RESEARCH REPORT

VTT-R-06743-17

Conformity assessment data model

Authors: Jarmo Alanen, Joonas Linnosmaa & Teemu Tommila

Confidentiality: Public

Report's title Conformity assessment data model	
Customer, contact person, address SAFIR2018 programme	**Order reference**
Project name Integrated safety assessment and justification of nuclear power plant automation	**Project number/Short name** 113347 / SAUNA
Author(s) Jarmo Alanen, Joonas Linnosmaa & Teemu Tommila	**Pages** 34
Keywords nuclear, instrumentation and control, systems engineering, qualification, safety demonstration	**Report identification code** VTT-R-06743-17

Summary

Conformity assessment of nuclear power plant systems, including qualification of subsystems and components is conventionally done based on a set of engineering and conformity assessment documents. Model-based systems engineering provides a more structured set of artefacts, not only for the design work, but also for the conformity assessment.

In this report we present a structured data model for the conformity assessment artefacts. The data model covers both the first party conformity assessment, traditionally known as verification and validation, as well as the third party conformity assessment, i.e. the attestation (qualification or certification). The data model is demonstrated in a Defence-in-Depth example of a spent fuel cooling control system. Before carrying out the demonstration, the claim hierarchy in accordance with the DiD requirements is discussed. The diversity requirement is selected for the example case.

Our demonstration verifies the applicability of our conformity assessment data model to a case that reflects a real case. The data model provides good traceability of artefacts ranging from the stakeholder domain to the organisation that designs the system and finally to the attestation organisation. With a proper tool, impact analysis can be carried out. Compared to traditional document based conformity assessment process, our data model has a good chance to be accepted by engineers if a good computer tool is available that hides the complexity of the data model and guides the users to put the engineering artefacts to correct locations and to establish the traces between the artefacts.

Confidentiality	Public

Tampere 20.12.2017

Written by	**Reviewed by**	**Accepted by**
Jarmo Alanen, Senior Scientist	Janne Valkonen, Senior Scientist	Johannes Hyrynen, Head of research area

VTT's contact address

Jarmo Alanen, PL 1300, FI-33101 Tampere; jarmo.alanen@vtt.fi, +358 40 501 5813

Distribution (customer and VTT)

SAFIR2018 program
VTT / archive, original

Preface

This report is a collection the blog posts written within the SAUNA project (Integrated safety assessment and justification of nuclear power plant automation) in the context of the SAFIR2018 programme (The Finnish Research Programme on Nuclear Power Plant Safety 2015–2018). The SAUNA project for year 2017 consisted of several tasks of which this report relates to Task 3.1 (Overall plant automation safety demonstration) of Work Package 3 (Safety demonstration practices). The goal of Task 3.1 was *"…to define a top-level framework for safety demonstration and assessment of I&C architecture.*" (An excerpt of the SAUNA 2017 project plan.)

The goal of this report is to document the created reference model and to provide the rationale for the design decisions.

Task 3.1 as well as the whole SAUNA project was steered by the Reference Group 1 (Automation, organisation and human factors). The authors thank the RG1, and especially Mauri Viitasalo (Teollisuuden Voima, TVO) for reviewing the report. We also thank Janne Valkonen (VTT) for performing the internal review of the report.

Tampere 31.12.2017
Authors

Contents

1. Introduction

This report is a collection the blog posts written within the SAUNA project (Integrated safety assessment and justification of nuclear power plant automation) of the SAFIR2018 programme (The Finnish Research Programme on Nuclear Power Plant Safety 2015–2018). This report collects the blog posts of Task 3.1 (Overall plant automation safety demonstration) of Work Package 3 (Safety demonstration practices).

Each blog post is a document item of its own. It means that each post has its own list of references where relevant, and each post has its internal numbering of figures and tables. In the following, however, joint lists of acronyms and definitions are provided.

Table 1. Abbreviations.

Abbreviation	Description
ConOps	Concept of Operations
DiD	Defence-in-Depth
I&C	Instrumentation and Control
IAEA	International Atomic Energy Association
NPP	Nuclear Power Plant
SE	Systems Engineering
SIL	Safety Integrity Level
STUK	Säteilyturvakeskus (Radiation and Nuclear Safety Authority)
V&V	Verification and Validation

Table 2. Key concepts.

Definition	Description
Artefact	A synonym to *Work product*
Attestation	Issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated [source: ISO 17000:2004] NOTE: In this report, attestation is considered to include the review activity (which we call assessment), although in case of certification at component level, the attestation may be independent of the review. Furthermore, the activities to prepare for the approval are included in the set of attestation activities.
Assurance case	Reasoned, auditable artefact created that supports the contention that its top-level claim (or set of claims), is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claims(s) NOTE 1: An assurance case contains the following and their relationships: • one or more claims about properties • arguments that logically link the evidence and any assumptions to the claims(s) • a body of evidence and possibly assumptions supporting these arguments for the claim(s)

Definition	Description
	• justification of the choice of top-level claim and the method of reasoning. [source: ISO/IEC 15026-1 2013] A collection of auditable claims, arguments, and evidence created to support the contention that a defined system/service will satisfy its assurance requirements. [source: Structured Assurance Case Metamodel (SACM) Version 2.0 (December 2015 draft)]
Certification	Third-party attestation related to products, processes, systems or persons [source: ISO 17000:2004]
Conformity assessment	Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled [source: IEC Glossary]
Determination	Activity to find out one or more characteristics and their characteristic values [source: ISO 9000:2015]
Model based systems engineering	Model based systems engineering (MBSE) is the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases. [Source: INCOSE Systems Engineering Vision 2020, INCOSE-TP-2004-004-02, September, 2007]
Process	Set of interrelated or interacting activities that transforms inputs into outputs. NOTE: In a broad sense, a process can be a system process or a systems engineering process. In the former case, the system-of-interest transforms its inputs to outputs (like sensor values to actuator actions); in the latter case, the organisation and tools that develop the system-of-interest transform input artefacts to output artefacts (like requirements specifications to architectural design). If there is a possibility to confuse with these two point of views, it is suggested to use phrases ‘system process’ and ‘SE process’ respectively. [source: ISO/IEC/IEEE 15288 2015, except the note, which is by the authors of this report]
Qualification	1. Qualification shall refer to a process to demonstrate the ability to fulfil specified requirements (corresponds to the qualification process of the ISO 9000 standard). [Source YVL Glossary by STUK] [ISO 9000:2015 does not define the term qualification (process) any more] 2. Process of determining whether a system or component is suitable for operational use. • Qualification is generally performed in the context of a specific set of qualification requirements for the specific facility and class of system and for the specific application. • Qualification may be accomplished in stages: e.g., first, by the qualification of pre-existing equipment (usually early in the system realization process), then, in a second step, by the qualification of the integrated system (i.e. in the final realized design).

Definition	Description
	• Qualification may rely on activities performed outside the framework of a specific facility design (this is called 'generic qualification' or 'prequalification'). • Prequalification may significantly reduce the necessary effort in facility specific qualification; however, the application specific qualification requirements must still be met and be shown to be met. **Equipment qualification**. Generation and maintenance of evidence to ensure that equipment will operate on demand, under specified service conditions, to meet system performance requirements. See IAEA GSR Part 4 (Rev. 1). • More specific terms are used for particular equipment or particular conditions; for example, seismic qualification is a form of equipment qualification that relates to conditions that could be encountered in the event of earthquakes. • The proof that an item of equipment can perform its function, which is an important part of equipment qualification, is sometimes termed substantiation. [Source IAEA Safety glossary] NOTE 1: In this report, we consider that *qualification* is an *attestation* activity required by an authority (internal or external), and we emphasise the distinction between *validation* and *qualification* by considering that the qualification process is assumed to only consist of the additional activities after the V&V activities in high rigour projects to attest the V&V results. We see this distinction important and commendable to provide for well capsulated qualification and V&V processes. NOTE 2: In some contexts, *licensing* is used as a synonym for *qualification*; in other cases, the term licensing is only used for plant level authorisation. Due to the vague usage of the term licensing, we do not define nor use the term licensing in this report.
Safety demonstration	The set of arguments and evidence elements which support a selected set of claims on the safety of the operation of a system important to safety used in a given plant environment. [source: Common position 2014] NOTE 1: When safety demonstration is presented in a structured fashion it can be called a safety related *assurance case* [source: Valkonen et al. 2016] NOTE 2: In some contexts, *safety demonstration* is treated as an activity; here we treat it as an artefact according to Common position (2014); *qualification* is the activity that assembles the safety demonstration.
System	Combination of interacting elements organized to achieve one or more stated purposes NOTE 1: A system is sometimes considered as a product or as the services it provides. NOTE 2: In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g., aircraft system. Alternatively, the word 'system' is substituted simply by a context-

Definition	Description
	dependent synonym, e.g., aircraft, though this potentially obscures a system principles perspective. NOTE 3: A complete system includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services, and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment. [source: ISO/IEC/IEEE 15288 2015]
Systems engineering	Interdisciplinary approach governing the total technical and managerial effort required to transform a set of stakeholder needs, expectations, and constraints into a solution and to support that solution throughout its life cycle [source: ISO/IEC/IEEE 15288 2015] Interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem: operations, cost and schedule, performance, training and support, test, manufacturing, and disposal. SE considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs. [source: INCOSE 2015]
Validation	Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled NOTE 1: The objective evidence needed for a validation is the result of a test or other form of determination such as performing alternative calculations or reviewing documents. NOTE 2: The word “validated” is used to designate the corresponding status. NOTE 3: The use conditions for validation can be real or simulated. [source: SFS-EN ISO 9000:2015] NOTE 4: In this report, we state that validation is carried out to assess conformity to the stakeholder requirements whereas verification is carried out to assess conformity to the system requirements.
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled NOTE 1: The objective evidence needed for a verification can be the result of an inspection or of other forms of determination such as performing alternative calculations or reviewing documents. NOTE 2: The activities carried out for verification are sometimes called a qualification process. NOTE 3: The word “verified” is used to designate the corresponding status. [source: SFS-EN ISO 9000:2015] NOTE 4: In this report, we state that verification is carried out to assess conformity to the system requirements whereas validation is carried out to assess conformity to the stakeholder requirements.

Definition	Description
Work product	An artefact associated with the execution of a process. There are four generic work product categories: services (e.g. operation); software (e.g. computer program, documents, information, contents); hardware (e.g. computer, device); processed materials. [source: ISO/IEC TR 24774 2010]

2. The blog posts

The SAUNA project provided a project internal blog platform to publish blog posts along the course of work to immediately report the thoughts and findings of the researchers. In Task 3.1 of the SAUNA project, it was planned from the beginning that the set of blog posts would constitute the final deliverable. This decision was done due to the fact that a traditional research report would take too big a portion of the low budget of the task.

