28th annual INCOSE international symposium
Washington, DC, USA
July 7 - 12, 2018

Architecture Design of Nuclear Power Plants Systems through Viewpoints-based Systems Analysis

Juan Navas
Thales Corporate Engineering
juan.navas@thalesgroup.com

Philippe Tannery
Framatome
philippe.tannery@framatome.com

Stephane Bonnet
Thales Corporate Engineering
stephane.bonnet@thalesgroup.com

Jean-Luc Voirin
Thales Airborne Systems
Thales Technical Directorate
jean-luc.voirin@fr.thalesgroup.com

Copyright © 2018 by Juan Navas. Published and used by INCOSE with permission.

Abstract. This paper presents a method to perform the architecture definition and design of Nuclear Power Plants (NPP) systems. This method is based on the viewpoints concept and on an existing Model-Based Systems Engineering (MBSE) approach that was tailored to address the complexity factors of NPP engineering, progressively guarantee the comprehensiveness of the design and facilitate the safety assessment. This paper also provides an illustration of how this method was applied to define the architecture of a Nuclear Island system, provides valuable findings for the designer organization regarding the deployment of MBSE approaches and presents their key benefits and future improvement actions.

Introduction

The challenges of Nuclear Power Generation. In 2015, Nuclear Power Plants (NPP) generated 2,441 TWh of electricity, about 10% of the world's total generation and one third of world's decarbonized production. The International Energy Agency, in accordance to scenarios in which the increase of global average temperature is limited to 2°C compared to preindustrial levels, envisages a major increase in the contribution from nuclear energy. It foresees about 17% of global electricity produced by NPP, in a world where consumption will have doubled [WNA 2016].

This context, alongside with the aging of existing NPP, may imply that the number of refurbishments and constructions of new nuclear reactors to be carried out in the following years will increase. Today, nuclear reactors' engineering, construction and licensing face important challenges. First of all, nuclear safety remains the key concern on nuclear reactors design. Everyone involved realizes that nuclear power is unique and that design and processes shall be continuously improved to ensure nuclear safety. Lessons learned from Fukushima accident, as well as changes on national and international regulations, shall ideally be taken into account as soon as possible, from the conceptual design stage. Safety authorities are more and more demanding on their requirements and on how the final design solutions satisfy the safety concerns. The methods that are put in place to develop such solutions are also challenged: for the sake of illustration, the size of the commissioning dossier of a third generation NPP may reach over 40 000 pages.

Secondly, NPP being complex Large Infrastructure Projects (LIP) [INCOSE IWG 2012], a high number of external and internal stakeholders is involved on NPP development. Complexity increases as outcomes required by these stakeholders are often in conflict, and the stakeholders are often entities whose decisions may be governed by political considerations and/or are not reachable by NPP designers. NPP development is also subject to laws and regulations, site conditions, industrial codes

and standards and public interest that often evolve during project execution. As NPP projects have a very long-time span, projects shall at least anticipate major changes required during NPP development, as the odds for them to occur are higher than for other kinds of projects.

Finally, cost of nuclear-sourced electricity shall remain competitive when compared to other sources of electricity. As engineering and construction costs represent a major part of investment costs, this means that major efforts aiming at the improvement of engineering performance and the reduction of construction time shall be made.

The case for the deployment of Systems Engineering approaches in NPP engineering. Systems Engineering (SE) methodologies have proven their relevance on several heavy industries such as aircraft, defense and aerospace. The deployment of SE practices correlates positively to technical, cost and schedule success of systems development projects [Honour 2013, Elm 2012]. Furthermore, these studies confirm that the SE activities that are more intensively performed at early stages of the project have a particularly positive correlation to projects' success. Among these SE activities we find: Project Planning, Requirements development and management, and Architecture and Trade Studies.

The hypothesis we aim to challenge in this paper is that reinforcing SE practices on NPP projects is as effective as for other industrial fields. A first analysis shows that the SE principles are relevant to the nuclear field: the systems approach, aiming at fully considering the system's environment throughout its life-cycle; the separation of needs from solutions and the focus on exhaustively exploring the needs, in order to reach a proper comprehension of the problem and hence a solution acceptable for all the stakeholders; the decomposition of the solution in manageable subsystems, in order to deal with the systems' complexity; and a common language and normalized deliverables, in order to harmonize the interfaces between development teams.

Nevertheless, in order to ensure the effectiveness of the SE approach in the nuclear field, a necessary step is the tailoring of SE practices to the specificities of nuclear industry. In this paper, we present how Systems Architecture Definition and Design practice was tailored to be performed for nuclear systems' design, and provide feedback on the tailoring process. We based our work on a Systems Architecture methodology that has proven its efficiency in other industrial fields and that follows the Model-Based Systems Engineering (MBSE) approach.

We focus on Architectural Design as the results of this activity have a strong impact on further stages of system development. It is also the responsibility of the Architecture team, which is a key actor of the project. Furthermore, a proper definition of systems' architectures has a strong positive impact on activities linked with project management such as WBS definition and configuration management.

The remaining of this paper is organized as follows: we first provide a background on the MBSE approach and the System Architecture and Design practice in which we based our work; next we present the foundations of the approach and the conceived methodology, as well as a case study on deploying this methodology during the Architectural Design of one of the major systems of a Pressurized Water Reactor (PWR)-type NPP: the Nuclear Island system, which transfers the heat produced inside its reactor in the form of pressurized steam to the Turbine Island in view of electrical power generation; then we summarize the main findings regarding the deployment of MBSE on nuclear engineering, both in terms of the tailoring process and of the feedback from engineering population ; finally we identify the future work that could be performed based on our results and conclude this paper.

Background

Systems' Architecture Definition and Design. This paper focuses on what will be called here System/Solution Architecture Definition and Design, a limited part of all architecture-related

activities, as described in international standards such as [ISO/IEC/IEEE 15288 2015]. This chapter provides a brief description of the goals of the ISO/IEC/IEEE 15288 technical processes that are fully or partially addressed by the MBSE method presented in the following chapters.

In 15288 technical processes, the major part of the Business or Mission Analysis process characterizes the problem and solution space, and determines potential solution class(es), at very high level. This process is mostly out of scope of Systems Architecture Definition and Design, but is an input for it, and more precisely for need analysis.

The Stakeholder Needs and Requirements Definition process also applies partially to Architecture Definition and Design, mainly in capturing capabilities needed by users and other stakeholders, their operational, functional and non-functional expectations, and transforming them into stakeholders' requirements.

Then, Architecture Definition and Design transforms the former stakeholder needs, into a solution-focused set of needs and requirements, so as to fulfil the users' expectations. This is fully in the scope of the System Requirements Definition process.

