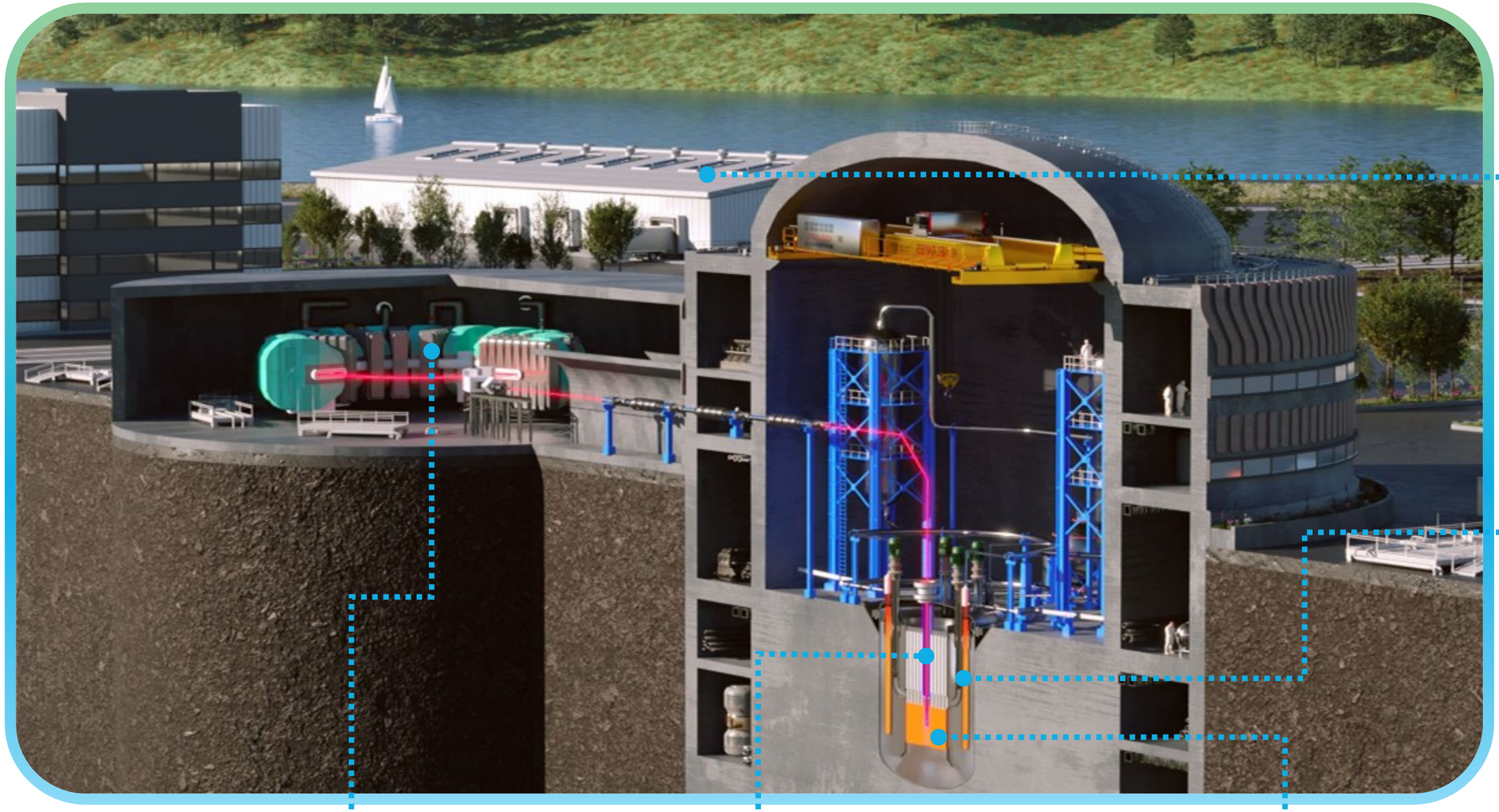
Engineering Compliance from the Ground Up: Deploying Model-Based Systems Engineering in the Nuclear Industry

Alexandre Amorim Carvalho, Transmutex SA
Oliver Bleisinger, :em engineering methods AG

15th of September 2025

START – scalable transmutation of nuclear waste and breeding U233

START
Subcritical
Transmuting
Accelerated
Regenerative
Technology



Pyroprocessing
Hot-fuel
99% separation

Lead-Cooled Sub-Critical Reactor
Fast-neutrons flux
High temperature

Cyclotron
800MeV – 5mA
85% availability

Spallation Target
4MW molten metal target

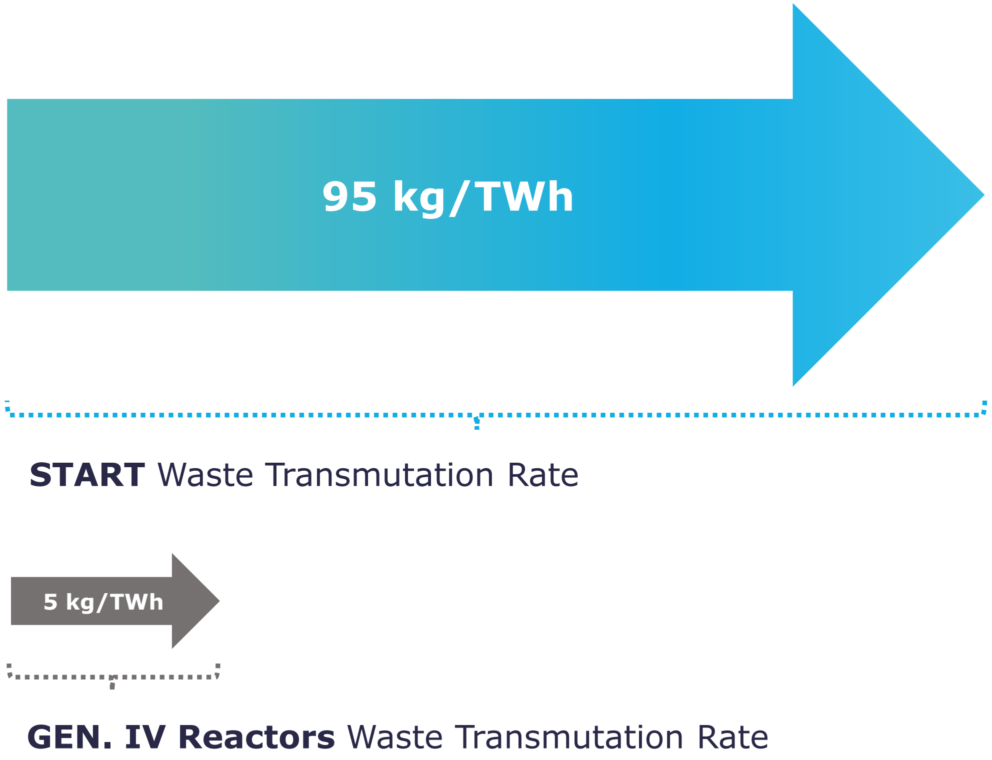
Waste + Thorium Fuel
Metal fuel

START to Optimize Deep Geological Storage

Impact for uranium long-lived waste from transmutation by START

5x to 225x
Reduction
Storage Volume*

300’000 to 300 years
Reduction
Lifetime Radioactivity



Source: CEA – Séparation transmutation des éléments radioactifs à vie longue– Dec. 2012 report (FR), p. 39 - link