In the following, the SAUNA project Task 3.1 blog posts are reproduced (with some formatting and spelling error corrections, as well as corrections according to the results of the report review) in the order from oldest to latest. The blog has been SAUNA project internal.

Task 3.1 scope and goals

We want to develop methods for the assessment of I&C architecture and its DiD-related properties (relevant for nuclear safety). The goal is to go towards model-based methods and tools. We focus on I&C but from a multidisciplinary viewpoint.

To do this, we intend to proceed from an outline of the concept of overall safety to the topics of system-level safety assessment and demonstration of I&C and then to focus in particular on Defence-in-Depth and diversity (D3). Key ideas would be demonstrated with a practical example. This represents a clear synergy between tasks T1.1 and T3.1, to be pursued at least on the conceptual level if finding a common example turns out to be too difficult.

The original objective of the Task 3.1 was as follows: "*The objective of T3.1 is to define a top-level framework for safety demonstration and assessment of I&C architecture. The relevant (DiD) requirements are captured from regulations and standards (e.g. EPRI 2014) and organised as a set (pattern) of claims and assessment criteria following the principles of structured assurance cases (ISO 15026). The main purpose is to develop an approach to determine the quality of architectural specifications, with particular attention devoted to safety and DiD capabilities (from task T1.1), such that the architectural specifications and their assessment artefacts are traced to other artefacts from plant and safety engineering, I&C design and qualification.*"

On the concept of overall safety

Safety is an emergent property. So, all parts of a (sociotechnical system) must work together (communicate, collaborate, coordinate).

Overall safety covers different engineering disciplines and types of hazards (nuclear, occupational, environmental, physical, security, etc.).

To be safe, an I&C system must:

- not take itself from the intended states (operation, standby, maintenance, etc.) into unwanted hazardous situations (careful design, reliability)
- monitor and anticipate its state (situation awareness) and to react proactively
- prevent hazardous events or mitigate their consequences if they occur (robustness, error-tolerance)
- move to a safe state
- recover normal operation
- learn from the experiences.

Reliability and robustness are not enough, but a system should have the capability of survive also unexpected and even extreme situations (resilience).

I&C is an essential part of the plant-level safety architecture, in which the Defence-in-Depth (DiD) principles are the main guideline for designers. Therefore, I&C must serve the plant's safety goals and fundamental safety functions by collaborating with other plant systems and human operators. In addition, DiD principles must be applied in the design and implementation of the I&C itself. This latter requirement is in the focus of our research.

On the claim hierarchy

As we have here a complex socio-technical system, we need to use an integrated approach in its assessment and safety demonstration. To do that, we must decompose the top-level claim "*The I&C architecture is safe*" in to a hierarchy of lower-level claims and assessment topics. This can be done in different ways depending on the application. Here are some possible decomposition strategies:

- distinction between the system and its development process:
    - the specification of the I&C architecture is adequate;
    - the development practices and organisations are adequate.
- compliance to regulatory requirements and expectations:
    - relevant regulations and standards have been used;
    - they have been correctly interpreted in architectural and process requirements;
    - all requirements are appropriately satisfied by the specification and implementation;
    - looking at the time dimension:
        - the plant I&C is safe when it is taken into use;
        - the plan I&C will remain safe in operation, maintenance and modifications.
    - management of threats:
        - all threats and mechanisms have been identified;
        - all threats have been properly managed by safety provisions.

These decompositions need to be combined and further refined according to the needs of the customer and features of the application. Let's first discuss the adequacy of the I&C architecture and its development process. DiD will be considered in later posts. Supposing that we are talking about a new-build or upgrade that is more or less ready for start-up, we might come to the following claim hierarchies:

- the I&C architecture is adequate (product assessment):
    - the specified Concept of Operations (ConOps) is appropriate for safe plant operation;
    - the I&C architectural requirements have been correctly defined;
    - the functional architecture is adequate;
    - the physical architecture is adequate;
    - suitable components, products and technologies have been selected;
    - the details of the I&C systems have been correctly designed and implemented;
    - etc.
- the development practices and organisations are adequate (process assessment):
    - the goals and scope of the work are appropriate;
    - relevant stakeholders and disciplines have been properly involved;
    - design and quality assurance methods are appropriate;
    - documentation is appropriate;
    - tools are adequate;
    - project management is well performed;
    - etc.

These topics need also to be further divided. For example human and organisational factors can be found as subtopics in the Concept of Operations and in functional and physical I&C architectures, as well as in the process assessment (e.g. as questions about user participation and HFE programme). In addition, DiD and diversity are aspects embedded in several topics in the list above.

On I&C architecture

I&C is understood here rather technically, i.e. including control equipment, software and tools located in process areas, equipment rooms and control rooms. However, interfaces to human users, process systems, electrical systems, operational environment and information systems are part of the picture, as well as procedures related to I&C operation and maintenance.

"Architecture" describes how elements of a whole are arranged and connected. It is a high-level view to the whole system. We understand "system" as a whole consisting of real-world entities, like equipment, software with data and people. An engineered system has a purpose, typically to perform or participate in an activity (or process).

According to a general SE principle, requirements come first, then functions and finally their physical implementation (the "system"). This happens, however, in an iterative, basically top-down fashion. Requirements and functions cannot be explicated without initial assumptions (concepts) of the system. Requirements are assigned to functions and system elements, and functions are allocated to system elements. In particular, we understand functions as capabilities of the system or its elements.

Thereby, we have a functional and a physical architecture (view). The functional architecture describes major system functions and data elements and the ways in which they interact. In the physical architecture we can see the decomposition to the system to system elements (devices and software components), their physical connections and the placement of the elements in the operational environment.

Concerning the terminology, we use the expression *I&C architecture* for all I&C systems and their functions in a plant, while *I&C system architecture* refers to the organisation of items in one I&C system (see IEC). The term *I&C function* can be used in functional requirements (e.g. by process engineers) and functional specifications.

On Defence-in-Depth

The core of DiD is in a series of consecutive defence lines against various threats. If one *defence line* fails, the next one takes over. *Physical DiD* is used to prevent propagation of harmful effects (e.g. radioactive material) with physical barriers. The purpose of *functional DiD* is to protect the barriers and to handle various plant conditions ranging from normal operation to severe accidents. These conditions are typically categorised into five *DiD levels* according to their severity and probability of occurrence.

I&C systems, such as operational automation, reactor protection system (RPS) and control room systems, typically serve one or more DiD levels. In order to avoid common cause and consequential failures, defence lines should be as independent as possible. The methods applied include *redundancy*, *functional isolation*, *physical separation* and *diversity*. This is, however, not fully possible in practice. For example, field devices must be shared and information transferred between redundancies and DiD levels.

DiD is about providing defences against various threats. Therefore, one strategy to assess the DiD capabilities of the I&C (system) architecture is to use one of the general strategies above and to make a distinction between internal and external threats (with respect to some agreed I&C system boundary) and their types/sources (see IAEA). Other options include, for example, assessment against regulations and standards and evaluation of specific DiD properties, such as diversity. So, the assessment or safety demonstration of I&C architecture and its DiD solutions could be based, e.g., on the following claims:

- external threats (to I&C) have been identified and managed:
    - threats used as design basis are adequate;
    - I&C is properly protected against fires, floods, etc.;
    - physical and cyber security is appropriate;
    - etc.
- internal threats have been identified and managed;
- regulatory requirements for I&C architecture and DiD have been fulfilled;

- DiD properties are adequate:
    - the functional and physical dependencies are not significant;
    - diversity has been applied sufficiently and in a proper way;
    - Common Cause Failures have been properly considered;
    - etc.
- appropriate methods and resources have been used.

Assessment of control systems

In this context, we want to assess I&C architecture and systems of a nuclear power plant, especially in regards to Defence-in-Depth properties. What does assessment mean? An excerpt from the IEC 60169-1 (2016) provides an insight into this (boldfacing by the authors of this document).

"***Assessment of a system is the judgement, based on evidence, of the suitability of the system for a specific mission or class of missions***.

To obtain total evidence would require complete evaluation (for example under all influencing factors) of all system properties relevant to the specific mission or class of missions.

Since this is rarely practical, the rationale on which an assessment of a system should be based is:

– the identification of the importance of each of the relevant system properties;

– the planning for evaluation of the relevant system properties with a cost-effective dedication of effort to the various system properties.

In conducting an assessment of a system, it is crucial to bear in mind the need to gain a maximum increase in confidence in the suitability of a system within practical cost and time constraints.

An assessment can only be carried out if a mission has been stated (or given), or if any mission can be hypothesized. *In the absence of a mission, no assessment can be made; however, examination of the system to gather and organize data for a later assessment done by others is possible. In such cases, the standard can be used as a guide for planning an evaluation and it provides methods for performing evaluations, since evaluations are an integral part of assessment.*

In preparing the assessment, it can be discovered that the definition of the system is too narrow. For example, a facility with two or more revisions of the control systems sharing resources, e.g., a network, should consider issues of co-existence and inter-operability. In this case, the system to be investigated should not be limited to the "new" BCS [Basic Control System]; it should include both. That is, it should change the boundaries of the system to include enough of the other system to address these concerns."

In the above text, influencing factors mean factors such as installation environment and environmental conditions. They determine the probability of unsuccessful mission.

Note that IEC 61069 is not targeted to safety functions: "*Where the BCS risk reduction is intended to be less than 10 (i.e. SIL < 1, per IEC 61508-4), then assessment comes under IEC*

61069. A BCS with a safety integrity level (SIL) or performing any safety instrumented function (SIF) is not covered by IEC 61069, where SIL is defined by IEC 61508-4 and SIF is defined by IEC 61511-1." Nevertheless, we might learn something from the IEC 61069 in defining the I&C architecture and systems assessment process. But let us first take a look at the conformity assessment process model by ISO/IEC 17000 (2004).

ISO/IEC 17000 (2004) defines the assessment process as depicted below (the Review and attest activity elaborated by the authors of this document).

