A Study About Pre-developed Software Qualification of Smart Devices Applied in NPP

Sheng-Chao Wang(✉), Tao Bai, Peng-Fei Gu, and Wang-Ping Ye

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, I&C Equipment Qualification and Software V&V Laboratory, China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, Guangdong, China
18566693557@163.com

Abstract. According to the research and analysis about the standards and Electric Power Research Institute (EPRI) relevant reports of commercial grade dedication (CGD) such as the pre-developed software of smart devices which perform intelligent measuring, communication and actuation devices employing programmed electronic components (PEC) to enhance the performance, the requirements for the pre-developed software qualification has been identified. And in combination with the tasks of IEEE 1012, a V&V model was proposed to guide the concrete execution of qualification activities such as suitability evaluation, quality evaluation, operating experience evaluation, additional system test and comprehensive assessment. Besides, it also helps establish the specification and process for the pre-developed software qualification. On the basis of that, a pre-developed software qualification was performed for each qualification activity, and forming some good practice in the process. At the same time some special considerations are put forward for the pre-developed software qualification. Furthermore, some critical qualification points has been captured and may provide some technical reference for subsequent CGD such as the pre-developed software of smart devices which will be applied in the HPR1000 and other nuclear power plants (NPPs).

Keywords: Pre-developed software · Smart devices · Software V&V · Standard requirements

1 Introduction

With the development of the smart technology, smart devices which can perform intelligent measuring, communication and actuation device employing PEC with embedded software to enhance the performance, have been increasingly used to replace the conventional devices in the safety instrumentation and control (I&C) systems of nuclear power plant (NPP) for improving economic efficiency. Although there are lots of advantages like greater accuracy, better noise filtering, in-built linearization and on-line calibration and diagnostics, a smart device is generally a commercial-off-the-shelf (COTS) product sold as black-box and it's hard to demonstrate the reliability and potentially increases risk of common cause failure (CCF). Therefore, even though there is extensive and mature application in other non-nuclear industries, a smart device

Y. Xu et al. (Eds.): *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, LNEE 507, pp. 48–57, 2019.
https://doi.org/10.1007/978-981-13-3113-8_6

should be thoroughly tested and evaluated, or dedicated for NPP safety application, especially for the pre-developed software (also called COTS software) of the smart device, which is directly effecting the safe and reliable operation of NPP and should be paid more attention to guarantee the safety function to be implemented correctly.

However, there are many issues for the pre-developed software qualification of smart devices applied in NPP, such as lack of unclear-specific, hidden changes, internal complexity, requiring manufacturer's intellectual property. Besides, it's lack of nuclear engineering experience for the pre-developed software independent qualification in the domestic. In order to meet related regulatory requirements and achieve the goal of going out of specified software matching with the HPR1000, it's necessary to carry out software qualification standard and technology research for the autonomous pre-developed software.

The study firstly researches the relevant guidelines and standards and refers to EPRI related technical reports, teases out the specific requirements for the pre-developed software. Then an appraisal plan is put forward including the qualification process and methods, and the implementation effort of the plan will be illustrated by a concrete engineering practice. Finally, the main technical points are summarized to provide technical reference for subsequent engineering practice.

2 The Analysis of Guides, Standards or Reports

The concept of CGD has already been proposed in the nuclear safety guide HAD 102/16 by China, but it has not yet formed a perfect and enforceable scheme or procedure, which mainly refers to the relevant standard system in Europe, America or international organization [1]. The Fig. 1 is the context diagram of relevant documents for CGD like pre-developed software qualification.

2.1 Requirements or Criteria of China

The requirements and recommendations were proposed in the annex I of the HAD 102/16 for the application and validation of software developed in accordance with high standard in other industrial safety critical application [1].

