Safety Guidance

Assessment of Pre-existing and Commercial-Off-The-Shelf Software For Use in Functions Important to Safety.

Abstract

This guide describes the evidence and the information necessary to Bel V to assess the adequacy of pre-existing and commercial-off-the-shelf software to perform functions which have an impact on safety.

Applicability: Digital I&C systems of nuclear installations

Keywords: digital upgrades - instrumentation and control – I&C - nuclear installations – NPP - pre-existing - software – COTS – safety assessment

Classification: Public

Distribution: Unrestricted

Valid until: NA

Bel V
Subsidiary of the FANC
Rue Walcourt 148 Walcourtstraat
B-1070 Bruxelles - Brussel

Versions	Dates	Remarks
01	05/07/2013	First issue

Disclaimer Notice

This document is not intended to be a substitute for Belgian legislative or regulatory documents, existing or future, which would by their publication, overrule or replace dispositions in this document.

Bel V is not responsible, directly or indirectly, neither for the use by third parties of the information, guidance, processes or equipments described in this document, nor for the consequences of that use.

Prepared by:	Pierre-Jacques Courtois (TRC 700)		05/07/2013
Verification:	Kris Beeckmans (TRC 700)		14/08/2013
Approval:	Pieter De Gelder (SIH)	Signed	Signed PDG 14/08/2013

Table of Contents

1 Introduction and Standard Basis

The standards CEI 60 880 and IEEE Std 7/4.3.2 - 2003 are in Belgium references to be followed for the development and use of software implemented in I&C systems and components important to safety[1] used in Nuclear Power Plants.

Under certain conditions, it may however be possible to consider the use of software which has not been specifically developed for nuclear applications according to these two standards. Then, the following principles can be taken into consideration:

- The principles of the report EPRI TR-106439 "*Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications*" of 1996, which was approved by the USNRC under the conditions of RG 1.152 (January 2006),
- The principles of chapter 15 and Annex I of the standard CEI 60880 (Ed 2-2006),
- The principles of chapters 1.4 and 1.15 of the document "*Licensing of safety critical software for nuclear reactors - Common position of seven European nuclear regulators and authorised technical support organisation – Revision 2013"*.

The minimal requirements given in Section 3 are based on the above principles, and define the information that Bel V feels necessary to assess the capabilities of pre-existing software for performing functions important to safety, when this software satisfies the conditions stated in section 2 here below.

2 General Applicability

This guide, and in particular the contents of Section 3, are applicable if and only if the pre-existing software based system or component satisfies the following general conditions:

[1] Systems and components "Important to Safety" are identified and classified on the basis of their function and significance to safety in IAEA Safety Guide No. NS-G-1.3: Instrumentation and Control Systems Important to Safety in Nuclear Power Plants.

2.1. The functionality implemented in software must be simple and limited. More precisely, the functions must be unambiguously *circumscribed*, *specified*, and amenable to *thorough coverage by verification and/or testing*, under all possible modes of operation in service.
The condition may, for instance, be satisfiable by a micro-processor controlled protection relay, but excludes complex software systems such as operating systems, man-machine interfaces, process control or nuclear instrumentation systems.
Assessment of the condition requires engineering judgement and Bel V approval.

2.2. The application hardware and software environment in which the pre-existing software is intended to operate, and the corresponding interfaces, must be specifically and uniquely defined.
The assessment of the aptitude of the software to perform its intended usage and the conclusions thereof are valid for the specified application, environment and interfaces only.

2.3. The experience feedback of the pre-existing software based component or system must be sufficient, adequately documented and pertinent for the expected usage.

3 Minimal Requirements

In order to provide the necessary evidence, the following assessment and documentation tasks should be performed:

3.1 To precisely identify *all* safety related functions to be ensured by the software, and to analyse the importance to safety of every function.
In particular, this analysis must:
- Anticipate all abnormal hardware and software operating conditions *(e.g.* defects of memory, processor, power supply, software), as well as any other event that could interfere with the intended functions;
- When a safety category scheme is applicable, allow the definition of the safety category of every function[2].

3.2 To validate the software implementation of the functions identified in 3.1.
The validation must take into account the possible abnormal operating conditions and events mentioned in 3.1, as well as the auto-tests and self-diagnostics of the system.
The validation can be based on tests realised by the manufacturer, and/or complementary specific tests by the user.
Errors detected by tests or otherwise must be recorded, analysed and subject to non regressive testing; corrections or countermeasures must be documented.

3.3 To specify the required performances (*e.g.* accuracy, response time, cycle time …), and to verify that they are satisfied.

[2] A safety category scheme is applicable in Belgium for software based systems used in NPP's.

3.4 To demonstrate that the functions identified in 3.1 in no way may be affected by other functions of the component or the system (*e.g.* through side-effects of interruptions, erroneous input data, inadequate use or maintenance).

3.5 To collect maximum information giving evidence of the quality
- of the software development, verification and validation processes,
- of the documentation of the software requirement specifications, the code and tests.

3.6 To obtain assurance of the maintenance of the integrity of the hardware and software configuration during the life time of the component/system, including those situations when revisions or modifications are necessary following errors detected in operation, on site or by other users.

3.7 To document and justify the operating experience of the use of the functions identified in 3.1; in particular, the historic of errors and software modifications, the pertinence of the past operational profiles and environmental conditions of use.
To define complementary tests to palliate possible significant discrepancies between the past usage and the current application.

3.8 To report the results of assessments made by qualification or certification bodies, nuclear or other.

4 Acceptance Basis

The licensee must justify that the software based system or component is capable of performing its required functions important to safety. On the basis of the evidence collected by the steps of Section 3, Bel V will assess the validity of this justification and the system/component adequacy to perform its functions in relation to its importance to safety.

For "safety-related software" (as defined by the IAEA classification, *cfr. e.g.* the Safety Guide NS-G-1.1, or belonging to class B or C as defined in standard CEI 61226), the experience feedback defined in 3.7, if justified pertinent, may in some cases complement specific missing elements of evidence relative to 3.2 and 3.5.

5 References

1. CEI 60880, Ed 2 (2006-05): Nuclear power plants - Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions.
2. CEI 61226, (2009) Nuclear power plants - Instrumentation and control systems important to safety – Classification of instrumentation and control functions.

3. IEEE Std 7-4.3.2-2003: IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.
4. US NRC RG 1.152: Criteria for use of computers in safety systems of nuclear power plants, rev 2, January 2006.
5. IAEA Safety Guide No. NS-G-1.1: Software for computer based Systems Important to safety in Nuclear power Plants.
6. IAEA Safety Guide No. NS-G-1.3: Instrumentation and Control Systems Important to Safety in Nuclear Power Plants.
7. Licensing of safety critical software for nuclear reactors - Common position of seven European nuclear regulators and authorised technical support organisation – Revision 2013. *Downloadable from Bel V website* (http://www.belv.be/images/pdf/12-10%20common%20position%20-%202013%20revision%20(secure).pdf)
8. EPRI TR-106439 “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications”, 1996.