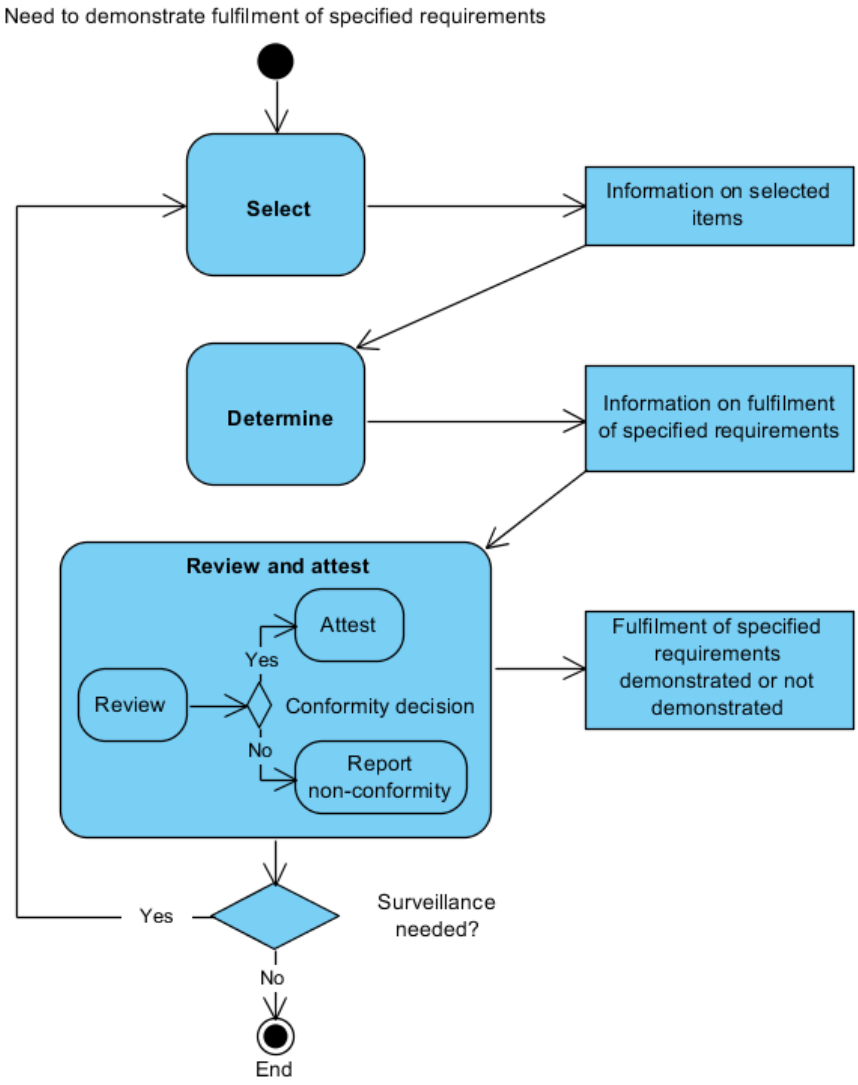

Figure 1. Conformity assessment process according to ISO/IEC 17000.

The process works for three parties, the first party, the second party and the third party. See Figure 2 below.

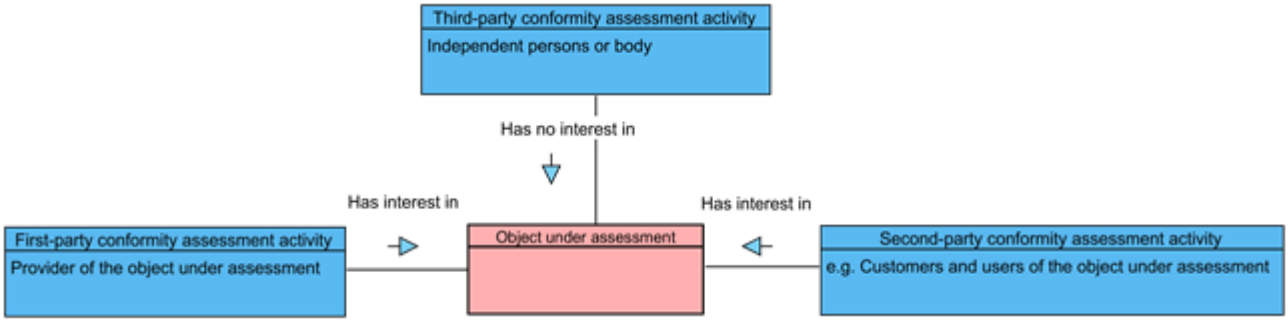

Figure 2. Conformity assessment parties.

The process model of ISO/IEC 17000 in Figure 1 is similar to the conformity assessment model by Alanen & Tommila (2016) with the difference that we call the third party conformity assessment activity attestation. We will apply the concepts and terminology of ISO/IEC 17000 in our conformity assessment data model presented in later posts.

References

Alanen, J. and Tommila, Teemu, T. 2016. A reference model for the NPP I&C qualification process and safety demonstration data Research Report: VTT-R-00478-16. VTT, 43 p. + app. 21 p.

IEC 61069-1. 2016. Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 1: Terminology and basic concepts. International Electrotechnical Commission (IEC), 90 p.

ISO/IEC 17000. 2004. Conformity assessment - Vocabulary and general principles. International Organization for Standardization (ISO) and International Organization for Standardization, 47 p.

Conformity assessment activities within the systems engineering processes

In our report (Alanen & Tommila 2016), we defined the systems engineering core loop and its data model. Now, we want to develop the data model by Alanen & Tommila (2016, Figure 15) by the artefacts that are needed and produced by the third-party conformity assessment activities, i.e. attestation activities. To do that we first create an overall activity model, which we here call the SE 8.0 model. The 'eight' part is depicted in Figure 1 and the 'zero' part in Figure 2.

The overall systems engineering core loops are redrawn below in Figure 1 to contain two loops, the design iteration loop and the first-party conformity assessment loop (see what the terms first-party and third-party mean in the blog post Assessment of control systems.

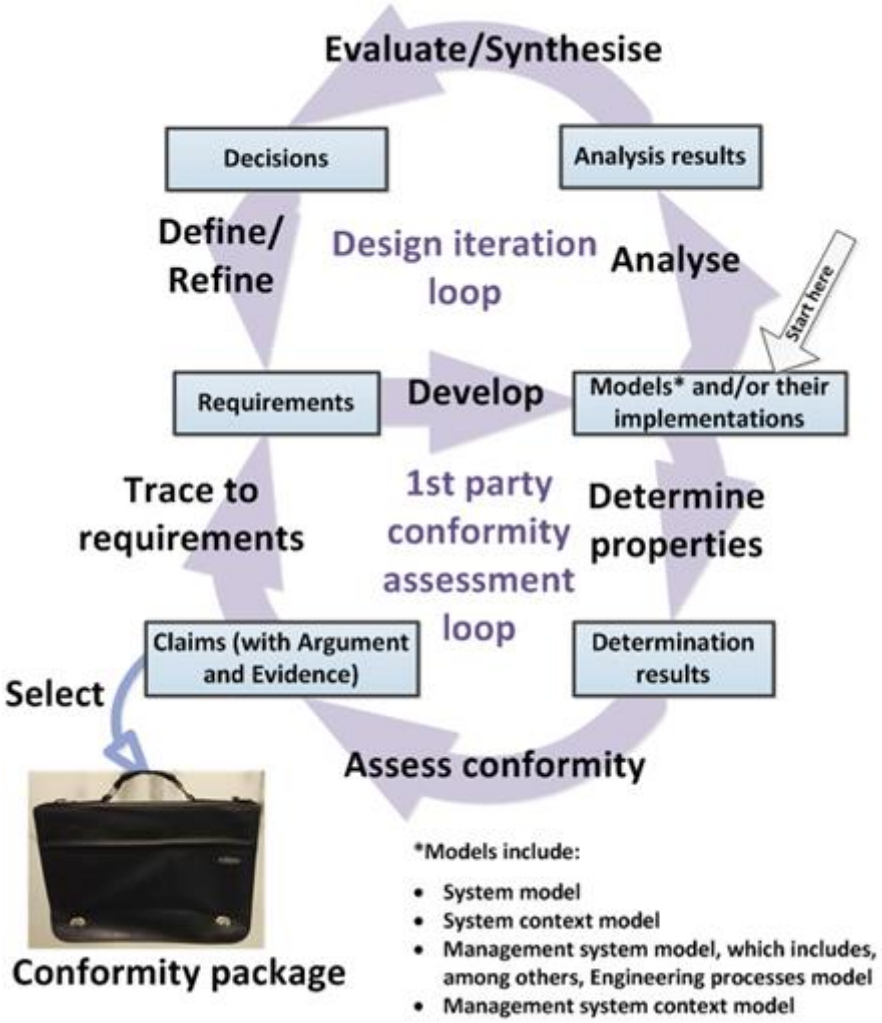

Figure 1. Systems engineering core loops; the 'eight' part of the SE 8.0 model.

The design iteration loop starts from very initial concept models of the system-of-interest. Thereafter the requirement capture can start. Based on the requirements the system model is developed and analysed. The set of requirements is updated based on the analysis results. After the system model has reached a maturity such that the designers believe that it satisfies a certain set of requirements, it is time to run the 1st party conformity assessment loop. The loop is started by determining the actual properties of the system-of-interest. Determination may involve testing, analysis, demonstration, etc. activities. Based on the determination results, conformity to the requirements is claimed. Note that the conformity assessment loop works both for verification and validation; in case of verification, conformity to system requirements is assessed, whereas in case of validation, conformity to stakeholder requirements is assessed.

