We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

4,800
Open access books available

122,000
International authors and editors

135M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS BOOK CITATION INDEX INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

6

Certification of software in safety-critical I&C systems of nuclear power plants

Lic. Tech. Risto Nevalainen
Tampere University of Technology
Pori, Finland
M.Sc. (Eng) Juha Halminen
Teollisuuden Voima Oy
Olkiluoto, Finland
Lic. Tech. Hannu Harju
VTT Technical Research Centre of Finland
Espoo, Finland
M.Sc. (Eng) Mika Johansson
FiSMA ry
Espoo, Finland

Nuclear power plants have well-defined processes to acquire and qualify safety-critical systems. Ultimate goal is to maximise safety, without compromises in quality and reliability. Each new device and system in nuclear power plant shall be classified and qualified according to its safety requirements. Using modern technology means in practice that more and more components have programmable features. The reliability of such components has proven to be difficult to demonstrate due to the nature of flaws in software.

Standards and guides used by national authorities set licensing criteria for software used in the safety-critical systems of nuclear power plants. Nuclear power companies use commonly same standards and guides as authorities to avoid interpretation problems in qualification and licensing. Standards can be either generic, safety specific of nuclear domain specific. Also system manufacturers and software development units have adopted either nuclear domain specific of generic safety standards. Prerequisites for high-quality software and systems are in place.

Conformance with standards is not any absolute guarantee for safety. It can be achieved only by use of several different approaches, which all provide their own evidences and support for qualification and licensing. Certification is one way to package different methods together and build trust in achievement of maximal safety. In fact, certification is already de-facto "must" in highest safety category of software intensive safety-critical systems.

Certification should be aligned with system acquisition, development and commissioning processes to improve total effectiveness of qualification. Then it is also cost-effective and proactive rather than additional and isolated activity.

As a part of Finnish nuclear research program SAFIR2010, a project called CERFAS has defined necessary software certification services for nuclear industry needs. Main areas of the service are process assessment and product evaluation. Certification employs also several other method families, like inspections and reviews, independent V&V, model checking, conformance with selected reference standard(s) and use of selected measurements and analyses. Safety case is the main framework to integrate all methods together.

Keywords
Safety-Critical Software, Certification, Safety Case, Process Assessment, Product Evaluation, Conformance with Standards, Safety Systems

1. Introduction

When the first versions of nuclear specific system and software standards were written some 20 – 25 years ago, no generic software and quality standards like ISO/IEC 15504 (Process Assessment) or IEC/EN ISO 61508 (Functional Safety) existed or were not commonly known. So, each party developed their own criteria and terminology for their own needs.
Quite typically, nuclear power instrumentation and control (I&C) systems are industrial products and are not designed and manufactured uniquely for each application. Their platform is based on standard solutions and may be developed for many different purposes. Some subsystems may be old and not easy to qualify during the system delivery. The main evidence may be their historical development process and current operational history. They have many versions and variants and new changes to come. Only some minor part of the whole delivered system may consist of customer-specific application. When the system will be delivered into the nuclear power unit, it may require separate qualification of platform and application. As a whole, complete qualification can be very time-consuming and expensive.
As a result of the described development, there is clear need for an integrated and effective method to qualify software intensive systems in nuclear power units. Integration has three major areas: 1) Definition and harmonisation of requirements for software intensive systems in their different safety levels, 2) Integration of several approaches like SPICE and Failure mode effects and criticality analysis method, FMECA, to improve confidence of qualification and 3) Integration of the system acquisition and qualification processes to improve total effectiveness of the acquisition, delivery and commissioning processes.
Certification of software intensive systems can help in qualification. Because certification is very rigor and expensive process, it is needed mainly for most safety-critical systems and components. Certification of software is often limited to platform components. Certificate is normally valid for any further use of same software version, and can reduce certification cost per delivery.
The objective of SPICE method is to evaluate the process capability. SPICE is a brand name for ISO/IEC 15504 Process Assessment standard. The capability measurement system is based on ordinal 5-point capability level scale. Basically any process can be evaluated using the measurement system. In most cases, some predefined process reference model is used. Most known models are defined by ISO itself. ISO/IEC 12207 is the standard for software life-cycle processes. ISO/IEC 15288 is similar model for systems engineering. In most cases I&C systems for nuclear power plants are developed using a combination of software and systems engineering processes.

A modified FMECA method Tiira [9] has been used to bring evidence to the qualification process of safety-critical system. FMECA is effective to focus in most critical parts of the system, which have highest potential to cause failures. In hardware components, many well-defined methods can be used to show evidence about reliability and potential to failures. Redundancy can be used to reach required reliability and failure prevention level. For software-intensive components standard FMECA is less applicable, because software failure statistics is typically incomplete. Instead of statistics, target values for software reliability are used in Tiira. Software reliability and probability of failures to occur may be difficult to predict, even to calculate.

2. Overview of the requirements for qualification

2.1 Classification of systems according to safety

STUK (Säteilyturvakeskus, The Finnish Radiaton and Nuclear Safety Authority) has defined four safety class levels for nuclear power unit (SC1 … SC4, SC1 being the highest). IEC 61508 defines four safety integrity levels (SIL1 … SIL 4, SIL4 being the highest). Some other standards have defined for example safety classes 1, 2 and 3 for systems, and safety categories A, B and C for functions. There is no clear mutual compatibility between various nuclear specific standards and their safety classifications. Also criteria and requirements to validate achievement of the defined safety class can be different. National regulators as STUK want to define their own requirements for the qualification process, to be able to carry out their monitoring and regulatory role.

Qualification of software intensive systems for nuclear power plant is needed in two different kind of contexts:

- Qualification of safety-critical systems. The main software reference standard is IEC 60880. Certification is often part of qualification (see section 7), especially for platform components. Safety category is mostly „A“, as defined in IEC 60880. SIL classification is normally not used directly, so SIL can be anything between 1– 4. Main focus is in product certification rather than process assessment, because of IEC 60880 and lisencing requirements.
- Qualification of safety-related systems. The main software reference standard is IEC 62138. Systems are normally industrial products, which can be used also in nuclear power plants after their qualification. Certification is normally not required in Finland for these systems, classified either in category B or C. Focus is mainly in process assessment, because of easier IEC 62138 and lisencing requirements.

