Safety as a Process Quality Characteristic

Timo Varkoi

Spinet Oy, Tampere, Finland
timo.varkoi@spinet.fi

Abstract. Software is increasingly been used to provide system functionality that is related to safety. From systems point-of-view safety is often considered to be a probabilistic property and development process has less significance. For software this approach is not necessarily valid. This article studies the applicable process scope in relation to safety requirements for software. Based on a new concept of process quality characteristics, process quality attributes for safety are tentatively defined. The aim of the presented process quality characteristic for safety is that risks related to achievement of safety goals in software development can be evaluated with process assessment. Key results would be increased trust in safety of software-intensive systems and established safety culture in development organizations.

Keywords: software process, safety, process quality, process assessment.

1 Introduction

Importance of safety in software development is increasing. Growing part of functionality is being developed using software. Industries that earlier have relied on electronic and electrical systems are turning into using software. Software based solutions have also helped in providing new functionality. Examples of these domains include automotive, medical, and energy industries.

Present day safety standards concentrate on the system aspect and their origins are mainly of hardware development. Reliability is a key concept when system or hardware safety is considered. Software products have their own product quality oriented standards, like ISO/IEC 25000 series [1], but there the role of safety is nominal. Safety-related activities in software development processes are to some extent presented e.g. in IEC 61508 standard [2], but the expected process attributes are missing.

In literature, many approaches to safety and reliability rely on probabilistic models. These models are difficult to apply to software due to the nature of software – there is no wear and tear in software and its reliability is difficult to evaluate without the system that runs it. Nevertheless, the studies of software reliability infer that the development process is an interesting factor of software reliability and safety.

This study defines an applicable process scope in relation to safety requirements for software. Based on a new concept of process quality characteristics, process attributes for safety are tentatively defined. The aim of this article is to test the idea of

T. Woronowicz et al. (Eds.): SPICE 2013, CCIS 349, pp. 1–12, 2013.

presenting safety, a highly important property in modern software development, as a process quality characteristic.

This article is structured as follows: Next, in Section 2, the concept of Process Quality is explained. Section 3 presents the existing process assessment models for safety domain. Section 4 discusses safety related processes based on literature review. Section 5 defines safety as a process quality characteristic. To conclude, section 6 summarizes the findings of this article.

2 Process Quality

For the time being, ISO/IEC JTC1/SC 7 Working Group 10 develops the ISO/IEC 15504 set of process assessment standards into a new set of ISO/IEC 33000 standards. In this development, a new concept of process quality has been introduced. Process quality concept harmonizes the terminology with product quality (Fig. 1). Process capability is seen as an important, but not the only, characteristic of a process. The basis of this thinking is that a process shall demonstrate successful implementation, trustworthiness, manageability and adaptability, which reaches beyond the capability approach that has guided process improvement and assessment from the 1990's.

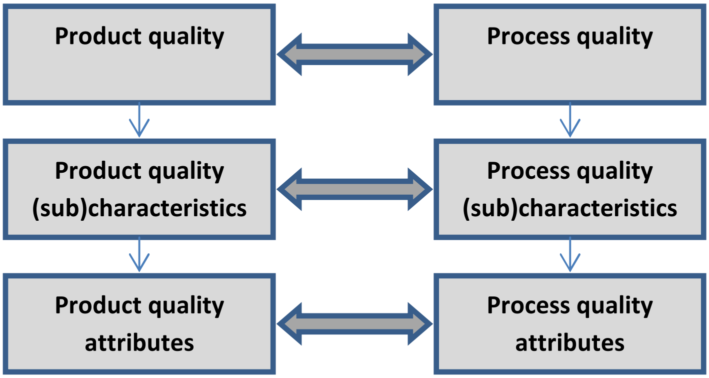
Product quality
Process quality
Product quality (sub)characteristics
Process quality (sub)characteristics
Product quality attributes
Process quality attributes

Fig. 1. Harmonized view of process and product quality concepts

Process quality is composed of quality characteristics, where the required set of characteristics depends on the applicable stakeholder needs and organization's business goals. In addition, process quality shall be measurable. The key terms can be defined as follows [3]:

- Process quality
  - ability of a process to satisfy stated and implied stakeholder needs when used in a specified context
- Process quality characteristic
  - a measurable aspect of process quality; category of process attributes that are significant to process quality

Earlier process assessment models have addressed capability as a process quality characteristic. In the future, several new characteristics of process quality are expected to arise, e.g. controllability, agility, and efficiency.