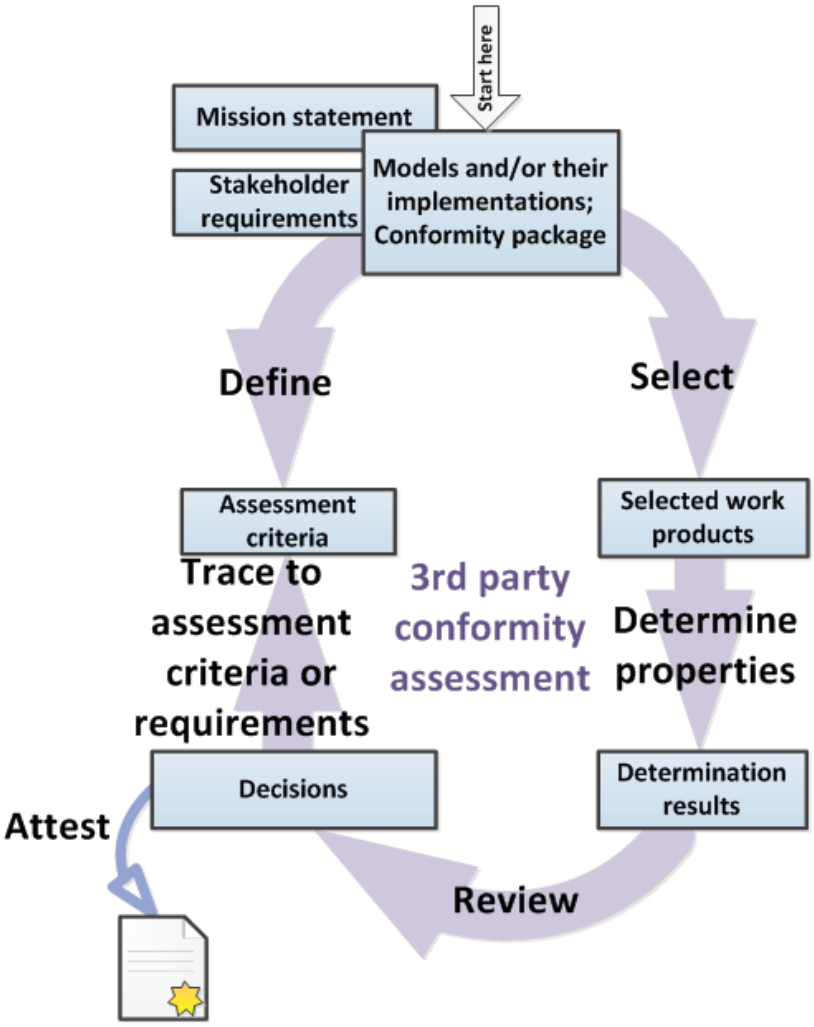

Figure 2. The third-party conformity assessment activities, the 'zero' part of the SE 8.0 model.

The attestation loop (i.e. the 3rd party conformity assessment loop) starts by selecting the work products and their conformity assessment artefacts to be assessed. The properties of the work products and especially the conformity assessment artefacts are determined. Based on the determination results, the attestor makes a decision about the adequacy of the conformity assessment artefacts based on the assessment criteria.

Note the following: In Figure 1, the assessor writes **claims** about the conformity to the requirements, whereas in Figure 2 the assessor (i.e. the attestor) writes **decisions** about the conformity to the requirements. This means that the main duty of the third-party assessor is to assess the trustworthiness of the first-party claims. The third-party assessor (the attestor) may, however, define additional determination cases to assess the actual properties of the object under assessment. Note also that the assessment criteria has to be based on the stakeholder requirements of the object under assessment; if that is not the case, the third-party is setting new stakeholder requirements that were not available for the provider of the object under assessment during the development and implementation activities. It is also possible to use the stakeholder requirements as the assessment criteria as such, e.g. "Requirement REQ-1234: [Requirement text] is satisfied." In fact, this is what the first party has to do when writing the claims about the conformity, because the supplier of the object under assessment shall validate the object against each stakeholder requirement.

The new artefacts, Mission statement, Decisions and Assessment criteria, introduced in Figure 2 will be added to our data model presented in (Alanen & Tommila 2016, Figure 15).

References

Alanen, J. and Tommila, Teemu, T. 2016. A reference model for the NPP I&C qualification process and safety demonstration data Research Report: VTT-R-00478-16. VTT, 43 p. + app. 21 p.

Claim hierarchy derived from YVL B.1

YVL B.1 (2013) states that the safety design of a nuclear power plant shall base on the Defence-in-Depth principle. This also requires the overall I&C architecture to follow the principles of Defence-in-Depth. The purpose of this text is to define a set of higher-level claims that are used as a baseline for assuring relevant parties that the Defence-in-Depth principle has been followed. In this context, we assume that a claim argues that a certain requirement is adequately followed and fulfilled. To define a set higher level claims we need a set of higher-level requirements which these claims would state to fulfil. In the following, we try to capture the essence of the Defence-in-Depth principle requirements for nuclear domain. Our goal was to capture the relevant DiD requirements from regulations and standards. As a starting point, for nuclear DiD requirements, we decided to follow the Finnish YVL guides, especially B.1. Furthermore, we captured some additional requirements from the common position paper DICWG-09 (2015) by Multinational Design Evaluation Programme. The requirements are outlined in the following:

Defence-in-Depth requirements from YVL B.1 & E.7

- Safety is based on five successive (redundant) levels of defence of equipment and procedures.
- Levels perform the three fundamental safety functions (control of reactivity, heat removal from the fuel and confinement of radioactive materials).
- Levels 1 and 2 prevent accidents whereas the remaining levels protect the plant, its operators and the environment from the adverse effects of accidents.
- These levels are independent from each other as is reasonably achievable.
- Independence of different Defence-in-Depth levels includes diversity, physical separation and functional isolation as is reasonably achievable.
- Systems and components used at different levels of defence shall be separated from one another by distance or protective structure, if there is an obvious possibility for consequential failures.
- The adequacy of the achieved independence shall be justified.
- A loss of single level of defence may not impair the operation of the other levels of defence.
- No single functional malfunction or failure should propagate between different levels of DiD.
- Functional isolation also covers electrical isolation and isolation of the processing of information between systems.
- Each of the levels are individually strong.

- Carefully researched, tested and proven high-quality technology shall be employed in the levels of Defence-in-Depth.
- Strength of individual levels of defence is ensured with redundancy and diversity.
- Redundant systems ensures the performing of required safety function even if any of them is rendered inoperable.
- Diversity gives defence against common cause failures by systems having different operating principles or differing from each other in some other manner.
- Consideration shall be given to potential technological developments.
- The possibility of common cause failures due to human error shall be reduced by applying a functional Defence-in-Depth principle.
- Operational preconditions of the personnel are ensured with efficient technical and administrative arrangements.

Defence-in-Depth requirements from DICWG-09

- Measures to maintain the required independence.
- Avoid unnecessary complexity and interactions, but still fully implement its safety requirements.
- Amenable to sufficient analysis or verification to facilitate an adequate safety demonstration.

The requirements from YVL B.1 are further evaluated to create a hierarchy of the requirements. See Figure 1 below. The main area in defining the hierarchy was to use the table-of-contents structure of YVL B.1. This means in practise that some of the headings need to be converted into requirements, e.g. the YVL B.1 section 4.3.2 heading: 'Strength of individual levels of defence in depth' is converted to a requirement: 'The licensee has to demonstrate the strength of individual levels of defence in depth.'

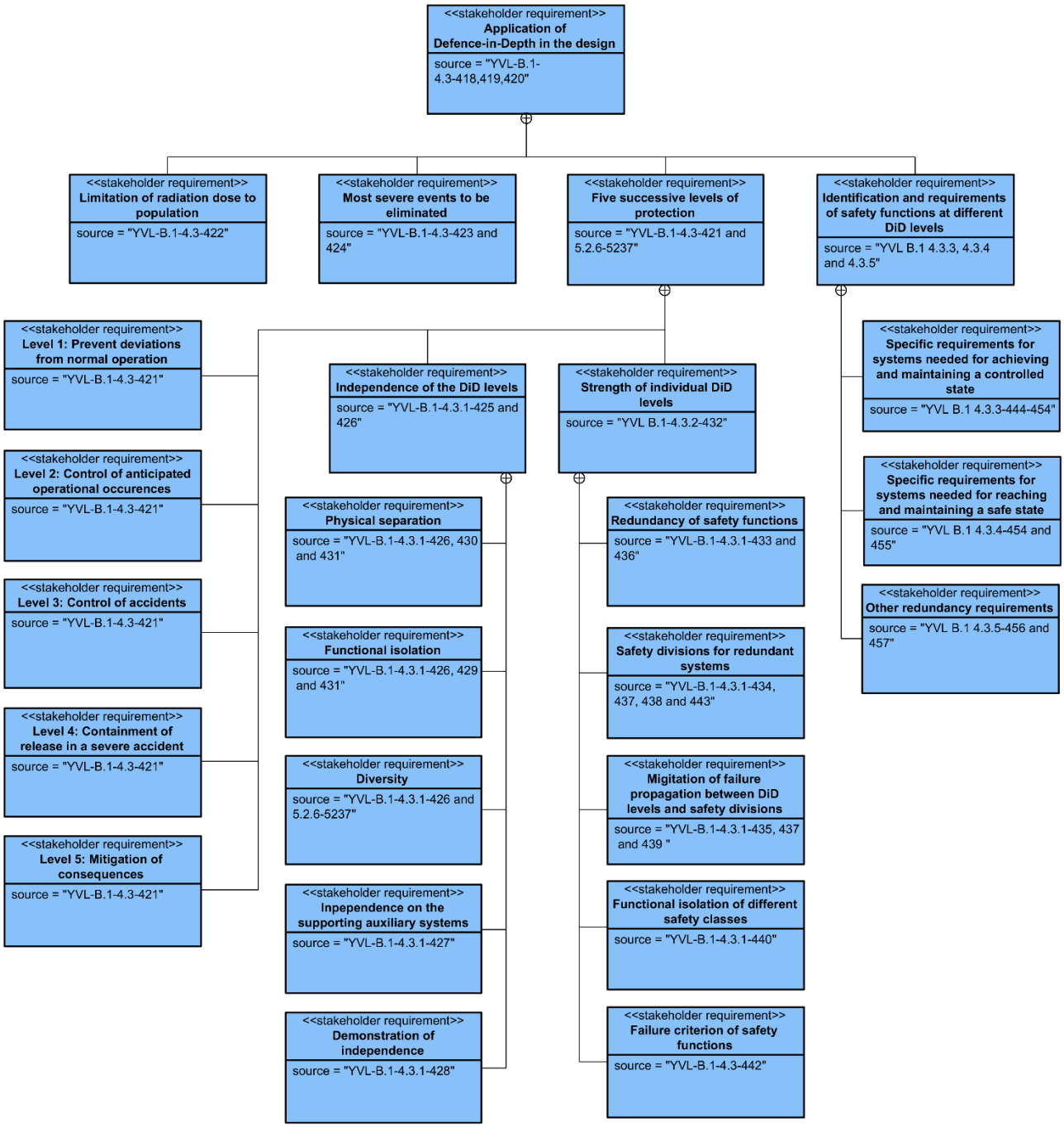

Figure 1. Hierarchy of DiD requirements derived from YVL B.1

This hierarchy can be directly used as the claim hierarchy in the conformity assessment process. Such approach is rather straightforward as long as there is only one standard against which the conformity assessment is done; if there are several standards from which the requirements are captured, the table-of-contents hierarchy cannot be utilised, because the different standards most probably do not follow the same table-of-contents hierarchy. Hence the system developer has to himself develop the requirements hierarchy for the requirements of a requirements category (such as DiD requirements) or at least finally create the claim hierarchy for the particular category.