Generic functional safety standard IEC 61508 uses term "safety-related” for any system. It can be used as additional reference and guidance for all kind of systems for nuclear power plants, belonging in safety category A, B or C. The term “safety system” should be used in category A systems.

One method for qualification of safety-related systems for nuclear power plants is called TVO SWEP (Software evaluation procedure). It has been developed originally during 2004 – 2006 as a joint effort of TVO, VTT Technical Research Centre of Finland and Finnish Software Measurement Association FiSMA. Main focus is systems in safety categories B and C. This article is mainly based on experiences from TVO SWEP in several deliveries for TVO.

During years 2007 – 2010 TVO SWEP was extended to safety-critical systems in safety category A. Many additional methods and techniques are needed to get required evidence. Quantitative understanding of product and safety is achieved by applying formal methods, like safety case.

2.2 Pre-qualification and qualification

The main phases of the qualification are **pre-qualification** and **application qualification**. SPICE is used mainly in the pre-qualification phase, together with relevant nuclear specific standards. Often pre-qualification covers the term certification. If needed, also application qualification is done, partly with the same methods. As a starting point, preliminary hazard analysis (PHA) is done as part of the user requirements definition step. A modified FMECA [9] method is used after PHA, and is maintained and completed during all qualification steps. Figure 1 shows the main steps of qualification and how it is integrated to main steps of system acquisition and development.

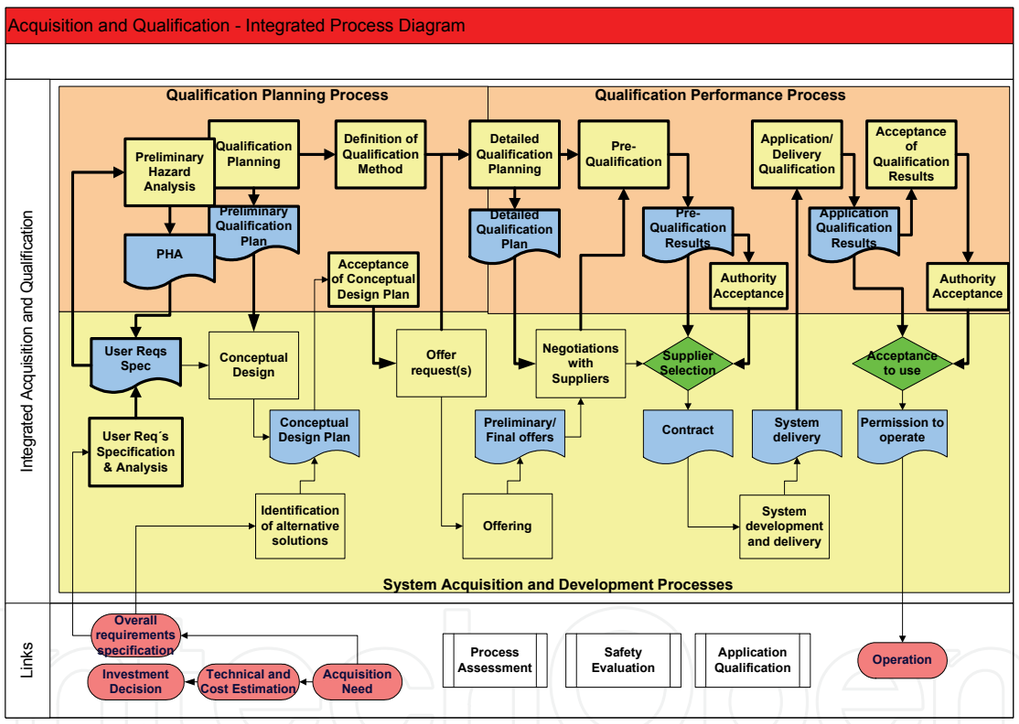


Fig. 1. The qualification process, integrated with I&C system acquisition

As Figure 1 illustrates, qualification is based on a detailed qualification plan. A typical input is PHA based on user requirements. It is very important to define safety requirements early in the acquisition process for each safety or safety-related function. When that is defined, the detailed qualification plan and tailoring of questionnaires can be done according to requirements.

Typically, the qualification needs a lot of technical data from system suppliers. Therefore the pre-qualification phase and necessary negotiations with system suppliers is in parallel with qualification planning. The suppliers are informed about the qualification, and are prepared to participate if needed.

Pre-qualification is meaningful to perform in full scale, if the system platform and the application are quite large systems and have typically several safety or safety-related functions. For small systems some less effort-intensive methods are used if possible. The pre-qualification is mainly a combination of detailed and evolved PHA, process assessment and conformance checks against necessary nuclear specific standards. Necessary documents are reviewed as part of assessment. Also verification and validation of technical documents and their safety functions are an essential part of the pre-qualification.
Qualification during application and system development is done when needed. As a process, it is quite similar as the pre-qualification. In most cases it includes further checks of system and application details. Also some additional requirements may evolve from selected normative standards. They may be identified during pre-qualification, but need more attention and evidence. Some typical topics are control of tests and their coverage during application development, and handling of system changes for each application.

3. ISO-based process assessment

ISO 15504 Part 5 (known as the SPICE model) is used in as the main source of process assessment in TVO SWEP method. The latest published ISO standard version ISO 15504 Part 5 is used as the baseline. Part 5 has all ISO 12207 processes and not all of them are relevant for qualification purposes. Many nuclear specific standards include quite similar concepts of processes as ISO 15504 Part 5, and they are also used as normative sources.
The workflow for process assessment shall satisfy ISO/IEC 15504 Part 2 requirements to be acceptable for qualification purpose. Workflow can be seen as combination of stakeholder responsibilities and main assessment phases. Figure 2 illustrates a typical workflow.