The concepts of process quality characteristics and attributes are used in this article to define safety as a new process quality dimension.

3 Existing Models for Safety Process Assessment

Safety, by definition, means the expectation that a system does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered [4]. Safety is considered in at least two present process assessment models: CMMI +SAFE from Software Engineering Institute [5], and ISO/IEC 15504 Part 10 [6]. These models apply capability as the relevant process quality characteristic.

A Safety Extension to CMMI-DEV, +SAFE, defines two additional process areas to CMMI-DEV to be used for assessment and improvement of an organization's capabilities for providing safety-critical products. This extension can be used standalone i.e. only the two named processes can be assessed. There is no direct link to any safety standards. The processes and their specific goals are listed below [5]:

- Safety Management (Project Management process category)
  - SG1 Develop Safety Plans
  - SG2 Monitor Safety Incidents
  - SG3 Manage Safety-Related Suppliers
- Safety Engineering (Engineering process category)
  - SG1 Identify Hazards, Accidents, and Sources of Hazards
  - SG2 Analyze Hazards and Perform Risk Assessments
  - SG3 Define and Maintain Safety Requirements
  - SG4 Design for Safety
  - SG5 Support Safety Acceptance

+SAFE is intended to be used for capability assessment of a supplier or potential supplier of safety-critical products and to improve an organization's capability in developing, sustaining, maintaining, and managing safety-critical products. The model recognizes safety function, safety case and safety lifecycle in the same meaning as IEC 61508.

ISO/IEC TS 15504-10 defines three processes for safety management, safety engineering and safety qualification to extend the ISO/IEC 15504 process assessment models for system and software lifecycle processes. The three processes and their purposes and expected outcomes are [6]:

- Safety Management process
  - The purpose of the Safety Management Process is to ensure that products, services and life cycle processes meet safety objectives.

  - As a result of the successful implementation of the Safety Management process:
    1) Safety principles and safety criteria are established.
    2) The scope of the safety activities for the project is defined.
    3) Safety activities are planned and implemented.
    4) Tasks and resources necessary to complete the safety activities are sized and estimated.
    5) Safety organization structure (responsibilities, roles, reporting channels, interfaces with other projects or OUs …) is established.
    6) Safety activities are monitored, safety-related incidents are reported, analysed, and resolved.
    7) Agreement on safety policy and requirements for supplied products or services is achieved.
    8) Supplier's safety activities are monitored.
- Safety Engineering process
  - The purpose of the Safety Engineering process is to ensure that safety is adequately addressed throughout all stages of the engineering processes.
  - As a result of the successful implementation of the Safety Engineering process:
    1) Hazards related to product are identified and analysed.
    2) Hazard log is established and maintained.
    3) Safety demonstration for the product lifecycle is established and maintained.
    4) Safety requirements are defined.
    5) Safety integrity requirements are defined and allocated.
    6) Safety principles are applied to development processes.
    7) Impacts on safety of change requests are analysed.
    8) Product is validated against safety requirements.
    9) Independent evaluations are performed.
- Safety Qualification process
  - The purpose of the Safety Qualification process is to assess the suitability of external resources when developing a safety-related software or system.
  - As a result of the successful implementation of the Safety Qualification process:
    1) Safety qualification strategy for external resources is developed.
    2) Safety qualification plan is developed and executed.
    3) Safety qualification documentation is written.
    4) Safety qualification report is produced.

