Business from technology

SAFIR2014: CORSICA
Coverage and rationality of the software I&C safety assurance

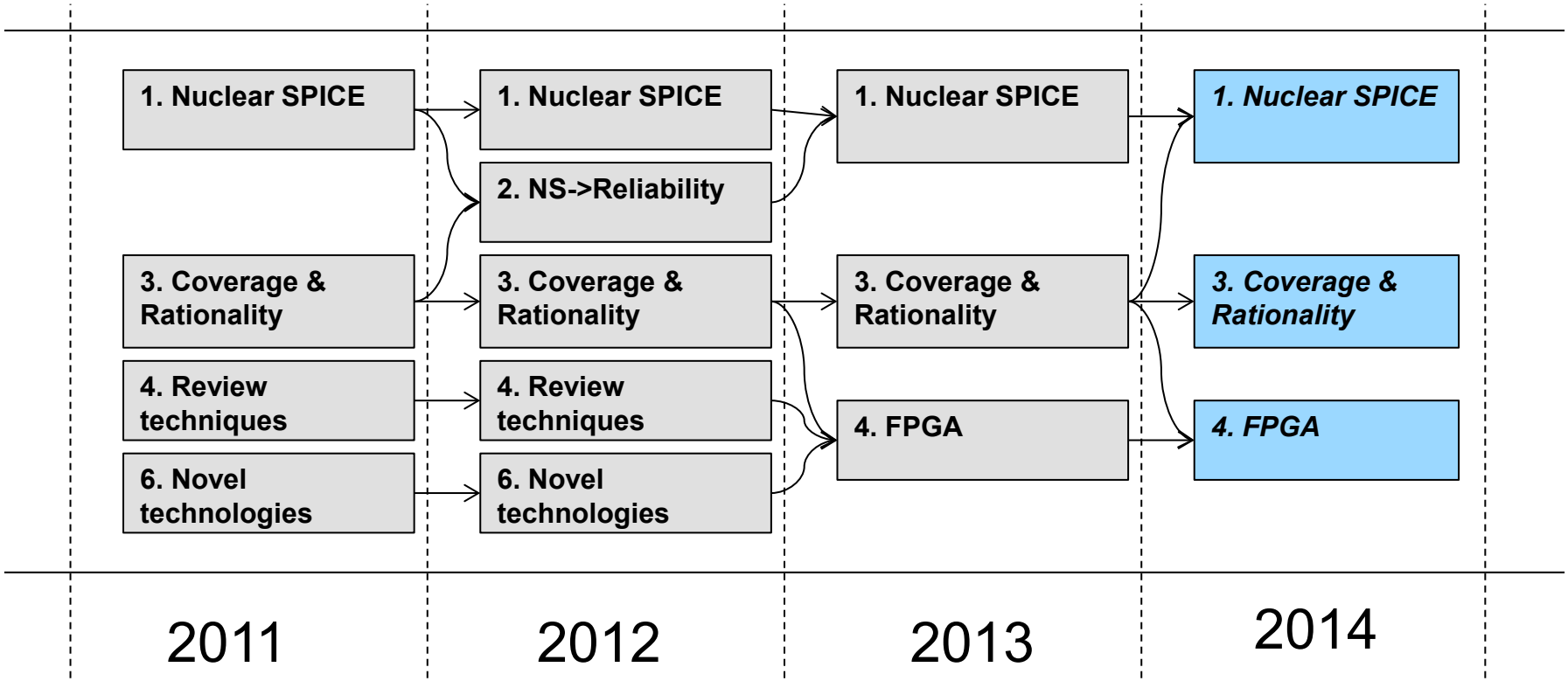
Mid-Term Seminar 21.-22.3.2013

Jussi Lahtinen, Jukka Ranta, Lauri Lötjönen VTT
Risto Nevalainen, Timo Varkoi, FiSMA