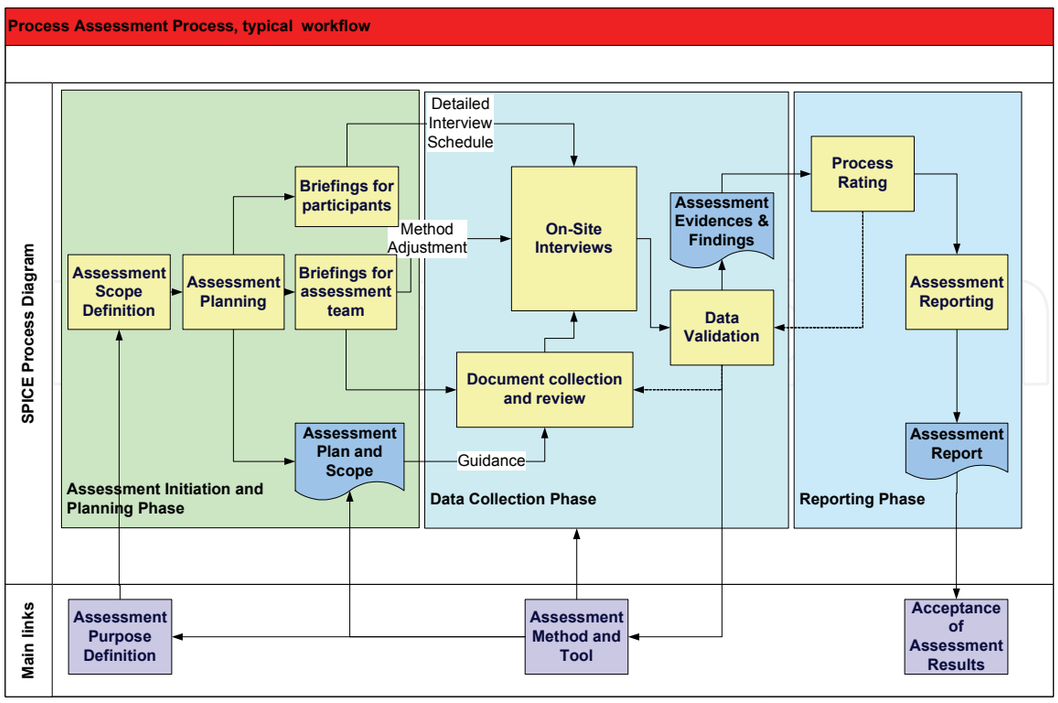


Fig. 2. A typical work flow of process assessment according to ISO/IEC 15504

The list of most relevant SPICE processes for qualification needs is presented in table 1. Not all SPICE processes are as relevant as others, and also the cost-effectiveness of process assessment indicates rather a short than complete list. The criterion for process selection has been alignment and integration of ISO 12207 processes and related nuclear specific standards in Table 1.

Process	Name	Main areas of integration with nuclear specific standards
ENG.1	Requirements elicitation	Detailed specification of safety functions and their SIL type according to PHA analysis results. Requirements for system testing.
ENG.2	System requirements analysis	Validation of each requirement, separate handling of safety requirements. Traceability.
ENG.3	System Architecture design	Allocation of each safety function. Overall architecture of the system. System validation planning.
ENG.4	Software requirements analysis	Specification and independent validation of each software function related to safety
ENG.5	Software design	Similarly as ENG.4. Planning of software verification tests.
ENG.6	Software construction	Module testing and documentation. Avoidance of unnecessary code.
ENG.7	Software integration	Test records. Validation of integration test results.
ENG.8	Software testing	Test records. Validation of software testing results.
ENG.9	System integration	Test records. Validation of system integration test results.
ENG.10	System testing	Test records. Validation of system test results.
ENG.11	Software installation	Installation test. Correct technical environment.
SUP.1	Quality assurance	Quality planning. Reviews and inspections at project level.
SUP.2	Verification	Independent tests and technical reviews.
SUP.3	Validation	Independent FAT and SAT tests.
SUP.7	Documentation	Done according to supplier's process and safety requirements.
SUP.8	Configuration management	Full traceability. Change control.
SUP.9	Problem resolution management	Full audit trail. Analysis of each defect and it´s impacts. Common causes of failures.
SUP.10	Change request management	Full change records. Analysis of each change.
MAN.3	Project management	Quality planning. Verification and validation planning.
MAN.4	Quality management	Quality management activities according to supplier's process.
MAN.5	Risk management	Avoidance of product related risks.
MAN.6	Measurement	Measurement-based testing and validation, if possible.

Table 1. List of typical SPICE processes used in process assessment and qualification

Each process is assessed up to capability level 3 or higher, if possible. Level 3 is considered as the required capability level, because only standard processes and an organisation-wide quality system is required for product oriented assessment in safety critical and –related systems. Some processes need a lot of refinements and elaborations to comply with safety-critical system context, and that is done as part of integration of SPICE and nuclear specific standards. In most cases, an interpretation of each SPICE element is not enough, also extension of the processes with additional practices or alternative checklists are needed.

The result of SPICE assessment is a capability level for each process and a number of evidences. They can be used as "mass evidence" for more detailed safety analysis. SPICE capability level is not always the best way to express the real capability of each process. Therefore also an "capability index" is calculated as a ratio of evaluated practices and their sum compared to target level of the process.
Conformance against nuclear specific standards and their safety requirements is done mainly in parallel with SPICE assessment. Most requirements are used as interpretation rules of base and generic practices of each SPICE process. Also complementary methods and evaluations are needed, especially in software and system validation.

4. Additional requirements for process assessment of safety-critical systems

4.1 Basic types of assessment

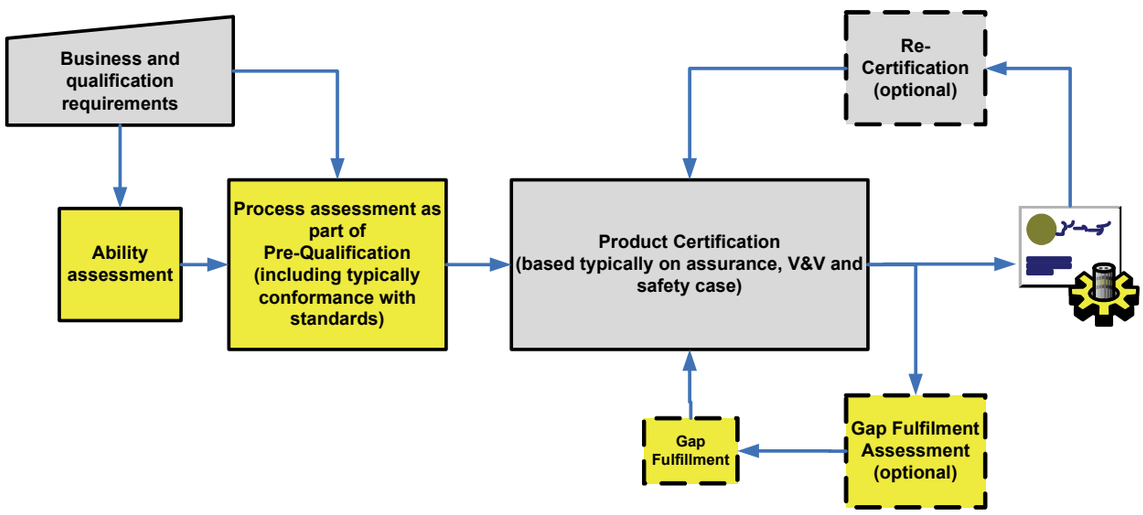


Fig. 3. Typical sequence of different process assessments (yellow boxes) during qualification and certification of safety-critical software