* Depends on official used-fuel management policy

Every component has been demonstrated – TRL 3 to 6

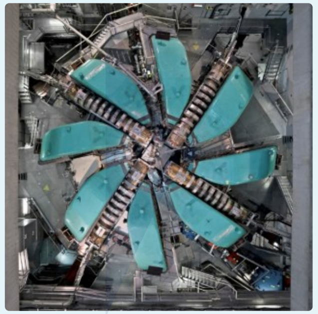
Accelerator Coupled Subcritical Core

CERN

Transmutation of Long-Lived Waste

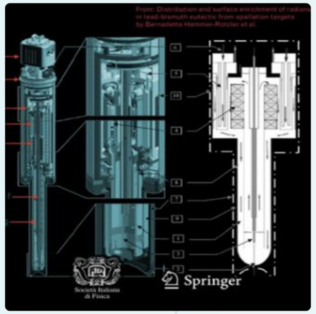
CERN

High-Power Cyclotron
(50+ years operation)



PAUL SCHERRER INSTITUT PSI

High-Power Spallation Target
(6+ months operation)



PAUL SCHERRER INSTITUT PSI

Lead-Cooled Reactor
(80,000+ hours operation)

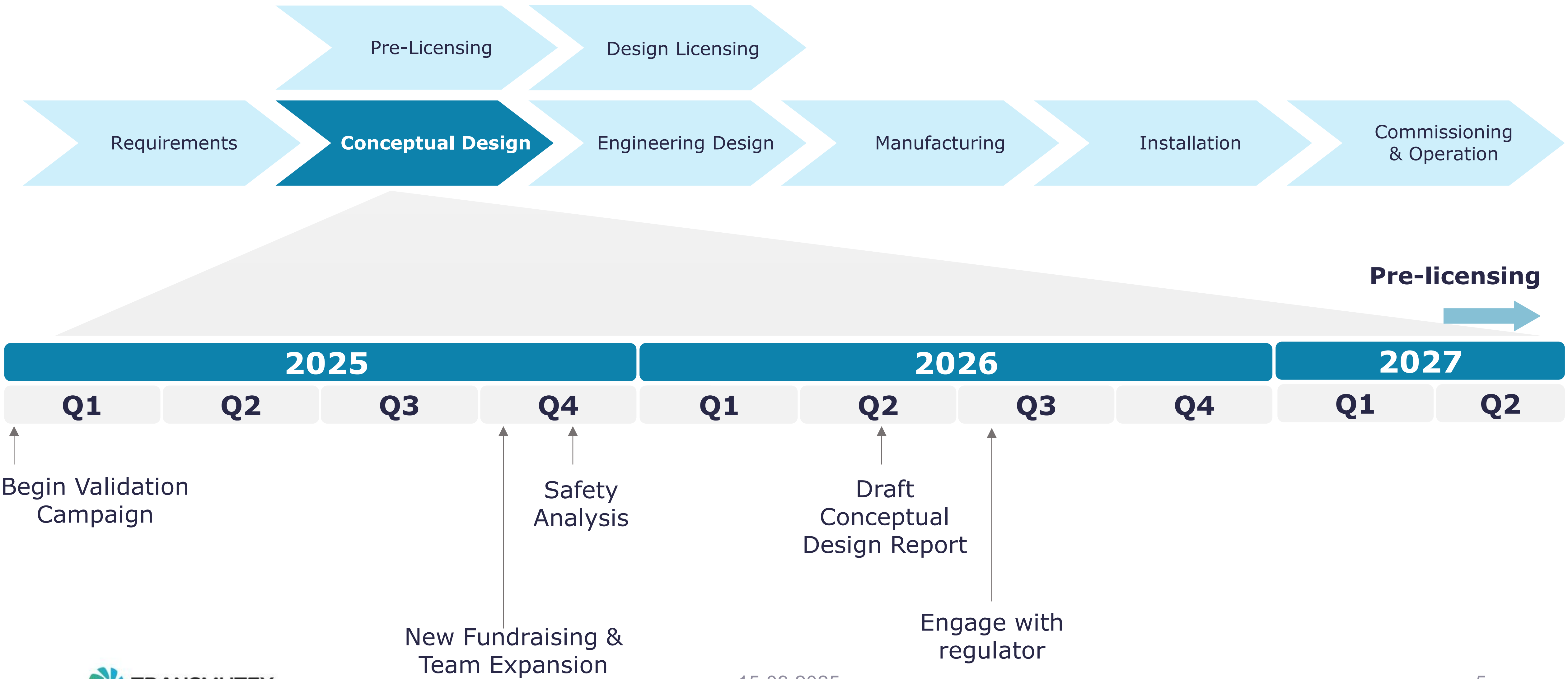
Alfa Class submarines

Recycling of Spent Fuel

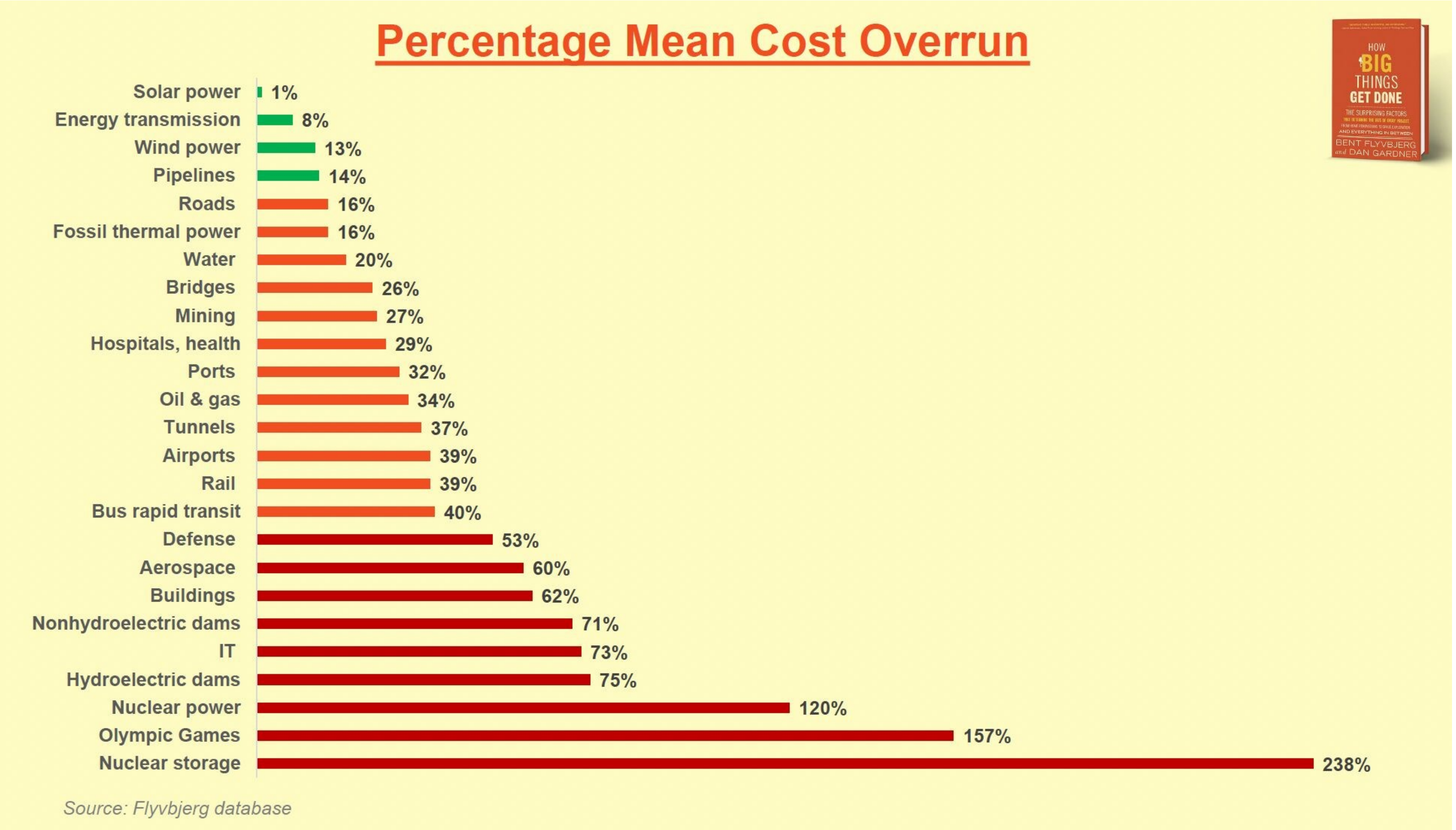
Argonne NATIONAL LABORATORY

Source: Accelerator: Experimental determination of the energy generated in nuclear cascades by a high energy beam. Transmutation: TARC experiment. Cyclotron: PSI proton accelerator. Target: PSI Seminar. Lead-Cooled Reactor: Cored Design of ALFRED. Thorium Fuel: Pyroprocessing Technologies

START – Project Roadmap



Statistics from Nuclear Megaprojects



SWISSED 2025 | ALEXANDRE CARVALHO, OLIVER BLEISINGER

MBSE Journey Map – Early 2024

- **Possible fields of action** (green)
- **Targeted Early 2024** (red)

engineering methods AG

Initiate → **Tailor** → **Rollout** → **Optimize**

Method

- Use Case Scoping (Targeted Early 2024)
- Modeling Guideline
- Pilot Methodology
- Integrate RE
- Integrate PLE
- V&V Integration
- Establish MBSE Vision (Targeted Early 2024)
- Select & Enhance Methods
- Integrate Software Engineering
- RE/MBSE Information Model
- Customize Architectural Views
- Review Guidelines

Modeling

- Best Practice Templates
- Requirements Modeling
- Functional Modeling
- Behavior Modeling
- Risk Analysis
- Architecture Modeling
- Feature Modeling

Support

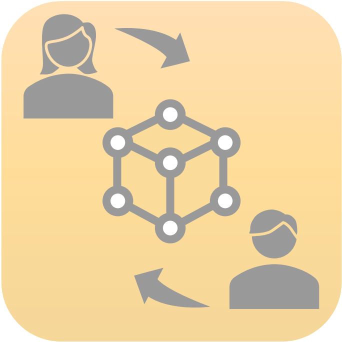