Architecture Definition process meets the second major contribution of Architecture Definition and Design, which is to find and describe the best answer to stakeholders needs in terms of system/solution architecture: selection of alternatives, description of functional and non-functional behavior, allocation to sub-systems or components, interface definition, etc. Tightly related to this one, the System Analysis process will be addressed by Architecture Definition and Design through assessment and via viewpoint-based analyses.

As part of the Design Definition process, the detailed definition and development or purchasing technical contract are defined, along with the strategy for Integration Verification Validation processes activities.

Views and Viewpoints. At the heart of System Architecture Definition and Design is the description and assessment of the system architecture. The [ISO/IEC/IEEE 42010 2011] standard promotes the use of Views, and Viewpoints to take into account stakeholders perspectives.

According to the standard, "an architecture view expresses the architecture of the system-of-interest in accordance with an architecture viewpoint (or simply, viewpoint)". Each stakeholder has his/her own Concerns, such as constraints, expectations or uses, on the architecture. These concerns are framed (formulated and scoped) by viewpoints; viewpoints might be considered as "mediators" between a stakeholder and the architecture description, so as for him/her to contribute to architecture building, assessment and use, according to his/her perspective and concerns. A view can be seen as the representation of the architecture description relating and focusing on a given viewpoint.

For the System/Solution Architecture definition and design, we could expect viewpoints (or perspectives) dealing with need (operational, functional, non-functional etc.), with solution description - at different levels of abstraction and according to different concerns (functional, structural, etc.), or with non-functional specialty engineering (safety, security, product line, resource management, reliability, environment, and many more), among others.

The Arcadia Model-Based Systems Engineering method. Arcadia is a model-based method devoted to systems, software, hardware architecture engineering [Voirin 2017]. It describes the detailed reasoning to understand the real customer need, define and share the product architecture among all engineering stakeholders, early validate its design and justify it, ease and master integration, validation, verification. Arcadia can be applied to complex systems, equipment, software or hardware architecture definition, especially those dealing with strong constraints to be reconciled (cost, performance, safety, security, reuse, consumption, weight…). It is intended to be embraced by most stakeholders in system/product/software/hardware definition as their common engineering reference.

Arcadia has been experimented and validated in many real-life contexts for several years. Its large adoption in many different engineering contexts witnesses of an industry-proven comprehensive method for system engineering, adapting to each context in a dedicated manner, and yet being tooled by the same powerful tools capitalizing knowledge.

Arcadia intensively relies on functional analysis. It introduces four engineering perspectives (cf. Figure 1): Operational Analysis, System Analysis, Logical Analysis and Physical Analysis. By doing so, it promotes a clear distinction between the expression of the need (covered by the first two perspectives) and the expression of the solution (by the last 2 perspectives).

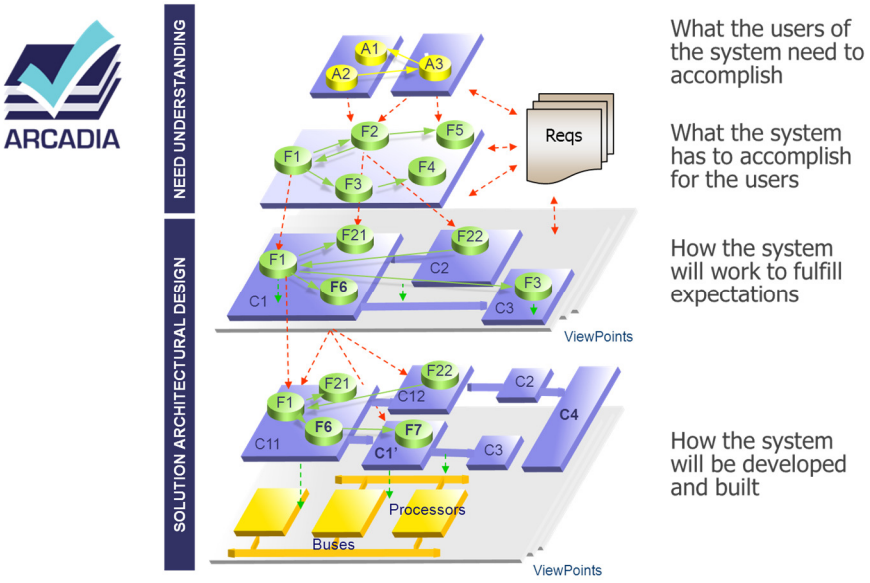

Figure 1. Arcadia engineering phases

The Capella MBSE tool. While the Arcadia method itself is tool-agnostic, it requires a modeling workbench to be effectively implemented. As the lack of properly tailored tools has proven to be a major obstacle to the implementation of MBSE in industrial organizations [Bonnet 2015], Arcadia is recommended to be implemented using the modelling workbench Capella [Capella 2017].

Capella guides users in applying the Arcadia method and assists them in managing complexity of systems design with automated simplification mechanisms. A model is built for each Arcadia engineering perspective. All models are related by justification links and are processed as a whole for impact analysis.

The original audience for the Arcadia/Capella solution was primarily systems engineers with diverse backgrounds and skills. Capella is neither a SysML profile nor a DSL. The core meta-model of the Capella notation has been strongly inspired by SysML and the diagrams provided are very similar. However, when considering the SysML language as a reference, the meta-model of Capella is simultaneously simplified, modified, and enriched.

- Simplified or modified: whenever SysML concepts were more complex than necessary to model architectures, they were either excluded (many low-level behavior modeling constructs are absent) or simplified (components, parts, instances);
- Enriched: Arcadia implements an architectural framework, where description languages such as SysML do not; the Capella tool implements this framework in its meta-model.

The main advantage of this hybrid approach is that Capella diagrams can be read and understood (to a certain extent) by engineers having no particular knowledge of Arcadia. Capella is an original solution in the landscape of modelling workbenches for several reasons:

- The tight coupling between the method and the tool, enforcing the implementation of the method at working levels and ensuring a homogeneous graphical aspect of models' diagrams;
- The availability of multiple productivity tools, helping end-users to create their models in a more efficient way: taking into account existing model parts to initialize others, improving the consistency and correctness of models by reducing human mistakes, transitions from one Arcadia perspective to another, brushing of layouts between diagrams, querying what an element is related to and which other views it appears in, etc.;
- The artifacts allowing to master the growing complexity of systems: simplifying the underlying modelling concepts, computing graphical simplifications favoring readability, understanding, and analysis, providing multiple entry points to the users to implement both top-down and bottom-up engineering approaches.

Finally, Capella is available as open source software. The openness of Capella is a guarantee of sustainability and freedom to customize, exploit, and enrich the tool according to specific needs. Open source means here that organizations can shape the future of Capella and take the control of their modelling environment.

Applying MBSE approach to Nuclear Systems Architecture Definition and Design

In this chapter we present how the Arcadia/Capella MBSE method and tool were adapted and seamlessly integrated to nuclear systems' Architecture Definition and Design. We start by providing an overview of the tailoring process and its results, then we provide more details on the tailoring specificities through an extract of the architectural design of the Nuclear Island system, one of the major systems of a NPP.