In CERFAS, we have specified three different basic types and "use cases" of process assessment (see figure 3). They are needed typically as a sequence:

- Short "ability assessment" to check overall readiness to develop and deliver safety-critical software. If overall ability of software organisation is low, then it leads to cancellation of the certification process or additional time to restart it. Document review is an essential part of this kind of light assessment.
- Full-scale "certification assessment" to support preliminary software qualification and provide evidence for software assurance and safety case during software certification process.
- "Gap fulfilment assessment" to prevent and fix potential causes of non-conformances of products and processes and their related risks when identified during certification process.

4.2 Ability assessment

Ability assessment is typically quite short, even only some days of effort. It can vary a lot, depending on the current level of software organisation and its products. Typical examples are:

- Assessment of software development processes (mainly ENG category in ISO/IEC 15504 Part 5).
- Review of core documentation or documents from a chosen specific topic, as evidences of process capability and conformance with selected reference standard(s).
- Conformance with selected reference standard(s), for example IEC 61508 Part 3, IEC 62138 or IEC 60880.

Quite often ability assessment is also a combination of several topics. To avoid heaviness and complexity of ability assessment, typical combination is only with two topics. An example could be conformance check + current implementation of bi-directional traceability.

4.3 Full-scale process assessment

Process assessment in CERFAS context is quite normal, SPICE – type process. Of course, it is more formal than most improvement oriented assessments. Evidences are collected and recorded systematically, and they are a solid basis for data collection, validation and ratings. Rigour of assessment is near to Scampi-A method in strictness and formalism [ARC1.2]. Results are reported as gaps to target level. Each gap can be classified by magnitude and risk, as defined in [ISO/IEC 15504-4].

One additional stakeholder in process assessment is the certification body. Typical responsiblity is that customer organisation orders certification from a certification body. They decide together which references and methods are used in certification. One basic requirement is independent team for process assessment. Each team member has to fulfil competence requirements. Stakeholders and their relationships in qualification/certification driven process assessment are presented in figure 4.

One other additional requirement is satisfaction of accreditation rules. They are defined in ISO17020 family of standards. Most requirements for process assessment are same as for management system standards (for example ISO 9001). Assessment process must be documented and include competence requirements. Assessment must contain audit trail between assessment phases and intermediate results. Finally, if assessment leads to process certificate, it must be publicly available for intended audience.

Most of accreditation requirements are built in process assessment standards and models. Both SPICE and CMMI model families have such guidance. A specific variant of full-scale process assessment is use of CMMI safety extension as a reference model [+SAFE]. It has two process areas focused on safety, namely Safety Management and Safety Engineering.

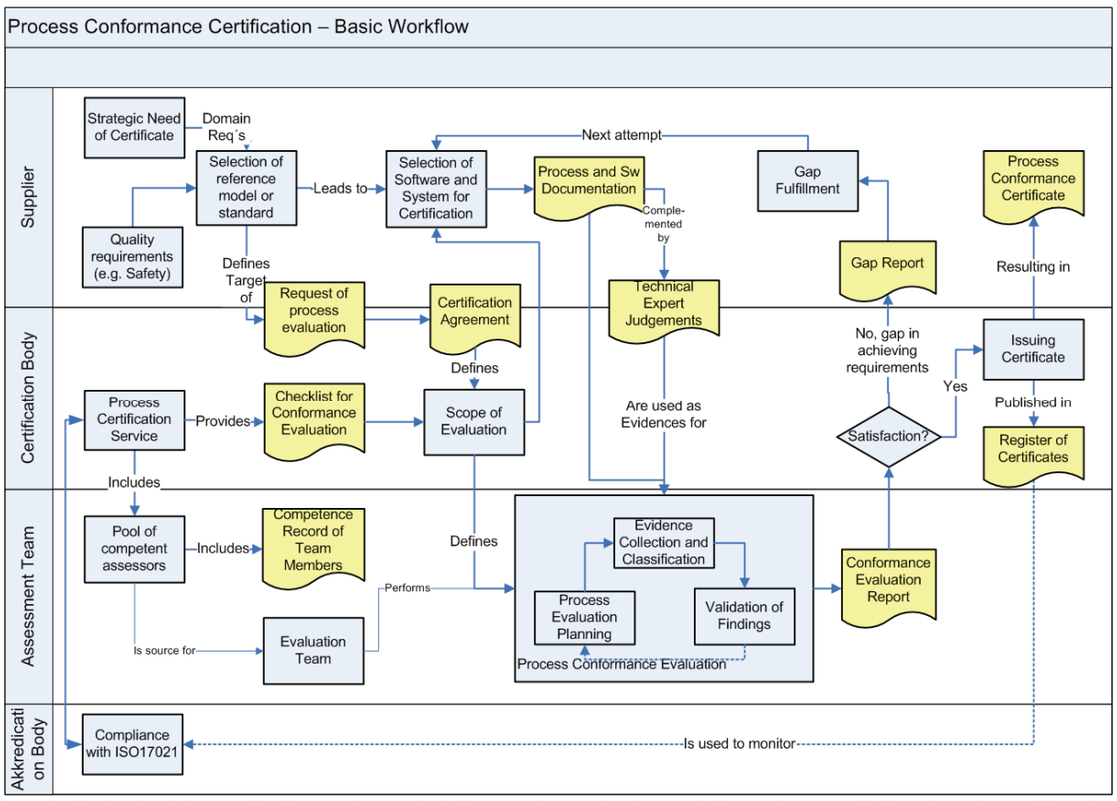


Fig. 4. Stakeholders, their main activities and typical workflow in qualification/certification oriented process assessment and conformance evaluation