- Impulse and Initial Analysis
- Tool-assessment
- Train MBSE Focus Group
- Tailor PLE/MBSE Toolchain
- Provide Project Libraries
- Review Concept (Targeted Early 2024)
- Train MBSE End Users/SMEs
- Coach MBSE End Users/SMEs & Application
- Maturity Assessment
- Assure Funding
- Tailor RE/MBSE Toolchain

Pilot Project (Proof-of-Value/Proof-of-Concept)

MBSE Target Picture Based on Use Cases

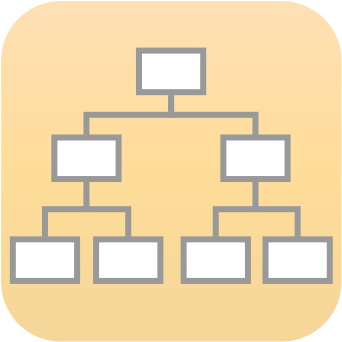
Excerpt of Best Practice Areas from Various Industry Partners

Focus for regulated industries

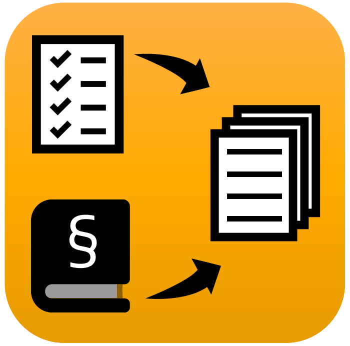


Visualization & Communication

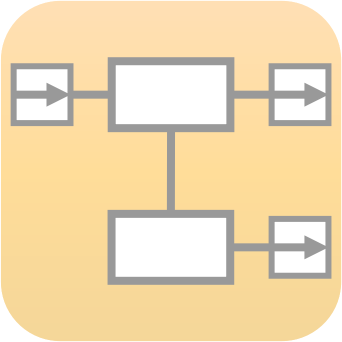
Requirements Elicitation



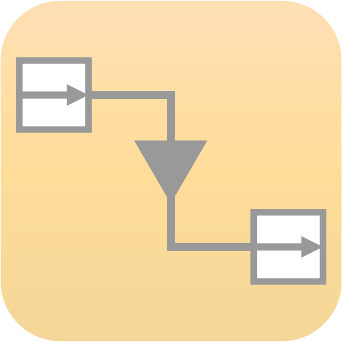
Requirements Breakdown



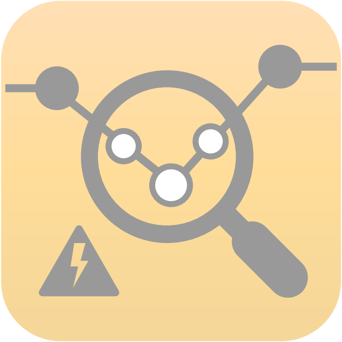
Specification & Compliance



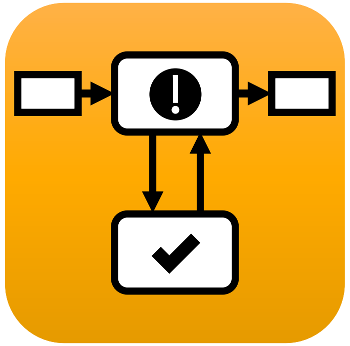
Functional & Logical Architecting



Interface Specification



Impact Analysis & Engineering Change



Safety & Risk Analysis

Derivation of Prioritized Fields of Action

Condensed Results on Initial Invest and ROI for Generic Use Cases

- Assumptions from :em AG experience

ROI = Return on Invest

MBSE Use Case	Impact of Pilot	Initial Invest	ROI-Potential	Time Till ROI
Functional & Logical Architecting	↑	→	→	→
Interface Specification	→	↓	→	↓
Requirements Elicitation	↓	↓	→	↓
Variants & Product Line Engineering	↓	↑	↑	↑
Dynamic Behavior Modeling	↓	↓	↓	↓
Impact Analysis & Engineering Change	↑	→	→	↓
Specification & Compliance	→	→	→	↓
Safety & Risk Analysis	→	→	→	↓

- Specification & Compliance targeted with **focus on Automatic Report Generation** for early ROI
- Additionally, **focus on Safety & Risks Analysis** as well as **Impact Analysis & Engineering Change**

