Additional Requirements for Process Assessment in Safety-Critical Software and Systems Domain

Mika Johansson ¹; Risto Nevalainen²

¹ Tampere University, Pori Unit, Finland
and FiSMA ry, Finland
² FiSMA ry, Finland

Abstract
Certification of safety-critical software is a multi-disciplinary topic. Process assessment is an essential part of that, but is not enough for software certification. Certification employs also several other method families, like inspections and reviews, independent V&V, conformance with selected reference standard(s) and use of selected measurements and analyses.

Process assessment supports directly qualification of safety-critical applications but is less relevant for certification of platforms and environments. Anyway, qualification and certification are closely related, because certification as a whole supports qualification and makes it more effective. It is possible to adapt and evolve process assessment so, that it supports both qualification and certification.

Typical process assessment is done for improvement purpose. In qualification and certification that is not so relevant as conformance and management of risks. In this paper we discuss about possibilities to develop process assessment to achieve that goal. In most cases assessment is a combination of several approaches.

Keywords
Safety-critical software, process assessment, conformance with standards
1 Introduction

"National Nuclear Power Plant Safety Research 2007-2010, SAFIR2010" is a Finnish four-year research programme. The objective of the programme is “to develop and maintain the nuclear safety expertise and deterministic and probabilistic methods to assess safety so that new matters related to nuclear safety appearing their significance can be assessed without delay” (SAFIR2010 2006). The planning period for national research on nuclear power plant safety up to 2010 contains granting licenses for the four power plants in use and that under construction. Know-how developed in publicly funded research programmes can be applied in licensing processes.

A research area of automation and control room in the research programme includes three on-going research projects, one of which is the “Certification facilities for software, CERFAS”. The main purpose of CERFAS is to develop facilities for a consortium called Software Certification Service. Conditions for services of consortium are the application of diverse expertise and effective evaluation tools. This leads into networking both in the project and in the certification services.

Certification can be based both on generic sets of criteria and domain specific requirements. Our goal is to combine these two approaches. Most important nuclear specific requirements are standards, which include requirements for safety critical systems and software. The most relevant is IEC60880, which can be used also directly as a reference for certificate. Qualification and licensing of safety class 2 I&C systems includes a conformance statement against IEC 60880, and that is already a kind of certificate. The other main reference is IEC 61513, which is based on generic IEC 61508 (functional safety). [Harju2008]

Figure 1: Main areas of topics in CERFAS project [Harju2008]
In process assessment we apply ISO/IEC15504 in quite similar way as in several other domains (automotive, medical devices, space for example). Anyway, process assessment does not work in isolation and is not enough as such. It needs to be integrated with several other approaches in software certification, as safety cases, conformance assessment and software measurement. These topics are covered in chapters 3 – 5 of this article. The concept is illustrated in Figure 2, showing some typical process assessment related topics.

Figure 2: Process assessment related topics in safety-critical software domain.

Figure 2 contains two types of topics. Some of them (clouds in figure 2) are heavily interconnected and are always part of process assessment, more or less. For example, development process defines directly what are the most important processes in assessment scope. Again, it defines what is the most essential documentation. It leads to product evaluation. Conformance with standards is always in core of certification, because certification is based on some defined reference.

Some topics are more focused (some typical ones are shown as circles in figure 2). They are sometimes mandatory elements in certification, like proper validation of development tools. Some others are more judgement-based, like human competences and their role in developing and validating safety-critical software. Traceability and product metrics are examples of topics, which have high relevance as evidences for safety case. Note that only some relationships (arrows) are presented in figure 2, mainly for illustration purpose.

2 Additional requirements in process assessment

2.1 Basic types of assessment

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.

- 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.

Figure 3. Typical sequence of different process assessments during qualification and certification of safety-critical software

2.2 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 IEC61508 Part 3 or IEC60880.

Quite often ability assessment is also a combination of several topics. In Figure 2 we presented some of them. 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.