ISO working group for process assessment [ISO/IEC JTC1 SC7/WG10] is developing a new reference and assessment model for safety related software domain, called ISO/IEC 15504 Part 10: Safety extension [ISO/IEC 15504-10]. The assessment model includes three new processes to be assessed. Two processes, Safety Management and Safety Engineering, follow the contents of CMMI safety extension. The third process, Tool Qualification, explicitly stresses the importance of the tools used to build safety related software. The assessment model is aligned with some selected safety standards. At the time of writing those are ISO/IEC 26262, IEC 61508, IEC 60880 and UK MoD Def Stan 00-56. In addition to the new processes, there will be also guidance on how to interpret software engineering processes of ISO/IEC 15504-5 and -6 in an assessment in safety related domain.

4.4 Gap fulfilment assessment

Third basic type of process assessment in CERFAS context is check of process improvements needed to get product certificate. This is needed in such cases that software is incomplete or erroneous during any phase of certification. Typical example could be design errors found during independent tests. Then the software organisation needs to change specification and/or design process so that errors can be prevented in advance or detected during design phase. Typical process improvement would be better inspection or quality assurance during early phases of software lifecycle. Sometimes also more formal process would be needed, maybe with model checking type quality assurance. These changes in development process

must be verified, and one easy and straightforward way is focused process assessment. There is nothing specific compared to normal SPICE – type process assessment in this phase.

4.5 Consolidation of process assessment in safety case analysis

In many industry areas, including nuclear industry, the safety of the system is documented in one or more safety cases. Bishop et al. define safety case as "A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment" [Bishop1998]. One of the key characteristics common to safety case and process assessment is that they both rely on objective evidences. Typically these evidences are more or less the same ones, but assessment and safety case might look after different aspects from the evidence. For example for code review report, process assessment view might see that the review is done according to process, software measurement view calculates the total coverage of code review and module testing, and competence view checks if the reviewers have had appropriate skills for the task, as shown in Figure 5.

Assessment result as such (full or partial result sets, or risk analysis based on the gaps) can also be used as evidence in safety case, claiming that system is (or is not) programmed properly, and thus increase the confidence that the overall system is (or is not) safe. For example, one might be more confident on the quality of the end product, if engineering processes are at capability level 3 rather than 1.

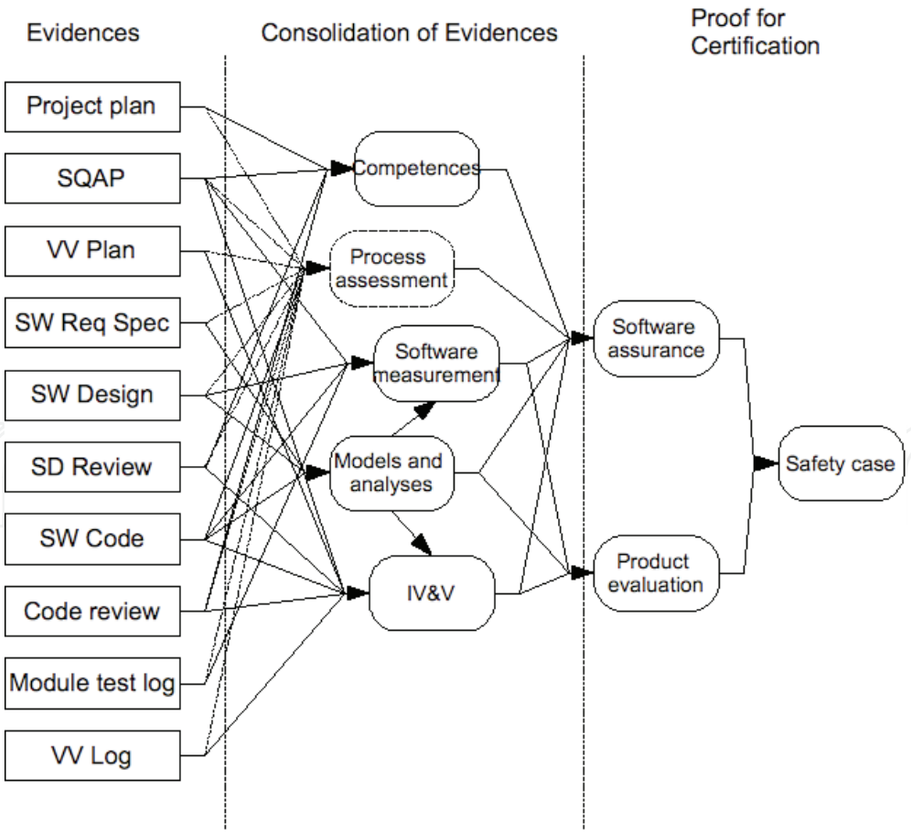


Fig. 5. Same evidences are consolidated into different modules for certification. The final claim that system is (or is not) safe consists of one or more safety cases.

How the actual consolidation is done is still in a conceptual phase. Any of the standards does not give detailed requirements. For example, they can require a certain metric to be collected, but the target values of the metrics are not defined. Also, the modules in Figure 5 could be arranged and linked in many ways, for example so that the "final result" would be Software Assurance Case.

5. Product safety evaluation with Tiira method

5.1 General

The starting point for safety analysis in TVO SWEP method is PHA (Preliminary Hazard Analysis). It defines the need for evidences to achieve required detection level for potential failures.

Tiira starts during or after the requirements specification phase. FMECA is used in requirements specification phase because it is important to

- evaluate as early as possible the failure modes of the I&C system/software in design and development project. The later the phase, the more difficult it is to find consequences of the failure mode and so estimate risk.
- follow the detection of potential software defects in sequential phases of design and implementation. Note. See later slides for the concept of detection.
- identify highest contributor to failures and follow how they are eliminated. This also means on early concentration of important factors of safety related failure modes.
- identify for reducing probability of failure occurring.