Introduction

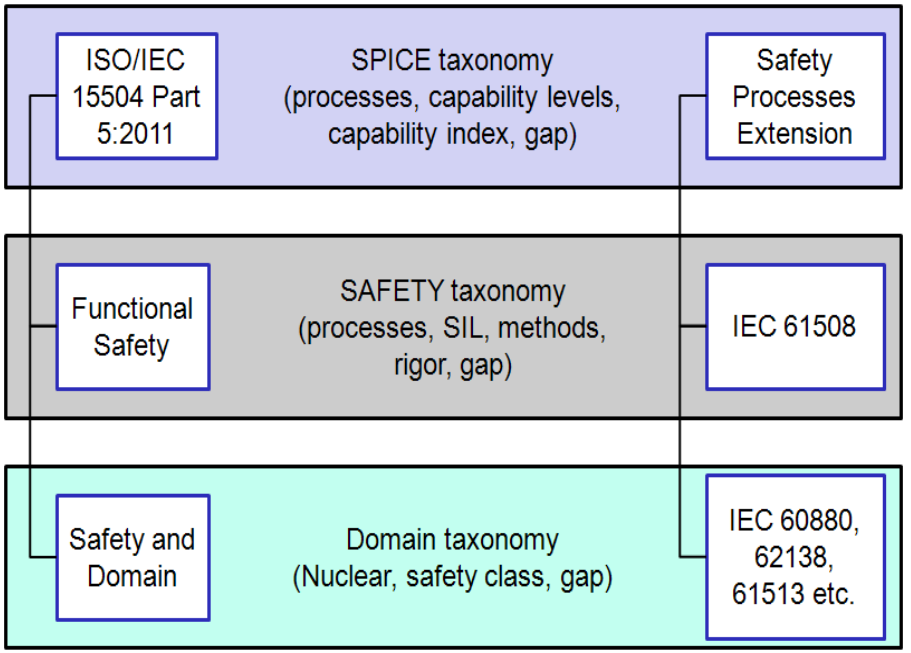
- CORSICA is based on previous SAFIR2010 program to develop approaches to qualify and certify software intensive I&C systems for nuclear power plants.
- Current CORSICA topics in SAFIR2014 program:
  - adequacy and relevance of process capability assessment in technical product evaluation;
  - coverage and rationality of required development and assurance methods;
  - certification and evaluation issues in using new technologies, for example FPGA;
  - use of new standards in technical safety evaluation of nuclear I&C systems.

Tasks in CORSICA 2011 - 2014



Assessment of system & software development process with Nuclear SPICE

- The aim is to create an integrated family of methods to assess the degree of compliance with selected standards
- SPICE provides a generic framework for assessment
  - content and criteria added from generic safety standards and from nuclear standards
- Nuclear SPICE is a method to assess process capability and compliance to standards
- Steps:
  - Nuclear SPICE Process Assessment Model (PAM)
  - Nuclear SPICE assessment process
  - Validation of Nuclear SPICE

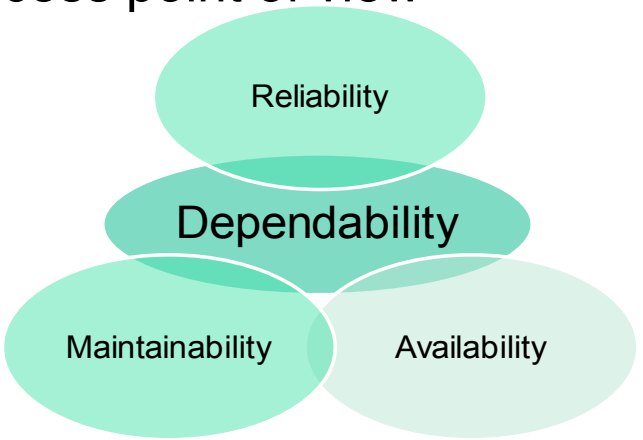


Software reliability and process assessment

- The original aim was to produce a mechanism to convert safety-critical process assessment (Nuclear SPICE) outcomes into a software reliability value.
  - State-of-the-art study tried to identify means needed to relate development practices to product quality, especially reliability.
  - Software reliability is a controversial concept and task was considered unsolvable.
  - The goal was adjusted to provide a wider viewpoint to process related risks regarding safety and dependability.
- Software reliability is related to the operation of the software.
- Software reliability and safety could benefit of software development process modeling and evaluation as a means to reduce software-related risks.