ISO/IEC TS 15504-10 provides a basis for performing a process capability assessment of processes with respect to the development of complex safety-related systems. It can be used standalone, too. There are links to IEC 61508 and ISO 26262 safety standards. The terminology used is similar to IEC 61508, including safety lifecycle, safety demonstration and safety case.

As we can see, the process scopes of both ISO/IEC 15504-10 and CMMI-DEV +SAFE cover roughly the same application areas: management, engineering and supply. Both models also consider that process capability defines the goodness of these processes and that capability levels are applicable. Anyhow, these models provide guidance when considering the important aspects of systems and software development in safety-related domains.

4 Safety from Process Perspective

Safety of a system is always considered as a characteristic of a product. There is no direct causality from the development process to the safety of a product. Despite of this, characteristics of the development process certainly can affect the safety of the product. The practice is that part of system functionality is considered to be safety-critical or safety-related and requirements for safety are set. Safety demonstration provides evidence that system or its components are considered safe within an acceptable risk.

Lots of of the studied literature relies on probabilistic models for safety. It seems that the same approach that has worked with electro-mechanical systems is believed to be applicable to software. The nature of software as a design rather than a product is largely ignored. Software reliability is a difficult concept and its quantification appears to be close to ineligible. On the other hand, most of the publications refer in some way to the development process as a factor of software reliability.

Lawrence [7] emphasizes software life cycle to improve safety and reliability. Smidts et al. [8] bases their work on heavy measurement of the development process to predict operational reliability. Chu et al. [9] apply quantitative methods to model software failures for probabilistic risk assessment (PRA).

The work of Leveson [10] sets reliability in totally new light when pursuing safety. Safety is seen in a wider perspective and the role of PRA is questioned. The relationship between reliability and safety is rejected. In her book, Leveson challenges the traditional models of causality that are based on the assumption that accidents are caused by component failure and making components reliable prevents accidents. The ideas are established on system theory. The book presents a new causality model and how it can be applied to safety engineering. Factors that affect in achieving safety goals can be divided into engineering, operations, and management. Leveson presents a new foundation for safety engineering. Two software reliability related postulations are presented in Table 1.

Table 1. Leveson's assumptions for new safety engineering principles [10]

Old Assumption	New Assumption
Safety is increased by increasing system or component reliability; if components do not fail, then accidents will not occur.	High reliability is neither necessary nor sufficient for safety.
Highly reliable software is safe.	Highly reliable software is not necessarily safe. Increasing software reliability will have only minimal impact on safety.

Fenton [11] uses probabilistic approaches to predict software defects and reliability. His work is focused on using Bayesian networks, but with a combination of both qualitative and quantitative measures.

The concepts of safety and reliability are used inconsistently in literature. The key findings are that there hardly is a direct connection between software reliability and safety, and that safety should not be considered as a characteristic of software. Nevertheless, all approaches take into account the development process as a source of safety risks. Therefore, safety analysis could benefit of process modeling and evaluation as a means to reduce software-related risks. Furthermore, process assessment models can be further developed to consider safety requirements and to address dependability including reliability issues. In summary, the safety related software development processes that emerge from the literature are:

- System requirements analysis (Chu)
  - system safety engineering (Leveson)
  - system architecture specification (Lawrence)
  - specification review and analysis (Leveson)
  - reuse (Leveson)
- Software requirements specification (Lawrence, Leveson, Smidts)
  - requirements safety analysis (Lawrence)
- Software design specification (Lawrence, Leveson, Smidts)
  - design safety analysis (Lawrence)
- Software implementation (Lawrence, Smidts, Lyu)
- System integration (Lawrence)
- Assurance (Leveson)
  - testing (Chu, Smidts, Leveson, Fenton, Lyu)
  - validation (Lawrence)
- Software installation (Lawrence)
- Software project management (Lawrence)
  - software safety planning (Lawrence)
- Software configuration management (Lawrence)
- Risk management (Fenton
- Measurement (Smidts, Fenton)

The processes are clustered to enable association to ISO/IEC 12207 Software Life Cycle Processes and ISO/IEC 15504-5 Process Assessment Model. The named processes can be found from the related authors' work.