Despite the fact that in this task we only elaborate the YVL B.1 requirements, the DiD requirements collected from EPRI [2014] are listed in Table 1.

Table 1. DiD requirements collected by EPRI [2014].

Rec Num	Source Document	Clause	Requirement/Guideline
E-183	IAEA NS-G-1.3, I&C Systems Important to Safety in NPPs, 2002	6,53	HUMAN-MACHINE INTERFACE MONITORING OF ACCIDENT CONDITIONS 6.53. Equipment for monitoring accident conditions should be capable of operating in the post-accident environment at the time of need and for the necessary period of time. The ranges of measurement of selected key parameters should extend to values that may be reached in events that could challenge barriers to the release of radioactive materials from the fuel, heat transport system or containment, or could result in the release of radioactive materials from one or more of these barriers.
E-209	IAEA SSR-2/1, Safety of NPPs: Design, Specific Safety Requirements, 2012	2,13	APPLYING THE SAFETY PRINCIPLES AND CONCEPTS THE CONCEPT OF DEFENCE IN DEPTH 2.13 There are five levels of defence: The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety. This leads to requirements that the plant be soundly and conservatively sited, designed, constructed, maintained and operated in accordance with the quality management and appropriate and proven engineering practices. To meet these objectives, careful attention is paid to the selection of appropriate design codes and materials, and to the quality control of the manufacture of components and construction of the plant, as well as to its commissioning. Design options that reduce the potential for internal hazards contribute to the prevention of accidents at this level of defence. Attention is also paid to the processes and procedures involved in design, manufacture, construction and in-service inspection, maintenance and testing, to the ease of access for these activities, and to the way the plant is operated and to how operating experience is utilized. This process is supported by a detailed analysis that determines the requirements for operation and maintenance of the plant and the requirements for quality management for operational and maintenance practices. The purpose of the second level of defence is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions. This is in recognition of the fact that postulated initiating events are likely to occur over the operating lifetime of a nuclear power plant, despite the care taken to prevent them. This second level of defence necessitates the provision of specific systems and features in the design, the confirmation of their effectiveness through safety analysis, and the establishment of operating procedures to prevent such initiating events, or else to minimize their consequences, and to return the plant to a safe state. For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or postulated initiating events might not be controlled at a preceding level and that an accident could develop. In the design of the plant, such accidents are postulated to occur. This leads to the requirement that inherent and/or engineered safety features, safety systems and procedures be provided that are capable of preventing damage to the reactor core or significant off-site releases and returning the plant to a safe state. The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth. The most important objective for this level is to

			ensure the confinement function, thus ensuring that radioactive releases are kept as low as reasonably achievable. The purpose of the fifth and final level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accident conditions. This requires the provision of an adequately equipped emergency control centre and emergency plans and emergency procedures for on-site and off-site emergency response.
E-211	IAEA SSR-2/1, Safety of NPPs: Design, Specific Safety Requirements, 2012	4,8	PRINCIPAL TECHNICAL REQUIREMENTS 4.8 Requirement 7: Application of defence in depth The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable.
F-054	IAEA SSR-2/1, Safety of NPPs: Design, Specific Safety Requirements, 2012	Req. 7	Requirement 7: Application of defence in depth The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable.
E-057	IEC 61513-2011, NPPs – I&C important to safety – General requirements for systems	3,14	3.14 Defence-in-Depth - The application of more than one protective measure for a given safety objective, such that the objective is achieved even if one of the protective measures fails.
U-142	NRC 10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events	c (1)	Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system.
U-143	NRC 10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events	c (2)	Each pressurized water reactor manufactured by Combustion Engineering or by Babcock and Wilcox must have a diverse scram system from the sensor output to interruption of power to the control rods. This scram system must be designed to perform its function in a reliable manner and be independent from the existing reactor trip system (from sensor output to interruption of power to the control rods).
U-144	NRC 10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events	c (3)	Each boiling water reactor must have an alternate rod injection (ARI) system that is diverse (from the reactor trip system) from sensor output to the final actuation device. The ARI system must have redundant scram air header exhaust valves. The ARI must be designed to perform its function in a reliable manner and be independent (from the existing reactor trip system) from sensor output to the final actuation device.
U-145	NRC 10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events	c (4)	Each boiling water reactor must have a standby liquid control system (SLCS) with the capability of injecting into the reactor pressure vessel a borated water solution at such a flow rate, level of boron concentration and boron-10 isotope enrichment, and accounting for reactor pressure vessel volume, that the resulting reactivity control is at least equivalent to that resulting from injection of 86 gallons per minute of 13 weight percent sodium pentaborate decahydrate solution at the natural boron-10 isotope abundance into a 251-inch inside diameter reactor pressure vessel for a given core design. The SLCS and its injection location must be designed to perform its function in a reliable manner. The SLCS initiation must be automatic

			and must be designed to perform its function in a reliable manner for plants granted a construction permit after July 26, 1984, and for plants granted a construction permit prior to July 26, 1984, that have already been designed and built to include this feature.
U-146	NRC 10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events	c (5)	Each boiling water reactor must have equipment to trip the reactor coolant recirculating pumps automatically under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner.
U-211	NUREG-0800, Chapter 7, Branch Technical Position (BTP) 7-17, Guidance on SelfTest and Surveillance Test Provisions	1,1	Echelons of Defense: The NRC staff identified four echelons of defense in NUREG/CR-6303: • Control System - The control system echelon usually consists of equipment that is not safety-related that is used in the normal operation of a NPP and routinely prevents operations in unsafe regimes of NPP operations. • Reactor Trip System - The RTS echelon consists of safety-related equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion. • Engineered Safety Features - The ESF echelon consists of safetyrelated equipment that removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel and primary cooling system, and containment) and the logic components used to actuate this safety-related equipment, usually referred to as the ESF Actuation System, and controls. • Monitoring and Indicator System - The monitoring and indicator system echelon consists of sensors, safety parameter displays, data communication systems, and independent manual controls relied upon by operators to respond to NPP operating events.
U-214	NUREG-0800, Chapter 7, Branch Technical Position (BTP) 7-19, Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems	1,4	Four Point Position: The NRC has established the following four-point position on D3 for new reactor designs and for digital system modifications to operating plants. The four points are quoted below: Point 1: "The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed." Point 2: "In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using bestestimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events." Point 3: "If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions." Point 4: "A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in Items 1 and 3 above." In this guidance, common software includes software, firmware, and logic developed from software-based development

			systems. Also, some errors labeled as "software errors" (for example) actually result from errors in the higher level requirements specifications used to direct the system development that fail in some way to represent the actual process.
U-227	Regulatory Guide 1.189, Fire Protection	5.3.1.3	Operator Manual Actions When one of the redundant safe-shutdown trains in a fire area is maintained free of fire damage by one of the means specified in Regulatory Position 5.3.1.1, then the use of operator manual actions may be credited with mitigating fire-induced operation or maloperation of components that are not part of the protected success path. The crediting of operator manual actions should be in accordance with the licensee's FPP and license condition. Operator manual actions may also be credited when an alternative or dedicated shutdown capability is provided as described in Position 5.4. All post-fire operator manual actions should be feasible and reliable. NUREG-1852 (Ref. 48) provides the technical bases in the form of criteria and technical guidance that may be used to demonstrate that operator manual actions are feasible and can be performed reliably under a wide range of plant conditions that an operator might encounter during a fire. The use of feasible and reliable manual actions alone may not be sufficient to address all levels of defense in depth. Therefore, fire prevention, detection, and suppression should be considered, in addition to the feasibility and reliability of operator manual actions. Because the fire protection requirements, including the protection of safe-shutdown capability and the prevention of radiological release, can be integrated in the planning and design phase, a new reactor plant should have minimal reliance on operator manual actions and alternative or dedicated shutdown systems (protection for fires in the main control room will require alternative shutdown capability).
E-195	WENRA Safety of New NPP Designs, Draft 9, 2012	3,1	3.1 POSITION 1: DEFENCE-IN-DEPTH APPROACH FOR NEW NUCLEAR POWER PLANTS New reactor designs and associated evolution of the Defence-in-Depth levels Refined structure of the levels of DiD The refined structure of the levels of DiD proposed by RHWG is as follows: ... *{See reference document}*
E-208	WENRA Safety of New NPP Designs, Draft 9, 2012	3,3	POSITION 3: MULTIPLE FAILURE EVENTS Safety demonstration For the additional safety features on level 3.b of the DiD concept it shall be shown that under the assumption of the postulated multiple failures first a controlled state[13] and later on a safe state[14] is reached and the radiological criteria of O_2 "No off-site radiological impact or only minor radiological impact" will be fulfilled analogue to the requirement on level 3.a.Once a controlled state is reached emphasis shall be paid to achieve a safe state in which the fundamental safety functions can be ensured and stably maintained for long time.
E-212	WENRA Safety Reference Levels for Existing Reactors, 24th September 2014	E 2.2	The defence-in-depth concept shall be applied to provide several levels of defence including a design that provides a series of physical barriers to prevent uncontrolled releases of radioactive material to the environment, as well as a combination of safety features that contribute to the effectiveness of the barriers. The design shall prevent as far as practicable: * challenges to the integrity of the barriers; * failure of a barrier when challenged; * failure of a barrier as consequence of failure of another barrier.

E-228	WENRA Safety Reference Levels for Existing Reactors, 24th September 2014	F 1.1	As part of defence in depth, analysis of Design Extension Conditions (DEC) shall be undertaken with the purpose of further improving the safety of the nuclear power plant by: enhancing the plant's capability to withstand more challenging events or conditions than those considered in the design basis, minimising radioactive releases harmful to the public and the environment as far as reasonably practicable, in such events or conditions.

References

Alanen, J. and Tommila, Teemu, T. 2016. A reference model for the NPP I&C qualification process and safety demonstration data Research Report: VTT-R-00478-16. VTT, 43 p. + app. 21 p.

EPRI. 2014. Principles and Approaches for Developing Overall Instrumentation and Control Architectures that Support Acceptance in Multiple International Regulatory Environments. EPRI Product Id: 3002002953. 366 p.

DICWG-09. 2015. Common position on safety design principles and supporting information for the overall I&C architecture. Multinational Design Evaluation Programme. 8 p.

YVL B.1. 2013. Safety design of a nuclear power plant. The Radiation and Nuclear Safety Authority (STUK), 15 November 2013, 46 p.