Framework for safety evaluation based on Nuclear SPICE

- Firstly, software reliability was studied from process point of view
  - Based on literature review
    - Software reliability is a difficult concept
    - Tedious to quantify
    - Implication to safety questionnable
    - Processes affect reliability (and safety)
  - Probability not applicable (e.g. SIL)

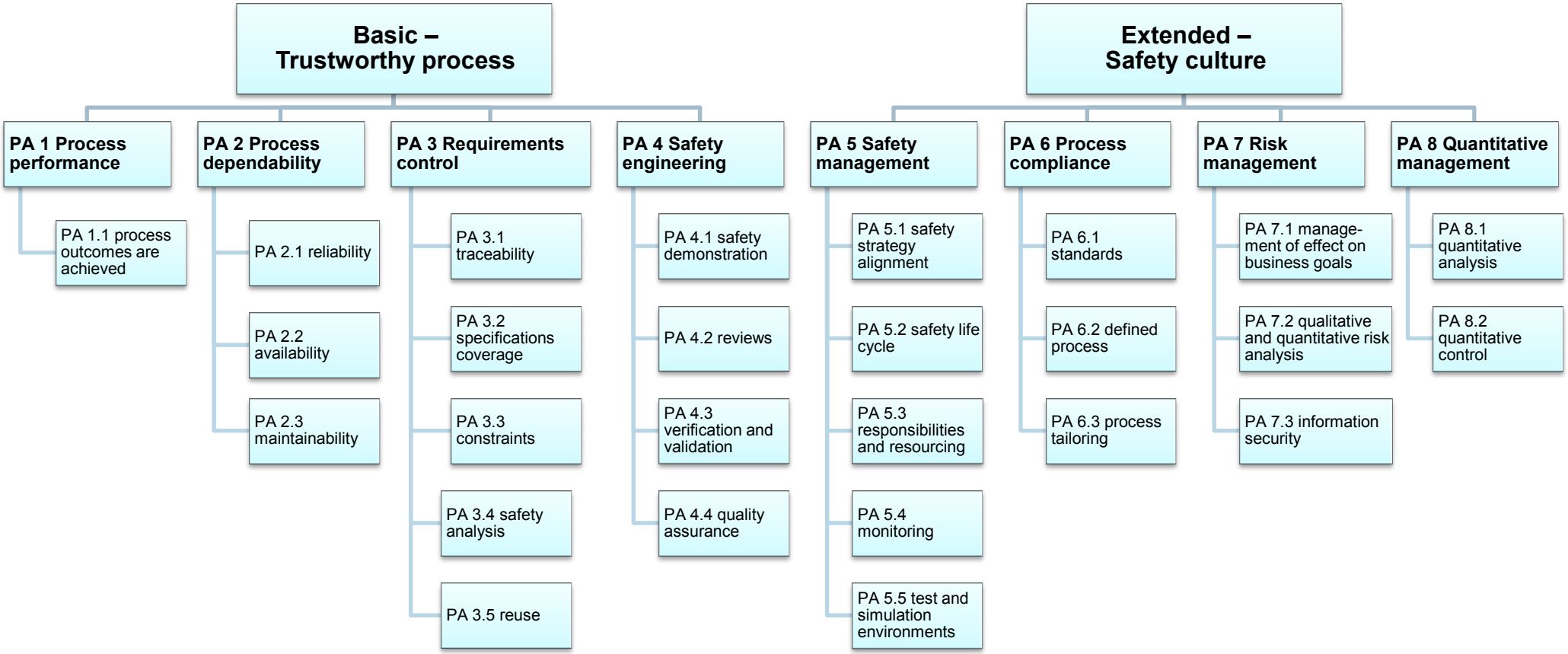


- Secondly, process assessment framework to evaluate safety characteristics of software development processes was developed
  - Based on a new Process Quality concept and ISO/IEC 330xx standards for Process Assessment
  - Defines relevant processes and process quality attributes
    - ***Safety as a Process Quality Characteristic***

Safety as a Process Quality Characteristic

- Integrate safety improving practices directly into system/software development processes
  - Safety dimension for process assessment
- Increased self-assurance, robustness and trust
- Key process quality attributes to deliver safe software – **trust in process**
  - Requirements control: traceability, coverage, constraints, reuse
  - Safety engineering: safety demonstration, reviews, assurance
  - Process dependability: reliability, availability, maintainability
- Key process quality attributes to manage safe software development – **safety culture**
  - Safety management: strategy, safety life cycle, resources, monitoring
  - Compliance: standards, defined process and tailoring
  - Risk management: risk mitigation, risk analysis, information security
  - Quantitative management: analysis and variation control
- The aim is **that risks related to achievement of safety goals can be evaluated with process assessment** using specifically defined process quality attributes

