Towards Systematic Compliance Evaluation Using Safety-oriented Process Lines and Evidence Mapping

Timo Varkoi[1], Timo Mäkinen[2], Barbara Gallina[3], Frank Cameron[2], Risto Nevalainen[1]

[1]Finnish Software Measurement Association – FiSMA ry, Espoo, Finland
timo.varkoi@fisma.fi, risto.nevalainen@fisma.fi
[2]Tampere University of Technology, Pori Department, Pori, Finland
timo.makinen@tut.fi, frank.cameron@tut.fi
[3]Mälardalen University, Västerås, Sweden
barbara.gallina@mdh.se

Abstract. The role of software is growing in safety related systems. This underlines the need for software process assessment in many safety-critical domains. For example, the nuclear power industry has strict safety requirements for control systems and many methods are applied to evaluate compliance to domain specific standards and requirements. This paper discusses the needs of the nuclear domain and presents alternatives to develop a process assessment method that takes into account domain specific requirements. The aim is to provide an approach that facilitates the use of assessment findings in evaluating compliance with the domain requirements and supports other assurance needs. Safety-oriented Process Line Engineering (SoPLE) is studied as a method for mapping assessment criteria to domain specific requirements. A binary distance metric is used to evaluate, how far a process mapping based method would solve problems found in compliance evaluation. Based on the results, SoPLE is applicable in this case, but process mapping is not adequate to facilitate compliance evaluation.

Keywords: Safety, Systems engineering, Process assessment, Process lines

1 Introduction

The growing use of digital instrumentation and control systems has amplified safety as a design constraint in many safety-critical domains. Domain specific safety requirements may also imply significant requirements for systems development processes. Process assessments are used to address the quality of the development processes. However, generic process assessment models (PAMs) may not adequately cover the domain specific requirements (DSRs) and additional effort is required to evaluate e.g. compliance to domain standards.

Most safety-critical domains have similar concerns with respect to domain specific and generic industry requirements. We have profound expertise in the nuclear power industry and therefore we limit the scope of this paper to that domain. Also, we use as examples of domain specific requirements the guidance given by the Finnish nuclear

safety authority and some international standards that address software in nuclear power plants.

The nuclear power industry is an example of a domain in which numerous national and international regulations involve safety requirements. As safety is a vital, many methods are used to ensure that instrumentation and control systems meet strict safety requirements. The increasing dependence on software in these systems emphasizes the need for software process assessments. To be effective, process assessment methods need to take into account DSRs.

Process assessments produce large amounts of evidence data that can be used to evaluate compliance to DSRs. This, however, is not a trivial task. First, the approach and level of details in different requirements sets impose some mapping between process models and safety standards. Second, the evidence (information used to demonstrate that safety requirements are met) may imply findings that are relevant to multiple requirements. For example, an inappropriate test report may be used as a negative evidence for verification, project management and/or documentation process. Similarly, an assessment finding may be relevant in evaluating multiple safety requirements.

We studied two approaches to address the issues related to compliance evaluation: one for mapping the models and one for analyzing the ability of a mapping based method to accelerate compliance evaluation. The aim is to find approaches that facilitate the use of assessment findings in evaluating compliance with the DSRs and can also support other assurance needs. First, we compared requirements found in domain standards with the more generic requirements of a PAM to identify the relationships. The study in this paper provides a satisfactory solution for mapping the PAM elements to DSRs. Second, we analyzed the use of actual assessment findings in compliance evaluation to identify any regularities. Also, the analysis of assessment findings and their relationship to DSRs was successfully performed, but the actual result is not adequate to solve issues in compliance evaluation.

We are not aware of existing work aimed at enabling systematic compliance evaluation via usage of safety-oriented process line engineering practices or investigating the applicability of process mapping using binary distance metrics. In this respect, our work is new.

The rest of the paper is organized as follows. In section 2, we present a domain specific process assessment method and the issues found in evaluating compliance to DSRs. Section 3 describes safety-oriented process line engineering as a possible solution to mapping model elements. In section 4 we use binary distance metrics to study the relevance of process mapping as means to get evidence for DSRs from assessment findings. Section 5 contains a discussion and presents ideas for future work.