In TVO SWEP there are two important specialties of occurrence of causes of failure modes. The first, occurrence is related only to the hardware faults. Hardware faults are not analyzed by Tiira, meanwhile, it is presupposed that occurrence of the I&C system will be calculated and the target value (SIL) is replaced as occurrence number. The second, systematic errors are analyzed by Tiira with the concept of detection.

5.2 Basic principles to perform Tiira

Tiira is a risk-driven analysis tool with which we can identify failure modes of I&C systems caused by potential software faults. In addition to failure modes, Tiira identifies potential effects and causes, and means to mitigate risk.

In Tiira, so called APN (Action Priority Number) is used [ref. FMECA IEC 60812]. APN is composed of three numbers: Severity (SEV), Occurrence (OCC) and Detection (DET). Numbers SEV and OCC are determined from plant or equipment under control. The number DET is determined in knowledge how well we can observe occurrence of the potential failure mode due to software fault. Many factors affect to the number DET, e.g. capability of development process, test processes, and test results (coverage), designs (fault tolerance, fault avoidance, etc.). The number DET is the most important APN factor controlled by Tiira.

5.3 FMECA sheet used in Tiira

The set of hypothetical failure modes is reduced to a set of meaningful failure modes by discarding those for which the APN is enough low.

Based on original safety requirements, each potential failure is classified according to its severity, using for example 1 – 5 scale. Similarly, also the probability of occurrence and required detection rate are classified 1 – 5. SIL levels from IEC/EN 61508 are used as a reference to map each safety function and its required detection rate. As a result, these factors are multiplied into APN number. The calculated APN for each potential failure indicates, how much evidence is needed to achieve acceptable level of failure detection and so the APN as a whole. Figures 6 and 7 explain in more details most important method features.

Figure 6 presents a Tiira sheet with one example. Explanations of existing conditions per column are:

- 8. Severity number SEV: ”How bad are the consequences of the failure mode?”
- 9. Occurrence number OCC: ”What are the chances of the failure mode or the cause actually happening?” In Tiira-table, OCC-number is provided mainly for electronic, mechanics, etc.
- 10. Detection number DET: ”What is the chance of catching the failure mode before it reaches the next operation or the customer?” For occurrence of software faults, DET-number is most important because control actions have impact on it more than SEV and OCC. In fact, SEV number remains the same during analysis.
- 11. Action Priority Number = SEV x OCC x DET
-

1 Ref.	2 Entry code	3 Potential failure mode (FM)	4 Effect on	5 Potential effect (E)	6 Potential cause (C)	7 Risk controls (RC)	8 Sev	9 Occ	10 Det	11 APN	12 Recommended action	13 Action taken	14 Sev	15 Occ	16 Det	17 APN
General	0	The irradiated fuel is too near the w ater surface of the pool	Safety	Danger of radiation for people at the pool	1. Operator drives the w agon too near the surface 2. Risk Controls are failed	1. Failure detection by operator at the pool, DET-1 2. Manual emergency stop, OCC-½ 3. Hardw ired emergency stop, OCC-1 4. Mechanical stop, OCC-1 5. Position alarm of the mechanical stop, DET-½ 6. Brake system 7. Radiation alarm, DET-½ 8. Lock keys	5	2,5	3	37,5	1. Position detection of the mechanical stop 2. Radiation protection 3. Programmable safety stop 1-3: OCC-1	For further SW error detection evaluation, DET-1	5	1,5	2	15

Fig. 6. Use of severity, occurrence and detection variables to calculate APN. An example of one potential failure mode is presented just for illustration.

Figure 6 has one example potential failure mode. Analysis of it gives result APN value 37,5. Highest acceptable value is 25 using 1 – 5 scale, because result of maximum values in SEV x OCC x DET equation is 5 x 5 x 1 = 25. So, some additional controls are needed. They are specified in columns 12 and 13, leading to new APN value 15, which is acceptable. As seen from columns 15 and 16, both OCC and DET values have been changed to reach accepted value.

5.3 Evidence collection and analysis in Detection Table

Figure 7 is a sample from a so called Detection Table of the TVO SWEP method. Figure 7 shows only app. 40 lines from total of 200 items to improve failure detection. The full Detection Table covers software life cycle and related QA and V&V activities. It covers also all SPICE processes in table 1.

	Total reduction detection number: 1		
		APPLICATION	
	Total average	0,72	0,71
Factors for verification rate		0,93	0,93
r	Size of the project	1	1
r	Degree of complexity of the design	1	1
r	Degree of novelty of the design	1	1
r	Degree of novelty of the technology	0,66	0,66
r	SIL	1	1
Verification of deriving the I&C requirements		0,92	0,66
SPICE	Pre-Q of the process, ENG.1 Req.s elicitation	0,66	0,66
r	Walkthrough of functional, performance and independence re	1	0,66
r	Walkthrough of the categorisation requirements, interfaces,	1	0,66
r	Walkthrough of plant constraints	1	0,66
Verification of I&C specification		0,83	0,77
SPICE	Pre-Q of the process, ENG.2 System requirements analysis	0,91	0,91
SPICE	Pre-Q of the process, ENG.3 System architecture design	0,92	0,92
r	Walktrough of the I&C architecture	1	1
r	Walktrough of functions assignment	1	1
r	Walktrough of required analysis	0,33	NA
o	Formalised descriptions of system specification		
o	Review of traceability and consistence (TA)		
Verification of system detailed design and implementation		0,00	0,00
r	Walktrough of system design	NA	NA
r	Walktrough of system implementation	NA	NA
o	Review of traceability (TA)		
Verification of SW Requirements Specification, SRS		0,96	0,96
SPICE	Pre-Q of the process, ENG.4 Software requirements analysis	0,88	0,88
r	Walkthrough of SRS	1	1
r	Walkthrough of interfaces with HW, users, etc.	1	1
o	Analysis of SRS (Formalised descriptions)		
o	Prototyping of SRS requirements		
o	Review of traceability (TA)		
Verification of system test plans		1,00	1,00
r	Inspection of test plan	1	1
o	Review of traceability (TA)		
Verification of SW Design Specification, SDS		0,76	0,54
SPICE	Pre-Q of the process, ENG.5 Software design	0,91	0,91
r	Review of SDS (Walkthrough or Inspection)	0,66	0,66
r	Assessment of performance parameters (Proto)	0,66	0
r	Traceability of allocated functions (TA)	0,66	0
r	Assessment of data required (Inspection)	0,66	1
r	Analysis of fault tolerance (Inspection)	1	0,66

Fig. 7. A sample from an Excel based checklist to calculate detection index DET. An example is presented just for illustration.