The list of processes serves as a reference in selecting applicable process scope for assessment in Section 5.1. Findings of the literature review set additional emphasis on requirements specification, analysis and tracing. The next section discusses the concept of Process Quality Characteristic as a means to develop process assessments to support safety goals.

5 Safety as a Process Quality Characteristic

Safety could be presented as a process quality characteristic to enable process assessment. Process-related safety means definition of relevant process attributes that contribute in achievement of safer products. Here we use the wider concept of safety, freedom from unacceptable risk, instead of a more closed definition as a property of a state or system. It is important to distinct safety as process characteristic from product safety.

This section presents a preliminary model to address safety by process assessment. First, an applicable process set is considered, and then a tentative set of process quality attributes is defined. The description of the safety process quality attributes is the first application of process quality characteristic since the process capability framework.

The process set is defined based on the relevant literature findings combined with lifecycle processes found in one of the key functional safety standards. Then corresponding processes are collected from ISO/IEC 15504-5 Process Assessment Model.

Two sets of process attributes are constructed based on author's expertise in process assessments in safety-critical domain. The selection of attributes reflects the experiences gained with process capability assessment in safety domain. Capability levels tend to be of low interest when the aim is to ensure that risks related to achievement of safety goals are mitigated. Different sources of information were used to define the contents of the attributes. These include standards ISO/IEC 15504; ISO/IEC 25010; and IEC 61508.

5.1 Applicable Process Set

ISO/IEC 15504 Part 5 [12] defines a process assessment model for life cycle processes. There are altogether 60 processes divided into seven categories. In the beginning, for safety considerations we can limit the relevant processes into the software development related processes and categories as listed in Table 2.

Table 2. Relevant processes for safety domain assessment

Category	**Process in ISO/IEC 15504-5**
System Lifecycle Processes (ENG)	
	ENG.1 Stakeholder requirements definition
	ENG.2 System requirements analysis
	ENG.3 System architectural design
	ENG.4 Software implementation
	ENG.5 System integration
	ENG.6 Systems qualification testing
Software Implementation Processes (DEV)	
	DEV.1 Software requirements analysis
	DEV.2 Software architectural design

Table 2. (*continued*)

	DEV.3 Software detailed design
	DEV.4 Software construction
	DEV.5 Software integration
	DEV.6 Software qualification testing
Software Support Processes (SUP)	
	SUP.1 Software documentation management
	SUP.2 Software configuration management
	SUP.3 Software quality assurance
	SUP.4 Software verification
	SUP.5 Software validation
	SUP.6 Software review

The rationale for selecting the processes is the combination of the literature findings and the relevant safety standards. The literature study brought up a list of processes (in Section 4) with a relation to software reliability and safety. Processes in Table 2 correspond to those processes except for the management processes (project management, risk management and measurement). Management processes do exist in ISO/IEC 15504-5 and may be considered in the later phase, if needed. In this model the management aspect will be covered by the extended process quality attribute set (in chapter 5.2). Documentation management is included to meet the documentation requirements of safety standards.

The second reference for the process scope is the IEC 61508 standard Part 3. The software development life cycle is depicted as a V-model (Fig. 3):