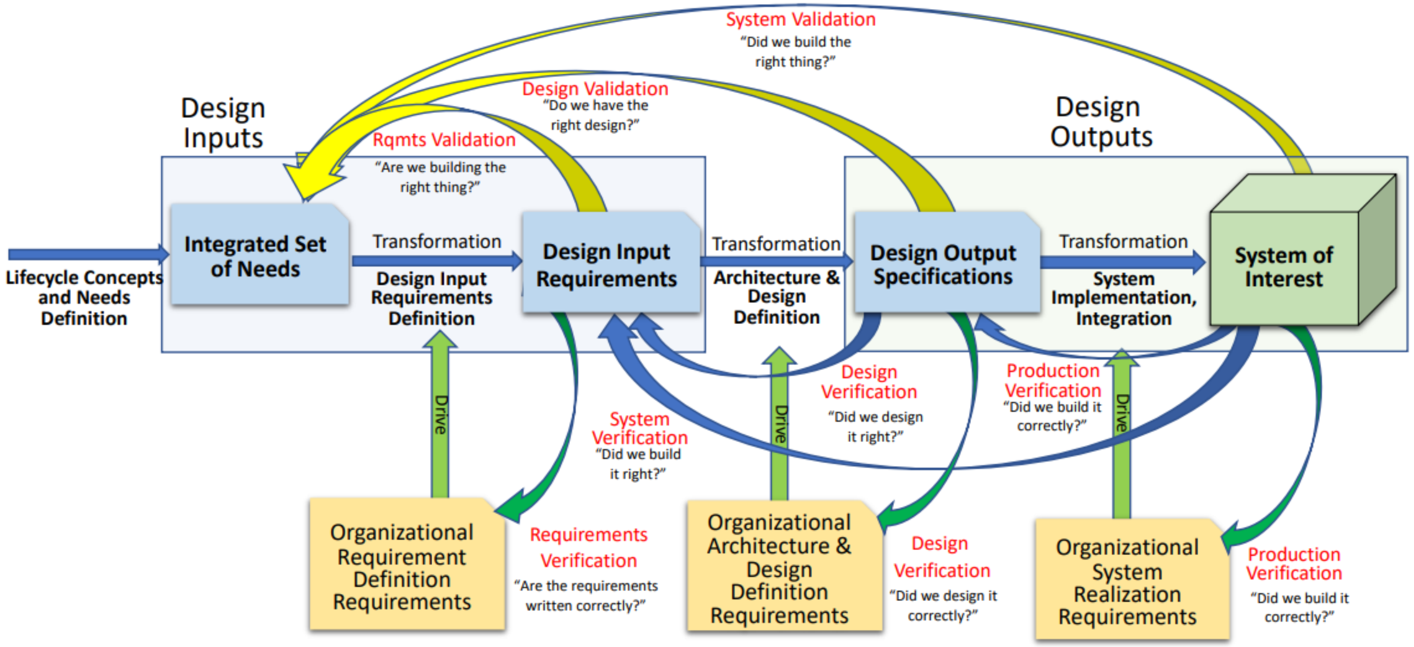
Specification & Compliance

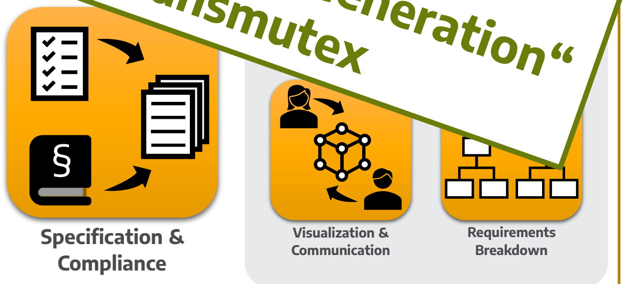
Generic Use Case Description from Industry Best Practices

„Renamed & Adjusted to „Automatic Report Generation" at Transmutex"

Writing of a comprehensive, complete and unambiguous requirements specification

- Define activities and criteria for guidance on requirement specification
- Set up validation mechanism and management of artefacts to fulfill regulations
- Tailor automatic generation of documents from model to organizational needs





Impact of MBSE

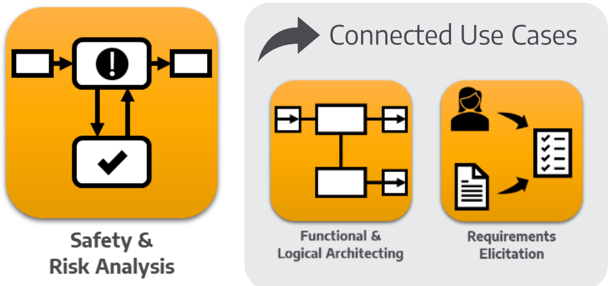
- Ensure requirements meet expectation of notified bodies and regulators
- Enhance management of specification artefacts
- Derive documents from model for homologation

Safety & Risk Analysis

Generic Use Case Description from Industry Best Practices

Analyze product-related risks and derive mitigation measures

- Perform analysis like FMEA, FTA or HARA
- Mitigate risks by additional requirements, design improvements or test cases
- Create traceability for safety-analysis, requirements and system architecture



System Analysis → **Failure Analysis and Risk Reduction** → **Communication**

1. Planning and Preparation
- Find Team & Moderator
- Define the scope of analysis and its boundaries

2. Structure Analysis
- Create product structure
- Analyze Interfaces and interactions

3. Functional Analysis
- Create & analyze the system functions & interactions
- Map direct and indirect Requirements to the functions
- Basis for Failure Analysis

4. Failure Analysis
- Definition & Description of Failures, Causes and Effects
- Cause Analysis

5. Risk Analysis
- Assessment of the significance, probability of occurrence and detection for each error chain of events
- Description and Evaluation of existing Counter-measures

6. Optimization
- Identification of risk reduction measures
- Implementation of measures
- Reassessment of risks after implementation

7. Result Documentation
- Communication& Documentation of results

by MBSE in early phases (no additional effort)

by MBSE in early phases (reduced effort)

Impact of MBSE

- Delivering functional analysis for safety & risk in early project phases
- Providing information / input for product context (usage, operational phase)
- Supporting safety & risk activities by methods & tools

Safety & Risk Analysis

Example of FMEA-Table & Safety Coverage Report

Example

Focus of MBSE is **supporting different activities in Safety, Risk & Reliability**

- FTA (Fault-Tree-Analysis), FMEA and **Functional Analysis provided „by design“** (no-additional work) of MBSE
- Mostly modeling and analysis making FMEA meetings partly redundant
- Safety overviews & **report** for safety and risk are **automatically generated** according to common standards

Criteria — Element Type: FMEA Item — Scope (optional): FMEA

#	Id	Classification	Item	Failure Mode	Subsystem	Local Effect Of Failure	Final Effect Of Failure	SEV	Cause Of Failure	OCC
1	F-28	mechanical	chassis : Chassis	Mechanical Damage	Room Control Unit	Loss of Power Supply	Access to Live Parts	4	Drop	3
2	F-36	mechanical	power Supply : Power Supply	Damage at Mains Cable Connection	Room Control Unit		Access to Live Parts	4	Abrasion during installation	5
3	F-40	mechanical	power Supply : Power Supply	Damage at Mains Cable Connection	Room Control Unit		Access to Live Parts	4	Low production quality	2
4	F-41	electrical	display : Displaying system	No Activity	Room Control Unit	Loss of User Interaction (Output)	Loss of User Interaction (Output)	3	No Power Supply	1
5	F-2	electrical	power Supply System : Power Sup...	Loss of Power Supply	Room Control Unit	Loss of Power Supply	Total loss of function	3	Loss of Power Supply	1
6	F-3	electrical	power Supply System : Power Sup...	No Activity	Room Control Unit	Loss of Power Supply	Total loss of function	3	Low production quality	2
7	F-4	electrical	advanced Control System : Advanc...	No Activity	Room Control Unit	Loss of control functionality	Loss of Heating Control Functionality	3	No Power Supply	1
8	F-5	software	mobile App : Mobile App	Connection loss	Room Control Unit	Loss of User Interaction (Input)	Loss of User Interaction (Input)	3	Network instability	4
9	F-42	software	mobile App : Mobile App	Connection loss	Room Control Unit	Loss of User Interaction (Input)	Loss of User Interaction (Output)	3	Network instability	4
10	F-6	electrical	user Input System : User Input Sys...	No Activity	Room Control Unit	Loss of User Interaction (Input)	Loss of User Interaction (Input)	3	No Power Supply	1
11	F-7	electrical	basic Control System : Basic Contr...	No Activity	Room Control Unit	Loss of control functionality	Loss of Heating Control Functionality	3	No Power Supply	1
12	F-9	electrical	sensor Module : Sensor Module	No Activity	Basic Control System	Loss of control functionality	Loss of Heating Control Functionality	3	No Power Supply	1