(a) Define the functions of existing software and evaluate the impact of these functions on safety.
(b) Clearly identify existing software like the program version.
(c) Clearly identify and fully confirm the interfaces of existing software required by user or other software, and provide evidence to indicate that no other call sequence is available.
(d) Develop and maintain the existing software according to good software engineering practice and quality assurance.
(e) The existing software used by the safety system should be subjected to the same assessment as the final product of the newly developed application software. If necessary, the reverse engineering should be implemented to evaluate the full specifications of the existing software.

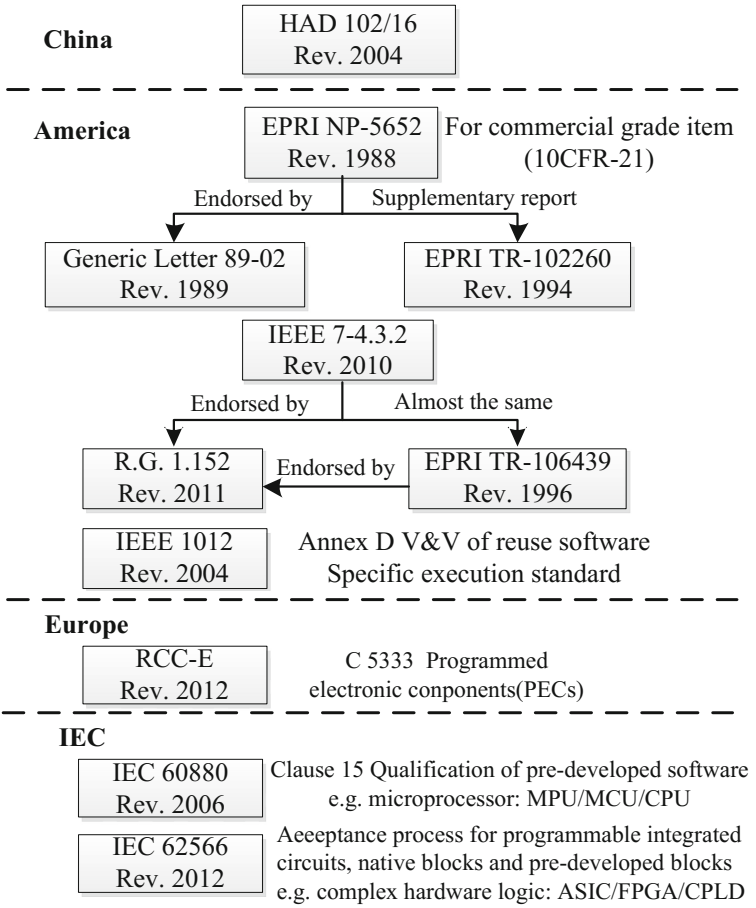

Fig. 1. Relevant documents of pre-developed software qualification

(f) Get the design documents and source code if there need to modify the existing software.
(g) The information should be available for the evaluation of the quality of existing software and the development process, and meet the requirements of assessing the quality level of existing software.

Acceptance of existing software shall be performed as follows.

(a) Verify the functions implemented by existing software meets all requirements described in the safety system requirement specification and other application specification.
(b) Verify existing software didn't refer to the functions that safety system requirements specification doesn't require, and isn't response to the adverse effects for the functions required.
(c) Compliance analysis between standard requirements used and software design.

(d) Validate the expected use of functions of existing software through test which includes the test completed by the supplier.
(e) Ensure the functions of existing software aren't used by the safety system, other software and user in the way that isn't specified and tested.

If possible, to get sufficient operation historical information and failure rate data and properly evaluate experience feedback based on the analysis of operation time, error report and delivery history in the related system's operation.

If relevant software development information isn't sufficient and available, the risk assessment should be carried out for safety impacted by the software fault.

2.2 Requirements or Criteria of Europe and America

After the investigation and research of the American nuclear industry practice, The EPRI published the technical report EPRI NP-5652 to guide the application of commercial grade item like pre-developed software of NPP in 1988, which expounds evaluation background, objective, basic concept, general process and basic method and puts forward a verifying method that consists of technical evaluation and acceptance [2]. And the guide report was endorsed by NRC through the Generic Letter 89-02 in 1989. After that, the EPRI published the supplementary report EPRI TR-102260 to complement some key issues of EPRI NP-5652 in 1994, including how to implement technical evaluation, general acceptance and evaluate the assessment procedure for commercial grade item [3].

