

# CORSICA

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

### Abstract

The aim of the CORSICA research project is to improve the safety evaluation of I&C software in nuclear industry by improving consciousness of process assessment and rationality of integrated evaluation methods. Main issues addressed were:

- support of process assessments in supplier evaluation and pre-qualification;
- consciousness of coverage and rationality of V&V-methods in software evaluation;
- novel technologies that require new qualification approaches.

### Conclusions

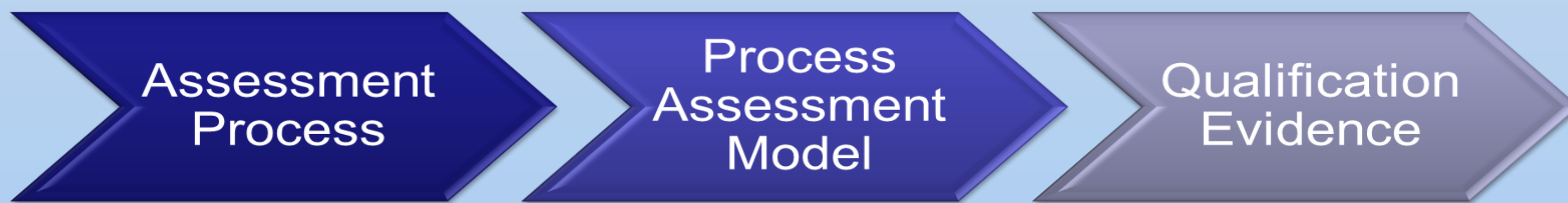
CORSICA project improved the safety evaluation of I&C software in nuclear industry by developing a method for process assessment and applicability of integrated evaluation methods. The Nuclear SPICE method supports assessment of safety critical I&C systems and software development processes. The need for assurance methods led to analysis of review techniques and development of test set generation for function block based systems. Increasing complexity and demands for safety were covered by studying certification and evaluation issues in using new technologies. The research produced methods that will be benefit the industry by providing concrete solutions to the identified issues.

### Nuclear SPICE assessment method

Use of systems containing software is increasing rapidly in the safety-critical domain. It creates pressure to develop more rigorous process assessment methods for assessing systems and software development. A process assessment model defines the processes in appropriate detail and an assessment process aims to ensure credibility and repeatability of assessment results. The Nuclear SPICE method consists of a process assessment model and a documented assessment process for safety-critical domain. The Nuclear SPICE method applies a classification scheme for assessment type that is a combination of assessment class and rigour in safety.

### Nuclear SPICE benefits

- defines a process assessment based approach to ensure quality in systems and software development for nuclear domain
- can be used to identify potential safety risks that are related to the development processes
- relies on ISO/IEC 15504 and 330nn standards
- assessments are flexible in scope and rigour
- delivers results fast, typically in 1 month



- Based on ISO/IEC 15504/330xx
- Flexible
- Rigour and scope

- I&C development
- Management, Engineering, Support and Safety processes
- Nuclear domain standards
- IEC 60880, 62138
- Regulatory guidance
- YVL, Common Position

- NPP supplier assessments and pre-qualification for I&C systems
- Coverage of standards and regulatory requirements

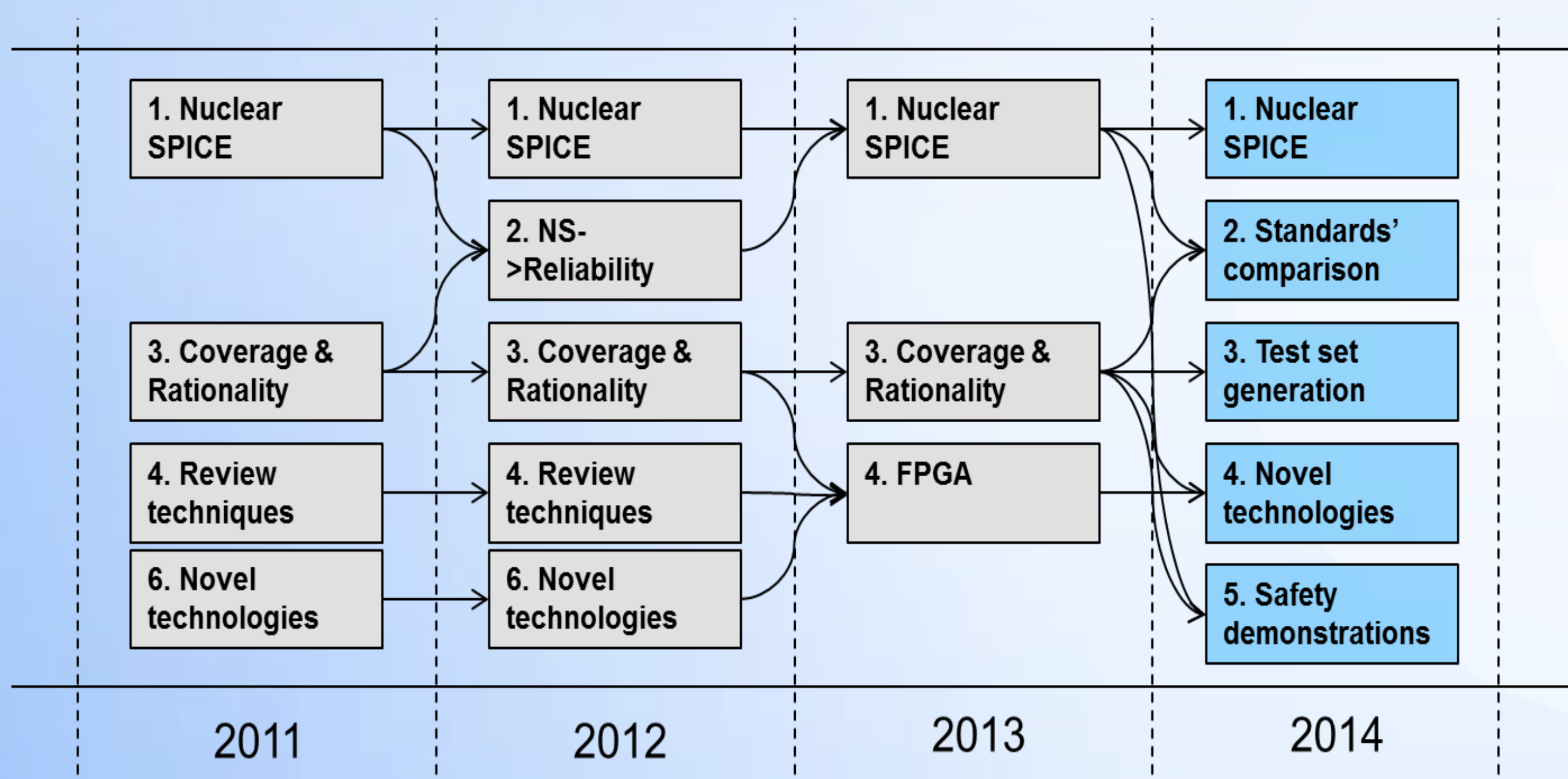
Assessment approach	Safety Class	IEC 62138	IEC 60880	YVL E.7	YVL B.1	Common Position
Self-assessment	-					
Process evaluation	-					
Supplier selection	-	(X)				
YVL evaluation	-			X	X	
Pre-qualification	none	X		(X)	(X)	
Pre-qualification	3	X		X	X	
Pre-qualification	2		X			
European level	3					X
National level	3	X		X	X	
Full conformance	2		X	X	X	X