Detection Table summarizes qualification findings in a composite index called "Total detection number DET". The idea is to use DET index as load or backing evidence in FMECA sheet (Column 10 – Column 16 in Figure 6). The table is separate for Pre-Qualification and Qualification phases. In most cases it is also separate for Platform and Application. Evidence in each phase is gathered by process evaluation (SPICE) and product safety evaluation (FMECA). Also compliance with nuclear specific standards is taken into account here.

SPICE capability level is converted to capability index, which summarizes detailed practice ratings at levels 1 – 3 for each process. It is normalized to get values between 0 – 1 for each capability level. Other evidences are detailed requirements from V&V processes, as defined in IAEA report no. 384 [6].

In the example of Figure 7, we present two columns for DET and its inputs. The right column is for the pre-qualification phase and the left column for the additional nuclear specific verification of the application. The pre-qualified system was in this case a radiation monitoring equipment. As seen in the example, also NA (Not Applicable) rating is allowed and used, if relevant input data or rating result is not available. Similar table is often needed also for the software platform.

In most cases the Severity and Occurrence parameters remain the same and only failure detection rate can be improved. As a result, Action Priority Number APN may reach an acceptable level. In our example (see columns 11 and 17 in figure 6) the goal was that each potential failure has APN value 25 or less. In our example that is the case, and the qualification has been successful. DET value has changed from 3 to 2, and Detection Table in figure 7 shows that we have achieved this one level reduction by a large amount of evidences and actions.

Finally, the aim is to determine the Reduction Detection Number RDN. RDN is typically a difference between DET number at FMECA table (see columns 10 and 16 in Figure 6 as an example). RDN can get a value 0 – 4. The Detection Table calculates the value of RDN automatically, based on the SPICE and V&V evidences. Calculated RND value is then used in Tiira FMECA table to reduce Detection rate. The index limits for for RDN value 0 - 4 are: <0.60, 0.60 – 0.74, 0.75 – 0.89, 0.90 – 0.98. 0.99 – 1.0.

6. Certification to support qualification

In Finland, a type acceptance certificate is required mainly in highest safety class of I&C equipments and systems in Nuclear Power Plants, and recommended in lowest safety classes. In the research project "Certification facilities for software (CERFAS)", the objective is to develop a Software Certification Service, SCS, able to certificate safety critical software for the demands in Finnish nuclear area. The framework of SCS is described in Figure 8.

Certification can be defined as "the process of assessing whether an asset conforms to predetermined certification criteria appropriate for that class of asset" [10]. This idea of conformance with criteria is the fundamental principle of certification. Certification is documenting compliance of a product and product development process to a standard such as IEC 60880 and IEC 61508 within a defined but possibly broad set of potential applications. In general, certification is seen in CERFAS as a service to support qualification and further licensing (Figure 8). Qualification includes a system qualification and an application qualification. The system qualification is documenting a justifiable argument to attain an

operating license for the complete realized system. On the other hand, the application qualification is documenting functional safety suitability for a specific system product in a specific target application.
Various areas of methods, standards and justification means are needed to support certification. Some examples are process assessment, product evaluation and use of different analyses and tests. For certification, an accredited Certification Body is needed. Type testing or other kind of Independent Verification and Validation (IV&V) is typically a fundamental part of the certification. Any CB needs a variety of services to run a certification service and to integrate different approaches as a coherent system.
Each certification type has its own assessment elements. The framework in CERFAS assumes that certification is based on some reference model, norm or set of criteria. Certificate itself is then a conformance statement against those requirements. Typically, such statement is justified by some methods, which include external audits, IV&V's, reviews and inspections, code analysis and type tests. Safety cases provide a formal argument to justify that a system is safe [11].

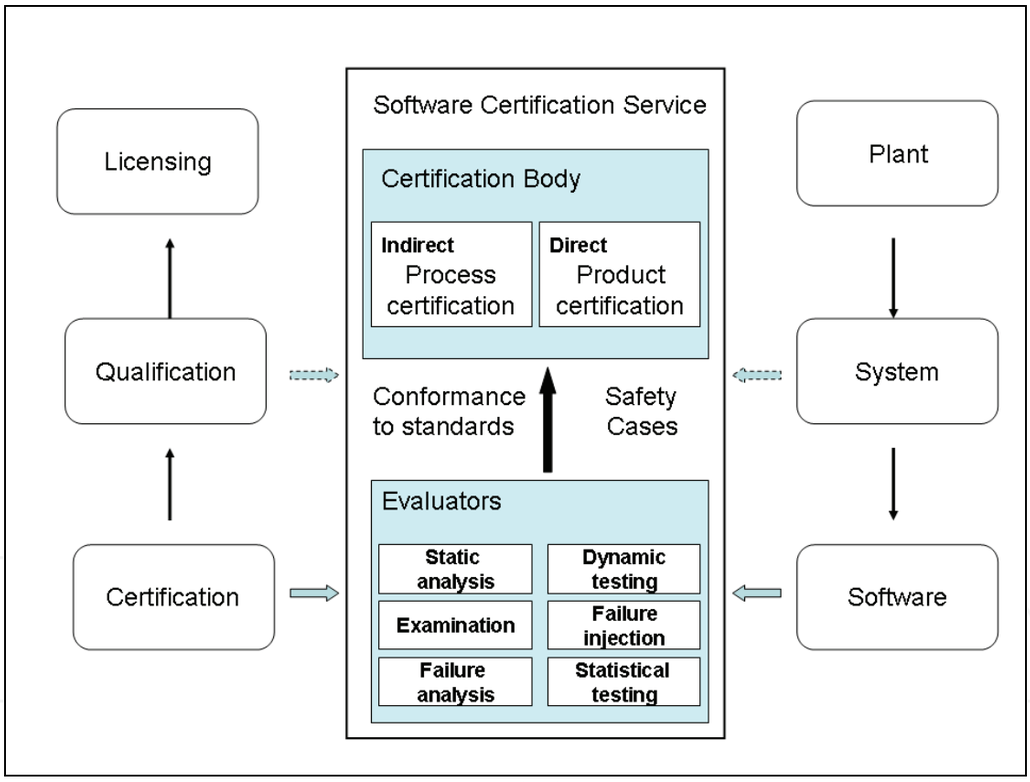


Fig. 8. CERFAS gives facilities for SCS including Certification Bodies and evaluators. Conformance to standards or other predetermined criteria is fundamental principle of certification.