Besides, the EPRI published the EPRI TR-106439 to discuss about the evaluation and method of the key characteristics of digital devices in 1996 [5]. The critical characteristics are physical critical characteristic evaluation, performance critical characteristic evaluation and dependability critical characteristic evaluation.

On the basic of a series of the studies by EPRI, the IEEE published IEEE 7-4.3.2-2010, which is almost the same with EPRI research reports above [4]. According to the requirements of this standard, the process of CGD of digital devices consists of the preparation phase, implementation phase and design review phase. And the NRC published the corresponding guidance R.G. 1.152-2011 to endorse the standard and EPRI TR-106439 through evaluation report [6].

For the requirements of guides, standards or technical reports, the IEEE 1012-2004 Annex D will be a good reference for the pre-developed software qualification, which put forward the detailed V&V activities and tasks [7].

Furthermore, the French standard RCC-E-2012 clause C5333 introduces the Characteristics and requirements of the programmed electronic components (PECs) [8]. For the PECs applied in the C1 and C2 classified systems, how to sufficiently guarantee in terms of their quality and reliability is related to development cycle, the follow-up of their software and hardware components, any existing experience feedback that may be available and their qualification.

2.3 Requirements or Criteria of IEC

The specific qualification requirements of pre-developed software is put forward in the IEC 60880 clause 15, mainly including suitability evaluation, quality evaluation, evaluation of operating experience and comprehensive assessment [9].

The IEC 62566-2012 provides how to select and assess pre-developed items when developing the HDL-Programmed Device (HPD) [10].

3 The Model of Pre-developed Software Qualification

For this study, the research object of smart device is a breaker (C1 classified system) with micro-logic trip unit, which belongs to mature commercial grade item and has been ten years of good performance so far. The functions of breaker are mainly realized by pre-developed software developed by ASIC technology. And the development language includes VHDL and C++. Therefore, this study is at the same time to consider the requirements of RCC-E-2012, IEC 62566-2012 and IEC 60880-2006 when performing the pre-developed software qualification. The suitability analysis of the three standards sees the Table 1.

Table 1. Standards suitability analysis of ASIC

RCC-E C5333-2	IEC 62566 clause 7	IEC 60880 clause 15	Conclusions
Development cycle and relevant documents	7.4 selection 7.4.2 Documentation review	15.3.2 Quality evaluation	The requirements of the standards are basically the same
Qualification requirements			
Supervision for software and hardware components and requirements for software modification	7.6 Modification for acceptance	15.4 Requirements for integration in the system and modification of PDS	
Available experience feedback data	7.4 selection 7.4.3 Operating experience review	15.3.3 Evaluation of operating experience	
Requirements of test and additional test	7.4 selection 7.4.2 Documentation review	15.3.1 Suitability evaluation 15.3.2 Quality evaluation	

After specifying the specific qualification requirements through Table 1, the qualification requirements were assigned to the verification and validation (V&V) activities and tasks of the IEEE 1012 that can be performed. The specific assignment and process of ASIC qualification can see the Fig. 2.