Process	Capability						Achieved Level
	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	CL	
ENG.1 Stakeholder requirements definition	F	F	L	L	L	2	
ENG.2 System requirements analysis	F	F	F	F	F	3	
ENG.3 System architectural design	F	F	F	F	F	3	
ENG.4 Software implementation	L	L	L	L	L	1	
ENG.5 System integration	L	F	L	F	L	1	
ENG.6 Systems qualification testing	F	F	F	F	F	3	
SUP.1 Software documentation management	F	F	F	P	P	2	
SUP.2 Software configuration management	F	L	F	F	F	2	
SUP.3 Software quality assurance	F	L	L	F	L	2	
SAF.1 Safety management	L	F	L	F	F	1	
SAF.2 Safety engineering	F	F	F	F	F	3	
SAF.3 Safety qualification	L	0	0	0	0	1	

Category	Selected process in ISO/IEC 15504-5:2012	Core set	Management set	Full conformance
<b>System Lifecycle Processes (ENG)</b>				
ENG.1 Stakeholder requirements definition		x		
ENG.2 System requirements analysis		x		
ENG.3 System architectural design		x		
ENG.4 Software implementation		x		
ENG.5 System integration		x		
ENG.6 Systems qualification testing		x		
ENG.7 Software installation		x		
ENG.8 Software acceptance support			x	
ENG.9A Operational use				x
ENG.10 Software maintenance		x		
ENG.11 Software disposal				x
<b>Software Implementation Processes (DEV)</b>				
DEV.1 Software requirements analysis		x		
DEV.2 Software architectural design		x		
DEV.3 Software detailed design		x		
DEV.4 Software construction		x		
DEV.5 Software integration		x		
DEV.6 Software qualification testing		x		
<b>Software Support Processes (SUP)</b>				
SUP.1 Software documentation management		x		
SUP.2 Software configuration management		x		
SUP.3 Software quality assurance		x		
SUP.4 Software verification		x		
SUP.5 Software validation		x		
SUP.6 Software review		x		
SUP.8 Software problem resolution		x		
SUP.9 Software change request management		x		
<b>Project Processes (PRO)</b>				
PRO.1 Project planning			x	
PRO.2 Project assessment and control			x	
PRO.4 Risk management			x	
PRO.5 Configuration management		x		
PRO.6 Information management		x		
PRO.7 Measurement		x		
<b>Agreement Processes (AGR)</b>				
AGR.2 Supply				x
AGR.2A Supplier tendering				x
AGR.2B Contract agreement			x	
AGR.2C product/service delivery and support			x	
AGR.3 Contract change management			x	
<b>Organizational Project-Enabling Processes (ORG)</b>				
ORG.1A Process establishment				x
ORG.2 Infrastructure management			x	
ORG.5 Quality management			x	
<b>Safety extension (SAF), as in ISO/IEC 15504-10</b>				
SAF.1 Safety Management			x	
SAF.2 Safety Engineering		x		
SAF.3 Safety Qualification			x	
<b>Additional processes in Nuclear SPICE (NUC)</b>				
NUC.1 Hardware design		x		
NUC.2 Qualification			x	
NUC.3 Operational experience			x	
NUC.4 Safety demonstration				x
NUC.5 Cybersecurity			x	
NUC.6 Software security				x

### Tasks in CORSICA 2011 - 2014

- Assessment of system and software development process with Nuclear SPICE
- Structure-based test generation
- Standards and regulatory requirements
- Use of novel technologies and methods in nuclear power plants



### CORSICA team members

Jussi Lahtinen, Janne Valkonen, Hannu Harju, Lauri Lötjönen, Jukka Ranta, Ossi Teikari

VTT Technical Research Centre of Finland Ltd  
P.O. Box 1000, FI-02044 Espoo

Risto Nevalainen, Timo Varkoi

Finnish Software Measurement Association FiSMA ry  
Tekniikantie 14, FI-02150 Espoo