7. Conclusions and future developments

Several real-life qualifications are already done by using TVO SWEP method. The goals of the method are achieved well, and the pre-qualification is effective. It is evident that TVO

SWEP needs still refinements and additional validation. Main difficulty is to collect evidences so systematically, that the necessary calculations and reports could be done as automatically as possible. Then the main focus can be in professional topics and may lead to useful win-win findings between TVO and the supplier.
Additional methods for software certification are also validated with real life cases. Certification is needed mainly in safety-critical systems. Attention is more in product evaluation than process assessment. Evaluation process is quite rigor and formal. Main form of results has been safety case, which quantifies all kind of evidences.
Other industries may have quite similar needs for qualification as nuclear power plants. For example control of railway and metro networks and traffic, electro medical devices like patient control systems and many military systems could be users of our method. Many standards are also under development, and can be seen as "second generation" of safety-critical systems. Some examples are ISO 26262 for vehicle industry and European standards for space industry (ECSS).

8. References

YVL 5.5, Instrumentation systems and components at nuclear facilities. STUK 2002. IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety – General Requirements for Systems. 2001.IEC 62138, Nuclear Power Plants Instrumentation and Control Computer-based systems important for safety Software for I&C systems of safety classes 2 and 3. 2001.

ISO/IEC 15504 Part 5. An Exemplar Process Assessment Model. 2006.

Safety Guide, Software for Computer Based Systems Important to Safety in Nuclear Power Plants. 2000.

IAEA 384, Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control. 1999.

IEC/EN 61508, Functional safety of electrical/electronic/ programmable electronic safety-related systems. 1998.

Common Position of European Nuclear regulators for the licensing of safety critical software for nuclear reactors, EUR 19265, 2000.

Harju, H. Ohjelmiston luotettavuuden kvalitatiivinen arviointi (The qualitative assessment of software dependability, Tiira method). VTT Technical Research Centre of Finland. VTT Research Notes 2066. 2000.

ISO/IEC 24765, Systems and software engineering vocabulary. 2009.

P. G. Bishop and R. E. Bloomfield. A methodology for safety case development, in Safety-Critical Systems Symposium, Birmingham, UK, Feb. 1998.

Author CVs

Risto Nevalainen

Director of Finnish Software Measurement Association FiSMA and Spinet Oy.
Mr. Risto Nevalainen (Lic. Tech.) has long experience in software measurement and quality topics. His working experience includes position as managing director of Finnish Information Technology Development Center during 1989-1995. Before that he had different research and management positions for example in Technical Research Centre (VTT),

Technical University of Helsinki (HUT) and Finnish Prime Minister's Office. Mr. Nevalainen has participated in ISO15504 (SPICE) standard development since beginning. He is Competent SPICE Assessor and ISO9001 Lead Assessor. Risto Nevalainen is co-editor of ISO/IEC 15504 Part 5 upgrade.

Juha Halminen

Qualification and Commissioning Engineer in TVO.

Mr. Juha Halminen has ten years experience in nuclear equipment quality topics. His working experience includes qualification of new equipment with or without software to nuclear power plant safety systems. He has been the key person in developing software qualification procedures for TVO. He also works as a commission inspector of nuclear power plant safety systems. Mr. Halminen has performed assessments and audits using SPICE, ISO 9001, IEC 62138, IEC 60880 and KTA 3507. He has participated in MAGIC project from 2006 to 2008. Before that he was participated in business development work in Russia. During 1994-1995 he was researching influence of contamination and humidity to building stones, concrete and mortar in IBW Germany.

Hannu Harju

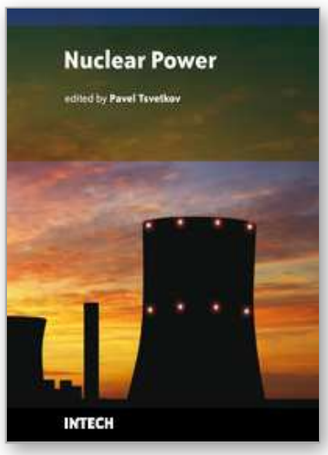
Senior Research Scientist in VTT

Lic.Tech. Hannu Harju has long experience of critical control systems and software. He has been as an assistant professor of system theory at Technical University of Lappeenranta and as a chief evaluator of control systems and software at Certification Department of Inspecta.

Mika Johansson

Inspector, Radiation and Nuclear Safety Authority Finland, on two year term from 2010 to 2012. Partner and co-founder, Spinet Oy.

Mr. Mika Johansson (M.Sc (Eng)) has been working as a trainer and consultant in quality and project management areas for more than ten years. He has been Executive Director in Finnish Software Measurement Association FiSMA from 2006 to 2010. In Spinet Oy, Mr. Johansson has performed assessments and audits using SPICE, CMMI, ISO9001, ISO/IEC 20000 and safety specific models since 2003. He has been part-time researcher in Tampere University of Technology in CERFAS project from 2007 to 2010. Mika Johansson is co-editor of ISO/IEC TR 15504-10 Safety Extensions.



Nuclear Power

Edited by Pavel Tsvetkov

ISBN 978-953-307-110-7

Hard cover, 388 pages

Publisher Sciyo

Published online 17, August, 2010

Published in print edition August, 2010

The world of the twenty first century is an energy consuming society. Due to increasing population and living standards, each year the world requires more energy and new efficient systems for delivering it. Furthermore, the new systems must be inherently safe and environmentally benign. These realities of today's world are among the reasons that lead to serious interest in deploying nuclear power as a sustainable energy source. Today's nuclear reactors are safe and highly efficient energy systems that offer electricity and a multitude of co-generation energy products ranging from potable water to heat for industrial applications. The goal of the book is to show the current state-of-the-art in the covered technical areas as well as to demonstrate how general engineering principles and methods can be applied to nuclear power systems.

InTech Europe

University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China

Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen