Software V&V for digital safety I&C systems in NPPs – Fundamentals and practical application

MIEDL Horst[1], LINDNER Arndt[2], and ZHANG Dan[3]

1. I&C, Safety and Security, TÜV Rheinland ISTec GmbH – Institut für Sicherheitstechnologie, Garching-Forschungszentrum Boltzmannstr. 14, Garching 85748, Germany (Horst.Miedl@de.tuv.com)
2. I&C, Safety and Security, TÜV Rheinland ISTec GmbH – Institut für Sicherheitstechnologie, Garching-Forschungszentrum Boltzmannstr. 14, Garching 85748, Germany (Arndt.Lindner@de.tuv.com)
3. Quality Department, China Techenergy Co., Ltd, Building 5 No.5 Yongfeng Road, Haidian District, Beijing 100094, P.R. China, (ZhangDan@ctecdcs.com)

Abstract: The development of digital safety I&C systems needs a careful consideration of the software qualification. Software qualification has to demonstrate that the software meets requirements given by standards regarding the life cycle, documentation, configuration management, requirements specification, design, implementation, tests, verification and validation (V&V), and the modification procedure. This paper provides fundamentals as well as TÜV Rheinland ISTec's software V&V procedure and the corresponding activities. The paper is completed by the description of a practical application of ISTec's approach.
Keyword: Digital safety I&C; software V&V

1 Introduction

The development of digital safety instrumentation and control (I&C) systems needs a careful consideration of the software qualification. Quality cannot be inserted into a product by expert evaluation and assessment. It must be inserted during the development and production process. Verification and validation is an essential part of the software development life cycle to obtain high-quality software products.

Verification is defined as the process of determining whether the quality or performance of a product or service is as stated, as intended or as required [1]. This means the assessment of the results of an individual activity against its input.

Validation is defined as the process of determining whether a product or service is adequate to perform its intended function satisfactorily [1]. This means the assessment of the final product against its documented objectives and requirements.

2 Fundamentals

2.1 Software versus hardware qualification

Hardware is usually qualified by testing. Typical examples are function tests, climatic tests, seismic tests, EMC tests, and runtime tests (*e.g.* 1000 h test regarding KTA, the body preparing German rules for equipment of nuclear power plants (NPP)).

Software requires another approach, because software performs complex functions and it cannot be tested 100%. Software is also not dependent on environmental impacts and it behaves "digital" (*e.g.*, abrupt behavior in case of failure). In addition, security aspects are of increasing relevance.

2.2 Software verification and validation

The software V&V activities comprise the verification of development documents (life cycle documentation) and the validation of the completely coded software components. Verification requires assessing and evaluating whether the documents themselves are consistent with the specifications of national and international standards as well as internal guidelines and rules of the software designer. Furthermore, the documents have to be assessed and evaluated to what extent they concur with the requirements established in the preceding phases. In case of generated software code, verification activities can combine development phases.

Validation requires assessing and evaluating whether the software meets the requirements stated in the requirement specification. Validation comprises extensive tests of the software.

Received date: February 2, 2015

The V&V activities are performed as reviews, analyses and tests. There are numerous methods and techniques to realize these activities. Annex E (informative) of the international standard IEC 60880:2006 [2] and Annex G of the standard IEEE Std 1012™-2004 [3] provide comprehensive discussion of V&V methods.

3 Software V&V procedure

TÜV Rheinland ISTec's software V&V procedure was originally modeled on the international standard IEC 60880:1986 [4] and has been adapted to the current version of IEC 60880:2006.

The software V&V activities are specified in form of checklists. The checklists are applied to the development documents of all safety software components, *i.e.* to

- Requirements specification
- Preliminary design specification
- Detailed design specification
- Source code
- Test documentation

The documents are reviewed and assessed according to the requirements of the applicable international standards and with respect to the consistent transition of one phase to the other within the software safety lifecycle.

In case of platform qualification, the software V&V may also include the evaluation of a representative I&C system built with the software components to demonstrate operability of the software and generic platform characteristics. Characteristics can be confirmed as generic ones if they are valid independent from the configuration of the hardware and software components.
The V&V activities and contents are detailed in the following subchapters.

3.1 Review of requirements specification

The requirements specification is the first and indispensable part of the development of software components and systems. It must define the functional, technical and qualitative requirements for the component to be developed. Additionally, it has to specify the quality assurance measures as well as acceptance conditions. In case of software components their role within the system has to be presented. Dependent on the safety requirements there are gradations with respect to content and methods for the development and review activities.

The description of the V&V activities concerning the requirements specification is organized in three sections. At first the consistency check shall demonstrate the transparency and the consistent usability of the document. The check of completeness related to content shall show that the component description is comprehensive and sufficient. Finally, evidence of suitable shall be provided that the layout format suits for the technical realization of the required functions.

