TAILORED MBSE APPROACH FOR SMR GEN IV ARCHITECTING

J. BOURDON
Assystem
Courbevoie, France
Email: jbourdon@assystem.com

A. ZOINO
Assystem
Courbevoie, France

A. GUERIN
Assystem
Courbevoie, France

N. BUREAU
Assystem
Courbevoie, France

L. BENMILOUD-BECHET
Assystem
Courbevoie, France

R. PLANA
Assystem
Courbevoie, France

J. JACHMICH
Assystem
Courbevoie, France

O. VINCENT
Assystem
Courbevoie, France

C. FOURNIER
Assystem
Courbevoie, France

J.F. BOSSU
Assystem
Courbevoie, France

F. CHENEAU
Assystem
Courbevoie, France

Abstract

The accelerating energy transition requires rapid access to decarbonized sources. Although Gen IV SMRs present a potential solution, they face challenges such as new licensing processes and architectural issues, as they must align with diverse global regulations and adapt to varied site-specific requirements, complicating standardization, and deployment. In the face of these challenges, the need for scalable, agile project structuring and organization is becoming increasingly apparent. This structure must be able to support the rapid expansion characteristic of Gen IV SMR projects, while also having the necessary flexibility to adapt to a dynamic reallocation of responsibilities. The core of the approach is the initial structuring of enterprise data models, core engineering processes and methodologies. By adopting a holistic Model-Based Systems Engineering (MBSE) approach that integrates key domains, with safety as the cornerstone, it is ensured that the resulting structuring of engineering data can meet demonstration expectations. In addition, the discussion focuses on the creation of a nuclear-specific layer in numerical tools to enhance the consideration of safety concerns during the architecture definition process. This materializes in the creation of a customized profile in an MBSE tool, which incorporates nuclear safety terminology and aligns with industry usage. By focusing on digital continuity, the approach guarantees a seamless transition between the various development phases, systems engineering processes and lifecycle phases. This means preserving the reliability of information (traceability) and promoting uniform communication (modelling). The paper will conclude by illustrating the potential benefits of our approach, particularly in safety demonstrations.

1. INTRODUCTION

The global shift towards decarbonization has become a paramount objective as nations grapple with the urgent need to reduce carbon emissions and mitigate the impacts of climate change. Central to this transition is the integration of sustainable energy sources that can provide reliable, low-carbon power. Amidst this evolving energy landscape, Generation IV Small Modular Reactors (Gen IV SMRs) have emerged as a promising solution. These advanced nuclear reactors offer the potential for safer, more efficient, and more flexible nuclear power generation. This introduction sets the stage for a comprehensive discussion on the potential and challenges of Gen IV SMRs, focusing on their unique capabilities and the obstacles that must be overcome to realize their full potential [1].

Architectural challenges in the design and deployment of Gen IV SMRs revolve around the need for innovative cooling systems, modular construction techniques, and advanced materials. For example, the implementation of passive safety features, which are integral to Gen IV designs, requires novel engineering solutions that are not yet fully proven in industrial settings. Regulatory challenges extend beyond licensing to include compliance with evolving safety standards and public acceptance. The diverse regulatory environments across different countries add complexity to the international deployment of SMRs.

Scalability and agility in project management are crucial for the successful deployment of Gen IV SMRs. These principles, which emphasize flexibility, iterative development, and rapid response to changes, can significantly enhance project efficiency and adaptability. For example, the agile methodologies employed in the software industry, such as Scrum and Kanban, have demonstrated substantial improvements in project delivery times and stakeholder satisfaction. Similarly, large-scale engineering projects, such as the construction of the International Space Station, have benefited from modular design and incremental development, enabling scalability and adaptability to evolving requirements [2].

Model-Based Systems Engineering (MBSE) represents a transformative approach to managing complex engineering projects. MBSE integrates various aspects of system design, analysis, and verification into a cohesive model, enhancing traceability and consistency. The principles of MBSE, rooted in the history of systems engineering, emphasize the use of formal models to represent system functions, requirements, and architectures. For the nuclear industry, MBSE can be tailored to incorporate safety integration at every stage of the design and development process, ensuring compliance with stringent regulatory standards. Tools such as SysML (Systems Modeling Language) provide a robust framework for developing and managing these models [3].

Within MBSE, specific tools and methodologies can help to take safety into account as early as possible in the design process. For example, Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA) can be federated with common MBSE frameworks, enabling detailed risk assessments and mitigation strategies. Digital continuity is also critical for maintaining the integrity and traceability of information throughout the project lifecycle. It ensures that all data, from initial design to decommissioning, is consistently managed and accessible.

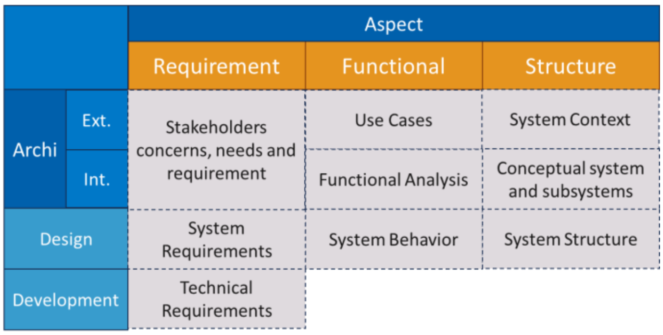
The article will discuss the extension of the current MBSE approach by integrating concepts and language from the nuclear safety domain. It ensures that engineering data structuring meets demonstration expectations through a nuclear-specific layer in numerical tools and a customized MBSE profile. Emphasizing digital continuity, the approach considers transitions between development phases, preserving information traceability and promoting uniform communication. The paper concludes by highlighting the potential benefits for design project delivery and safety demonstrations.

2. EXTENDED MBSE FRAMEWORK FOR NUCLEAR SYSTEMS

2.1. MBSE framework presentation

This section presents a succinct overview of the Model-Based Systems Engineering (MBSE) framework that forms the basis for the tailoring efforts. This framework is derived from the Magic Grid, an MBSE methodology promoted by Dassault Systèmes. The Magic Grid [4] provides a structured approach to system development, emphasizing the integration of requirements, functional, and structural aspects to create a cohesive and comprehensive system model.

The FIG. 1. illustrates the MBSE framework, structured into three main aspects: Requirement, Functional, and Structure. These aspects are further detailed across three levels: Architecture (both external and internal), Design, and Development. In the Requirement aspect, the framework begins with addressing stakeholders' concerns, needs, and requirements at the architectural level, moving to system requirements during the design phase, and concluding with technical requirements in the development phase. The Functional aspect covers use cases and functional analysis at the architectural level and system behaviour description during design. The Structure aspect outlines the system context, conceptual systems, and subsystems, at the architectural level and the detailed system structure during design. This framework ensures that all main aspects of the system are addressed systematically.