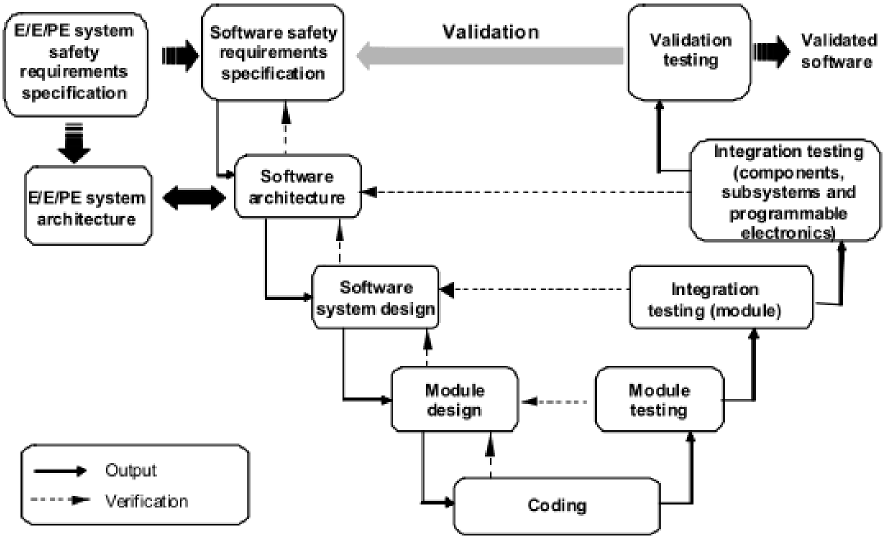
E/E/PE system safety requirements specification
Software safety requirements specification
Validation
Validation testing
Validated software
E/E/PE system architecture
Software architecture
Integration testing (components, subsystems and programmable electronics)
Software system design
Integration testing (module)
Module design
Module testing
Coding
Output
Verification

Fig. 2. Software systematic capability and the development lifecycle (the V-model) [2]

Also the IEC 61508 V-model processes are covered by the selected process set of Table 2.

5.2 Process Quality Attributes for Safety

Next, we specify tentative sets of process quality attributes (PA) for process assessment in safety domain. The basic set is intended to include attributes that meet the elementary requirements for trustworthy software development. The extended set adds process attributes that support management of processes that support safety activities. Especially the extended set requires further elaboration.

In a process assessment, each process is evaluated using a set of process quality attributes. As a result, when achievement of attributes is evaluated, better understanding of process related risk is gained. Each process attribute shall be described with corresponding Generic Practices, Generic Resources and Generic Work Products to enable collection of adequate assessment evidence.

Basic Set of Process Quality Attributes for Safety

The basic set is intended to define the process quality attributes that are essential to deliver safe software and to demonstrate trustworthiness of the processes. All of the attributes should be applicable to the ENG and DEV processes in Table 2, and for the SUP processes at least PA 1 and PA 2 are applicable.

First concern is to check that the process exists; process performance is the standard attribute for this. Process dependability ensures that the process is robust enough for continuous software development with high quality requirements. The literature emphasizes requirements specification and management; this is covered by requirements control attribute. Safety engineering adopts practices from safety process assessment models. Descriptions for the basic set attributes are:

- **PA 1 Process performance**
  - PA 1.1 process achieves its defined process outcomes
    - activities are performed and work products produced

- **PA 2 Process dependability**
  - PA 2.1 reliability
    - process performs as required in normal conditions
  - PA 2.2 availability
    - process can be performed when needed
  - PA 2.3 maintainability
    - process can be modified easily to add capabilities
    - performance can be improved
    - faults and errors can be corrected

- **PA 3 Requirements control**
  - PA 3.1 traceability
    - process supports traceability

    - PA 3.2 specifications coverage
        - functional, non-functional and safety requirements are included
    - PA 3.3 constraints
        - unwanted functionality is excluded
    - PA 3.4 safety analysis
        - requirements relationship to safety is understood
    - PA 3.5 reuse
        - requirements are analyzed for reuse opportunities
        - safety requirements of the reusable components are analyzed

- **PA 4 Safety engineering**
    - PA 4.1 safety demonstration
        - safety cases and other argumentation are evaluated
    - PA 4.2 reviews
        - reviews are performed and documented
    - PA 4.3 verification and validation
        - testing that work products meet their requirements and are applicable for their intended use
    - PA 4.4 quality assurance
        - processes and work products comply with standards, requirements and plans

Extended Set of Process Quality Attributes for Safety

The extended set intends to evaluate the implementation of safety culture. Safety management is the first step to organization-wide safety policy. Process compliance looks at both external and internal process definitions. Risk management aims at reducing and controlling process related risks including information security. Quantitative management attribute aligns safety process quality to ISO/IEC 15504 process capability level 4. Descriptions for the extended set attributes are:

