Safety: a new process quality characteristic?

STX-METRI Annual Seminar 1.11.2012

Timo Varkoi, FISMA ry
Topics

- **Process quality**
  - Process quality characteristics
  - Process robustness

- **Safety**
  - Safety domain
  - Safety integrity

- **Dependability**
  - Software reliability

- **Alternatives for safety characteristics**
Process quality theses

- Process shall demonstrate
  - successful implementation
  - trustworthiness
  - manageability
  - adaptability
- Process quality is composed of quality characteristics
  - required set of characteristics depends on the business goals of an organization
- Process quality shall be measurable
Process quality

- ability of a process to satisfy stated and implied stakeholder needs when used in a specified context
  - (ISO/IEC 33001 CD3 proposed definition)
Process quality characteristic

- a measurable aspect of process quality; category of process attributes that are significant to process quality
  - (ISO/IEC 33001 CD3 proposed definition)
Harmonized view

Product quality

Product quality (sub)characteristics

Product quality attributes

Process quality

Process quality (sub)characteristics

Process quality attributes
Tentative process quality characteristics

Controllability
- set and control goals
- measurement

Agility
- coordination
- dexterity
- flexibility

Capability
- achieving business goals
- organizational maturity

Robustness
- dependability
- risks
- information security

Efficiency
- performance
- predictability
- improvability
Robustness

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

- risks
  - management of events that effect achievement of business goals
  - qualitative and quantitative risk analysis for a process

- information security
  - preservation of confidentiality, integrity and accessibility of information [20000-1] during the execution of a process
Safety

- freedom from unacceptable risk
Key safety concepts

- **safety management**
  - ensures that products, services and life cycle processes meet safety objectives

- **safety engineering**
  - ensures that safety is adequately addressed throughout all stages of the engineering processes
  
  (ISO/IEC TS 15504-10 Safety extension)

- **safety culture**
  - policy and strategy used within an organization to support the development, production, and operation of safety related systems
  
  (ISO 26262)
Integrating different levels of abstraction

ISO/IEC 15504 Part 5:2012

SPICE taxonomy (processes, capability levels, capability index, gap)

Safety Processes Extension

Functional Safety

SAFETY taxonomy (processes, SIL, methods, rigor, gap)

IEC 61508

Domain Safety

Domain taxonomy (Domain, safety class, gap)

ISO 26262, IEC 62304, IEC 60880, etc.
Safety integrity

- probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time
  - Functional Safety - IEC 61508

- safety integrity level - SIL
  - discrete level, corresponding to a range of safety integrity values, SIL 4 is the highest and SIL 1 has the lowest
  - target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation:

<table>
<thead>
<tr>
<th>Safety integrity level (SIL)</th>
<th>Average frequency of a dangerous failure of the safety function [h⁻¹] , (PFH)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>≥ 10⁻⁹ to &lt; 10⁻⁸</td>
</tr>
<tr>
<td>3</td>
<td>≥ 10⁻⁸ to &lt; 10⁻⁷</td>
</tr>
<tr>
<td>2</td>
<td>≥ 10⁻⁷ to &lt; 10⁻⁶</td>
</tr>
<tr>
<td>1</td>
<td>≥ 10⁻⁶ to &lt; 10⁻⁵</td>
</tr>
</tbody>
</table>
Dependability - *luotettavuus*

- Reliability
  - *toimintavarmuus*
- Maintainability
  - *ylläpidettävyys*
- Availability
  - *käyttövarmuus*
dependability

- **(1)** trustworthiness of a computer system such that reliance can be justifiably placed on the service it delivers *(IEEE 982.1-2005 IEEE Standard Dictionary of Measures of the Software Aspects of Dependability, 2.2)*

- **(2)** measure of the degree to which an item is operable and capable of performing its required function at any (random) time during a specified mission profile, given item availability at the start of the mission *(ISO/IEC/IEEE 24765:2010 Systems and software engineering – Vocabulary)*

*Note:* Reliability, availability, and maintainability are aspects of dependability.
reliability

- (1) the ability of a system or component to perform its required functions under stated conditions for a specified period of time (ISO/IEC/IEEE 24765:2010 Systems and software engineering – Vocabulary)

- (2) capability of the software product to maintain a specified level of performance when used under specified conditions (ISO/IEC 9126-1:2001 Software engineering -- Product quality -- Part 1: Quality model, 6.2)

**Note:** Wear or aging does not occur in software. Limitations in reliability are due to faults in requirements, design, and implementation. Failures due to these faults depend on the way the software product is used and the program options selected rather than on elapsed time.

**See Also:** availability, MTBF
availability

- **(1)** the degree to which a system or component is operational and accessible when required for use *(ISO/IEC/IEEE 24765:2010 Systems and software engineering – Vocabulary)*
- **(2)** ability of a component or service to perform its required function at a stated instant or over a stated period of time *(ISO/IEC 20000-1:2005 Information technology -- Service management -- Part 1: Specification, 2.1)*

*Note*: often expressed as a probability. Availability is usually expressed as a ratio of the time that the service is actually available for use by the business to the agreed service hours.

*See Also*: error tolerance, fault tolerance, robustness
maintainability

- (1) the ease with which a software system or component can be modified to change or add capabilities, correct faults or defects, improve performance or other attributes, or adapt to a changed environment (ISO/IEC/IEEE 24765:2010 Systems and software engineering – Vocabulary)
- (2) the ease with which a hardware system or component can be retained in, or restored to, a state in which it can perform its required functions (ISO/IEC/IEEE 24765:2010 Systems and software engineering – Vocabulary)

Note: Modifications may include corrections, improvements or adaptation of the software to changes in environment, and in requirements and functional specifications [ISO/IEC 9126-1]

See Also: extendability, flexibility
software reliability

- (1) the probability that software will not cause the failure of a system for a specified time under specified conditions (ISO/IEC/IEEE 24765:2010 Systems and software engineering – Vocabulary)

  Note: The probability is a function of the inputs to and use of the system as well as a function of the existence of faults in the software. The inputs to the system determine whether existing faults, if any, are encountered.

Hard to quantify!
Software reliability, two possible viewpoints

Highly reliable software is not necessarily safe. Increasing software reliability will have only minimal impact on safety. (N. Leveson, 2011)
Alternatives for safety characteristics

What are the process quality requirements to satisfy the needs – i.e. the results of achievement for process attributes?
Different goals

- **Safety integrity**
  - Hard to quantify for software
  - Focus on reliability in-use

- **Dependability**
  - Focus on requirements, constraints, design and implementation
  - Justifiable trust

- **Reduction of risk** is common ground
  - Risks can be identified in assessments based on weak or missing practices
  - Rather qualitative than quantitative
Discussion, comments

THANK YOU!

- Timo Varkoi, FiSMA ry, timo.varkoi@gmail.com