2.3 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/IEC15504-4].
One additional stakeholder in process assessment is the certification body. Typical responsibility is that customer organisation orders certification from a certification body. They decide together which references and methods is 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.

![Process Conformance Certification – Basic Workflow](image)

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

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 ISO9001). 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.

### 2.4 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.

3 Additional requirements in models and references

3.1 Standards for safety-critical software and systems

In CERFAS context the primary standard for safety-critical software is IEC 60880, software aspects of computer-based systems performing category A functions, or in Finnish legislation, safety class 2 (the highest one were digital systems are allowed). IEC 60880 sets requirements and also recommendations for the development processes. Each phase of the lifecycle is addressed. The largest amount of requirements is in software design and construction topics. In the latter there are special clauses for tools and 3rd party software components like COTS.

Although many requirements of IEC 60880 are for processes, the standard claims that the most important aspects of software safety are two product-related technical features or design principles, namely self-supervision and avoidance of common cause failures. The annexes have very detailed design and programming requirements for the software product, from architectural approach to the memory usage.

The other standard used is IEC 61508, functional safety of electronic systems. The part 3 addresses software, while part 1 defines general requirements for functional safety management system. As in IEC 60880, the software lifecycle has been divided into phases, and there are specific requirements for each phase.

Although IEC 61508 claims that it is for safety related systems, some of the requirements are more strict than in safety-critical IEC 60880. For example, competences must be managed in more details, verifications are stricter and there must be independent audits during the project.

Neither of these standards have the concept of process capability nor maturity. Safety integrity levels in IEC 65108 are not comparable on process capability levels by any means. Requirements can only be divided into mandatory and optional ones, and they are either fulfilled or not. [IEC60880] [IEC61508-1] [IEC61508-3]

There are lots of other standards, from IEC 61508 based domain specific standards to many military models, but these have not been included in CERFAS.

3.2 Additional processes in generic PAM models

The software lifecycle phases in IEC 60880 and in IEC 61508 are rather basic ones, and they can be easily mapped to ISO/IEC 15504-5 processes and process' indicators. These standards include are also some requirements, where existing ISO/IEC 15504-5 processes are too open for interpretation, or are non-existent.

In the Table 1, most relevant ISO/IEC 15504-5 processes are listed, and they are mapped with most suitable chapter(s) in safety standards [Halminen 2007]. In the end of the table there are some requirements, which are not addressed in detailed enough way in part 5. These new process areas are software security, pre-developed software (PDS), development tools and safety life cycle management [Johansson 2009].

PDS and tools could be assessed using existing SUP.6 Product evaluation, but the process doesn't explicitly bring up multiple phases of the evaluation process, nor very important aspect in safety development, analysing and collecting the operational (usage) history data. Safety lifecycle management could be assessed using MAN.3 Project management with many additional notes, but since it is one of...
the key processes, it is better have own process for it. This process can also be used as one option for the ability assessment. Security is not addressed in part 5 at all. In practice, the content of the process is about requirements management, but it seems that there are benefits in separating safety or security requirements management from normal requirements. The last row, functional safety assessment, has been left out in CERFAS context, since the assessment is (typically) performed by an independent organisation. [Johansson2009].

Interesting finding is that measurement is not not a separate topic in safety standards. Many kinds of analyses are required, and they require lots of collected data. In this topic safety standards belong to previous generation and need to be updated. ISO/IEC 25000 standard may help in this, because it provides a quality model and a set of measures for software and systems. Safety is one topic there, but not yet well covered.

