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 VBV-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 330m standards;
* assessments are flexible in scope and rigour;
* delivers results fast, typically in 1 month.

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

Nuclear SPICE processes and categories:

<table>
<thead>
<tr>
<th>Process</th>
<th>Category</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAF.1</td>
<td>Safety management</td>
<td>1</td>
<td>Safety management process management</td>
</tr>
<tr>
<td>SAF.2</td>
<td>Safety engineering</td>
<td>2</td>
<td>Safety engineering process management</td>
</tr>
<tr>
<td>SAF.3</td>
<td>Safety qualification</td>
<td>3</td>
<td>Safety qualification process management</td>
</tr>
<tr>
<td>SAF.4</td>
<td>Safety assurance</td>
<td>4</td>
<td>Safety assurance process management</td>
</tr>
</tbody>
</table>

Nuclear SPICE processes and categories:

<table>
<thead>
<tr>
<th>Process</th>
<th>Category</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAF.1</td>
<td>Safety management</td>
<td>1</td>
<td>Safety management process management</td>
</tr>
<tr>
<td>SAF.2</td>
<td>Safety engineering</td>
<td>2</td>
<td>Safety engineering process management</td>
</tr>
<tr>
<td>SAF.3</td>
<td>Safety qualification</td>
<td>3</td>
<td>Safety qualification process management</td>
</tr>
<tr>
<td>SAF.4</td>
<td>Safety assurance</td>
<td>4</td>
<td>Safety assurance process management</td>
</tr>
</tbody>
</table>

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

Finland's Software Measurement Association FISMA ry

Espoo, Finland

2011

1. Nuclear SPICE
2. Safety processes
3. Coverage & Reliability
4. Review techniques
5. Novel technologies
6. Safety demonstrations

2012

1. Nuclear SPICE
2. Safety processes
3. Coverage & Reliability
4. Review techniques
5. Novel technologies
6. Safety demonstrations

2013

1. Nuclear SPICE
2. Safety processes
3. Coverage & Reliability
4. Review techniques
5. Novel technologies
6. Safety demonstrations

2014

1. Nuclear SPICE
2. Safety processes
3. Coverage & Reliability
4. Review techniques
5. Novel technologies
6. Safety demonstrations