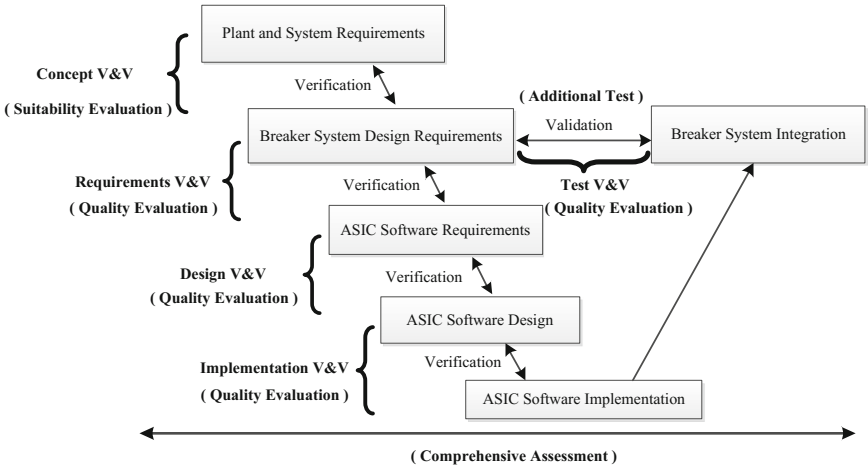

Fig. 2. Process of pre-developed software qualification

4 Qualification and Results of ASIC

Because the breaker will eventually be used for the three generation NPP HPR1000 to perform safety functions, V&V team performed suitability evaluation, quality evaluation, evaluation of operating experience and additional system test in order to guarantee high reliability of the ASIC.

(1) Suitability evaluation

- Required input documentation
  - System specification documentation
  - PDS specification and user's documentation
- Evaluation requirements
  - Comparison of the system and PDS specification
  - Identification of modifications and missing point
- Performing evaluation
  - According to the required input documentation and evaluation requirements, the adaptive V&V tasks are suitability analysis and traceability analysis which can be well to identify of modifications, missing point or inconsistencies through comparison of the system and PDS specification.
  - And the efforts of the V&V tasks performed had found two kinds of anomalies. The one is the requirements of system specification documentation don't reflect in the PDS specification and user's documentation. The other one is the requirements of timing characteristic of the ASIC can't be proved.
- Preliminary evaluation conclusion
  - The conclusion of suitability evaluation is that complementary work is needed to clarify the anomalies or provide convincing proof.

(2) Quality evaluation

- Required input documentation
  - Design documentation
  - Life cycle documentation
- Evaluation requirements
  - Analysis of design
  - Analysis of the quality assurance (QA)
  - Identification of missing point
- Performing evaluation
  - According to the required input documentation and evaluation requirements, the adaptive V&V tasks are applicable standards compliance analysis of the RCC-E, IEC 62566 and IEC 60880 and traceability analysis.
  - The applicable standards compliance analysis is to evaluate the compliance between the requirements of the standards and input documentation. The AISC design shall be consistent with the constraint of the system architecture and deterministic internal behavior. If a behavior adopted is different from the requirement of the standards in the ASIC development, it shall be analyzed and justified. And if there is a secondary function of the software, the influence to the main function shall be analyzed.
  - The traceability analysis is mainly to validate the bidirectional tracing relationship between input documentation, ensuring its correctness, accuracy, completeness and consistency.
  - And the effort of the V&V tasks performed was to find an anomaly that the development team widely uses self-developed tools for ASIC development and test, which the reliability of the tools has not been fully guaranteed.
- Preliminary evaluation conclusion
  - On the basis of the evaluation effort above, it's necessary to require the additional test and documentation or operating experience evaluation.

(3) Evaluation of operating experience

- Required input documentation and evaluation requirements
  - The methods for collection of data and recording the PDS version operating time
  - The operating history of finding, defects and error reports and of modifications.
- Performing evaluation
  - According to the required input documentation, evaluation requirements and the results of the suitability evaluation and quality evaluation, the evaluation of operating experience was to evaluate the evidence provided by the supplier of breaker including the pre-developed software. The evidence is the operating experience of the product collected globally by the supplier through automated management and configuration tools and the operating time is about ten years.

- Preliminary evaluation conclusion
  - The conclusion of the evaluation is that the supplier provides sufficient operating experience.