Criteria — Element Type: Block,Part Property,Activity — Scope (optional): Design

#	Design Element	Covered By Reliability Analysis	Covered By Safety Analysis
1	user Input System : User Input System	F-6 user Input System Failure1	
2	touchDisplay : Touch Display	F-22 touchDisplay Failure1 F-23 touchDisplay Failure2	
3	sensor Module : Sensor Module	F-8 sensor Module Failure1 F-9 sensor Module Failure2	
4	power Supply : Power Supply	F-19 power Supply Failure1 F-20 power Supply Failure2 F-21 power Supply Failure3 F-36 power Supply Failure4 F-37 power Supply Failure5 F-38 power Supply Failure6 F-39 power Supply Failure7 F-40	
5	mobile App : Mobile App	F-5 mobile App Failure1 F-42	
6	lighting Control Module : Lighting Control Module	F-10 lighting Control Module Failure1 F-11 lighting Control Module Failure2	
7	LC Display : LC Display	F-15 LC Display Failure1 F-16 LC Display Failure2	
8	HVAC Logical Control module : HVAC Control Module	F-13 HVAC Logical Control module Failure1 F-14 HVAC Logical Control module Failure2	
9	electronic PCB M2HVAC : Electronic PCB M2HVAC	F-26 electronic PCB M2HVAC Failure1 F-27 electronic PCB M2HVAC Failure2	
10	electronic PCB M1HVAC : Electronic PCB M1HVAC	F-24 electronic PCB M1HVAC Failure1 F-25 electronic PCB M1HVAC Failure2	
11	chassis : Chassis	F-28 chassis Failure1	R-1 Risk of electrical shock at mains R-2 Risk of electrical shock at mains
12	button Bar : Button Bar	F-17 button Bar Failure1 F-18 button Bar Failure2	
13	basic functionality module : Basic Functionality Module	F-12 basic functionality module Failure1	
14	basic Control System : Basic Control System	F-7 basic Control System Failure1 F-34 basic Control System Failure2 F-35 basic Control System Failure3	
15	power Management Module : Power Management Module	F-29 Failure4	
16	advanced Control System : Advanced Control System	F-4 Failure3 F-30 advanced Control System Failure1 F-31 advanced Control System Failure2 F-32 advanced Control System Failure3 F-33 advanced Control System Failure4	
17	power Supply System : Power Supply System	F-2 Failure1 F-3 Failure2	

Current MBSE Set-Up

Requirements Management Tool

Jama Connect

- Requirements
- Verifications and results
- FMECA
- Other risk analyses

Architecture Tool

CATIA Magic

- Imports and “satisfies” requirements
- Functions
- Structure
- Measures of Effectiveness

Our selected MBSE trinity:

- Language: SysML
- Tool: CATIA Magic (cameo systems modeler)
- Methdology: Magic Grid

MBSE Capabilities at Transmutex

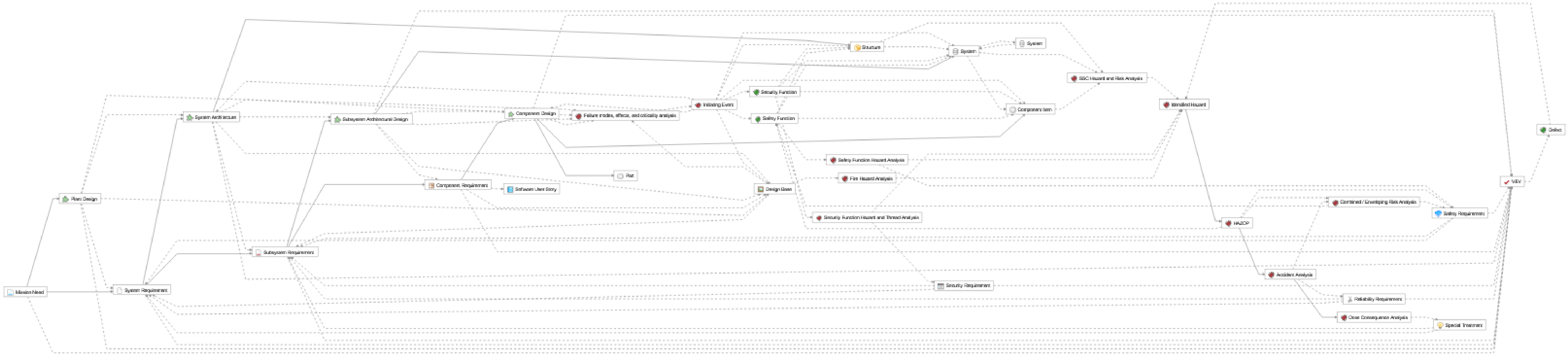
Capabilities with guidelines

- **Safety and Risk Analysis**
- **Export of Reports**
- Launching of external simulations (SysML to Ansys)
- Editing SysML profiles
- Jama Connect - CATIA Magic integration
- **Impact analysis**
  - Requirements tool
  - SysML model
- Model Diagrams Validation with Subject Matter Experts (implementation ongoing)

Capabilities to be developed

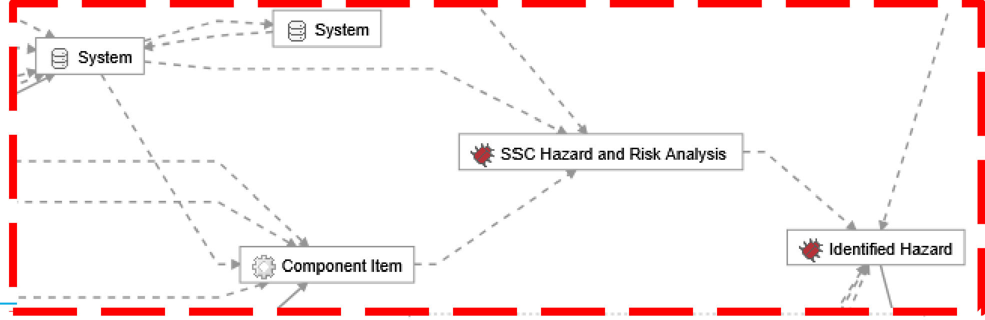
- Trade-off studies
- Continuous validation of requirements within SysML
- Integrated reliability analysis
- Other safety processes: functions categorization, SSC's classification, initiating events, hazard analysis, etc.
- Optimization of the system
- Model diagrams approvals and baselines