3.2 Review of documents of subsequent phases

Basis for the composition of the documents of the subsequent phases are the tasks and requirements specified in the requirements specification as well as the documents of the directly preceding phase. The tasks are analyzed, if necessary re-structured and grouped according to data processing aspects, and described in form of functions which can be realized by data processing means.

Just as for the requirements specification three sections of V&V activities are distinguished:

- Consistency check
- Check of layout and description format
- Check of completeness related to content

The review tasks as described for the requirements specification can be transferred to the documents of the subsequent phases, i.e. the preliminary design, the detailed design and the test documentation. The review tasks depend on the organization of the specific phase model of the development life cycle.

3.3 Review of test documentation

For the verification and qualification of coded program parts (modules, integrated software components, program units) the test of the programs is of decisive importance. This includes the selection of suitable test cases and the observation that the behavior is compliant to the requirements. For the effective preparation of testing of the programs (selection of an exhaustive test set for a defined test strategy) a series of complementary and additional

program analyses can be foreseen, besides the actual tests for correctness and robustness. Therefore, the review of the test specification and test report includes not only the check of the planned and executed program tests (test strategy, selection of test cases, test execution, test evaluation) but also the assessment and evaluation of the program analyses to be applied.
Just as for the requirements specification the three sections of V&V activities described above are applicable.

3.4 Traceability of requirements

Analyses have to be carried out to check the formal and technical traceability of the functional and non-functional requirements. The formal traceability is related to the complete transition of the requirements during all phases of the development life cycle. The requirements are traced downwards to the final software code and upwards to the V&V activities.

Traceability includes demonstration that all testable requirements are tested and vice versa.
The technical traceability is related to the consistency and plausibility of the contents of the derived/refined requirements, design decisions or other phase outputs. Consistency and plausibility is analyzed with respect to the preceding phase and between the phase outputs themselves.

3.5 Review of compliance with programming rules

For the transfer of the program design into the source code language a set of rules has to be obeyed in the context of "good programming style" in order to obtain improved readability, modifiability and testability. Some requirements, *e.g.* the limitation to certain language constructs, are indispensable precondition for specific validation techniques and effective program testing.

3.6 Review procedure

The following figure illustrates TÜV Rheinland ISTec's software V&V procedure. The basic principle is the review of the documentation including their consistency, formal aspects, and functional aspects.

The documents are assessed for internal consistency and completeness (self-contained assessment) and for consistency with superior documents, respectively with the requirements from previous development phases.
Every document is examined in form and content and special attention is paid to the conformity with the applicable standards.
The formal check evaluates aspects, e.g. meaningful identification, consistent use of references or clear structure and comprehensible document text including figures and tables. Source code analysis is executed to assess the compliance with programming rules and conventions, e.g. no recursions, limited use of global variables, structuredness, *etc.*

Checks against general development principles like top-down design, modularity, well-defined structures, normed structure elements, and autonomous design units, are evaluated as part of the content assessment. During the content assessment functional consistency, correctness and completeness are evaluated by, *e.g.*

- Check of correct and complete transition of functional and non-functional requirements
- Check that test execution covers all essential requirements
- Presence of certain information in the development documents, *e.g.* tasks' description, internal and external interface description, failure behavior, quality measures, *etc.*

Fig. 1 Review procedure.

The continuous lines in Fig. 1 aim to describe the independent assessment activities. In the case of key findings requiring the repetition of the independent assessment, the dashed lines indicate that assessment

activities has to be redone and a comparison of the revised document with the old revision shall confirm that the required changes have been done.

Questions, comments, and findings concerning the documentation are recorded in Lists of Open Points (LOPs). The LOPs' contents are structured in tables of

- minor issues (*e.g.* typing errors, form errors)
- requests (*e.g.* wrong descriptions of technically correct items, inconsistent or insufficient descriptions)
- key issues (*e.g.* non-conformance with IEC standards, or equipment characteristics)
- compliance with standard requirements

The LOPs are communicated to the developer who gives answers to the LOP and revises - if necessary - the corresponding document. The developer's answers are to be checked for compliance. This procedure is repeated until all open points are resolved (dashed lines in Fig. 1).

The V&V activities are finalized by assessment reports that summarize the contents of the LOPs, and provide the assessment conclusion. In case of successful assessment conclusion TÜV Rheinland ISTec issues certificates.

4 Practical application

4.1 Introduction

China Techenergy Co. Ltd. (CTEC), a joint venture co-funded by China Guangdong Nuclear Power Group and Beijing Hollysys Co. Ltd., does engineering design of digital I&C systems, system integration, and technical service for nuclear power plants.

CTEC has developed the digital I&C platform FirmSys to be used in systems important to safety for nuclear power plants. In order to qualify the FirmSys platform for the international market, CTEC asked TÜV Rheinland ISTec to carry out - as third party - the independent verification and validation (IV&V) of the FirmSys platform software.