2 Process Assessment in Nuclear Power Domain

2.1 Nuclear SPICE

Nuclear SPICE [1] is a method to evaluate the development processes when delivering software systems in the nuclear power domain. Its main purpose is to reduce risks in deliveries and to systematically collect evidence for safety qualification. The Nuclear

SPICE method consists of a process assessment model and an assessment process. The process assessment model contains the reference processes and a scale to evaluate the quality of each process. The assessment process is a documented guide for performing assessments and to ensure repeatability of assessment results.

Nuclear SPICE is based on the latest ISO/IEC process assessment standards and process models (also known as the SPICE models) [2,3], domain specific safety standards and regulatory requirements. Nuclear SPICE is applicable to systems and software engineering processes. The process reference model in the latest edition is based on the recently revised ISO/IEC 15288 standard [4] for System life cycle processes. Base practices, tasks and information products are used as assessment indicators.

There are three main roles in the assessment: 1) the *assessors* who perform the assessment (one assessor is the lead assessor); 2) the *assessee* who represents the organization to be assessed; 3) the *sponsor* who acquires the assessment. Depending on the nature of the assessment, there are rules governing the independence of the assessors. There may be other stakeholders, e.g. national/international authorities who receive the assessment results.

The Nuclear SPICE assessment process [5] is presented in Fig. 1. The main phases of the assessment process are: Planning, Data collection, and Reporting. In the *planning phase* the lead assessor prepares the assessees' organization and ensures adequate resources for the assessment. This phase is important in creating trust between the assessor and the other involved parties. The assessors' aim in the *data collection phase* is to collect adequate evidence for a consistent assessment result. In the *reporting phase* the assessors produce one or more reports and provides all parties with the results in an understandable format including face-to-face feedback. The assessment process describes the activities within the phases. Detailed tasks within the activities are defined and templates are provided for the assessment output.

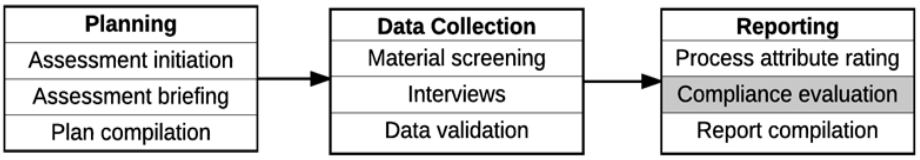

Fig. 1. Nuclear SPICE Assessment Process

Compared with ordinary SPICE assessments, Nuclear SPICE defines an additional activity for *Compliance evaluation*. This activity is an important part of the assessment in nuclear power industry, since complying with the domain standards is a key issue in qualification of the systems relevant to safety. For the nuclear power domain, the relevant standards are IEC 60880 [6] and IEC 62138 [7]. Since Nuclear SPICE was developed in Finland, requirements by the national nuclear safety authority are also important for us. These requirements are described in the YVL guidance [8,9], which defines safety requirements concerning the use of nuclear energy in Finland. These may also be considered in the evaluation. Compliance evaluation is not intended to be used

to claim compliance to one or more relevant standards, however, it may provide information or evidence on the achievement of individual requirements [5].

The collected assessment findings and ratings are analyzed and mapped to selected standards and requirements. The selection of standards and requirements for compliance evaluation is documented in the assessment plan. Possible issues with the assessed processes are identified and reported based on the lead assessor's expert judgment of these processes. Compliance evaluation does not imply any compliance of the actual software product and is optional depending on the assessment goal.

2.2 Nuclear Power Domain Specific Safety Requirements

The engineering of software based instrumentation and control systems to be used for safety purposes in nuclear power plants (NPPs) is a challenge due to the safety requirements to be fulfilled. The safety software used in NPPs, which is often required only in emergencies, has to be fully validated and qualified before being used in operation. To achieve the high dependability required, special care has to be taken throughout the entire life cycle, from the basic requirements, the various design phases and verification and validation procedures for operation and maintenance. The main aim of the IEC 60880 standard is to address the related safety aspects and to provide requirements for achieving the high software quality necessary [6].