(4) Additional system test

- Required input documentation
  - System design requirements specification documentation
  - PDS specification and user's documentation
- Evaluation requirements
  - Confirm that the breaker can meet the functional and interface requirements.
- Performing evaluation
  - According to the required input documentation and evaluation requirements, V&V team firstly analyzed the test requirements and combed out the requirements items. Based on this, it's to prepare V&V plan and corresponding test description. Then, it's to design the test case for the each test requirement.
  - And the result of system test showed that the design of breaker covered the functional and interface requirements. However, there are some abnormal items, which is the performance parameter like the time response is inconsistent with specific requirement.
- Preliminary evaluation conclusion
  - The conclusion of system test is that retest is needed or the development team needs to clarify the anomalies and make it justified.

(5) Comprehensive assessment

- Required inputs
  - The results of suitability evaluation, quality evaluation, evaluation of operating experience and additional system test.
- conclusion
  - The applicability of the commercial grade item of breaker, which will be used in NPP to perform safety functions, depends on the handling of the found anomalies and the supplementary clarifications by the supplier.

(6) Special consideration

For the product of the breaker including the pre-developed software performing safety functions in NPP, the hazard analysis and security analysis are needed. FMEA method is recommended for hazard analysis. And the specific requirements of security analysis can see the clause 5.7 of IEC 60880, mainly focus on the security during design and development and the user access. After that, it's to execute the risk analysis on the basis of the hazard analysis and security analysis. When the inputs of the tasks of the qualification activities above aren't available and may reduce visibility into the pre-developed software products and processes, some techniques listed below are optional to compensate for the lack of the inputs. Each has varying strengths and weaknesses. Therefore, it's need to consider

performing multiple techniques to offset the weaknesses of one technique with strengths of the others when high confidence is demanded.

- Black box testing
- Review developer's QA
- Operational history
- Audit results
- Artifacts
- Reverse compilation
- Prototyping
- Prior system results

5 Conclusions

According to the research and analysis about the standards and EPRI relevant reports of CGD, the requirements for a smart device breaker including pre-developed software has been identified. And in combination with the tasks of IEEE 1012, a V&V model was proposed to guide the qualification activities, which also helps establish the specification and process for the pre-developed software qualification. On the basis of that, the pre-developed software qualification had been performed and formed some good practice in the process. All of qualification efforts can be the evidence as the evaluation for the reliability of the pre-developed software and promote the confidence of the software used to perform safety functions. Furthermore, some critical qualification points has been captured and may provide some technical reference for subsequent CGD such as the pre-developed software of smart devices which will be applied in the HPR1000 and other NPPs.

References

1. HAD 102/16: Nuclear Power Plants-Systems Important to Safety-Software Aspects for Computer-based Systems. National Nuclear Safety Administration (2004)
2. EPRI NP-5652: Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications (NCIG-07). Electric Power Research Institute (1988)
3. EPRI TR-102260: Supplemental Guideline Application of EPRI Report NP-5652 Commercial Grade Items. Electric Power Research Institute (1994)
4. IEEE Std.7-4.3.2: IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations. Institute of Electrical and Electronics Engineers (2010)
5. EPRI TR-106439: Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Application. Electric Power Research Institute (1996)
6. R.G. 1.152: Criteria for Use of Computers in Safety Systems of Nuclear Power Plants. Regulatory Guide Office of Nuclear Regulatory Research of U.S. Nuclear Regulatory Commission (2011)
7. IEEE 1012: IEEE Standard for Software Verification and Validation. Institute of Electrical and Electronics Engineer (2004)

8. RCC-E: Design and Construction Rules for Electrical Equipment of Nuclear Islands. French Association for Design, Construction and In-service Inspection Rules for Nuclear Island Components (2012)
9. IEC 60880: Nuclear Power Plants-Instrumentation and Control Systems Important to Safety-Software Aspects for Computer-based Systems Performing Category A Functions. International Electro-technical Commission (2006)
10. IEC 62566: Nuclear Power Plants - Instrumentation and Control Important to Safety-Development of HDL-programmed Integrated Circuits for Systems Performing Category A Functions (2012)