		Aspect		
		Requirement	Functional	Structure
Archi	Ext.	Stakeholders concerns, needs and requirement	Use Cases	System Context
	Int.		Functional Analysis	Conceptual system and subsystems
Design		System Requirements	System Behavior	System Structure
Development		Technical Requirements		

FIG. 1. Simplified MBSE Framework used as basis for the tailoring

In the next part, the paper will discuss the extension of the requirements, followed by the functional aspect, the structural aspect, and finally the introduction of a new concept encapsulated in a new aspect: the nuclear safety assessment.

2.2. Extension of requirements aspect

First, stakeholders' safety concerns need to be captured and modelled. It is the needs and concerns of the stakeholders (regulatory bodies, customers, applicants, detractors, operators, etc) that will then guide all the work of deriving and defining the system requirements that will have to be considered by the system architect in his definition of the system architecture. To enable this capture, based on the vocabulary usually used in this field [5], we have integrated new stereotypes in the requirement aspect. These new stereotypes are illustrated in the FIG. 2.

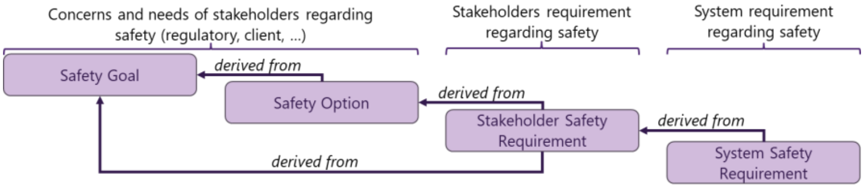

Concerns and needs of stakeholders regarding safety (regulatory, client, ...)
Stakeholders requirement regarding safety
System requirement regarding safety
Safety Goal
derived from
Safety Option
derived from
Stakeholder Safety Requirement
derived from
System Safety Requirement
derived from

FIG. 2. New stereotypes added in the requirement aspect.

The provided figure illustrates a derivation structure of requirements supporting requirements engineering related to safety property. It begins with the identification of the highest-level objectives and progressing downwards to specific technical criteria. At the top of this derivation structure are the **safety goals**, representing the highest-level objectives related to safety. They may represent the Fundamental Safety Functions (reformulated as a requirement) to be performed by the nuclear facility. These goals are the initial concepts identified, setting the direction for all subsequent safety-related requirements.

Derived from the safety goals are the **safety options**, which are potential strategies or solutions formulated to achieve these high-level safety objectives. These options provide practical approaches and reduce the space for possible solutions to meet the established safety goals. Moving further down, the **stakeholder safety requirements** are derived from the safety options. These requirements address the safety concerns and expectations of various stakeholders, including customers, regulatory bodies, and other interested parties, ensuring that the proposed safety strategies align with the broader stakeholder needs. These are the data consumed by the architect to define the architecture of his system.

The next level down involves the **system safety requirements**, which are developed based on the stakeholder safety requirements. They are produced from the architect's work and will be an input for the system design. At the base of the hierarchy are the **technical requirements**, which are the most specific and detailed level of criteria. These requirements provide the technical specifications necessary for the system's safe operation. The classification of SSC corresponds to this type of requirement, as each classification is associated with a specific set of requirements that the SSC must meet.

Using system engineering principle, this approach facilitates comprehensive safety requirements management by systematically addressing safety at every level of the system. It is particularly applicable in the architecture and design of complex systems in industries such as nuclear. Furthermore, this methodology aids in achieving regulatory compliance by ensuring that all safety aspects are thoroughly covered and integrated into the system.

2.3. Extension of functional aspect

In addition to the requirement aspect, which enables the refinement of expectations from a system by detailing the criteria and specifications necessary to meet stakeholder needs, it is essential to describe what the system is intended to do (its missions) and how it will achieve these objectives (its functions). This involves outlining the system's missions, which define its primary purposes and goals, as well as identifying the specific functions that will be implemented to accomplish these missions. By articulating both the missions and functions, we provide a comprehensive understanding of the system's operational objectives and the functional mechanisms that will be employed to fulfil these objectives.

For the nuclear industry, it is particularly important to identify which functions contribute directly or indirectly to the three fundamental safety functions:

- Control of reactivity: The capability to safely shut down the reactor and maintain it in a safe shutdown condition during and after appropriate operational states and accident conditions.
- Cooling of radioactive material: The capability to remove residual heat from the reactor core, the reactor and nuclear fuel in storage after shutdown, and during and after appropriate operational states and accident conditions.
- Confinement of radioactive material: The capability to reduce the potential for the release of radioactive material to ensure that any releases are within prescribed limits during and after operational states and within acceptable limits during and after design basis accidents.

Understanding these contributions is critical for ensuring the system's overall safety and reliability. By mapping out how each function supports these essential safety goals, we can ensure that all necessary measures are in place to prevent accidents and mitigate hazards. Through detailed modeling, we can visualize and analyze the interactions between various system functions, identify potential vulnerabilities, and implement strategies to reinforce system resilience.

By integrating stereotypes into our modeling framework, we enhance our ability to communicate the specific safety-related aspects of the system. These stereotypes enable a deeper understanding of how each function contributes to the overall safety objectives. These stereotypes are illustrated in the FIG. 3.

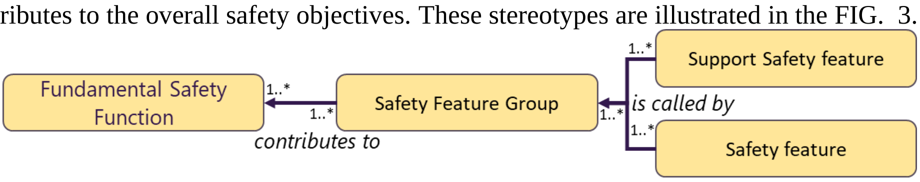


FIG. 3. New stereotypes added in the functional aspect.

At the top of the hierarchy is the **fundamental safety function** which represents the core safety objectives critical to the system's overall safety.

In the functional analysis, fundamental safety functions are decomposed as **safety feature groups** are identified. These safety feature groups are a set and sequence of safety features and safety support features involved in achieving a system functionality related to safety. This group comprises various safety features that collectively contribute to achieving the fundamental safety functions.