IEC 60880 is one of the strictest standards for software development. It includes requirements and recommendations for the development of software to be used in the highest safety class. Requirements for software to be used in lower safety classes at NPPs are described in IEC 62138. To some extent, the requirements in both standards follow the same approach and address similar issues. Both IEC 60880 and IEC 62138 address the development process and the software to be produced. We have analyzed the IEC 60880 standard and found that most of the requirements are process-related and suitable for indicators in process assessment. Table 1 presents one group of the requirements related to the specification of software requirements. These requirements are used later in section 3.2 to demonstrate mapping of PAM elements to DSRs.

Table 1. Some specific requirements from IEC 60880 and their corresponding types.

IEC 60880 6.1 Specification of software requirements	**Type of requirement**
6.1.1 The software requirements shall be derived from requirements of the safety systems and are part of the computer-based system specification.	Process
6.1.2 The software requirements shall describe what the software has to do and not how the software shall do it.	Process
6.1.3 The software requirements shall specify: – the application functions to be provided by the software; – the different modes of behavior of the software, and the corresponding conditions of transition; – the interfaces and interactions of the software with its environment; – the parameters of the software which can be modified manually during operation, if any;	Process (Categories of requirements) Software (Content of specification)

IEC 60880 6.1 Specification of software requirements	Type of requirement
– the required software performance, in particular response time requirements; – what the software must not do or must avoid, when appropriate; – the requirements of, or the assumptions made by, the software regarding its environment, when applicable; – the requirements if any, of standard software packages.	
6.1.4 Due to the significance of this phase of software development, the process of laying down software requirements shall be rigorous.	Process (Quality; vague requirement)
6.1.5 The software requirements specification shall be such that compliance of the I&C system to the requirements of IEC 61513 can be demonstrated.	Process
6.1.6 The constraints between hardware and software shall be described	Process (Performance) Software (Content)
6.1.7 A reference to the hardware requirements specification shall be made within the software requirements specification for any hardware design impacts.	Process (Performance) Software (Content)
6.1.8 Special operating conditions such as plant commissioning and refueling shall be described down to the software level for the functions that are impacted.	Software (Content)

2.3 Issues in Compliance Evaluation

Even though, the value of process assessment as such is recognized in many safety-critical domains, there is also a practical need to collect evidence for system qualification needs. The domain specific standards define what evidence is needed and a significant amount of it is related to process assessment data and results. Efficient management of that data requires first, a systematic approach for mapping the PAM and DSRs; second, a flexible technical solution to manage the assessment findings and their use in compliance evaluation.

The mapping between a PAM and DSRs is based on a systematic analysis of the existing process assessment indicators (base practices, tasks and information products) and the relevant domain related requirements and recommendations. Frequently changing models and requirements are challenging when keeping the mapping up-to-date.

The context of issues in compliance evaluation is displayed in Fig. 2. The assessors compile a set of observations, called assessment findings, based on the interviews and material screening of the data collection. Data collection is based on a PAM. These assessment findings can be used as supporting evidence that certain DSRs are being met. However, in general the assessors do not know in advance, which DSRs will be covered by the findings and which DSRs will require further investigation. Currently, compliance evaluation can be up to 25% of the assessment effort and requires scrupulous manual work to complete.

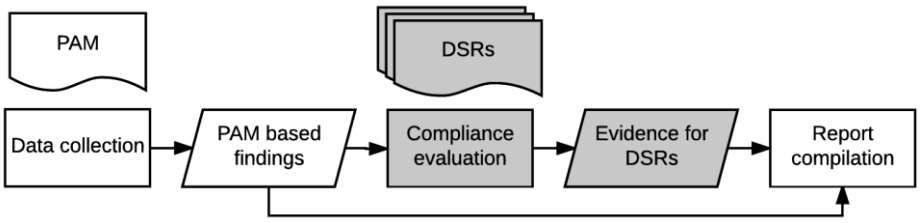

Fig. 2. Context of Compliance Evaluation

In the next two sections, we discuss two possible approaches to address the issues in compliance evaluation. First, safety-oriented process line engineering is applied in mapping the PAM and domain specific safety standards. Second, a binary distance metric is used to analyze existing assessment data to map findings to requirements. Our aim is to reduce the effort needed in qualification and enable the reuse of the evidence data for multiple purposes after a process assessment.

