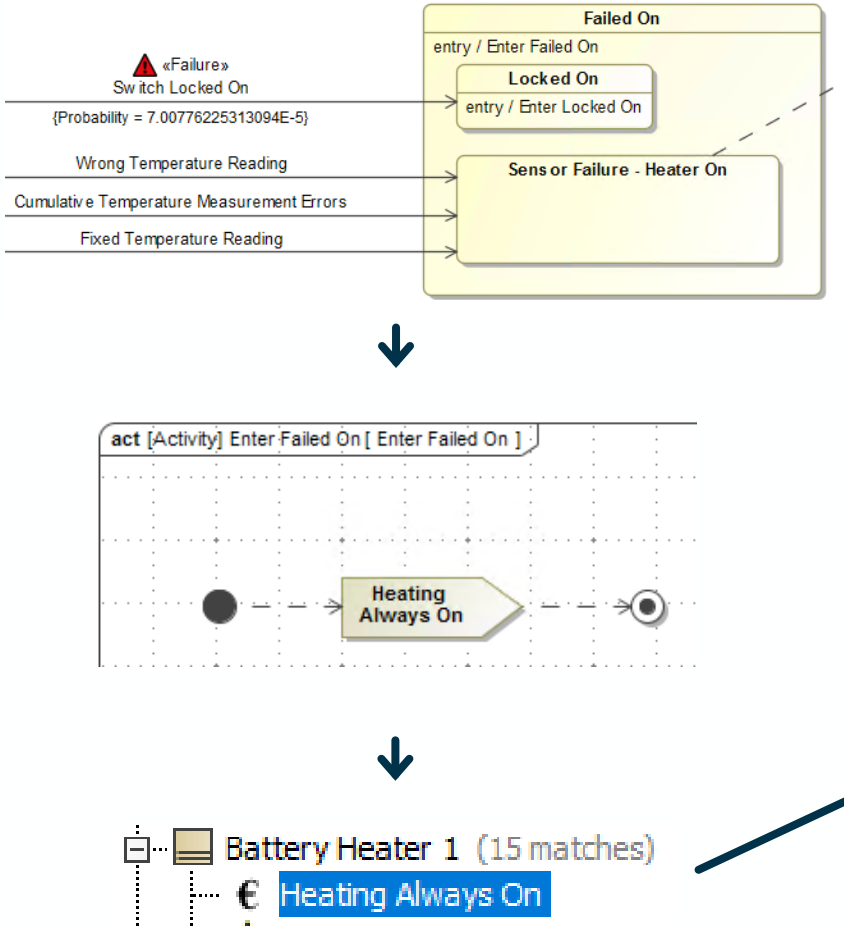
Effect

EXAMPLE: FAILURE PROPAGATION

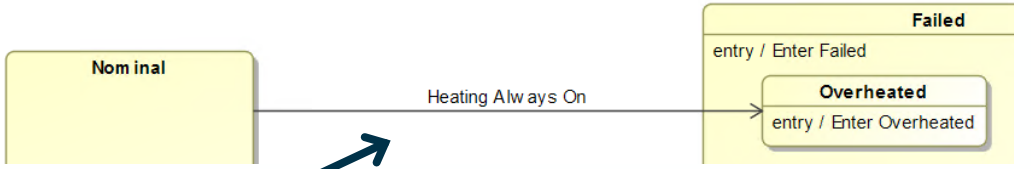


EXAMPLE: FAILURE PROPAGATION

Component 1



Component 2



Retrieving the Fault Management information as FMEA

- FMEA view inside Cameo
- Export in CSV format ➔ Adapts to existing interfaces

Item	Potential Failure Mode	End Effect	Potential Cause(s)
Battery 1	Cell Short-Circuit	EFFECT: Power Bus Reduced Power in Eclipse	EVENT: Battery 1 Faulty Connector
Battery 1	Cell Short-Circuit	EFFECT: CubeSat Loss of Spacecraft	EVENT: Battery 1 Faulty Connector
Battery 1	Cell Short-Circuit	EFFECT: CubeSat Mission Degradation	EVENT: Battery 1 Faulty Connector
Battery 1	Cell Short-Circuit	EFFECT: CubeSat Loss of Mission	EVENT: Battery 1 Faulty Connector
Battery 1	Cell Short-Circuit	EFFECT: Battery 1 No Battery Power	EVENT: Battery 1 Faulty Connector
Battery 1	Cell Short-Circuit	EFFECT: Power Bus No Power in Eclipse	EVENT: Battery 1 Faulty Connector
Battery 1	Cell Short-Circuit	EFFECT: Power Bus No Power in Eclipse	EVENT: Battery 1 Faulty Connector
Battery 1	Cell Short-Circuit	EFFECT: Power Bus No Power in Eclipse	EVENT: Battery 1 Faulty Connector

EXAMPLE: KEY TAKEAWAYS

Advantages

- Streamlined workflow
- Independent from existing model
- Elements can be created at any level
  - ➔ Allows for black-box analysis, simplifies the ownership separation with suppliers

Trade-off

- Lacks interaction with the rest of the model

WHAT IS AVAILABLE

- Methodology description, **SysML profile** and User Manual
  - ➔ **Fully covers** the ECSS requirements for FMEA
- FMEA generation through **Cameo SysML plugin** (*developed by NASA supplier*)
  - ➔ **Partially covers** the ECSS requirements for FMEA
- Example developed on **Cubesat demonstrator**

WORK PLANNED

- **Improve current methodology** with interactions between RAMS elements and the rest of the model
- Introduce the methodology to a **real-life situation** ➔ ESA YPsat project
- **Develop the artefact generation** toolset to be fully compliant with ECSS requirements, allowing user to have a platform ready to be used in ESA projects
- **Write guidelines** on how to implement MBMA methodology, would serve as basis for a dedicated ECSS Handbook

THANK YOU FOR YOUR ATTENTION

Q&A at the end of the session

Contact information

- Clement Puybareau: Clement.Puybareau@esa.int
- Isabelle Conway: Isabelle.Conway@esa.int