At the next level, a differentiation is made between **safety features** and **support safety features**. Safety features are the primary elements that directly implement the safety functions. Safety Features refer to the primary functions directly responsible for contributing to the realization of the fundamental safety function. These features include specific processes or mechanisms designed to prevent accidents, mitigate hazards, or protect users and the environment. Support Safety Features, as auxiliary functional elements, aid the primary safety features in performing their roles more effectively.

2.4. Extension structure aspect

It is necessary to incorporate specific stereotypes into the structural aspect based on terminology used in the IAEA glossary. These stereotypes will help in clearly defining and distinguishing various elements related to safety within the system model. By adopting these standardized terms, we can ensure that item important to safety are explicitly represented. The FIG. 4. provides a detailed classification of items important to safety within a nuclear facility, categorizing them according to the IAEA glossary [6].

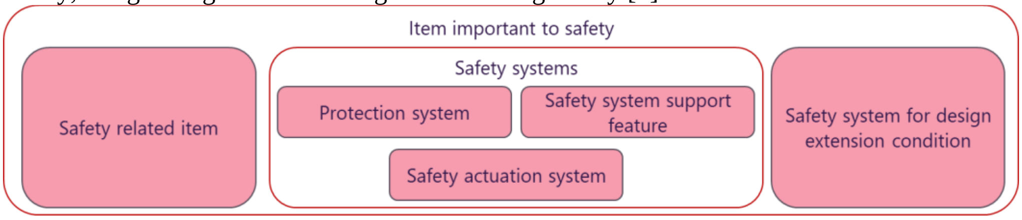


FIG. 4. New stereotypes added in the structure aspect

An **item important to safety** refers to any Structure, System, or Component whose malfunction or failure could lead to radiation exposure of site personnel or the public. An item important to safety can be:

- **Safety systems** are integral to ensuring the fundamental safety functions. These systems can be specialized in:
  - **Protection system**: This system monitors the reactor’s operation and automatically initiates actions to prevent unsafe conditions upon detecting abnormal situations. It encompasses all electrical and mechanical devices and circuitry, from sensors to actuation device input terminals.
  - **Safety actuation system**: This collection of equipment is required to perform the necessary safety actions when initiated by the protection system.
  - **Safety system support features**: These are equipment that provide essential services such as cooling, lubrication, and energy supply needed by the protection and safety actuation systems.
- **Safety-related items** are important to safety but are not part of the designated safety systems or safety features for design extension conditions. These include systems like the reactor coolant system, which are essential for maintaining overall safety but do not fall directly under the safety system category. These systems are crucial for normal operation and in preventing abnormal conditions from escalating into more serious incidents.
- **Safety system for design extension conditions** are items designed to perform safety functions during design extension conditions, applicable to scenarios beyond typical design basis accidents. They ensure the facility can handle these extended scenarios, providing an additional layer of safety. The concept applies to both research reactors and nuclear fuel cycle facilities.

2.5. Extension of the framework with nuclear safety aspect

To enhance the system modelling framework, additional concepts focusing specifically on nuclear safety assessment have been integrated. This extension provides detailed elements that are particularly useful for architects in reinforcing system analysis and strengthening the proposed system architecture.

Utilizing concepts provided by ISO 26262 [7], a standard for assessing functional safety in the automotive industry, the approach has been adapted to replace typical automotive situations with those relevant to a nuclear plant. The categories of operational conditions proposed in the FIG. 5 are customizable and can be adapted to suit the specific approaches used by different companies. These categories are to be populated with different specific operation conditions which compounded together define an operational situation. By incorporating these elements, system analysis can be based on an understanding of the different states and scenarios the system may face. The new elements, as presented in FIG. 5, enable modelling and analysis of operational situations.

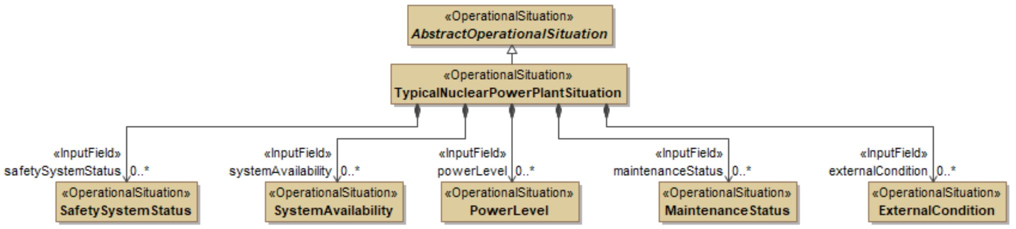


FIG. 5. New stereotypes add in the nuclear safety assessment aspect

The provided figure illustrates the structure of the Operational Situation Library, specifically tailored for a nuclear power plant. Five specifics operational conditions categories are identified. These categories are:

- **SafetySystemStatus** pertains to the operational status of safety systems within the nuclear plant, ensuring all protective measures are functional and ready to respond to safety-critical situations.
- **SystemAvailability** refers to the readiness and availability of key systems essential for maintaining normal and emergency functions, critical for the continuous and safe operation of the plant.
- **PowerLevel** indicates the power output levels at which the nuclear plant is operating, essential for maintaining reactor stability and safety.
- **MaintenanceStatus** captures the status of maintenance activities within the plant, including scheduled maintenance, ongoing repairs, and any deviations from planned routines, ensuring all systems function correctly and safely.
- **ExternalCondition** involves external environmental factors such as weather and natural hazards that can impact the plant's operation, requiring adjustments in operational protocols and additional safety measures.

Postulated Initiating Events (PIEs) are hypothetical scenarios or events that could potentially disrupt the normal operation of a nuclear facility, leading to conditions requiring the activation of safety systems. These events are carefully considered during the design and safety assessment of the facility to ensure that adequate safety measures are in place to manage and mitigate their consequences. PIEs can include a range of situations, such as equipment failures, operator errors, or external events like earthquakes or floods.

The functional concepts of Safety feature groups are directly linked to PIEs. Safety feature groups consist of various safety functions (and involved systems in their realization) designed to respond to these initiating events. To add detailed in the system analysis the concept of PIEs is also added in this aspect.

All the concepts presented above are linked with trace links to ensure comprehensive traceability from the safety goal down to the individual components, while also maintaining a connection to the postulated initiating events (PIEs) considered. This traceability framework enables an alignment between high-level safety objectives and the specific systems and components designed to achieve them. It ensures that each safety feature and operational condition is directly tied to the corresponding safety goals and PIEs, providing a coherent and structured approach to system analysis related to safety properties. This set of trace links, illustrated in the facilitates thorough documentation and verification processes, ensuring that every element of the architecture is accounted for and properly integrated into the overall safety strategy.