3 Model Element Mapping

3.1 Safety-oriented Process Line Engineering

Safety-oriented process line engineering (SoPLE) [10,11] consists of the concurrent engineering of a set of safety-oriented processes. A Safety-oriented process line (SoPL) represents a set of safety-oriented processes, which may exhibit: full commonalities, partial commonalities (structured process elements that are partially equal), and variabilities. A full commonality can be identified when a process element is present in all processes belonging to the set. A partial commonality can be identified when a structured process element, which contains a common substructure, is present in all processes belonging to the set. Finally, variability can be identified when a process element may vary (e.g., optionality, alternative).

To engineer according to SoPLE, a process engineer should first delimit the scope of the line, then engineer the domain (i.e., model the SoPL), finally, derive (safety-oriented) processes from the SoPL. The fundamental process elements to be interconnected to model processes are the following: tasks (which represent independent units of work), work products (e.g., deliverables), roles, guidance, and tools. Additional information on SoPLs as well as SoPLs Engineering (SoPLE) and its application can be found in [10,11,12].

3.2 Application of SoPLE: focus on commonalities & variability identification

We next give a brief application of SoPLE to identify commonalities between PAM indicators (base practices, tasks, and information products) and domain specific requirements. First, we delimit the scope of the line by considering IEC 60880 and Nuclear SPICE. Then, we perform a manual comparative study aimed at revealing commonalities and variabilities between PAM indicators and DSRs.

PAM elements can, to some extent, be mapped to DSRs. As an example, IEC 60880 *Configuration management requirements* correspond largely to Nuclear SPICE *Configuration management process*. Similarly, IEC 60880 *Specification of software requirements* (see Table 1) can be mapped to *System requirements definition process* in the Nuclear SPICE PAM. This mapping, presented in Table 2, is an example of the PAM/DSR mapping that is required as the basis for analyzing the adequacy of the PAM indicators in meeting the DSRs. In this case, also the evidence related to the process is mainly evidence for the DSRs.

Table 2. Example of mapping PAM indicators to domain specific requirements

PAM indicators of *System requirements definition process*	**IEC 60880 (Table 1)**	**Process element and type**
TEC.3.BP1: Prepare for system requirements definition.	6.1.1	Task/Commonality
TEC.3.BP2: Define system requirements	see steps below	Task/Commonality
1) Define each function that the system is required to perform.	6.1.1, 6.1.2	Step
2) Define necessary implementation constraints.	6.1.2	Step
3) Identify system requirements that relate to risks, criticality of the system, or critical quality characteristics.	6.1.3, 6.1.2, 6.1.8	Step
4) Define system requirements and rationale.	6.1.2	Step
TEC.3.BP3: Analyze system requirements	see steps below	Task/Commonality
1) Analyze the complete set of requirements.	6.1.4, 6.1.5	Step
2) Define critical performance measures that enable the assessment of technical achievement.	6.1.4, 6.1.3	Step
3) Feedback the analyzed requirements to applicable stakeholders for review.	(Annex A.2.3.4)	Step
4) Resolve system requirements issues.	6.1.8	Step
TEC.3.BP4: Manage system requirements	see steps below	Task/Partial commonality
1) Obtain explicit agreement on the system requirements.	-	Step
2) Provide key information items that have been selected for baselines.	(in Configuration management)	Step
3) Maintain traceability of the requirements.	6.1.7, (7.1.4.5)	Step
System Description	system specification	Work product/Commonality
System Requirements	software requirements; hardware requirements	Work product/Commonality
System Requirements Report	-	Work product/Variability
Critical Performance Measures	-	Work product/Variability
Traceability Mapping	-	Work product/Variability

4 Evidence Mapping

4.1 Evidence Base Approach

Nuclear SPICE has a special activity for compliance evaluation. It is used to evaluate the DSRs that originate from the domain safety standards or regulatory instructions. The evidence is based on assessment findings and results. Often, findings of one indicator might imply findings for entirely other areas. For example, suppose when assessing verification, it is found that tests exist that are not directly traceable to requirements. This could indicate weaknesses in test planning or requirements definition.

The compliance evaluation activity is quite a laborious task. It is difficult to analyze manually a large amount of evidence. Therefore, a systematic handling of the evidence is needed to fully make use of the collected information. To ease the assessor's burden, it would be convenient if a software tool existed which could help in mapping the assessment indicators to DSRs. Such a tool to manage the evidence base does not currently exist. In what follows we take the first steps in studying the feasibility of such a tool. For data we use three completed assessments as cases. The data contains assessment findings and ratings of three real-life assessments performed recently with Nuclear SPICE. The data is cleaned to ensure anonymity and cleared for research purposes by assessees and assessment sponsors. In all three cases, three DSR sets were present in the compliance evaluation: IEC 62138 [7], YVL B.1 [8], and YVL E.7 [9]. We focus on YVL E.7, which contains requirements of Finland's Radiation and Nuclear Safety Authority. Our aim here is to see if an assessment indicator maps to the same, or nearly the same, DSRs of YVL E.7. If so, a tool to manage the evidence base, which is based on the mapping of the indicators of the assessment model and the DSRs, would probably support the compliance evaluation activity. However, if the similarity is low, the tool might have to consider more the assessment findings which are the basis for the evidence.

4.2 Using a Binary Distance Metric

The study concentrated on the base practices of the assessment model and the YVL E.7 requirements. The binary distance metric proposed by Lance & Williams [13] was used to measure the difference of mapped elements in the three assessment cases.

Given sets R and S, let $common(R,S)$ and $noncommon(R,S)$ be the number of common and noncommon elements of R and S. Lance & Williams' distance measure is computed as follows:

$$d(R,S) = \frac{noncommon(R,S)}{2 \times common(R,S) + noncommon(R,S)}$$

The value of $d(R,S)$ is always between 0 and 1. If $d(R,S) = 0$, sets R and S are the same. If $d(R,S) = 1$, sets R and S have no common elements. For example, if $R = \{\alpha, \beta\}$ and $S = \{\alpha, \delta, \theta\}$, then $common(R,S) = 1$ and $noncommon(R,S) = 3$ and $d(R,S) = 2/5$. The measure $d(R,S)$ is undefined, if sets R and S are both empty.

Table 3 presents samples of the result representing different kinds of distances found in the study.

Table 3. Distances of element mappings in different assessments

Indicators (base practices)	**YVL E.7 related findings**			**Distance metric**			
	A	**B**	**C**	***d*(A,B)**	***d*(A,C)**	***d*(B, C)**	**avg.**
Ensure consistency.	322 525 612	322 525 612	322 525 612	0,00	0,00	0,00	0,00
Construct software.	623	563 623 627	331 623 648	0,50	0,50	0,67	0,56
Test integrated software against requirements.	644		627 644 648	1,00	0,50	1,00	0,83
Prepare software for release.	646	633 643 644		1,00	1,00	1,00	1,00
Plan the safety qualification of external resources.	339 563 616	339 616	312 334 339 563 616	0,20	0,25	0,43	0,29

In the first column of Table 3 there are some base practices from the assessment model. The next three columns correspond to the three case assessments (labelled A, B and C). For each assessment and each base practice there is a set of YVL E.7 requirements that were mapped to the base practice in question. For example, for assessment A, only requirement 623 was mapped to the base practice '*Construct software*'. The number 623 and all other numbers in the A, B and C columns are simply labels for different YVL E.7 requirements. The columns labelled *d*(A,B), *d*(A,C) and *d*(B,C) are distance measures for the three different pairs of assessments. The last column contains the average of *d*(A,B), *d*(A,C) and *d*(B,C).

Table 3 contains only a small portion of the entire mapping between bases practices and YVL E.7 requirements for assessments A, B and C. In total, there are 87 base practices and 48 YVL E.7 requirements. For 33 of the base practices, at least two of the three assessments had non-empty sets of YVL E.7 requirements. For the remaining 54 base practices, at least one of the distance measures *d*(A,B), *d*(A,C) and *d*(B,C) was undefined. If we only consider the 33 base practices where *d*(A,B), *d*(A,C) and *d*(B,C) were all defined, then the mean of all 33×3 distances is 0,68 while the median of the means for these 33 base practices is 0,78. These are quite high distance measures and they indicate that the mappings between the assessment model and YVL E.7 requirements depend very much on the assessment instance. The reason for the result might be context dependency, which supports the idea of some kind of evidence based tool.

In any event, the lack of consistent mappings between base practices and YVL E.7 requirements indicates that any software tool to help an assessor would require some

sophistication. For example, simply offering the assessor a complete set of all possible YVL E.7 requirements related to a given base practice and asking for approval or rejection would probably be more irritating than helpful.

5 Discussion and future work

In this paper, we have analyzed process assessment models, domain specific requirements and assessment findings. The aim was to find solutions that can help in compliance evaluation that, by experience, is very tedious. Some progress can be seen, but a major breakthrough is still missing. Considering the rigor required because of the strict requirements of the nuclear domain, any dubious methods or tools cannot be recommended.

One obvious constraint is the process assessment approach itself. Systems development is assessed using a process assessment model that cannot address all safety requirements of the domain. Many requirements are product-oriented or address other stakeholders than the systems developer.

Safety-oriented process line engineering can easily be applied to mapping process assessment models and domain specific requirements. This helps in the development of the process assessment model when trying to adopt the assessment model in using different sets of requirements. The requirement sets vary because of the safety class of the system, or national requirements, for instance. There is also some support for compliance evaluation: the mapping documents the obvious requirements that need to be checked.

The complicated part of compliance evaluation is the management of the evidence data. There are lots of findings that may imply exact finding for an assessment indicator, but they may give random findings to other indicators. The same applies for domain specific safety requirements. We tested a binary distance metric to see how consistent is the mapping between assessment indicators and one particular domain specific requirement set. With this distance metric, we obtain numerical results. What we observed was that some mappings are consistent, while the majority are more random. This confirms the supposition that proceeding directly from assessment indicators to domain requirements is difficult. A noticeable constraint is the availability of the assessment data. Assessments are always confidential and any information related to them needs to be specifically cleared. Another issue is the comparability of the data: different models and requirement sets are used, and they also tend to change over time.

Fig. 3 summarizes the associations between PAM and DSRs. The associations represent links between the elements of the hypothetical ’Evidence Base’ that help an assessor to conduct the compliance evaluation activity in Nuclear SPICE. The SoPLE approach can be used to identify beforehand common features between PAM and DSRs. When such commonalities exist, the assessor can produce supporting evidence for DSRs directly from the assessment ratings. Compliance evaluations in earlier assessments produce links when an assessment finding is selected as an evidence for a DSR. These links are based on an expert's judgements. Distance measures between the elements of PAM and DSRs collate the previous links. Using the measures, we could

get answers to questions such as what PAM elements are typically associated with findings which are relevant to use as evidence for a DSR.

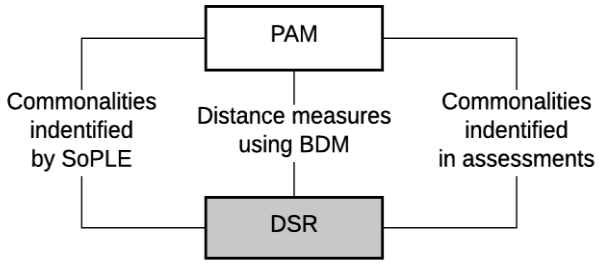

Fig. 3. Associations between PAM and DSRs

We are aware and we share the concerns regarding current standardization schemes including their inefficiency and in some cases their imprecision, see Bender et al [14], Knight and Rowanhill [15], and others. However, in this paper we do not contribute to investigating how to improve such schemes by proposing new formulations or rational explanations within the standard but on how to make the compliance evaluation more systematic, since we believe that standards will always exist. We, however, believe that our findings will have a beneficial impact when planning new schemes or simplification of existing ones.

The compliance evaluation activity in Nuclear SPICE is considered very important by the assessment sponsors and the assessors. Further studies with larger amounts of data can be justified, even though our work indicates that a complete, tool-based solution might not be achievable. On the other hand, even a partial solution to support analysis and use of assessment evidence would be useful in assessment reporting.

Further work is needed on both PAM/DSR and evidence mappings. Also, consideration of the needs of different stakeholders, like authorities, assessors, NPPs and suppliers, is required. Even though, process assessment has proven to be an efficient method in evaluating systems development, including safety requirements, compliance evaluation remains one of the more tedious activities in it.

Acknowledgements. This work has been jointly funded by the Finnish national nuclear safety program SAFIR2018 (http://safir2018.vtt.fi/) and Finnish Software Measurement Association, FiSMA (www.fisma.fi), and the EU and VINNOVA via the ECSEL JU project AMASS (No. 692474) (http://www.amass-ecsel.eu).

References

1. Varkoi T, Nevalainen R, Mäkinen T (2013) Toward Nuclear SPICE – integrating IEC 61508, IEC 60880 and SPICE. Journal of software: Evolution and process, Wiley 2013
2. ISO/IEC 33001 (2015) Information technology – Process assessment –Concepts and terminology

3. ISO/IEC 33020 (2015) Information technology – Process assessment – Process measurement framework for assessment of process capability
4. ISO/IEC/IEEE 15288 (2015) Systems and software engineering — System life cycle processes
5. Varkoi T, Nevalainen R, Mäkinen T (2016) Process Assessment in A Safety Domain - Assessment Method and Results as Evidence in an Assurance Case. In Proceedings of QUATIC 2016, Lisbon, Portugal, September 6-9, 2016, pp. 52-58. IEEE Computer Society 2016
6. IEC 60880:2006 Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions
7. IEC 62138:2004 Nuclear power plants – I&C Systems Important to Safety – Software aspects for computer-based systems performing category B or C functions
8. STUK (2013a) YVL B.1, Safety design of a nuclear power plant, Finnish Radiation and Nuclear Safety Authority, 2013
9. STUK (2013b) YVL E.7, Electrical and I&C equipment of a nuclear facility, Finnish Radiation and Nuclear Safety Authority, 2013
10. Gallina B, Sljivo I, Jaradat O (2012) Towards a Safety-oriented Process Line for Enabling Reuse in Safety Critical Systems Development and Certification. Post-proceedings of the 35th IEEE Software Engineering Workshop (SEW-35), IEEE Computer Society, ISBN 978-1-4673-5574-2, Heraclion, Crete, Greece.
11. Gallina B, Kashiyarandi S, Martin H, Bramberger R (2014) Modeling a Safety- and Automotive-oriented Process Line to Enable Reuse and Flexible Process Derivation. Proceedings of the 8th IEEE International Workshop on Quality-Oriented Reuse of Software (QUORS), IEEE Computer Society, Västerås, Sweden.
12. Gallina B, Kashiyarandi S, Zugsbrati K, Geven A (2014) Enabling Cross-domain Reuse of Tool Qualification Certification Artefacts. Proceedings of the 1st International Workshop on DEvelopment, Verification and VAlidation of cRiTical Systems (DEVVARTS), Springer, LNCS, Florence, Italy.
13. Choi S-S, Cha S-H, Tappert C C (2010) A Survey of Binary Similarity and Distance Measures. Systemics, cybernetics and informatics, Volume 8, Number 1, 2010
14. Bender M, Maibaum T, Lawford M, Wassyng A (2011) Positioning Verification in the Context of Software/System Certification. Proceedings of the 11th International Workshop on Automated Verification of Critical Systems (AVoCS 2011), Electronic Communications of the EASST Volume 46, 2011
15. Knight J C, Rowanhill J (2016) The Indispensable Role of Rationale in Safety Standards. A. Skavhaug et al. (Eds.): SAFECOMP 2016, LNCS 9922, pp. 39–50, Springer, 2016.