<table>
<thead>
<tr>
<th>ISO/IEC 15504-5 Process</th>
<th>Process Name</th>
<th>IEC 60880 ref.</th>
<th>IEC 61508-3 ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENG.1</td>
<td>Requirements elicitation</td>
<td></td>
<td>In IEC 61508-1</td>
</tr>
<tr>
<td>ENG.2</td>
<td>System requirements analysis</td>
<td></td>
<td>In IEC 61508-1 and – IEC 61508-2</td>
</tr>
<tr>
<td>ENG.3</td>
<td>System Architecture design</td>
<td></td>
<td>In IEC61508-2</td>
</tr>
<tr>
<td>ENG.4</td>
<td>Software requirements analysis</td>
<td>6.1, Annex A</td>
<td>7.2</td>
</tr>
<tr>
<td>ENG.5</td>
<td>Software design</td>
<td>7, Annex A, Annex B</td>
<td>7.4.2, 7.4.3, 7.4.5</td>
</tr>
<tr>
<td>ENG.6</td>
<td>Software construction</td>
<td>7, Annex B</td>
<td>7.4.2, 7.4.6, 7.4.7</td>
</tr>
<tr>
<td>ENG.7</td>
<td>Software integration</td>
<td>7</td>
<td>7.4.8</td>
</tr>
<tr>
<td>ENG.8</td>
<td>Software testing</td>
<td>8</td>
<td>7.4.8</td>
</tr>
<tr>
<td>ENG.9</td>
<td>System integration</td>
<td>9</td>
<td>7.5</td>
</tr>
<tr>
<td>ENG.10</td>
<td>System testing</td>
<td>9.3</td>
<td>7.3, 7.7</td>
</tr>
<tr>
<td>ENG.11</td>
<td>Software installation</td>
<td>12.1</td>
<td></td>
</tr>
<tr>
<td>SUP:1</td>
<td>Quality assurance</td>
<td>5.5</td>
<td>7.1</td>
</tr>
<tr>
<td>SUP:2</td>
<td>Verification</td>
<td>8</td>
<td>7.9</td>
</tr>
<tr>
<td>SUP:3</td>
<td>Validation</td>
<td>10</td>
<td>7.7</td>
</tr>
<tr>
<td>SUP:7</td>
<td>Documentation</td>
<td>Annex F</td>
<td>5</td>
</tr>
<tr>
<td>SUP:8</td>
<td>Configuration management</td>
<td>5.6</td>
<td>6.2.3</td>
</tr>
<tr>
<td>SUP:9</td>
<td>Problem resolution management</td>
<td>9.4, 10.4</td>
<td>(7.8)</td>
</tr>
<tr>
<td>SUP:10</td>
<td>Change request management</td>
<td>11</td>
<td>7.8</td>
</tr>
<tr>
<td>MAN.3</td>
<td>Project management</td>
<td>5.3, 5.4</td>
<td>7.1</td>
</tr>
<tr>
<td>MAN.4</td>
<td>Quality management</td>
<td>5.5</td>
<td>6</td>
</tr>
<tr>
<td>MAN.5</td>
<td>Risk management</td>
<td></td>
<td>61508-1</td>
</tr>
<tr>
<td>MAN.6</td>
<td>Measurement</td>
<td>(some metrics in Annex B)</td>
<td></td>
</tr>
<tr>
<td>New process</td>
<td>Software security</td>
<td>5.7</td>
<td>(weakly in IEC 61508-1)</td>
</tr>
<tr>
<td>New process</td>
<td>Development tools</td>
<td>7.2, 14</td>
<td>7.4.4</td>
</tr>
<tr>
<td>New process</td>
<td>Pre-developed software</td>
<td>15</td>
<td>Annex D</td>
</tr>
<tr>
<td>New process</td>
<td>Safety lifecycle management</td>
<td>5 (partly)</td>
<td>7.1.2 IEC 61508-1</td>
</tr>
<tr>
<td>NA</td>
<td>Functional safety assessment</td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Mapping between 15504-5, IEC 60880 and IEC 61508 [Johansson2009]
4 Additional requirements in assessment results

4.1 Conformance vs capability results

Conformance result is typically flat and linear, based more or less Yes/No scale. Each non-conformance is recorded separately and the evaluation result consists mainly from those findings. So, it is a kind of list of negative findings. This kind of evaluation is typical when an organisation is evaluated against some requirement standard. Typical example would be ISO9001 or ISO20000 audit.