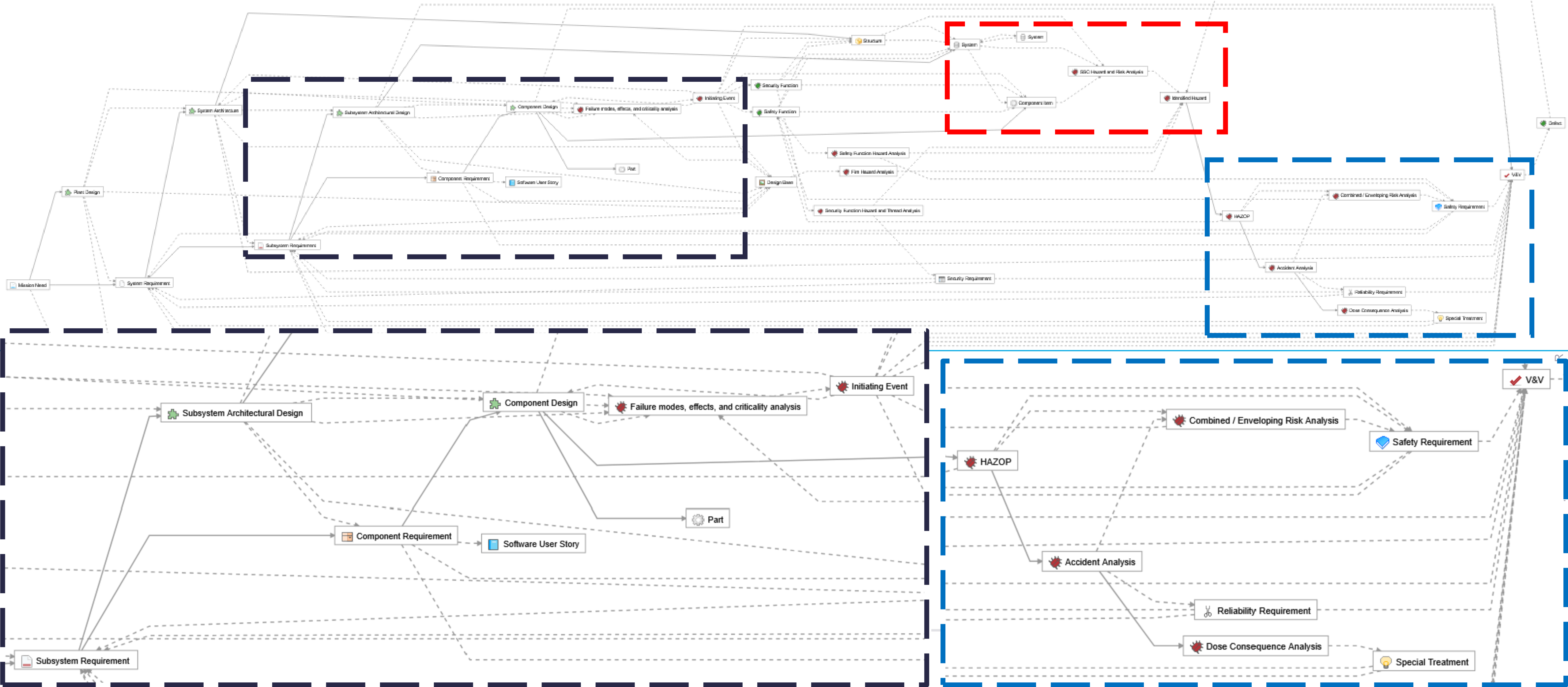
Engineering Compliance



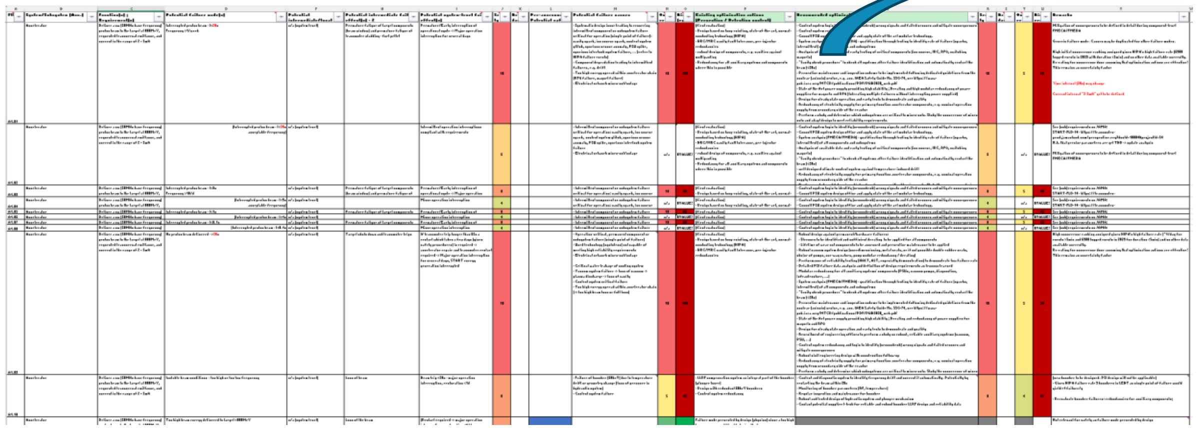
SWISSED 2025 | ALEXANDRE CAR

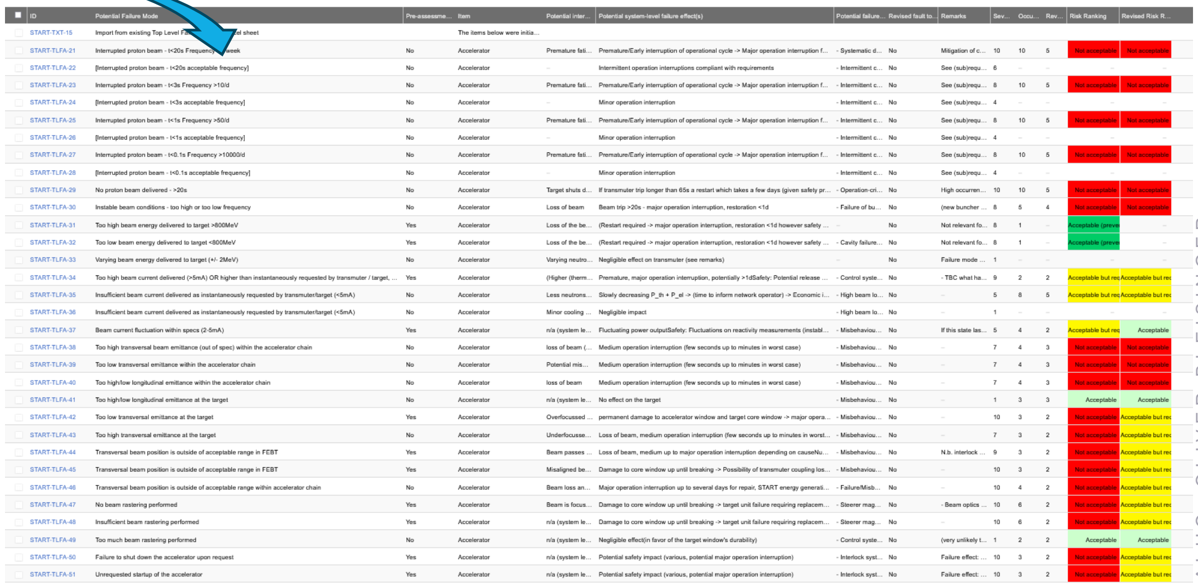
Engineering Compliance





Use Case: Safety and Risk Analysis

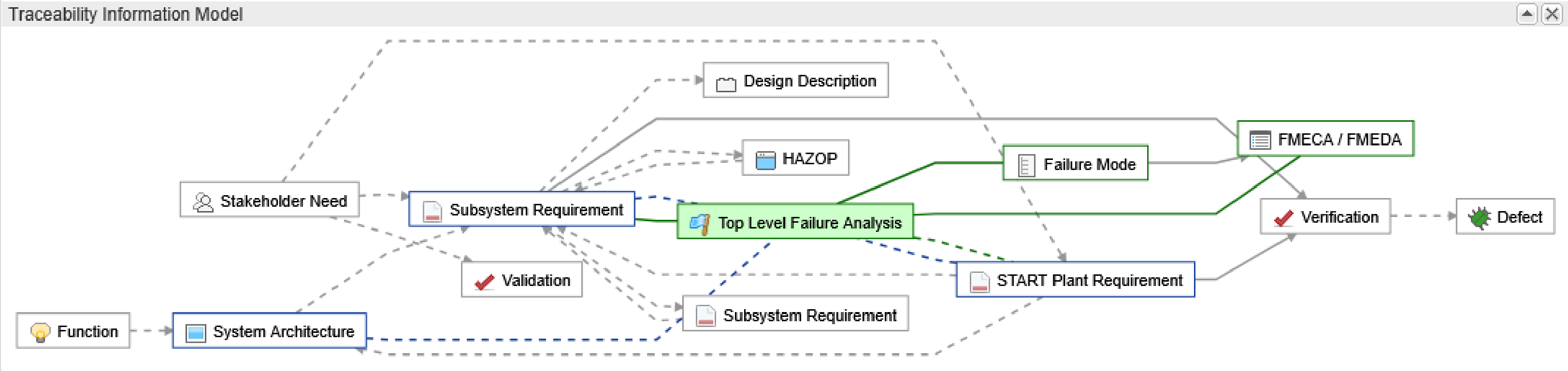




Top Level Failure Analysis excel sheet has become a list of traceable items.

Top Level Failure Analysis items are now living in the requirements management tool and tracing to:

- Failure modes
- Requirements
- Tasks (pushed to planning)



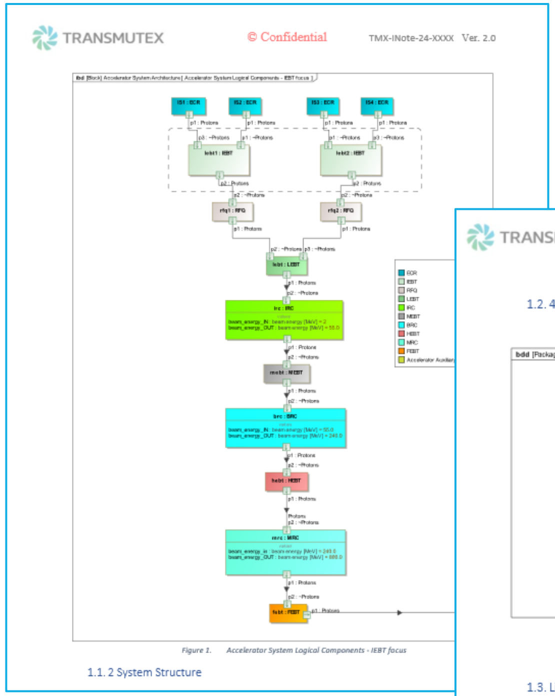
Use Case: Automatic Report Generation

- Design Description: Velocity language allows us to export data from SysML model
- Requirements lists are exported from Jama – takes 1 second.

Successful demonstration of automatic report generation with the support of :em using our internal documents template.

Conceptual Design Reports of the START plant systems will be generated from the SysML model and requirements management tool

AI is being considered to translate the reports to nuclear-legal language



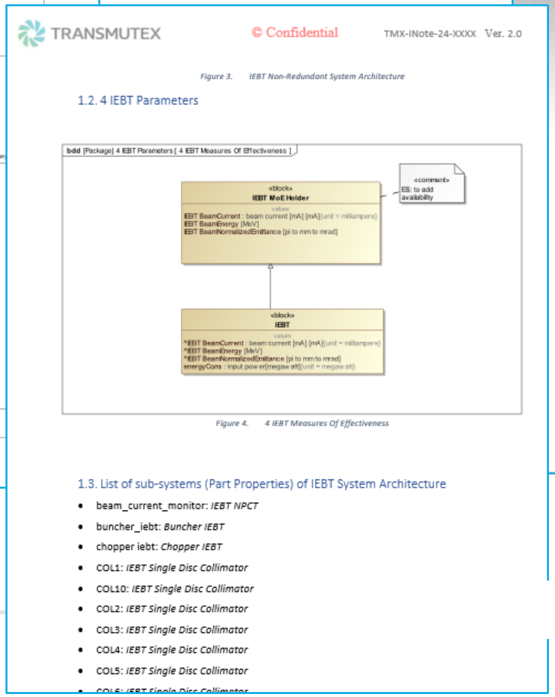

TRANSMUTEX © Confidential TMX-INote-24-XXXX Ver. 2.0