Conformity assessment data model completed

In (Alanen & Tommila 2016, Figure 15) we presented the safety demonstration data model that encompasses the actual engineering artefacts (requirements and design/implementation artefacts), determination artefacts (artefacts relating to testing, analysis, etc.) and conformity artefacts (claims, arguments and evidences). It provides a traceability information model for the artefacts related to the upper three levels of the following four-layer development process model (see Figure 1).

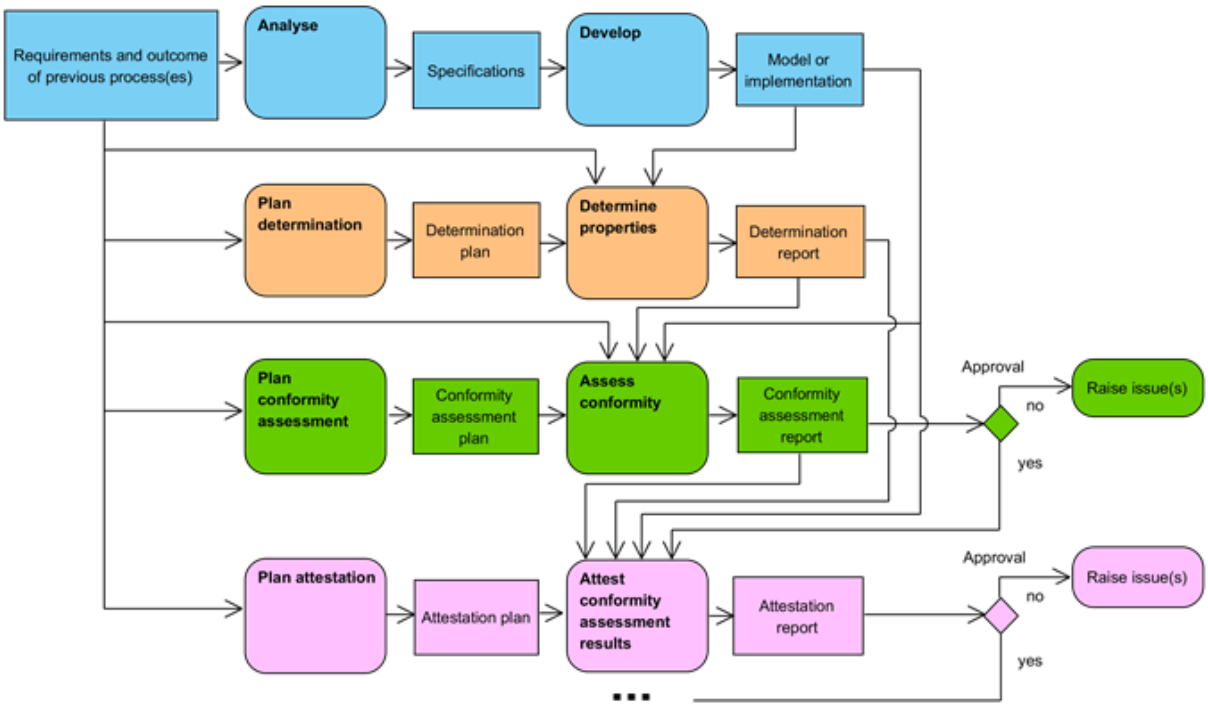

Figure 1. Develop, determine properties, assess conformity and attest conformance – development process overview.

Below in Figure 2 we reproduce the particular data model with some minor updates. This data model covers the artefacts relating to the 'eight' part of our SE 8.0 process model (see the Blog post Conformity assessment activities within the systems engineering processes).

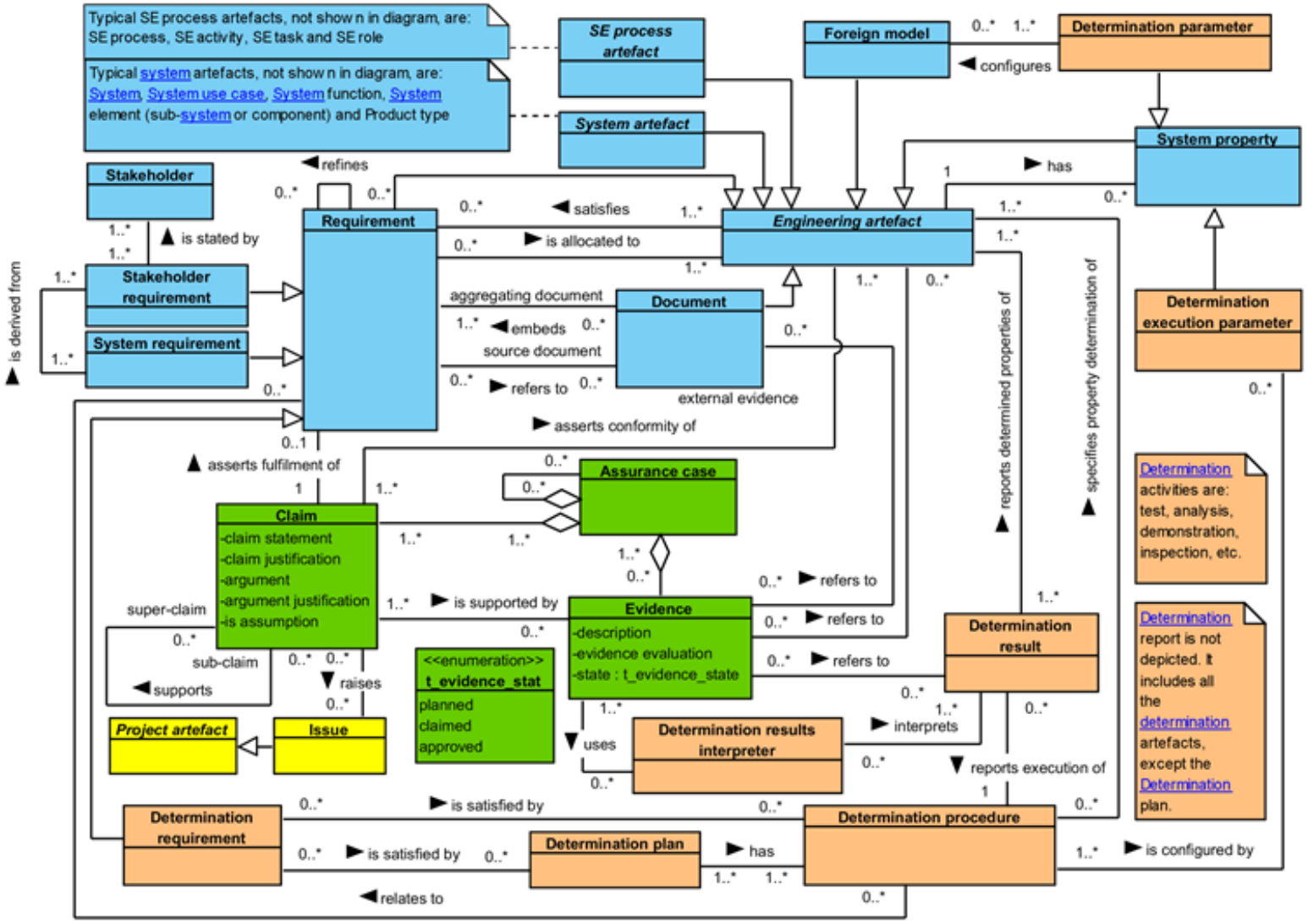

Figure 2. Our suggested data model for the main development artefacts, determination artefacts and conformity artefacts.

To complete the traceability model to also include the attestation process, we provide in Figure 3 the data model for the attestation artefacts (the 'zero' part of our SE 8.0 process model; see the Blog post Conformity assessment activities within the systems engineering processes).

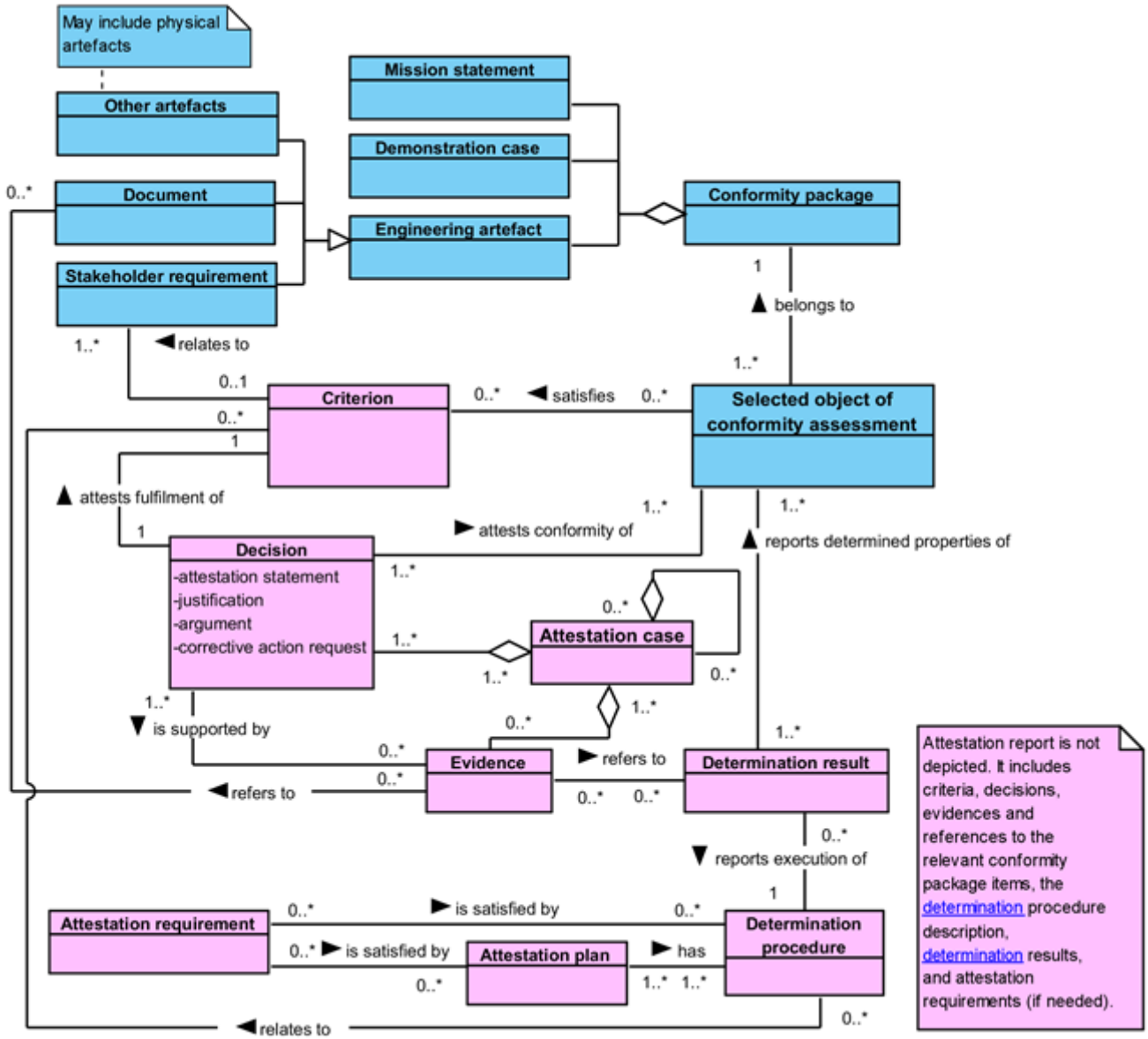

Figure 3. Our suggested data model for the attestation artefacts.