Process Attributes for Safety



Coverage and rationality of methods

- Functional testing plays a major role in the V&V of safety critical software of instrumentation and control in nuclear power plants
- Challenges:
  - as a test is derived from the specification, it can only detect non-conformance to that specification, and cannot be used to prove software correctness
  - full test coverage with respect to completeness and correctness is practically impossible
- Solutions:
  - Software reviews, inspections and walkthroughs are techniques to be applied to any artefact of system and software
  - Operational profile is used by analysing the software environment to tell criticality and frequency of the use of the software

Comparing U.S. NRC reactor trip software review process to the Finnish regulatory requirements

- Identifying the difference between the NRC and STUK regulatory requirements makes the approval of their systems easier
- The NRC-IEEE framework emphasises analysis and making of plans, whereas the STUK-IEC framework emphasises the management of requirements
- Safety classifications of I&C systems are different in U.S and Finland.
  - In U.S, there are one safety class and four echelons of defence, which are only conceptual.
  - In Finland there are two safety classes and absolute safety borders between systems which belong to different safety classes.
- Significant differences are in the implementation of backup systems
- NRC refers to IEEE standards, STUK mainly refers to IEC 60880

Reading techniques

- Reviews and inspections are typically used to locate software defects in the early life-cycle phases
- Perspective-Based Reading (PBR)
  - examines a software artefact description from the perspectives of the artefact's stakeholders in order to identify defects
  - Reviewers themselves create high-level work products based on the reviewed document. This leads to a more profound understanding of the system.
- Applied to the review of nuclear domain conceptual design plans
- Review instructions were written for five perspectives:
  - an automation designer,
  - a control room designer,
  - an electrical designer,
  - a safety designer, and
  - a regulator.

Use of novel technologies in nuclear power plants

- Interest in the use of field programmable gate array (FPGA) technology in nuclear power plant (NPP) automation has increased
- Demonstration of software-based systems' reliability and safety in the licensing process is difficult and laborious
- FPGAs are seen as an option that provides flexibility and capability similar to software but with
  - lower complexity,
  - simpler system structure, and
  - improved hardware performance.
- Cyber security issues are also considered to be lesser with FPGAs than with software
- Case study: Stepwise Shutdown System (SWS)

Deliverables 2011

Task	Report
1.1	FiSMA report 2011-1: S4N method description - Nuclear SPICE PRM and PAM. FiSMA 2012.
1.1	Nevalainen, Mäkinen, Varkoi: Towards SPICE for Nuclear (S4N) – Integrating IEC 61508, IEC 60880 and SPICE. EuroSPI 2011 conference.
1.2	FiSMA report 2011-2: S4N Assessment Process - Requirements for Nuclear SPICE assessment. FiSMA 2012.
3	Rationality of functional testing at Category A software, VTT Working Report.
4	Application of the Perspective Based Reading technique in the nuclear I&C context, VTT Technology.
6	Current state of FPGA technology in a nuclear domain, VTT Technology.

Deliverables 2012

Task	Report
1.1	FiSMA report 2012-1: Nuclear SPICE PAM for pre-qualification process assessment. FiSMA 2013.
1.2	FiSMA report 2012-2: Nuclear SPICE assessment process. FiSMA 2013.
1	Varkoi T., Nevalainen R., and Mäkinen T.: Toward Nuclear SPICE – integrating IEC 61508, IEC 60880 and SPICE. Journal of Software: Evolution and Process, published online 18.2.2013.
1	Development and use of standard based qualification procedures for safety systems and equipment in OL1 and OL2 nuclear power plants. Presentation in a workshop “Application of IEC/SC45A – CLC/TC45AX standards in nuclear installations”, Petten 27.4.2012
1 & 2	Safety Issues In Process Assessment. SPICE 2012 conference tutorial, 29.5.2012.
1 & 2	Integrating different assessment approaches to evaluate safety-critical software development in nuclear domain, EuroSPI 2012 Industrial proceedings, Functional safety workshop, 27.6.2012.
2	FiSMA report 2012-3: Framework to evaluate software reliability based on Nuclear SPICE. FiSMA 2013.
3	Planning a review process for software of reactor trip system. Supplementary requirements to U.S. NRC. Research Report VTT-R-06436-12.
4	Development of a Review Technique for Conceptual Design Plans. Research report VTT-R-08337-12.
6	Working report: Multi-core Processing from NPP I&C Perspective. VTT Technology.
6	FPGA Implementation of the Stepwise Shutdown System. VTT Research report. VTT-R-06053-12..

CORSICA
Coverage and rationality of the software I&C safety assurance

Thank you for your attention!