- **PA 5 Safety management**
    - PA 5.1 safety strategy alignment
    - PA 5.2 safety life cycle
        - defined activities involved in the implementation of safety-related systems
    - PA 5.3 responsibilities and resourcing
    - PA 5.4 monitoring
    - PA 5.5 test and simulation environments

- **PA 6 Process compliance**
    - PA 6.1 standards
    - PA 6.2 defined process
    - PA 6.3 process tailoring

- **PA 7 Risk management**
    - PA 7.1 management of events that effect achievement of business goals
    - PA 7.2 qualitative and quantitative risk analysis for a process
        - probabilistic risk analysis
    - PA 7.3 information security
        - preservation of confidentiality, integrity and accessibility of information during the execution of a process

- **PA 8 Quantitative management**
    - PA 8.1 quantitative analysis
        - measurement objectives
        - measures
    - PA 8.2 quantitative control
        - techniques
        - causes of variation

6 Conclusions

This report studies software safety from process point of view. The idea is that risks related to achievement of safety goals can be evaluated with process assessment using specifically defined process quality attributes.

Process quality is composed of quality characteristics, where the required set of characteristics depends on the applicable stakeholder needs and organization's business goals. In addition, process quality shall be measurable.

Probabilistic models for safety are difficult to apply to software. Assessment of the software development processes may provide additional information to evaluate safety risks of software intensive systems. It requires that process assessment models are further developed to take into account safety requirements and to address e.g. dependability issues.

A new concept of Process Quality Characteristics is presented in this article and two tentative sets of process quality attributes for process assessment in safety domain were developed to support achievement of safety goals in software development. A set of applicable development related processes is also defined.

The basic set of process quality attributes for safety is intended to include attributes that meet the elementary requirements for trustworthy software development. The extended set adds process attributes that support implementation of safety culture in an organization.

The aim of the presented process quality characteristic for safety is that risks related to achievement of safety goals can be evaluated with process assessment using specifically defined process quality attributes.

The presented process safety approach and the defined process quality characteristic for safety are tentative. Hopefully this article opens discussion of how software processes can support the increasing safety requirements for software.

Acknowledgements. This work has been partially funded by Finnish national nuclear safety program SAFIR2014. In project CORSICA, new approaches and V&V methods have been developed for software-intensive system safety. A method called Nuclear SPICE implements an assessment approach for safety-critical domain.

References

1. ISO/IEC 25010:2011 Systems and software engineering–Systems and software Quality Requirements and Evaluation (SQuaRE)–System and software quality models (2011)
2. IEC 61508-3 Ed. 2.0, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements (2009)
3. ISO/IEC 33001 DIS, Information technology – Process assessment – Concepts and terminology (2013)
4. ISO/IEC/IEEE 24765:2010, Systems and Software Engineering Vocabulary, http://pascal.computer.org/sev_display/index.action
5. +SAFE, V1.2, A Safety Extension to CMMI-DEV, V1.2, CMU/SEI-2007-TN-006 (March 2007)
6. ISO/IEC TS 15504-10.4:2011, Information technology — Process assessment — Part 10: Safety extension (2011)
7. Lawrence, J.D.: Software Reliability and Safety in Nuclear Reactor Protection Systems. NRC, CR6101 (1993)
8. Smidts, C.S., et al.: A Large Scale Validation of a Methodology for Assessing Software Reliability. NRC (2011)
9. Chu, T.-L., et al.: Development of Quantitative Software Reliability Models for Digital Protection Systems of Nuclear Power Plants. NRC (2011)
10. Leveson, N.G.: Engineering a Safer World: Systems Thinking Applied to Safety. MIT (2011)
11. Fenton, N., Neil, M., Marquez, D.: Using Bayesian Networks to Predict Software Defects and Reliability. In: Proceedings of IMECHE 2008 (2008)
12. ISO/IEC 15504-5:2012, Information technology – Process assessment – Part 5: An exemplar Process Assessment Model (2012)