Process assessment result is much more structural. It consists from a list of processes, and each of them has a number showing the achieved level. Additionally, each process may have more technical results, like process attribute ratings. Rating scale is more continuous, as a minimum 4-point NPLF scale. SPICE- and CMMI-models have also an additional presentation, organisational maturity.

Safety standards, like generic IEC61508 and nuclear IEC60880, are conformance oriented. They may have and/or require also advanced calculations and analyses, for example to evaluate reliability of software and system. IEC61508 is done around concept of safety integrity level, and typical SIL is 3 or 4 for safety critical systems. It employs typically a set of corrective and preventive actions to achieve required reliability.

The regulatory authorities primarily need conformance results, to ensure that the system fulfils legal requirements. Finnish regulator in nuclear power industry (STUK) has its own requirements for licensing of safety-critical systems, called YVL5.5. It has requirements for technical processes and V&V, and they can be covered by conformance models. But YVL5.5 has requirements also for (quality) management system in the supplier organisation. That leads to some kind of combined multi-model solution, to cover all YVL5.5 requirements.

The licensee organisation is interested, in addition to conformance results, in the basic process capability results with risk analysis based on gaps. That can be done in several ways, but capability determination mode of ISO/IEC15504 is one specific and sophisticated model for that.

Combination of conformance and capability result is possible to achieve by classifying each evidence in both model types. Also models must be mutually mapped to cover all requirements. One problem in mapping is, that generic requirements are often more abstract and then more open for various interpretations. They are often more strict, at least when taken literally.

4.2 Assessment results and safety case

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 module might see that the review is done according to process, software measurement module calculates the total coverage of code review and module testing, and competence module checks if the reviewers have had appropriate skills for the task, as shown in Figure 5.

Assessment results as such (full or partial result sets, or risk analysis based on the gaps) can also be used as one 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.
How the actual consolidation is done is still in a conceptual phase. Any of the standards do not give detailed requirements. For example, they can require a certain metric to be collected, but the target values of the metrics are never 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 Conclusions

This article has introduced some aspects of process assessment when it is used as part of software certification. The concepts have been piloted in the field, and they will be tested further in the next year. CERFAS project will be finished in the end of 2010, and the Software Certification Service is immediately launched based on the project research results. The drivers for the project have been both legal and economical. The Finnish Nuclear Power Guide requires certified software in the highest safety class, so there is a need to develop a national certification scheme and certification service. Certification also shortens the actual qualification and licensing process, when the software based systems are deployed in the plant. Currently the qualification process is very costly, so all the methods and models which can support it can mean a huge savings to plant operators.

Process assessment, according our current knowledge, provides interesting insights in the safety aspects of a software product. For example, if there are gaps found in the relatively light-weight assessment, heavier methods like model checking can then focus on those weaknesses trying to find if
they are endangering the actual safety. Also the ability assessment fulfills one of the industry needs, since a well documented method to get a the first go/no-go decision in purchasing process saves resources at later stages. Still, the process assessment is only a complementary method when the final validity of the product is analysed.

6 Literature


7 Author CVs

Mika Johansson

Executive Director in FiSMA, partner and consultant in Spinet Oy, and part-time researcher in Tampere Technical University, Pori unit.

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 since 2006. In Spinet Oy, Mika has performed assessments and audits using SPICE, CMMI, ISO9001, ISO/IEC 20000 and safety specific models since 2003.

Risto Nevalainen

Current position as a senior researcher in Tampere Technical University, Pori unit (part-time). Senior Advisor of Finnish Software Measurement Association FiSMA in software standardization and process improvement topics.
Mr. Risto Nevalainen (Lic. Tech.) has long experience in software measurement and quality topics. Nevalainen has been managing director of STTF Oy since 1996. His working experience includes also 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), Finnish Prime Minister’s Office and Finnish Economic Planning Centre. Mr. Nevalainen has participated in ISO15504 (SPICE) standard development since beginning. He is Competent SPICE Assessor since 1996 and ISO9000 Lead Assessor since 1991.