The project was spilt into three phases:

- Preparatory Phase A from November 2011 to April 2012 for the preliminary assessment of the platform software concept and of the software of the main processing unit,
- Phase B from February 2013 to November 2013 for the final assessment of the platform software concept and of the software safety modules,
- Phase C from December 2013 to August 2014 for the detailed assessment of the complex programmable logic device (CPLD) logic software, the engineering workstation software tools, and the function block (FB) library.

4.2 Assessment scope

The assessment was applied to the platform concept description, the development and test documentation of the FirmSys platform software including the software safety modules, the CPLD logic software in net communication modules, code transformation modules of the engineering workstation software, and of the function block library used for application software development. These documents cover relevant process and product issues.

The IV&V procedure contained activities for requirements analysis, design, coding and testing. The activities were organized according to the software life cycle phases as applied to the FirmSys platform concept and software, and to the software safety modules.

The detailed assessment has been carried out in order to prove compliance of the software and its development life cycle with the requirements based on the international standards as listed in Table 1.

4.3 IV&V procedure

The IV&V was performed by TÜV Rheinland ISTec and assisted by the V&V team of CTEC. The V&V team of CTEC is independent from the development team of CTEC. TÜV Rheinland ISTec has been responsible for the overall IV&V works and results approval. Any issue raised by the IV&V team was collected in Lists of Open Points (LOP). The LOP collected and categorized the IV&V findings in tables of minor issues, requests and key issues. Compliance with standard requirements was documented in specific tables of the LOP.

All open points have been clarified by the development team of CTEC. The clarification results were verified and closed by TÜV Rheinland ISTec assisted by the V&V team of CTEC. The overall

software assessment activities and assessment results were compiled in assessment reports. The assessment reports summarized the contents of the LOPs and gave the assessment conclusions. In addition, the assessment reports gave detailed reference to the assessed documents and code files. The referenced data was uniquely identified by checksums using the method of RIPEMD-160. Together with the assessment reports TÜV Rheinland ISTec issued certificates. The certificates corroborate the basic suitability of FirmSys platform concept and software. The FirmSys software safety modules are suitable to implement the software of I&C functions important to safety in NPPs.

The assessment was performed in form and content, applying the requirements of the standards given in table 1 and with respect to the consistent transition of one phase to the other within the software safety life cycle. In order to locate potential deficiencies all assessed documents were subjected to formal checks, consistency checks, and functional checks.
In addition, the following analyses were performed for the development documents.

- Criticality analysis,
- Requirements allocation analysis,
- Traceability analysis,
- Interface analysis,
- Hazard analysis,
- Security analysis, and
- Risk analysis.

For the test documents the following analyses were applied.

- Traceability analysis,
- Hazard analysis,
- Security analysis, and
- Risk analysis.

Table 1 Applied standards

IEC 61513:2011, Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems, Ed. 2.0, 2011-08
IEEE Std 7-4.3.2™-2010, Standard criteria for digital computers in safety systems of nuclear power generating stations, 2010-08
IEC 60880:2006, Nuclear power plants - Instrumentation and Control Systems important to Safety - Software aspects for computer-based systems performing category A functions, Ed. 2.0, 2006-05
IEC 62566:2012, Nuclear power plants – Instrumentation and control important to safety –Development of HDL-programmed integrated circuits for systems performing category A functions, Ed.1.0, 2012-01
IEEE Std 1012™-2004, IEEE Standard for Software Verification and Validation, 2005-06

In case of IEEE Std 7-4.3.2™-2010 also the differences to the former version from the year 2003 were taken into account during assessment.

5 Conclusions

This paper provides fundamentals as well as TÜV Rheinland ISTec's software V&V procedure and the corresponding activities. The procedure has been successfully applied by TÜV Rheinland ISTec for the generic qualification of the software of different I&C equipment and system platforms.

In case of platforms hardware and software components relevant for possible I&C system applications are integrated to be tested as a representative system. The representative system contains hardware and software components which are typically expected by an I&C system. Generic platform characteristics are qualified as invariant as far as possible. That means that the platform characteristics are valid independent from the configuration of the hardware and software components. If this is not the case, the qualification result is restricted to the corresponding configuration which the platform characteristic is valid for.
This paper shows the application of the V&V procedure to the digital I&C platform FirmSys of CTEC. It is to be used in systems important to safety for nuclear power plants.

References

[1] IAEA Safety Glossary, Terminology Used in Nuclear Safety and Radiation Protection, 2007
[2] IEC 60880:2006, Nuclear Power Plants - Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions, 2006
[3] IEEE Std 1012™-2004, Standard for Software Verification and Validation, 2005
[4] LINDNER, A., and WACH D.: Experiences Gained from Independent Assessment in Licensing of Advanced I&C Systems in Nuclear Power Plants, Nuclear Technology **143** (2003), pp. 197-207
[5] MIEDL, H., and MARTZ J.: Qualification of Integrated Tool Environments (QUITE) for the Development of Computer-Based Safety Systems in NPP, NPIC & HMIT, Albuquerque, USA, 2006