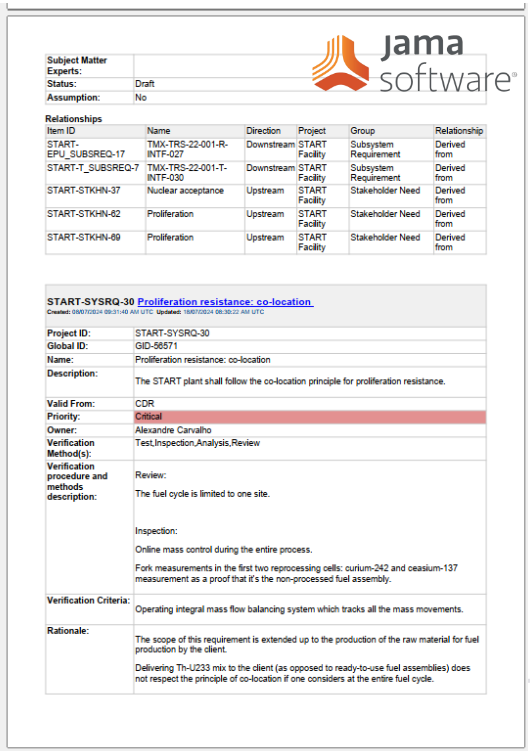
Figure 3. IEBT Non-Redundant System Architecture

1.2. 4 IEBT Parameters

Figure 4. 4 IEBT Measures Of Effectiveness

1.3. List of sub-systems (Part Properties) of IEBT System Architecture

- beam_current_monitor: *IEBT NPCT*
- buncher_iebt: *Buncher IEBT*
- chopper iebt: *Chopper IEBT*
- COL1: *IEBT Single Disc Collimator*
- COL10: *IEBT Single Disc Collimator*
- COL2: *IEBT Single Disc Collimator*
- COL3: *IEBT Single Disc Collimator*
- COL4: *IEBT Single Disc Collimator*
- COL5: *IEBT Single Disc Collimator*



Subject Matter Experts:	
Status:	Draft
Assumption:	No

Relationships

Item ID	Name	Direction	Project	Group	Relationship
START-EPU_SUBSREQ-17	TMX-TRS-22-001-R-INTF-027	Downstream	START Facility	Subsystem Requirement	Derived from
START-T_SUBSREQ-7	TMX-TRS-22-001-T-INTF-030	Downstream	START Facility	Subsystem Requirement	Derived from
START-STKHN-37	Nuclear acceptance	Upstream	START Facility	Stakeholder Need	Derived from
START-STKHN-62	Proliferation	Upstream	START Facility	Stakeholder Need	Derived from
START-STKHN-69	Proliferation	Upstream	START Facility	Stakeholder Need	Derived from