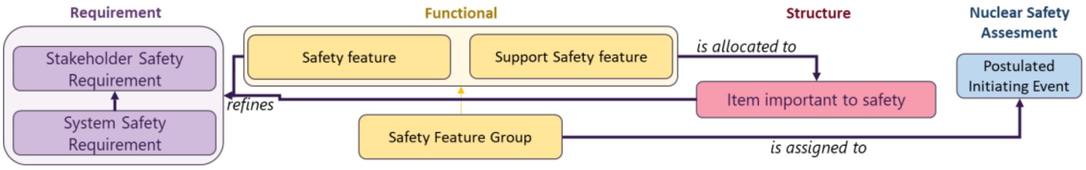


FIG. 6. Trace links between each added stereotype in the overall framework

3. APPLICATION

3.6. Case study presentation

Our use case focuses on a High-Temperature Gas-cooled Reactor (HTGR) system, a type of advanced nuclear reactor known for its high thermal efficiency and inherent safety features. Based on various publicly available documents, we have focused our modelling efforts specifically on the Reactor Cavity Cooling System (RCCS). The RCCS is a critical safety component designed to manage and remove heat from the reactor cavity. Notably, the RCCS possesses a unique functionality that allows it to switch to a passive mode in the event of a malfunction. In this passive mode, the system continues to effectively remove heat from the cavity, ensuring the safe evacuation of residual heat even when active cooling mechanisms fail.

3.7. Elaborated model

The diagrams and tables developed for this application are presented in the appendix.

The modelling of the High-Temperature Gas-cooled Reactor (HTGR) safety architecture begins with the definition of requirements. The FIG. 7 delineates the HTGR safety objectives, stakeholder safety requirements, and system safety requirements.

Following the establishment of requirements, the identification of Postulated Initiating Events (PIEs) is conducted. The FIG. 8 lists various hypothetical scenarios that could potentially disrupt normal operations.

The next phase involves detailing the operational conditions, as illustrated in FIG. 9. This figure categorizes distinct operational states, including system availability, power levels, maintenance status, safety system status, and external conditions. These conditions provide context for understanding system behaviour under various scenarios.

Following this, a use case analysis considering PIEs is performed, as depicted in FIG. 10. This analysis examines the Reactor Cavity Cooling System (RCCS) use cases in both normal and abnormal operational states, specifically considering the effects of PIEs. The use cases explain the system's functional responses under different conditions, highlighting the interplay between various safety features and system elements.

A detailed of a specific use case is presented through an activity diagram, shown in FIG. 11. This diagram provides a view of the processes involved in actively removing decay heat during an off-normal state.

The allocation of functions to safety-relevant items is illustrated in an internal block diagram, as seen in the FIG. 12. This diagram shows the physical layout and interconnections of the components.

Lastly, a relation map encapsulates the interconnections among all modelling elements, offering an overview of how a PIE is considered within the overall safety architecture. The FIG. 13 visualizes the traceability from safety goals through requirements, operational conditions, use cases, activity, and components. This comprehensive mapping ensures that every aspect of the MBSE framework is interconnected, facilitating a thorough understanding of the system's resilience to initiating events.

The comprehensive modeling approach described above provides a framework for the architecture description of the high-temperature gas-cooled reactor (HTGR) related to safety. By systematically defining requirements, identifying postulated initiating events, detailing operational conditions, analyzing use cases, and ensuring traceability through activity and internal block diagrams, the framework addresses the complex safety challenges inherent in operating a nuclear power plant.

4. CONCLUSION & PERSPECTIVES

The tailored Model-Based Systems Engineering (MBSE) approach presented in this paper provides a comprehensive framework for addressing the complex safety and operational challenges associated with Generation IV Small Modular Reactors (SMRs). By integrating nuclear-specific terminology and concepts into the MBSE framework, this approach ensures that safety considerations are embedded at every stage of the system's lifecycle. The extension of the requirements, functional, and structural aspects, along with the introduction of a nuclear safety assessment layer, enhances the ability to systematically manage safety and operational data.

This holistic approach not only facilitates regulatory compliance but also promotes consistency and traceability, crucial for the efficient and safe deployment of SMRs. The application of this framework to a High-Temperature Gas-cooled Reactor (HTGR) case study demonstrates its practical utility in managing safety-related information and processes.

Looking forward, the continued refinement and application of this tailored MBSE approach will be critical for advancing the deployment of Gen IV SMRs. Future work should focus on further integrating digital tools and platforms to support real-time data management and analysis, enhancing the agility and scalability of nuclear projects. Additionally, expanding collaboration with regulatory bodies and industry stakeholders will be essential to align this approach with evolving standards and best practices, ultimately ensuring the safe and efficient deployment of advanced nuclear technologies.

ACKNOWLEDGEMENTS

Gratitude is extended to Benjamin Baudouin and Quentin Pierron from Assystem for their assistance in constructing the example use-case and for their contributions to the understanding of key concepts.

The team at Dassault Systèmes is also acknowledged for their support in understanding the tools and methodologies necessary to extend the language within the MBSE framework.

REFERENCES

[1] JACHMICH, J., et al. (2023). Pour une ingénierie et une gestion de projets adaptées aux réacteurs modulaires avancés. Revue Générale Nucléaire, 2023(4), (French)

[2] STOCKMAN, B., & BOYLE, J. (2020). International Space Station: Systems engineering case study. Air Force Center for Systems Engineering.

[3] OBJECT MANAGEMENT GROUP. (2019). OMG Systems Modeling Language (OMG SysML), Version 1.6. Needham, MA: Object Management Group

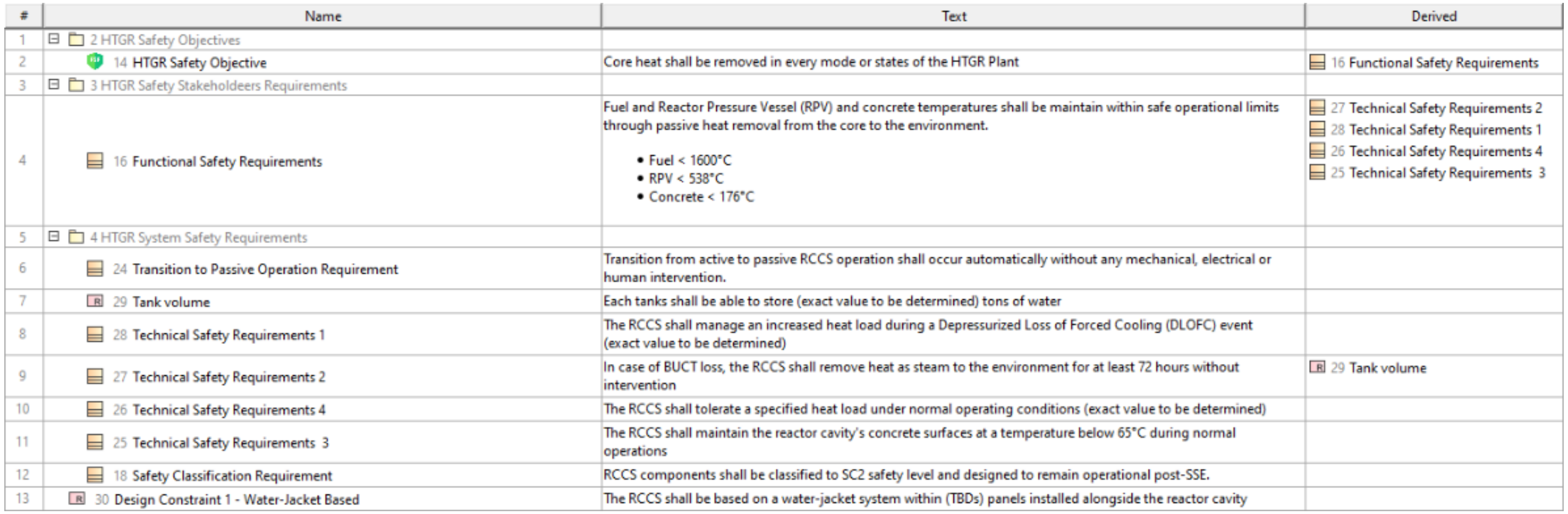
[4] ALEKSANDRAVICIENE, A., & MORKEVICIUS, A. (2021). MagicGrid book of knowledge (2nd ed.). Dassault Systèmes.

[5] ROUMILI, E. (2022) Contribution to the demonstration of nuclear safety in a model-based engineering context: Methodological proposal. (Doctoral dissertation, IMT Mines Alès)

[6] INTERNATIONAL ATOMIC ENERGY AGENCY. (2022). IAEA Nuclear Safety and Security Glossary: Terminology Used in Nuclear Safety, Nuclear Security, Radiation Protection and Emergency Preparedness and Response (2022 Interim Edition). International Atomic Energy Agency.

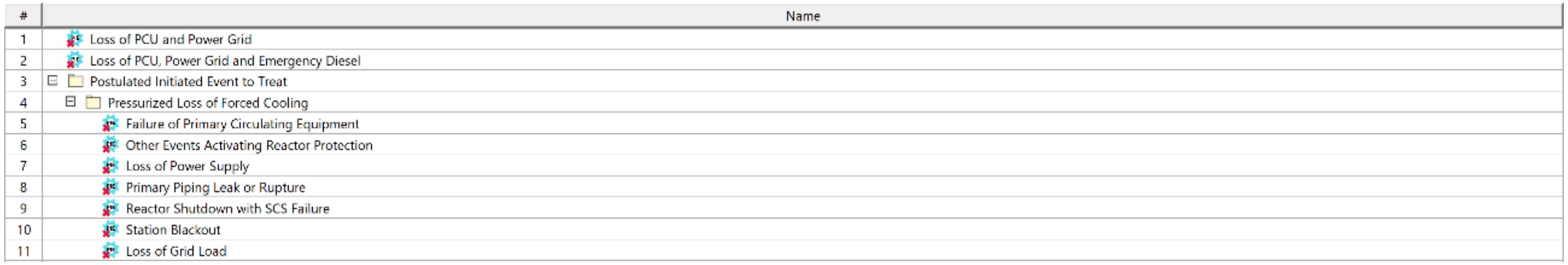
[7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2018). ISO 26262-1:2018 Road vehicles — Functional safety — Part 1: Vocabulary. Geneva, Switzerland: International Organization for Standardization.

APPENDIX



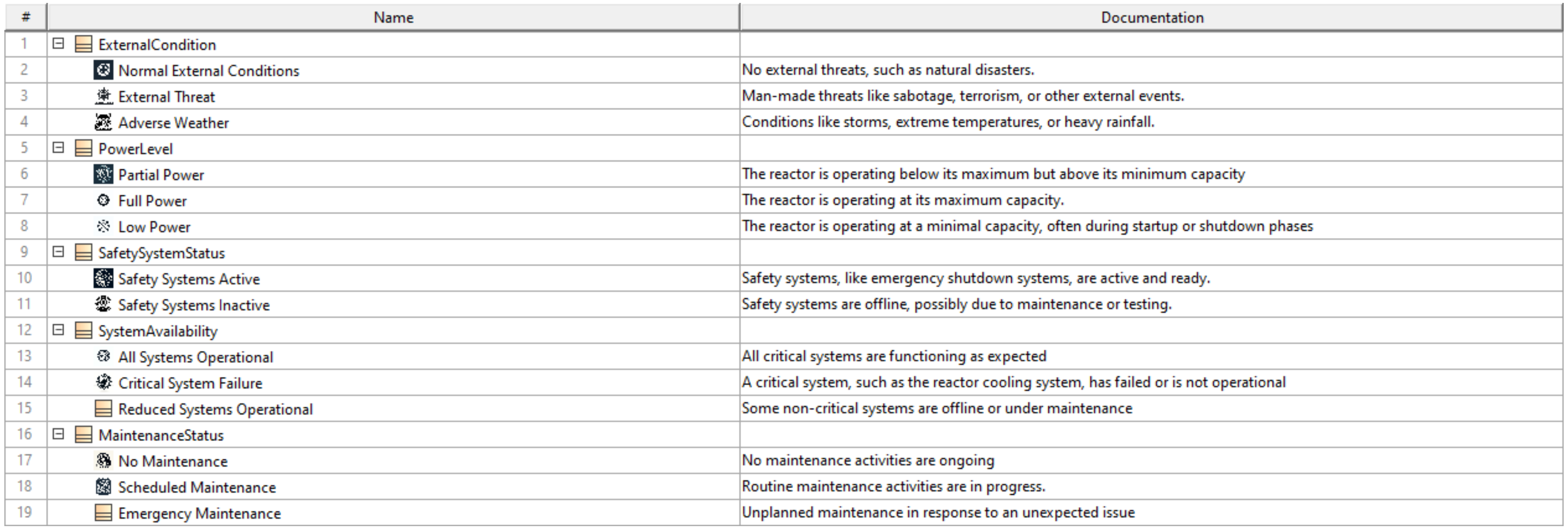
#	Name	Text	Derived
1	2 HTGR Safety Objectives		
2	14 HTGR Safety Objective	Core heat shall be removed in every mode or states of the HTGR Plant	16 Functional Safety Requirements
3	3 HTGR Safety Stakeholdeers Requirements		
4	16 Functional Safety Requirements	Fuel and Reactor Pressure Vessel (RPV) and concrete temperatures shall be maintain within safe operational limits through passive heat removal from the core to the environment. • Fuel < 1600°C • RPV < 538°C • Concrete < 176°C	27 Technical Safety Requirements 2 28 Technical Safety Requirements 1 26 Technical Safety Requirements 4 25 Technical Safety Requirements 3
5	4 HTGR System Safety Requirements		
6	24 Transition to Passive Operation Requirement	Transition from active to passive RCCS operation shall occur automatically without any mechanical, electrical or human intervention.	
7	29 Tank volume	Each tanks shall be able to store (exact value to be determined) tons of water	
8	28 Technical Safety Requirements 1	The RCCS shall manage an increased heat load during a Depressurized Loss of Forced Cooling (DLOFC) event (exact value to be determined)	
9	27 Technical Safety Requirements 2	In case of BUCT loss, the RCCS shall remove heat as steam to the environment for at least 72 hours without intervention	29 Tank volume
10	26 Technical Safety Requirements 4	The RCCS shall tolerate a specified heat load under normal operating conditions (exact value to be determined)	
11	25 Technical Safety Requirements 3	The RCCS shall maintain the reactor cavity's concrete surfaces at a temperature below 65°C during normal operations	
12	18 Safety Classification Requirement	RCCS components shall be classified to SC2 safety level and designed to remain operational post-SSE.	
13	30 Design Constraint 1 - Water-Jacket Based	The RCCS shall be based on a water-jacket system within (TBDs) panels installed alongside the reactor cavity	

FIG. 7. Extract from the goals, needs and requirements related to safety.



#	Name
1	Loss of PCU and Power Grid
2	Loss of PCU, Power Grid and Emergency Diesel
3	Postulated Initiated Event to Treat
4	Pressurized Loss of Forced Cooling
5	Failure of Primary Circulating Equipment
6	Other Events Activating Reactor Protection
7	Loss of Power Supply
8	Primary Piping Leak or Rupture
9	Reactor Shutdown with SCS Failure
10	Station Blackout
11	Loss of Grid Load

FIG. 8. Extract of the modelled Postulated initiating events



#	Name	Documentation
1	⊟ ExternalCondition	
2	Normal External Conditions	No external threats, such as natural disasters.
3	External Threat	Man-made threats like sabotage, terrorism, or other external events.
4	Adverse Weather	Conditions like storms, extreme temperatures, or heavy rainfall.
5	⊟ PowerLevel	
6	Partial Power	The reactor is operating below its maximum but above its minimum capacity
7	Full Power	The reactor is operating at its maximum capacity.
8	Low Power	The reactor is operating at a minimal capacity, often during startup or shutdown phases
9	⊟ SafetySystemStatus	
10	Safety Systems Active	Safety systems, like emergency shutdown systems, are active and ready.
11	Safety Systems Inactive	Safety systems are offline, possibly due to maintenance or testing.
12	⊟ SystemAvailability	
13	All Systems Operational	All critical systems are functioning as expected
14	Critical System Failure	A critical system, such as the reactor cooling system, has failed or is not operational
15	Reduced Systems Operational	Some non-critical systems are offline or under maintenance
16	⊟ MaintenanceStatus	
17	No Maintenance	No maintenance activities are ongoing
18	Scheduled Maintenance	Routine maintenance activities are in progress.
19	Emergency Maintenance	Unplanned maintenance in response to an unexpected issue

FIG. 9. Extract of operational conditions modelled and categorized.

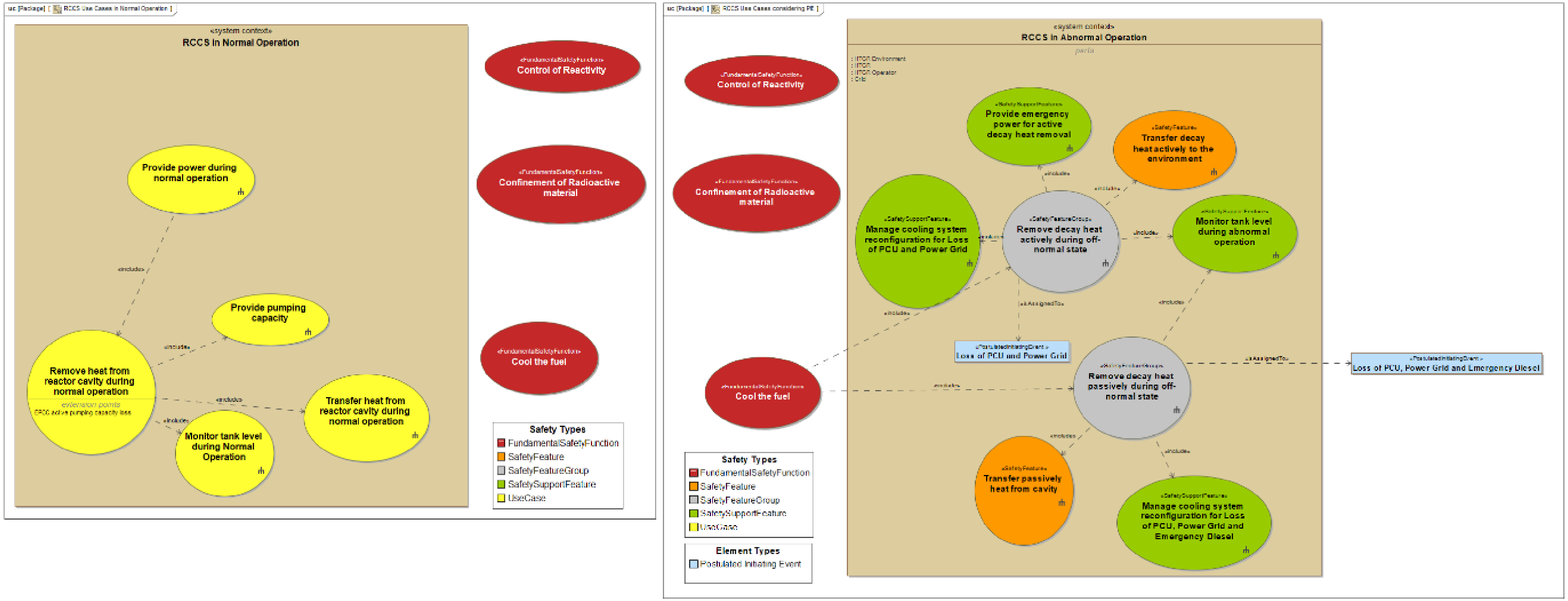

uc [Package] [RCCS Use Cases in Normal Operation]
«system context»
RCCS in Normal Operation
Provide power during normal operation
«include»
Provide pumping capacity
«include»
Remove heat from reactor cavity during normal operation
extension points
EPCC active pumping capacity loss
«include»
Transfer heat from reactor cavity during normal operation
«include»
Monitor tank level during Normal Operation
«FundamentalSafetyFunction»
Control of Reactivity
«FundamentalSafetyFunction»
Confinement of Radioactive material
«FundamentalSafetyFunction»
Cool the fuel
Safety Types
🟥 FundamentalSafetyFunction
🟧 SafetyFeature
⬜ SafetyFeatureGroup
🟩 SafetySupportFeature
🟨 UseCase
uc [Package] [RCCS Use Cases considering PIE]
«FundamentalSafetyFunction»
Control of Reactivity
«FundamentalSafetyFunction»
Confinement of Radioactive material
«FundamentalSafetyFunction»
Cool the fuel
«system context»
RCCS in Abnormal Operation
parts
: HTGR Environment
: HTGR
: HTGR Operator
: Grid
«SafetySupportFeature»
Provide emergency power for active decay heat removal
«SafetyFeature»
Transfer decay heat actively to the environment
«SafetySupportFeature»
Manage cooling system reconfiguration for Loss of PCU and Power Grid
«SafetyFeatureGroup»
Remove decay heat actively during off-normal state
«SafetySupportFeature»
Monitor tank level during abnormal operation
«include»
«isAssignedTo»
«PostulatedInitiatingEvent»
Loss of PCU and Power Grid
«SafetyFeatureGroup»
Remove decay heat passively during off-normal state
«isAssignedTo»
«PostulatedInitiatingEvent»
Loss of PCU, Power Grid and Emergency Diesel
«SafetyFeature»
Transfer passively heat from cavity
«SafetySupportFeature»
Manage cooling system reconfiguration for Loss of PCU, Power Grid and Emergency Diesel
Safety Types
🟥 FundamentalSafetyFunction
🟧 SafetyFeature
⬜ SafetyFeatureGroup
🟩 SafetySupportFeature
🟨 UseCase
Element Types
🟦 Postulated Initiating Event

FIG. 10. Example of a use case diagram for the functional aspect

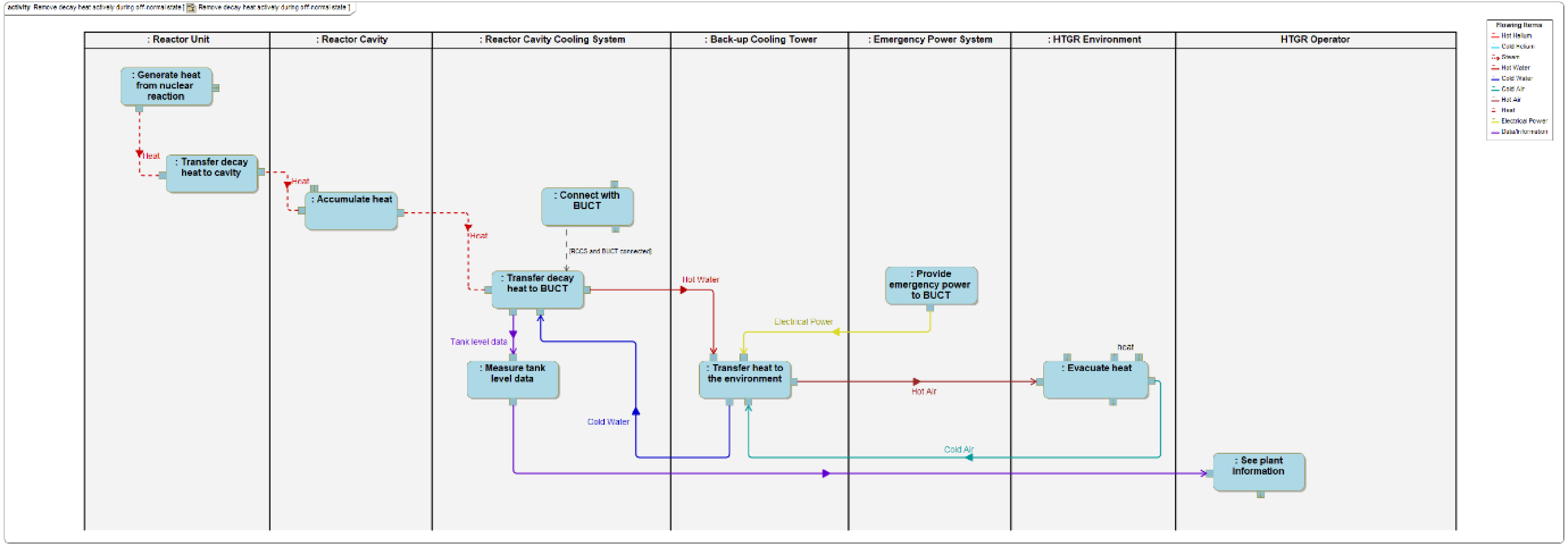


FIG. 11. Example of an activity diagram (mitigation scenarios) for the functional aspect

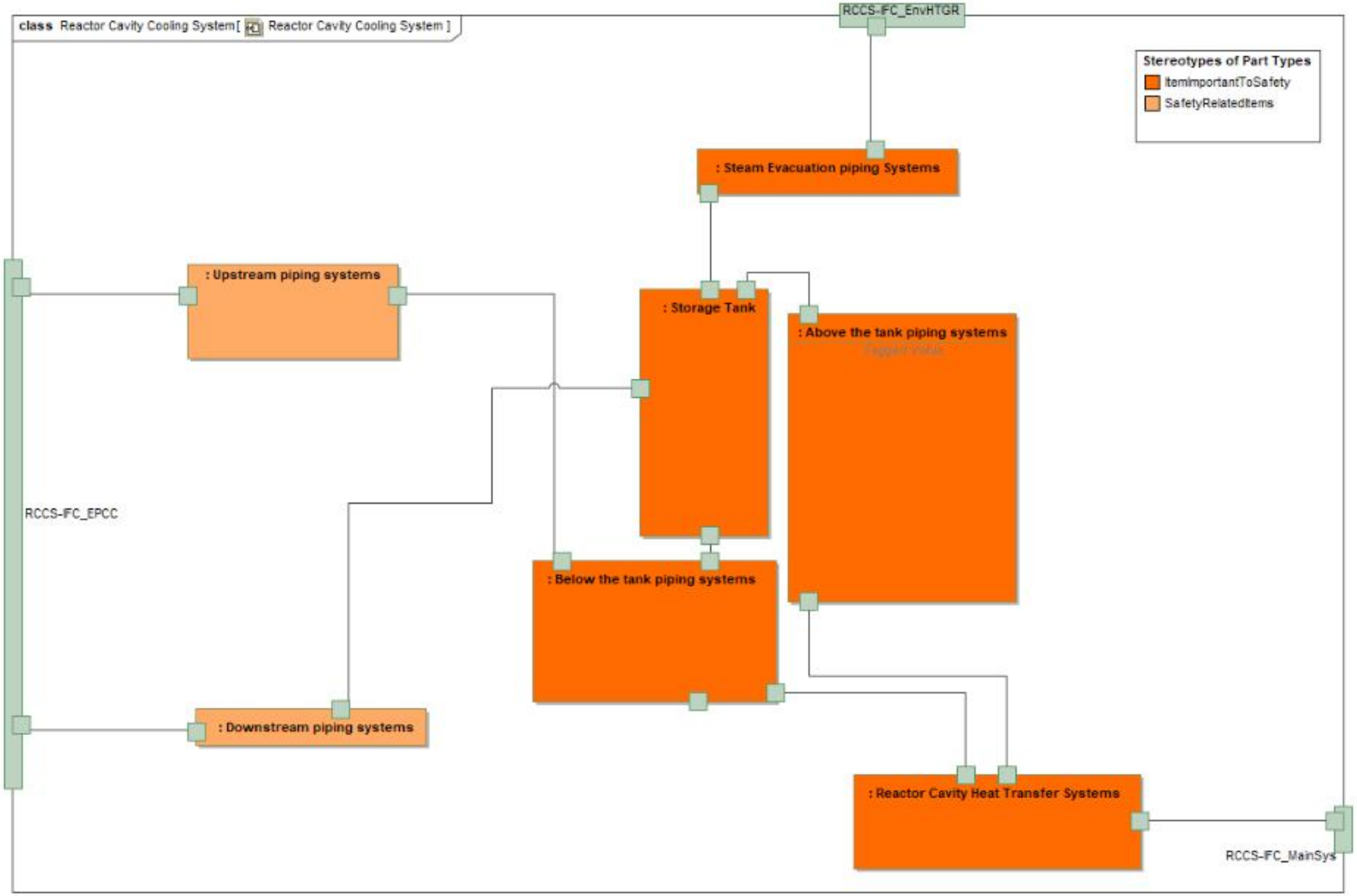

class Reactor Cavity Cooling System [Reactor Cavity Cooling System]
RCCS-IFC_EnvHTGR
Stereotypes of Part Types
ItemImportantToSafety
SafetyRelatedItems
: Steam Evacuation piping Systems
: Upstream piping systems
: Storage Tank
: Above the tank piping systems
RCCS-IFC_EPCC
: Below the tank piping systems
: Downstream piping systems
: Reactor Cavity Heat Transfer Systems
RCCS-IFC_MainSys

FIG. 12. Example of an internal block diagram for the structure aspect considering safety

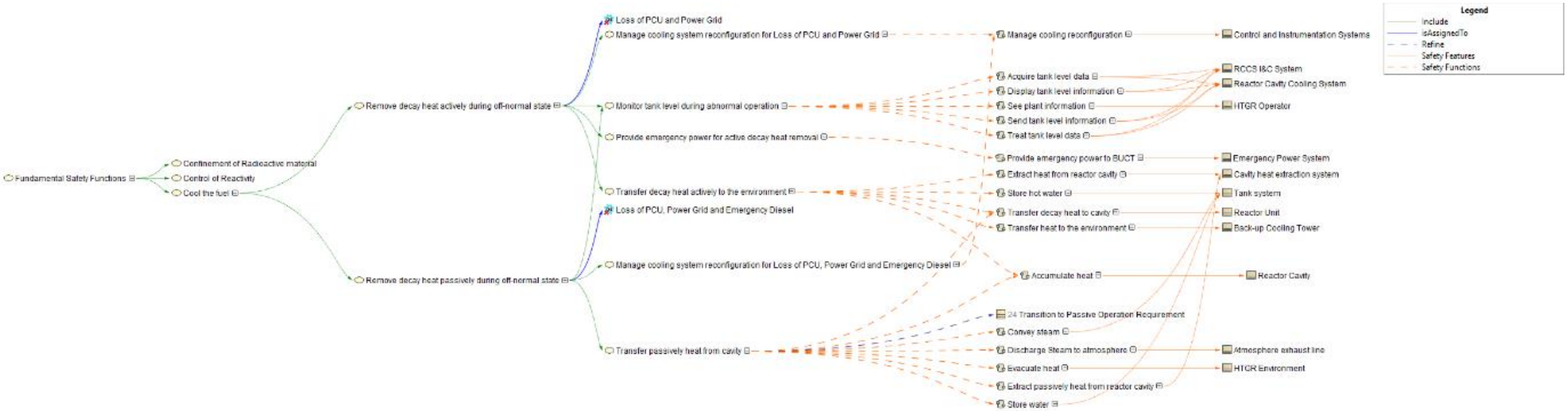

Fundamental Safety Functions
Confinement of Radioactive material
Control of Reactivity
Cool the fuel
Remove decay heat actively during off-normal state
Remove decay heat passively during off-normal state
Loss of PCU and Power Grid
Manage cooling system reconfiguration for Loss of PCU and Power Grid
Monitor tank level during abnormal operation
Provide emergency power for active decay heat removal
Transfer decay heat actively to the environment
Loss of PCU, Power Grid and Emergency Diesel
Manage cooling system reconfiguration for Loss of PCU, Power Grid and Emergency Diesel
Transfer passively heat from cavity
Manage cooling reconfiguration
Acquire tank level data
Display tank level information
See plant information
Send tank level information
Treat tank level data
Provide emergency power to BUCT
Extract heat from reactor cavity
Store hot water
Transfer decay heat to cavity
Transfer heat to the environment
Accumulate heat
24 Transition to Passive Operation Requirement
Convey steam
Discharge Steam to atmosphere
Evacuate heat
Extract passively heat from reactor cavity
Store water
Control and Instrumentation Systems
RCCS I&C System
Reactor Cavity Cooling System
HTGR Operator
Emergency Power System
Cavity heat extraction system
Tank system
Reactor Unit
Back-up Cooling Tower
Reactor Cavity
Atmosphere exhaust line
HTGR Environment
Legend
Include
isAssignedTo
Refine
Safety Features
Safety Functions

FIG. 13. Example of a traceability map from fundamental safety function to item relevant for safety