The model in Figure 3 is similar to the conformity assessment and determination artefacts in Figure 2 with the difference that Requirement is replaced by Criterion, Claim is replaced by Decision and Assurance case is replaced by Attestation case. Note also that the two determination artefacts share the colour with the other attestation artefacts (not the colour of the determination artefacts in Figure 2) to emphasise the fact that, in this case, determination is performed at the attestation level, typically by an independent attestor, and because the determination activities concentrate here mostly on the Conformity package, not on the actual product, although in many cases also the actual products may be tested, demonstrated, analysed, etc. within the context of the attestation process.

References

Alanen, J. and Tommila, Teemu, T. 2016. A reference model for the NPP I&C qualification process and safety demonstration data Research Report: VTT-R-00478-16. VTT, 43 p. + app. 21 p.

SE 8.0 conformity assessment data model in practice

In this post, we provide a simple case that uses the SE 8.0 conformity assessment data model presented in the previous post (Conformity assessment data model completed). Our case example comes from the SAFIR2018 program project SAUNA Task 1.1. The particular task deals with model based assessment of Defence-in-Depth properties of a system. The example system-of-interest in the particular task is a spent fuel cooling control system. The example case is documented in (Papakonstantinou et al. 2017). An overview of the case study is provided in Figure 1.

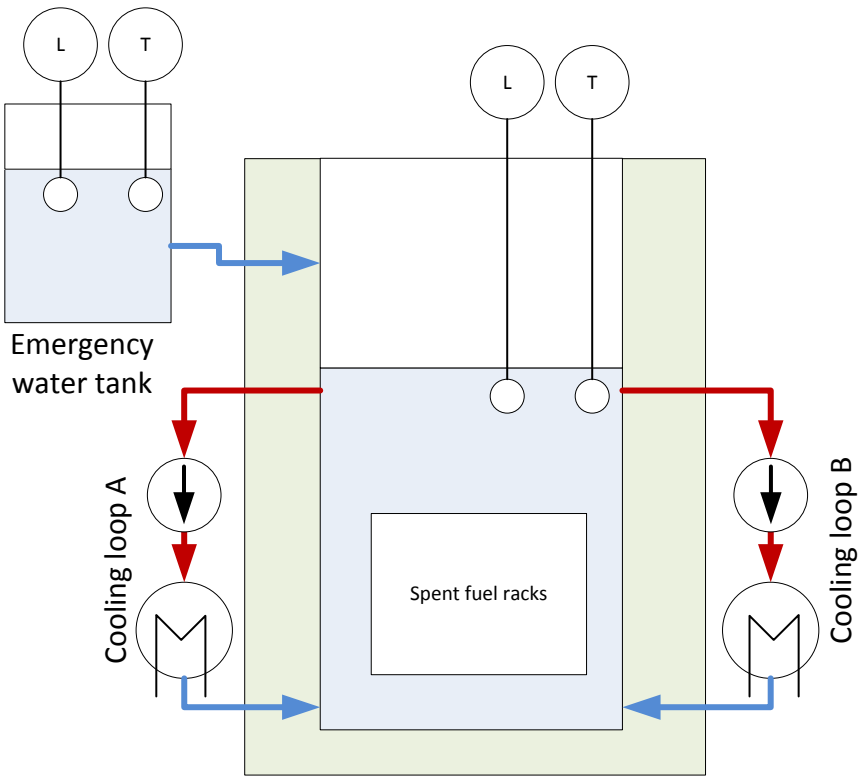

Figure 1. An overview of the case study, the spent fuel cooling system of a Nuclear Power Plant with two redundant cooling loops and an emergency cooling system (Papakonstantinou et al. 2017).

The spent fuel cooling control system architecture model is illustrated in Figure 2.

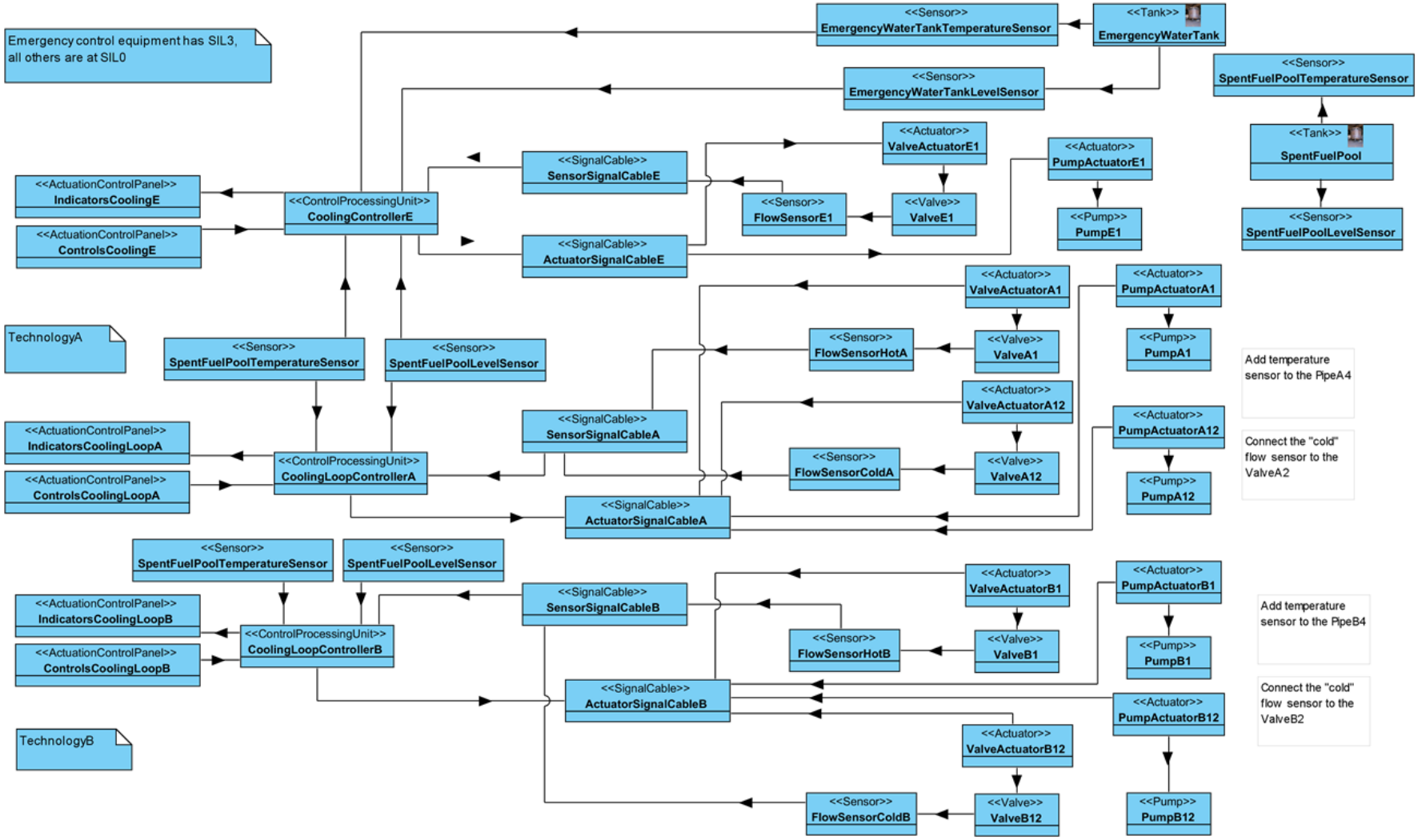

Figure 2. The control system diagram; the controller contains the 'diversity' DiD property, e.g. micro-controller, simple Boolean logic or analogue relays; all automation components have safety classification (Papakonstantinou et al. 2017).

For the particular case, a High Level Interdisciplinary Model (HLIM) of the spent fuel cooling control system was created using UML class diagram notation. A set of rules according to the Defence-in-Depth requirements were established, and a computer tool to check the HLIM against the rules was created.

In this post we demonstrate as to how the HLIM and the HLIM design analysis tool could be used to assess the conformity to the DiD requirements of the spent fuel cooling control system, and furthermore, how to use our model to organise the attestation (qualification) artefacts to provide good traceability to conformity assessment artefacts. In our demonstration, we focus on the Rule 4 of (Papakonstantinou et al. 2017): "Automation components of redundant control systems should utilize diverse technology".

In Figure 3, the relevant artefacts of the example case of (Papakonstantinou et al. 2017) are allocated to the first part of our conformity assessment data model. The conformity assessment loop is completed with conformity assessment artefacts (the dark green artefacts in Figure 3) and with one attestation artefact that is assumed to be available before the actual attestation activity.