START-SYSRQ-30 Proliferation resistance: co-location
Created: 08/07/2024 09:31:40 AM UTC Updated: 18/07/2024 08:30:22 AM UTC

Project ID:	START-SYSRQ-30
Global ID:	GID-56571
Name:	Proliferation resistance: co-location
Description:	The START plant shall follow the co-location principle for proliferation resistance.
Valid From:	CDR
Priority:	Critical
Owner:	Alexandre Carvalho
Verification Method(s):	Test,Inspection,Analysis,Review
Verification procedure and methods description:	Review: The fuel cycle is limited to one site. Inspection: Online mass control during the entire process. Fork measurements in the first two reprocessing cells: curium-242 and ceasium-137 measurement as a proof that it's the non-processed fuel assembly.
Verification Criteria:	Operating integral mass flow balancing system which tracks all the mass movements.
Rationale:	The scope of this requirement is extended up to the production of the raw material for fuel production by the client. Delivering Th-U233 mix to the client (as opposed to ready-to-use fuel assemblies) does not respect the principle of co-location if one considers at the entire fuel cycle.

The Setting

Before MBSE

- No Systems Engineering in the organization
- Ambitious, complex project – a good client for MBSE
- No other examples of MBSE in nuclear
- No relevant prior experience with MBSE
- Management was convinced of the vision

Today

- Systems engineering is embedding Transmutex
- MBSE supports handling complexity
- We know of other nuclear projects implementing MBSE
- We are surrounded by MBSE expert consultants
- Management is convinced of the implementation

But it's not enough.

- More basic knowledge of systems engineering is needed to all technical staff
- More experienced systems engineers are needed

Lessons Learned

- Starting early
  - “catch up” with the “design” is a race against time.
  - Systems Engineering should drive the design activities.
- An MBSE vision of a digital project was shown to management
  - That vision is reviewed regularly.
  - Milestones are celebrated and shared.
  - That vision is given to newcomers before they have time to open word or excel.
- Easier to convince management of implementing MBSE processes than systems engineering processes
  - Downside is some think MBSE is digital transformation
  - Some people have more difficulties to understand the value of systems engineering
- Our requirements management tool was surprisingly easy to use
  - So we push as much data as possible to it to be visualized by all team members

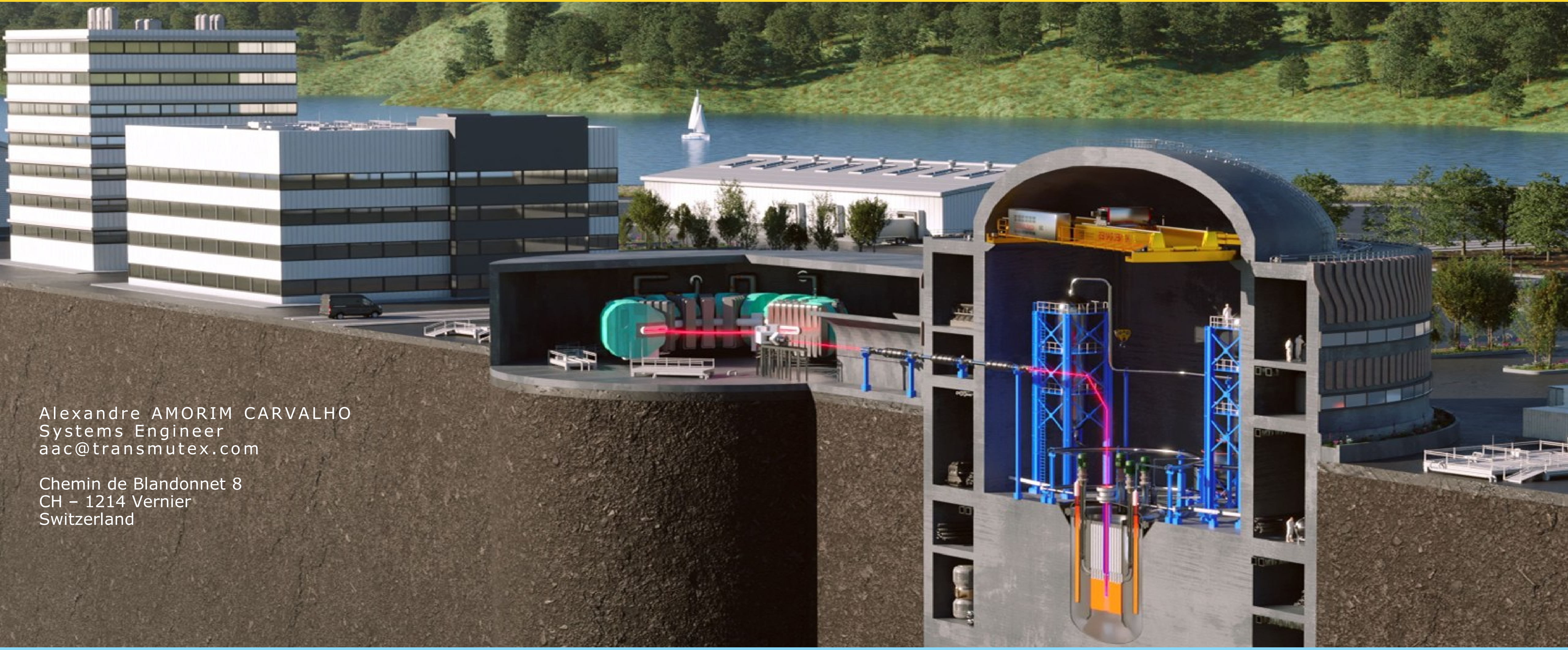
Lessons Learned

- Proper definition of the MBSE vision and goals was instrumental to define the Language, Tool and Methodology trio.
- Training is really important
  - We chose to teach SysML and methodology to experts in particle accelerators, reactors, control systems.

    → Useful but not optimal
  - The profiles of people chosen to model were very discussed: fast learners, motivated by the vision
- The implementation with each team takes a long time and requires follow-up (change of behaviour!)
- Modelling take time and resources
  - 1 modelling sprint every month with clearly defined goals. Each modeler is allocated 9h of modelling for those goals.
  - Project managers don't always see the benefit → modelling goals must be partially aligned with the managers interests
  - 0.4 FTEs for SysML modelling is not enough! (that's <u><2% of the total team</u>)
- Co-modelling sessions within the team and with consultants were a success:
  - Homogenize the modelling style
  - Best practices emerge
  - A culture around systems thinking develops during these sessions

Future Outlook

- Continue developing the capabilities as the need arises
- Increase systems engineering effort
  - Embedding 1 systems engineer FTE per team
  - Online consultants while we cannot hire
- Ramp up the systems engineering awareness
  - Training at arrival of all staff for
    - Systems engineering processes in place
    - Digital thread
  - Giving access to the tools as viewer + relevant training
    - Jama
    - SysML html model



Alexandre AMORIM CARVALHO
Systems Engineer
aac@transmutex.com

Chemin de Blandonnet 8
CH – 1214 Vernier
Switzerland

Lower cost – Sustainable – Non-proliferant

TRANSMUTEX
Reinventing Nuclear