Methodology overview. The key success factor on effectively tailoring the Arcadia method to nuclear engineering is to address the main tasks performed by engineering teams and to deploy SE practices that result on better and faster architectural design without penalizing project's schedule milestones. To do so, we associated the main engineering task with an Arcadia engineering perspective and identified the Capella models that most appropriately supported them. While doing so, we also identified models that would add more value to the architectural design or that could anticipate future design tasks.

Figure 2 summarizes the mapping of six main engineering tasks into the Arcadia engineering perspectives. In this paper we focus on the tasks that have been mapped to System Analysis and Logical Analysis perspectives, as they were the most relevant perspectives of the Nuclear Island case study that will be presented in the following chapter.

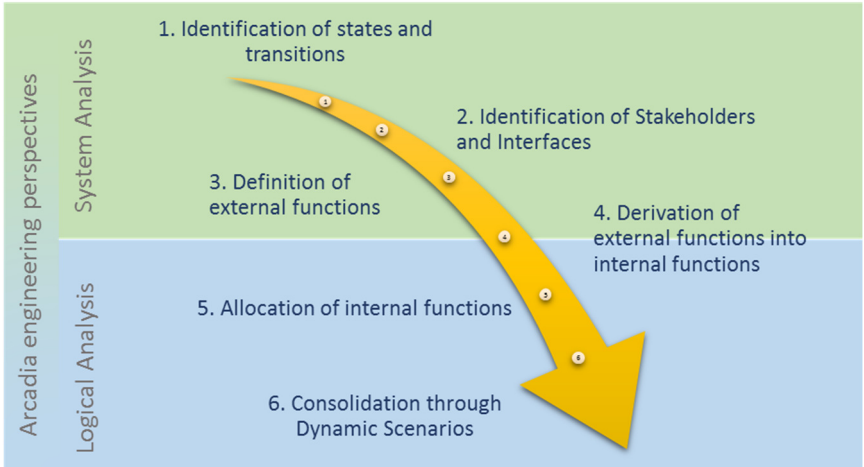

Figure 2. Tailored Arcadia method

The Nuclear Island System. In order to illustrate and provide details on how the MBSE approach is applied on nuclear systems engineering, we rely on a case study on the architectural design of the Nuclear Island system.

PWR-type NPP include two major systems: the Nuclear Island system and the Conventional Island system. The Nuclear Island's main operational mission is to transfer the heat produced inside the reactor core in the form of pressurized steam to the Conventional Island, in which a steam turbine and a generator use the thermal energy to perform mechanical work on a rotating output shaft and generate electrical energy. Other NPP major systems are in strong interaction with both the Nuclear Island and the Conventional Island, such as the Electrical Systems providing power to equipment in all situations and Control Systems regulating and supervising the whole process.

Nuclear Island optimal architecture is determined by NPP's business goals such as the targeted power generation capacity, the capability to support load variations, the type of nuclear fuel to be used, the lifetime of components, the maintenance constraints and components' replacement policies, among others. But above all, Nuclear Island architecture shall comply with safety requirements and shall guarantee that its subsystems can perform the safety functions during its entire lifecycle: control of nuclear fuel reactivity, nuclear heat removal and containment of radioactive material.

Task 1 - Nuclear Island lifecycle and states. All Nuclear Island lifecycle stages are considered while performing its architecture design. Nuclear Island lifecycle stages are closely related to NPP's ones. They cover the Design of the system (which is usually performed in a progressive way, from conceptual design to detailed design), the Procurement, Erection, Commissioning, Operation, Maintenance, Upgrades and the Decommissioning of the system.

For the sake of simplicity, the Nuclear Island analysis illustrated in the following chapters of this paper only consider the operational states of a NPP, i.e. the Nuclear Island's Operation phase. We define Normal Operational States based on [IAEA 2016, IAEA 2000]: startup, power production, shutdown, maintenance and testing. Some Abnormal Operational States covering upset and emergency conditions, are also addressed in the following chapters.

Figure 3 shows the Capella model of the Nuclear Island life-cycle stages, focusing on operational states and the transitions from a state to another one. At this stage the transitions are defined only by a short description of the event that enables/triggers them. Transitions, as well as subsystems sub-states and the complex combination of states across system levels, are progressively refined and enriched during the following tasks but not detailed in this paper [Bonnet et. al. 2017].

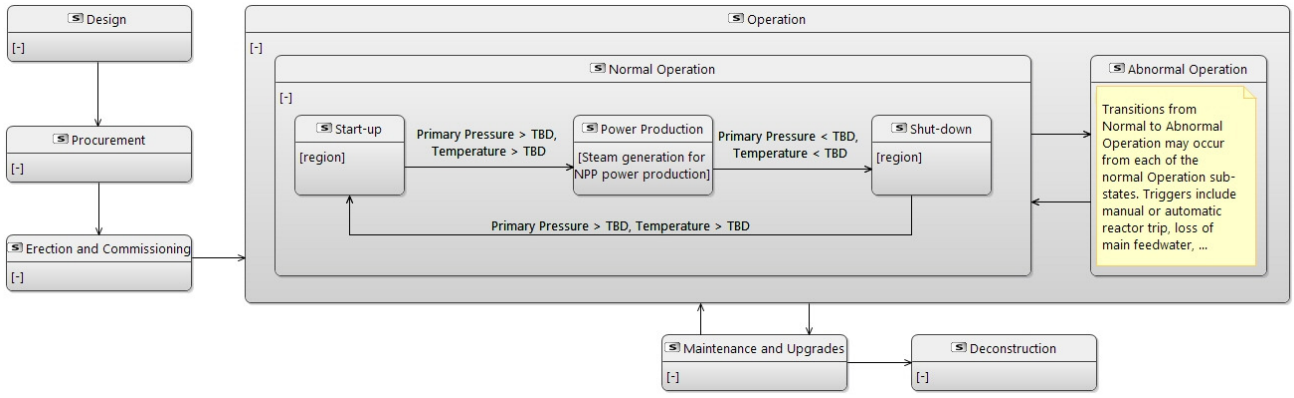

Figure 3 – Nuclear Island lifecycle phases and operational states

Tasks 2 and 3 - System Analysis perspective. The goal is first to consolidate the boundaries of the Nuclear Island system: the functions it shall perform to satisfy stakeholders' needs, and the constraints that shall be taken into account during its design.

The second task is hence to determine the system's stakeholders, i.e. the entities that are concerned by the system, and how the Nuclear Island interacts with them. This is done by considering each life-cycle stage of the Nuclear Island development and identifying the organizations, individuals and other systems that may be in interface, directly or indirectly, with the system. These external interfaces are defined and prioritized: those which shall be clearly defined at the current stage of design in order to reduce the uncertainties of the architecture are considered as critical and hence prioritized.

Figure 4 shows the model that supports this analysis. The Nuclear Island system is at the center. A subset of the stakeholders that interact with the Nuclear Island during the operational states are presented. The interfaces identified in the diagram are those considered as key ones to define the envelope architecture of the Nuclear Island. They may include interfaces with servicing systems providing items necessary for the operation of the Nuclear Island, e.g. compressed and regular air. The external interfaces are defined by a short description and the life-cycle stage in which they are materialized (not shown in the diagram). They shall be progressively completed, refined and enriched with functional and non-functional requirements during the further steps of the analysis.

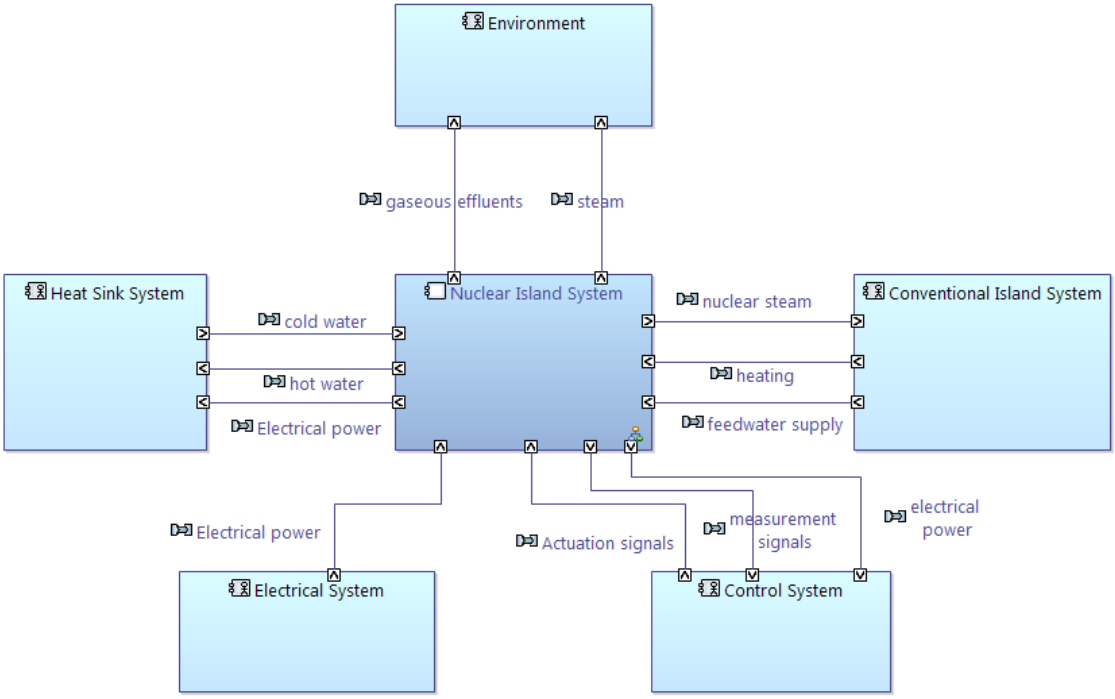

Figure 4. Nuclear Island main stakeholders and interfaces (operational states only)

The third task is to determine the functions that are ensured by the Nuclear Island. For this purpose, the APTE method [de la Bretesche 2000] is implemented: NI states and stakeholders are simultaneously considered and answers to questions such as "how the system interacts with the stakeholder at a given state" are sought, enabling the identification of Nuclear Island external functions. Interactions may be from the stakeholder to the system, from the system to the stakeholder, or combinations of these (e.g. from a stakeholder to the system and then to another stakeholder).

During a NPP development project, Nuclear Island development is likely to be performed concurrently with other NPP major systems' development. Hence it is recommended for architecture teams not only to identify their system-of-interest external functions, but also to ensure the consistency with the external functions of the systems it interacts with. This is done by engaging discussions and performing reviews of the exchanges between their external functions, involving

interfaced systems' architects and downstream design teams if necessary. Reviews lead to defining decoupling values if uncertainty of interfaces is still high. Such a collaborative definition of exchanges and interfaces allow the architecting population to consolidate the scope of their systems. The use of MBSE tools promotes this approach, as the interfaces defined previously are associated to the exchanges between systems' external functions.

Furthermore, identifying the functions of the surrounding systems allow Nuclear Island architecture team to define *Functional Chains*, i.e. to identify which functions are involved on achieving a common, higher-level goal. The Functional Chain is the implementation of an external function of the higher-level system, in this case the NPP itself.

The model diagram in Figure 5 provides an extract of the resulting Nuclear Island functions. A Functional Chain, *Transfer thermal power from Nuclear Island to the Conventional Island by steam release*, is presented. It shows how Conventional Island and Nuclear Island's functions are performed in order to achieve in a coordinated way one of the main operational missions of the Nuclear Island.

At this stage of the analysis, architecture teams shall have acquired a comprehensive understanding of the needs for a Nuclear Island: the requirements that are applicable to the system as a whole, its operational life-cycle, the functions it shall perform in order to comply with its requirements and the interfaces with its environment, other industrial systems, external human actors and organizations.

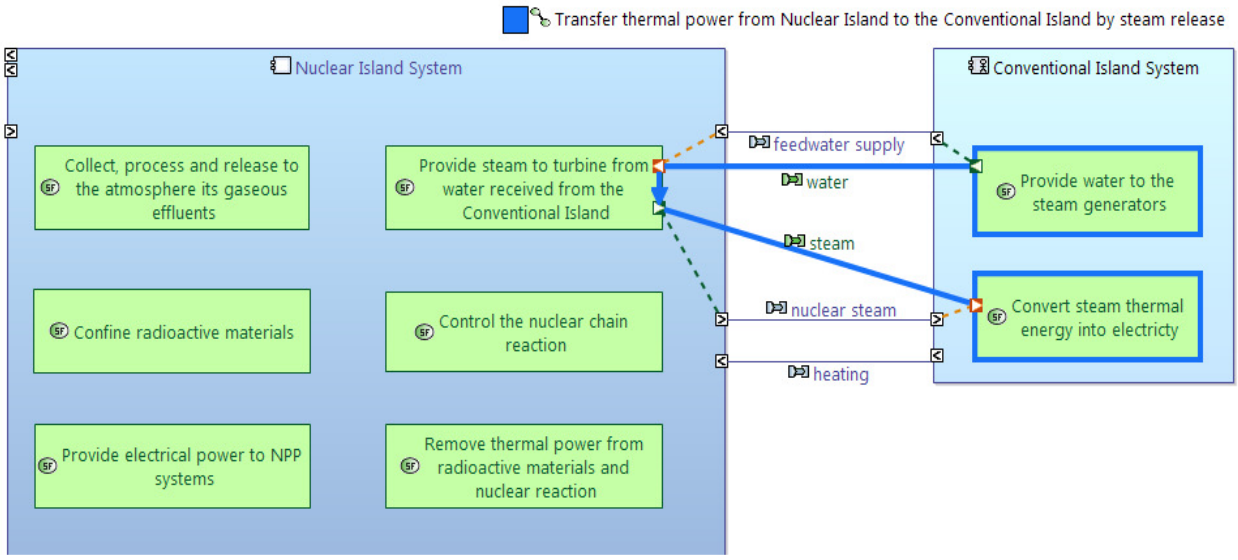

Figure 5. Nuclear Island external functions (extract) and *Transfer thermal power from Nuclear Island to the Conventional Island by steam release* Functional Chain

Tasks 4 and 5 - Logical Analysis perspective. The Logical Analysis focus on the solutions, i.e. the system architecture satisfying the needs analyzed and formalized during the previous perspective. This is done through the definition of the subsystems and/or components that interact together in order to achieve the functions of the Nuclear Island system, and the definition of the boundaries of these subsystems and the requirements which are applicable to them.

The stakes of this step are high, as the requirements over the systems and components that will actually be built, commissioned and operated are defined at this stage. Therefore, it is highly recommended to work on several architecture alternatives and to compare them using pre-defined criteria that not only includes technical aspects, but also costs and schedule-related aspects. In this chapter, we present how a single alternative is developed; later on, we provide further information on how trade-offs between several architecture alternatives are performed.

Most of the time NPP models are conceived as improvements of previous models that have been already licensed, built and in operation: industrial models already exist for the procurement, erection and commissioning of existing nuclear systems. The first task of the analysis is hence to consider the state of the art of Nuclear Island design and to inherit the system decomposition of previous models – their Product Breakdown Structure (PBS), in order to integrate the existing technologies and industrial models into the architectural tradeoffs that will be performed later. This decomposition will serve as a reference for the further architecture and design tasks: the requirements and functions that will be derived from Nuclear Island's ones and the tradeoffs between the allocation alternatives may refine and even redefine the boundaries of the subsystems and hence the Nuclear Island architecture. In this paper, a reference PBS is defined for the Nuclear Island system, decomposed in 5 subsystems: Heat Production system, Steam Transfer system, Fuel Handling system, Containment system and Auxiliary systems.

Task 4 consist in decomposing the Nuclear Island external functions into less complex functions that together specify how the Nuclear Island functions are achieved, called internal functions. As external functions are often related to more than one state of the system, the decomposition task is performed exhaustively for each function and state. This may result on several alternatives of internal functions' arrangements for each external function, especially when considering constraints from an existing PBS. It is recommended to keep these alternatives and to consider them during trade-offs analysis (cf. "Architectural Trade-offs" chapter).

The model diagram in Figure 6 illustrate the decomposition of system function *Provide steam to turbine from water received from the Conventional Island* at *Power Production* operational state. Note how the Functional Chain *Transfer thermal power from Nuclear Island to the Conventional Island by steam release* has been enriched, as it now concerns three internal functions of the Nuclear Island. Note also that during this task it may also become necessary to define functions that are not decompositions of the Nuclear Island external functions but new functions instead; this is the case for *Control thermal power level*: in order to provide load variation capabilities, the Nuclear Island shall deliver several steam flowrates, which makes emerge a regulation function. Similarly, some internal functions issued from the decomposition of an external function may also contribute to the implementation of other external functions. In both cases a traceability link shall be defined with the corresponding external functions.

The functional requirements linked to Nuclear Island external functions, as well as the non-functional requirements applicable to the whole Nuclear Island scope, are treated in a similar way: they are decomposed by analyzing each phase/state of the system.

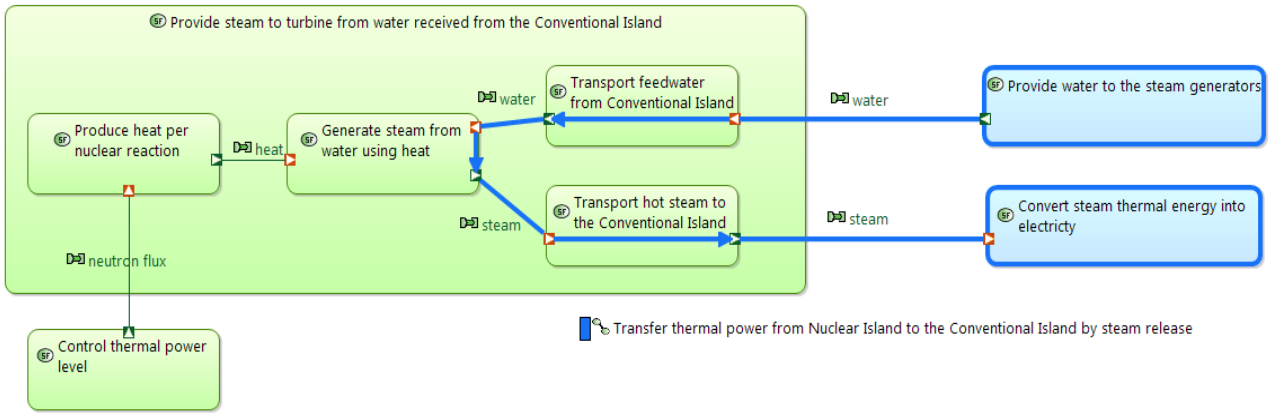

Figure 6. Transfer thermal power from Nuclear Island to the Conventional Island by steam release Functional Chain after decomposition of Nuclear Island external functions into internal functions

Task 5 consists in allocating the internal functions, their associated requirements and the non-functional requirements, to the reference subsystems of the Nuclear Island. At this step, all the allocation alternatives shall be considered and compared in order to find an optimal allocation with regard to the safety and business objectives of the Nuclear Island system (cf. "Architectural Trade-offs" chapter). The model diagram in Figure 7 shows a possible allocation of functions into Nuclear Island subsystems. Note that two of the Nuclear Island systems contribute to the achievement of the Functional Chain *Transfer thermal power from Nuclear Island to the Conventional Island by steam release*: Heat Production and Steam Transfer systems.

At this stage, a first release of Nuclear Island subsystems requirements specifications may be performed. Its scope is circumscribed to the key stakeholders, key requirements and key interfaces of the Nuclear Island that size the architecture of the Nuclear Island issued from trade-offs analysis. The release of this preliminary version allows subsystems' architectural teams to perform Tasks 1 to 3 and to anticipate further tasks without major risks of design changes once the final version is released.

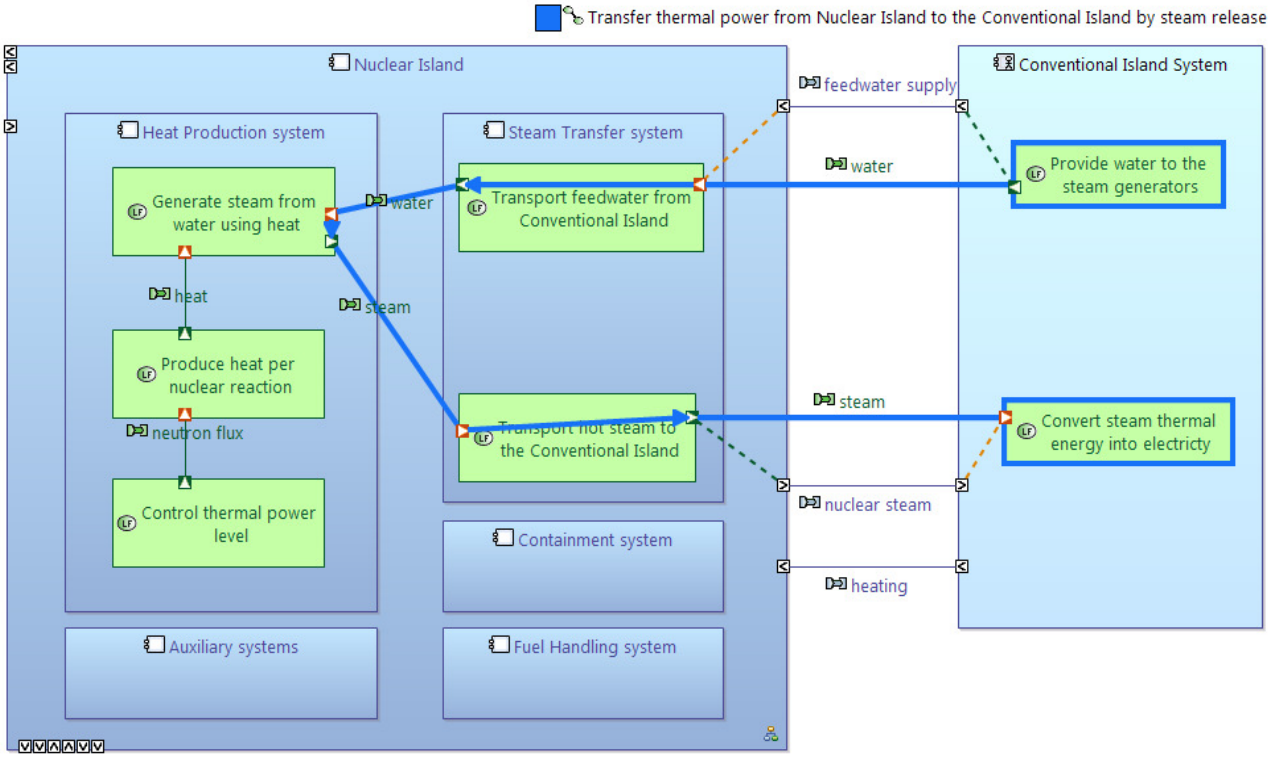

Figure 7. Transfer thermal power from Nuclear Island to the Conventional Island by steam release Functional Chain after allocation of functions into Nuclear Island subsystems

Task 6 – Dynamic scenarios for consolidating the Logical Analysis. The goal of this task is to check the comprehensiveness of the architecture and to reach confidence on the whole requirements on the Nuclear Island system being considered and that the architecture fully satisfies them. This is achieved by challenging the defined architecture with scenarios and checking that the existing functions and requirements properly specify the expected behavior of the Nuclear Island subsystems. Scenarios are used to get insurance that the emergent properties of systems have been takin into account in defining their architecture and design.

Two kinds of scenarios are considered at this step: normal scenarios and dysfunctional scenarios. The former are scenarios in which the normal operational states of the system are scanned; the latter include scenarios triggered by one or several simultaneous malfunctions on subsystems' components and that forces the Nuclear Island system to switch from normal to abnormal operation state.

Scenarios are “run” manually during workshops gathering architecture team’s members, as well as members of other relevant systems and downstream subsystems’ architecture teams. Events are triggered and responses of the subsystems are estimated from the functions and requirements allocated to them. When functions and requirements do not describe the expected behavior well enough, these can be refined or new functions and requirements could be created at this point. Figure 8 shows an extract of a scenario of isolation of the Nuclear Island due to an abnormal event.

Given the high number of scenarios that may be run, the most critical ones, i.e. those that will mostly contribute to the reduction of risks and uncertainties in the system architecture, shall be performed first. At the end of this task, the Nuclear Island subsystems requirements specifications may be updated to its final version and released. At later phases of design, the execution of scenarios may be performed by simulations in order to improve the representativeness of the architecture model and better and faster support architectural tradeoffs, as it is done by [Frey 2010].

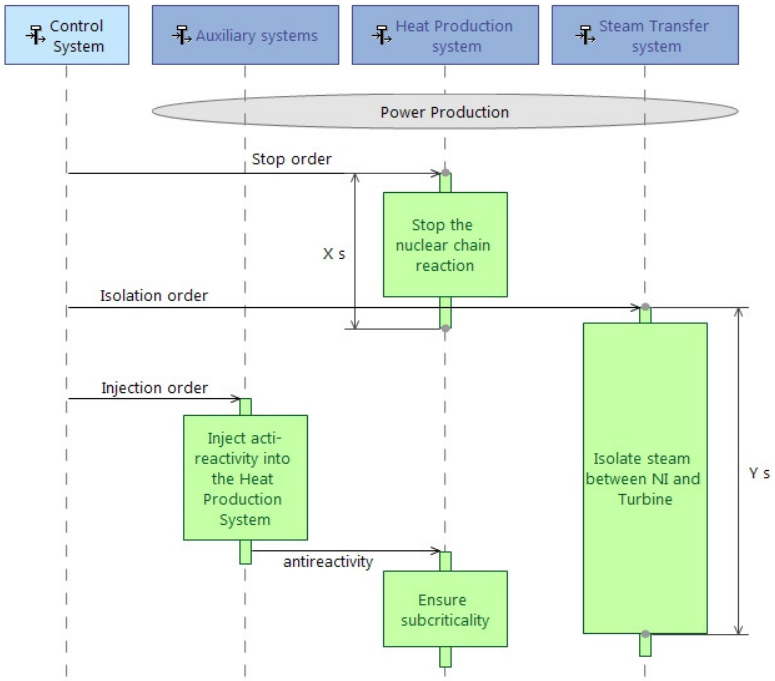

Figure 8. Extract of a dynamic scenario of an abnormal situation

Physical Analysis. The Nuclear Island system being a composition of systems at their turn composed of physical components like pumps and valves, the constraints introduced by the components that implement the functions defined before are rather left to be analyzed by the architecture teams of Nuclear Island subsystems. These constraints include the required independence of redundant fluid circuits and the required technology diversity for components, among others.

Exceptions may occur if the physical architecture of subsystems are known during Nuclear Island architecture design. Indeed, technical and economic considerations may lead to choose a previous design for a given subsystem. In such a case, the Logical Analysis may be extended to cover these constraints. For instance, the choice of an existing Safety Injection system may lead to streamline the number of internal functions of the Nuclear Island that are allocated to its Auxiliary Systems subsystem, since the capabilities of the mechanical components are already known.

Architectural tradeoffs. It is recommended to develop a set of architecture alternatives that shall be compared in order to choose the solution for the system’s architectural design problem that provides the higher added-value. The alternatives may come from using different reference PBS, different technologies for physical components implementations, different internal functions or different allocations of internal functions to subsystems.

First, e comparison criteria shall be defined as soon as possible, e.g. during the System Analysis step. It shall cover the safety and business goals of the Nuclear Island system. Criteria may comprise: Safety goals, including safety policies and performance of safety functions; Engineering costs and schedule; Procurement, Erection and Commissioning costs and schedule; Reuse policies, among others

Trade-off analysis may be driven manually using the Arcadia/Capella tool, e.g. identifying the impact that the changes on allocation of functions have over the dynamic scenarios, by evaluating the changes on the models. Architectures' trade-off analysis and evaluation can also be automated by formalizing and implementing them using Arcadia/Capella viewpoints. The major benefit of such approach is that the time between the launch of the evaluation and its results is drastically reduced, opening the possibility of agile trade-off analysis of architectural choices.

More generally speaking, the trade-offs between different functional and non-functional constraints is performed in two steps: the first step addresses a multi-viewpoint confrontation (including safety, product line, performance constraints and more) by engineering model analysis, in short loop. This allows testing each elementary architecture decision against all major viewpoints simultaneously, so that, for instance, a drag and drop of a component will instantaneously be identified as improving performance but introducing common failure modes and therefore degrading safety. The second step uses the engineering model to feed single viewpoint dedicated tools (such as dysfunctional simulation and as fault tree analysis), so as to secure the former design decisions by a more detailed, fine grained analysis. Both steps may use "rainy days" failure scenarios in order to analyze each architecture alternative behavior in this context. Detailing these aspects should be the subject of another paper.

Requirements Engineering. Several engineering tasks tightly intertwined to architecture definition were not addressed in this paper for space reasons. One of them is the system's functional and non-functional requirements engineering, which includes: requirements' elicitation and analysis, negotiation, early verification and validation, documentation and traceability, and management. Top-level requirements serve as the basis for the architecture analysis steps. Conversely, findings made during these steps and architectural choices initiate the creation, modification or removal of requirements. This tight relation between requirements and architectures has been modelled by the twin-peaks model [Nuseibeh 2001] for software development.

Managing complexity and detailed analysis. The Nuclear Island is a complex, "deep PBS" system. When the MBSE approach is applied to such a system, it does not address the very fine grain of detailed design, and therefore many decisions at this level may be challenged when going further in depth. Similarly, in IVV phases, this level of detail is not sufficient for analyzing flaws or integration problems and detailed system behavior. In order to extend the benefits of the MBSE approach, it shall be applied recursively to several levels of the system/subsystems decomposition, as promoted by Arcadia. This results in models with increasing level of detail applied on a more and more limited part of the system. In order to preserve consistency between these different models, automatic model transformation may be used.

Main findings on deploying the MBSE approach to nuclear systems engineering

The MBSE approach presented here and illustrated through the Nuclear Island system example has also been applied to other NPP systems at different stages of their engineering process. The approach has proven to be flexible enough to be tailored to different development cycles and to systems of different nature: fluid systems, simulation systems, and control and supervision systems.

Deploying a common approach to modeling architectures within a project or an organization eases the application of common rules and the analysis of common findings. The benefits of MBSE are being progressively assessed by engineering teams as deployment of the approach progresses, in

particular regarding the assessment of the benefits of a recursive application of the approach to lower level sub-systems and equipment. The following paragraphs detail the up to date findings.

Added value at each step of design. Each NPP system's architecture team, which is accountable of the architecture of each node in the NPP PBS, makes explicit the value added between the analysis of the needs (system analysis) and the produced high-level solution (logical analysis). Hence it is clearer to determine which architectural decisions are made at their level and which ones are cascaded to lower level PBS nodes architecture teams. This favors the definition of the best technical solutions, as it is done by the proper architecture teams at the proper PBS level.

States engineering. Each node in the NPP PBS's architecture team is encouraged to properly define its states, including normal operation and abnormal operation phases, in consistency with the states of the highest-level node, i.e. the NPP. This has a positive impact on achieving a clear definition of requirements from an upper level system to a lower level system: indeed, upper level systems do the spadework of lower-level ones which deal with simpler states and hence simpler requirements. For instance, higher PBS levels could deal with transverse and complex issues such as the dynamic related core reactivity in normal and abnormal conditions, while lower level PBS nodes such as injection systems would deal with simpler contexts such as the injection or isolation states.

Functional Chains. The breakdown of the NPP product into several PBS levels allow architecture teams to be accountable of the architecture of a defined scope, which is defined by the boundary of their system of interest. This breakdown also implies that multiple PBS nodes contribute to the achievement of high-level NPP functions. When PBS nodes architecture accountability is distributed among several teams / organizations, a cross-cutting concept is necessary to ease the integration of their respective contributions.

Functional Chains have proven useful on playing this role. By linking together lower level functions, they usefully compensate for silos emerging from the major interfaces imposed by the PBS. Furthermore, key Functional Chains may be used as the backbone for Integration, Verification, Validation and Qualification strategies at very high levels of the PBS.

Scenarios. Similarly, the modeling of scenarios is a powerful validation feature towards increasing robustness of the design across architects responsible for systems involved in scenarios which are transverse to them.

Return of experience and perspectives

Return of Experience. The benefits witnessed by the architecture teams regarding the engineering process include:

- A better communication and definition of responsibilities scopes between stakeholders – the architecture teams considered that the technical exchanges with transversal disciplines such as safety or human factors, and with other systems' and sub-systems architecture teams, were more productive when supported by common and normalized graphical representations provided by Arcadia/Capella: "a good sketch is better than a long speech". In particular, the justification of the architectures and the third-party validation of the architectural design tasks were positively impacted.
- A unique source of information about the system's architecture – the Arcadia/Capella models encapsulate all the critical information about the architecture being developed, becoming the reference database for architecture and easing information capitalization (e.g. extract of Interface Control Document tables). Furthermore, the consistency of architecture data is ensured by the automatic update of data and diagrams when modifications are performed.

- A fast learning curve – the Arcadia/Capella concepts and diagrams are rather well adapted to the nuclear engineering population, which is composed of engineers that have not been necessarily exposed to modelling approaches such as UML or SysML.

In order to take advantage of the benefits of the MBSE approach, some limitations shall be overcome and the necessary preconditions for success shall be ensured:

- The development of viewpoints that enable the evaluation of architectures shall be planned and performed long before its use. This is not always possible due to project-related constraints or because the evaluation criteria cannot be fully specified when starting architectural design. Hence, an enterprise-wide organization may be necessary to ensure that viewpoints are available for projects at the right moment.
- Further work shall be performed to clarify how the MBSE approach may be tailored to the architecture design of infrastructure systems such as buildings and ancillary structures. The architecture of such systems is strongly influenced by geographical constraints and space considerations. An integration with 3D model tools may be considered in these cases.

Perspectives. The following perspectives have been defined regarding the deployment of MBSE approaches in nuclear engineering:

- Viewpoints – involved architecture teams identified several viewpoints considered as relevant to be developed to support trade-offs, including viewpoints for safety analysis, for evaluating the performance of critical functional chains, for supporting the analysis of variabilities and the choice of architectural components.
- MBSE as an enabler for a better integration with other technical processes – the systems' architectural design being a key input for several other technical processes, the formalization of the architectural design brought by the MBSE approach could also benefit processes such as safety evaluation, human factors engineering, Integration, Verification, Validation & Qualification (IVVQ) and in-site integration of equipment and systems. An advanced integration level would also include integration between MBSE tools and specific tools such as simulators and 3D models.
- MBSE as an enabler for a better integration with project management – the integration of a MBSE tool as a component of a wider Product Life-cycle Management solution, could also benefit technical management processes such as configuration management in which project management also play a key role. Indeed, the NPP architecture progressively being refined by architecture teams could be used as the backbone of the digital enterprise, enabling for instance a quicker reaction to design changes by improving impact analysis, accelerating the integration into design of the operations and maintenance return of experience.

Conclusion

This paper presented the tailoring of an established MBSE method and tool so to ensure a positive impact on Nuclear Power Plants engineering task, and particularly during architectural definition and design. Benefits were witnessed both in supporting the technical production, by contributing to the exhaustiveness of design, safety justifications and third-party assessment; and in the daily interactions between engineering teams, by providing a common and normalized graphical representation, by introducing concepts that make teams work in a more collaborative and agile way. In order to guarantee these benefits, a tailoring of MBSE concepts and models shall be performed conjointly with future users, in order to cope with their discipline and project-specific constraints.

References

B. de la Bretesche, 2000, 'La méthode APTE : Analyse de la valeur, analyse fonctionnelle'.

Bonnet S, Voirin J-L, Exertier D, Normand V, 2017, 'Modeling system modes, states, configurations with Arcadia and Capella: method and tool perspectives', 27th Annual INCOSE International Symposium.
Bonnet S, Voirin J-L, Normand V , Exertier D, 2015, 'Implementing the MBSE Cultural Change: Organization, Coaching and Lessons Learned', 25th Annual INCOSE International Symposium.
Capella, 2017, Capella Polarsys Website : https://www.polarsys.org/capella/.
Elm J, Goldenson D, 2012, 'The Business Case for Systems Engineering Study: Results of the Systems Engineering Effectiveness Survey, CMU/SEI-2012-SR-009, Software Engineering Institute, Carnegie Mellon University.
Frey T, Valencia M, 2010, 'Enhancing Systems Engineering Agility with Modeling and Simulation', Johns Hopkins APL technical digest.
Honour E.C, 2013, 'Systems Engineering Return on Investment', PhD Thesis, Defence and Systems Institute School of Electrical and Information Engineering, University of South Australia.
IAEA, 2016, INTERNATIONAL ATOMIC ENERGY AGENCY, 'Safety of Nuclear Power Plants: Commissioning and Operation. Specific Safety Requirements', No. SSR-2/2 (Rev. 1).
IAEA, 2000, INTERNATIONAL ATOMIC ENERGY AGENCY, 'Safety Guide - Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants', No. NS-G-2.2.
INCOSE IWG, 2012, INCOSE Infrastructure Working Group, 'Guide for the Application of Systems Engineering in Large Infrastructure Projects'.
ISO/IEC/IEEE 15288, 2015, 'Systems and software engineering – System life cycle processes'.
ISO/IEC/IEEE 42010, 2011, 'Systems and software engineering – Architecture description'.
Nuseibeh, B, 2001, 'Weaving together requirements and architecture'. Computer, 34(3) pp. 115–119.
Voirin J-L, 2017, 'Model-based System and Architecture Engineering with the Arcadia Method', ISTE Press, London & Elsevier, Oxford, 2017
WNA, 2016, World Nuclear Association, 'World Nuclear Performance Report 2016'.

Biography

Juan Navas is a Systems Architect with 10 years' experience on performing and implementing Systems Engineering practices in industrial organizations. He has worked on the design and the procurement of instrumentation & control systems and simulation systems for petrochemical plants, nuclear fuel cycle plants and nuclear power plants. He has lead projects to improve software and systems engineering performance following Model-Based Systems Engineering approaches. He has supported several companies in aerospace, naval and nuclear energy sectors, on implementing best engineering and project management practices. He holds a PhD on embedded software computer science (Brest, France), a MSc Degree on control and computer science from MINES ParisTech (Paris, France) and Electronics and Electrical Engineering Degrees from Universidad de Los Andes (Bogota, Colombia).

Philippe Tannery is Transformation director in the I&C business unit of Framatome (ex-AREVA NP). He holds a Master's Degree in Sciences (mathematics, physics, chemistry) from the Ecole Polytechnique (Paris, France), a Master's Degree in Marine Engineering and Naval Architecture from MIT (Boston, USA), and a Master's Degree from ENSTA Paris Tech (Paris, France). He has worked on the maintenance and design of nuclear submarines and consulted in Engineering for several industries in the aerospace, automotive, offshore, oil&gas sectors. He has also facilitated R&T agreement signatures in the European Defence Agency. In AREVA NP, he has been deputy technical director for the development of twin nuclear reactors in China, and manager for Design performance improvement, contributing to the deployment of Systems Engineering and MBSE.

Stephane Bonnet is the Design Authority of the Thales MBSE workbench for systems, hardware and software architectural design. He holds a PhD in software engineering. He dedicates most of his time

to MBSE training and coaching activities worldwide, for Thales and other organizations. He helps systems engineering managers and systems architects implement MBSE approaches on operational projects. He is animating networks of experts from all Thales domains and business units to capture operational needs and orient the method and workbench evolutions and roadmaps.

Jean-Luc Voirin is Director, Engineering and Modeling, in Thales Defense Missions Systems business unit and Technical Directorate. He holds a MSc & Engineering Degree from ENST Bretagne, France. His fields of interests include architecture, computing and hardware design, algorithmic and software design on real-time image synthesis systems. He has been an architect of real-time and near real-time computing and mission systems on civil and mission aircraft and fighters. He is the principal author of the Arcadia method and an active contributor to the definition of methods and tools. He is involved in coaching activities across all Thales business units, in particular on flagship and critical projects.