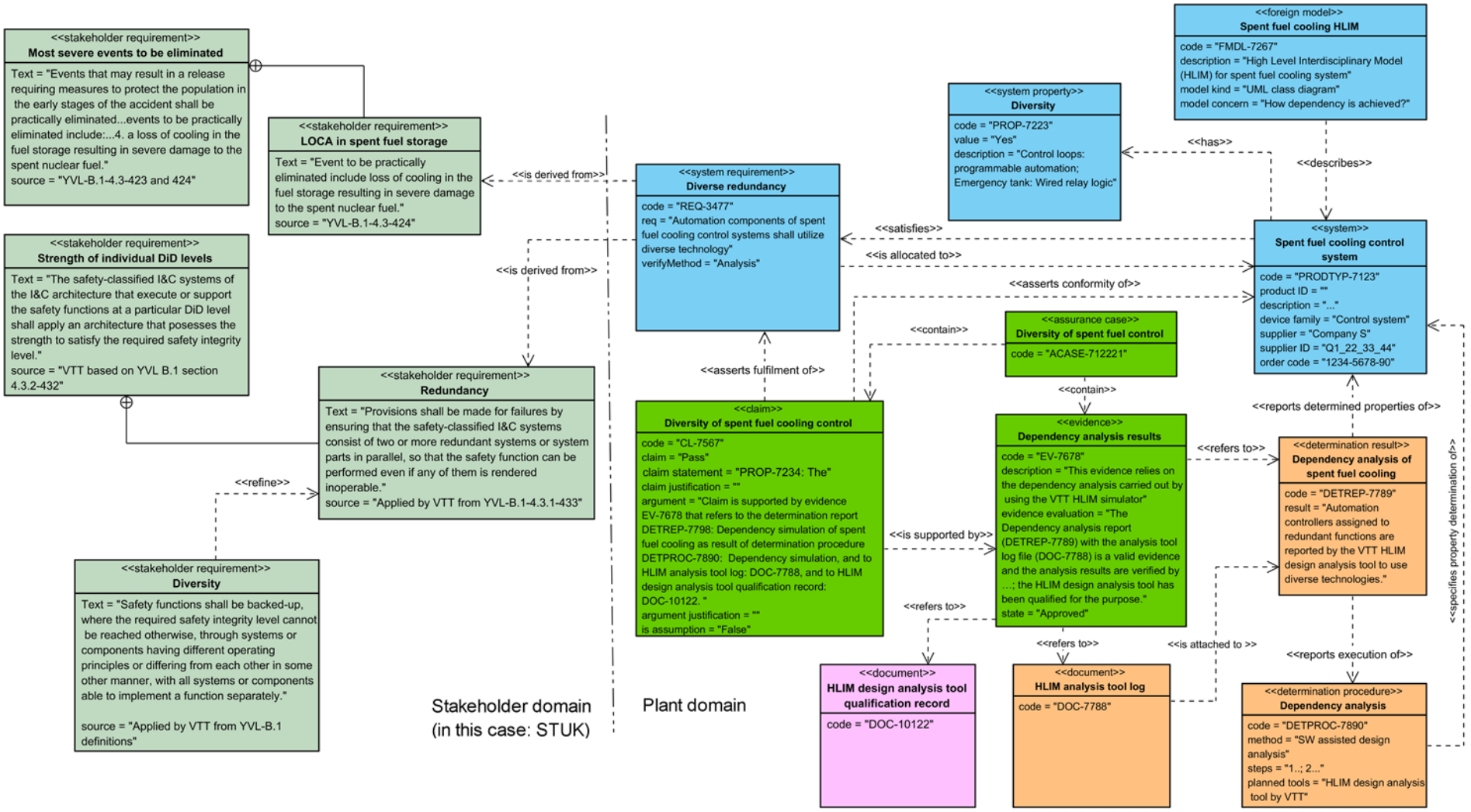

Figure 3. Conformity assessment part (i.e. Figure 2 of conformity assessment data model presented in the previous post [Conformity assessment data model completed]).

The diagram in Figure 3 starts from the stakeholder requirements (in this case an excerpt of DiD requirements from YVL-B.1). In the plant domain, system requirements are derived from the stakeholder requirements; in this example, a diversity requirement is stated. It is allocated to the Spent fuel cooling control system. An architecture model is created using our High Level Interdisciplinary Model principle (an UML class diagram, see Figure 2). The designer believes that the Spent fuel cooling control system has a diversity property and thus satisfies the diversity requirement. To verify that, the actual diversity property is determined by running the HLIM design analysis tool. The tool reports that the redundant parts of the Spent fuel control system indeed use diverse technologies. This result is reported and the tool log file is attached to the report. Consequently, conformity to the diversity requirement can be claimed. The determination report will be used as the evidence for the claim. Furthermore, in a real case, the HLIM design analysis tool would be qualified for its purpose. Hence, the particular qualification record is also referred to in the evidence.

In Figure 4, the relevant artefacts of the example case of (Papakonstantinou et al. 2017) are allocated to the second part of our conformity assessment data model. The second part deals with the third party attestation, in this case, qualification of the spent fuel cooling control system. The example covers only one requirement, the diversity requirement.

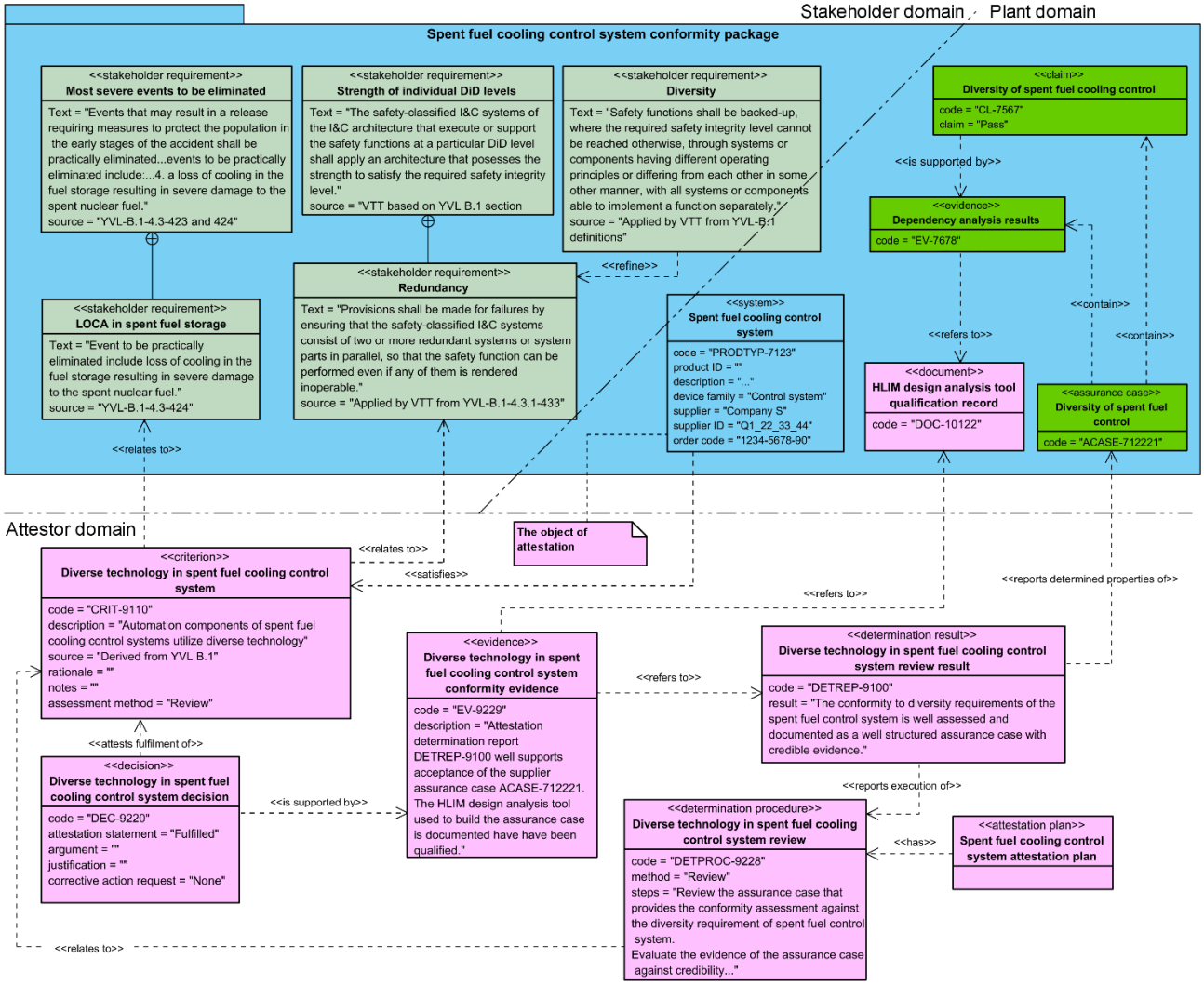

Figure 4. Attestation part (i.e. Figure 3 of conformity assessment data model presented in the previous post [Conformity assessment data model completed]).

The diagram in Figure 4 starts with the relevant artefacts from the conformity package ('safety case') provided for the attestor organisation by the supplier of the spent fuel cooling control system. It includes both the original stakeholder requirements (the YVL B.1 DiD requirements), the conformity assessment artefacts (including one existing attestation artefact, the HLIM design analysis tool qualification record) and description about the object of attestation. The main objective of the attestor is to assess the conformity assessment artefacts to decide whether the conformity claims are valid or not. Based on the stakeholder requirements (in the example, the requirements related to diversity), the attestor defines the criterion for accepting the suppliers claim about fulfilling the stakeholder requirement. (Luckily, the criterion is here the same as the suppliers system requirement.) Attestation involves review of the conformity assessment artefacts. The results of the review are used as the evidence to make the decision that the particular diversity criterion is fulfilled.

Our demonstration verifies the applicability of our conformity assessment data model to a case that reflects a real case. Next, our plan is to evaluate the model in a real industrial case with an industrial partner. The data model provides good traceability of artefacts ranging from the stakeholder domain to the organisation that designs the system and finally to the attestation organisation. With a proper tool, impact analysis is possible to carry out. Nevertheless, even in this rather simple example, it was not very easy to decide, which of the artefacts should be included in the conformity assessment and attestation loops. Compared to traditional document based qualification process, our data model has a good chance to be accepted by engineers if a good computer tool is available that hides the complexity of the data model and guides the users to put the engineering artefacts to correct locations and to establish the traces between the artefacts. When the data is in the correct locations, automatic or semi-automatic document generation for various purposes in various formats is possible.

In the following, some of the most relevant benefits of such a structured, model based, conformity assessment are listed:

- clear placeholders are provided for data that is captured from engineers via forms that include hint texts to support the engineer to input the relevant data; tendency to write unnecessary prose is minimised;
- automatic or semi-automatic document generation is possible;
- original data is in a single repository, not in copies of word processing documents; document chaos is avoided;
- it is possible to arrange systematic traceability with impact analysis.

The challenges of such a structured conformity assessment data model are as follows:

- if the computer tool that is used to apply the data model is poor, usage of the data model will fail due to its complexity; consequently, the engineers will turn to traditional document based engineering;
- it is difficult to change the mental attitude of experienced engineers away from the document based engineering.

References

Papakonstantinou, Nikolaos & Tommila, Teemu & O'Halloran, Bryan & Alanen, Jarmo & Van Bossuyt, Douglas. (2017). A Model Driven Approach for Early Assessment of Defense in Depth Capabilities of Complex Sociotechnical Systems. V001T02A079. 10.1115/DETC2017-67257.