Study on Itemized Requirements of Safety Digital I&C System in NPP

Tao Bai[1(✉)], Ji-Xiang Shu[2], Peng-Fei Gu[1], and Ya-Nan He[1]

[1] State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, I&C Equipemnt Qualification and Software V&V Laboratory, China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, Guangdong, China
tao_bai@cgnpc.com.cn
[2] Shenzhen Middle School, Shenzhen, China

Abstract. Software reliability for digital instrumentation and control (I&C) systems is critical, which malfunction may give wrong action and endanger the nuclear power plants. Software verification and validation (V&V) is an effective means of improving software reliability. With the further research on safety-critical software used for NPPs, the quality of V&V has become key concern of the safety regulatory authorities around the world. Traceability is the basic requirement on I&C functions during the life cycle V&V activities. In this paper, necessity of implementing itemized requirements on I&C function is studied according to the nuclear safety regulations and related standards. What's more, key points of itemized requirements are proposed by learning from CPR1000 NPPs' project experience. It would be helpful to ensure the software V&V quality with proper workload.

Keywords: Digital I&C system · Safety software · Software life cycle · Itemized requirements · Verification and validation

1 Introduction

Nowadays, more and more digital instrumentation and control (I&C) systems are adopted by nuclear power plants (NPPs). Especially safety-critical digital protection system is used as critical safeguard against the severe accidents like reactor core damage, release of radioactive materials and etc. It is the software that realizes control functions executed by CPU, which malfunction may give wrong action and endanger the nuclear power plants. Therefore, software reliability for digital I&C systems is critical to the safety of NPPs. Different from the stochastic failure of analog I&C systems, software failure may be caused by systematic design fault, human error and tools failure. Some traditional analog system (hardware) reliability analysis methods are not applicable to software. Software reliability qualitative analysis and quantitative analysis methods are still in discussion. The consensus amongst the world's experts is that rigid lifecycle quality management, and verification and validation (V&V) are the most effective ways to improve the software reliability presently. With the further

Y. Xu et al. (Eds.): *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, LNEE 507, pp. 226–232, 2019.
https://doi.org/10.1007/978-981-13-3113-8_26

research on safety-critical software used for NPPs, the quality of V&V has become key concern of the safety regulatory authorities around the world.

According to the requirements of nuclear safety regulations and related standards, some mandatory software V&V activities through life cycle phases are defined for the different safety-graded software explicitly [1–4]. For safety-critical software, the required scope, intensity and degree of rigor associated with the V&V activities and tasks are the highest among all graded I&C systems. It should be mentioned that traceability analysis is the most basic one for safety-critical software and I&C systems and affects the quality of other V&V activities directly. Traceability analysis is also required by EUR [5]. It is used to confirm implementation and validation of requirements, where neither any extra function is allowed, nor is any necessary function missed. The quality of traceability analysis depends on the granularity of itemized I&C function requirements. The finer granularity of itemized I&C function requirements is, the easier it is to find the potential software failure, and the higher quality the traceability analysis gets. However, it also means heavier burden of V&V activity. Therefore how to effectively itemize I&C functions is an important question.

In this paper, the V&V activities through software life cycle related nuclear safety regulations and standards are analyzed in Sect. 2. Necessity of implementing itemized requirements on I&C function during software development life cycle is studied according to the nuclear safety regulations and related standards in Sect. 3. What's more, key points of itemized requirements are proposed by learning from some NPPs project experience in Sect. 4. Finally, Sect. 5 gives the conclusion.

2 Software Life Cycle

ISO/IEC 12207 defines the software life cycle processes at a high level and their corresponding minimum tasks, but how to perform these tasks is not given clearly [6]. As shown in Fig. 1, V&V processes related to the software life cycle are defined in IEEE 7-4.3.2 and IEEE std. 1012 [2, 3]. Seven processes for software life cycle are defined, including Acquisition, Supply, Development, Operation, Maintenance, Organizational and Other Supporting. Moreover, Development Processes are divided into six phases further, i.e., Concept, Requirements, Design, Implementation, Test, and Installation and checkout. Different mandatory V&V activities and tasks with their assessment criteria are defined for safety-graded software as part of the software life cycle explicitly. Verification of a software product of a phase should be performed before the start of the next phase and shall be performed before the completion of the next phase, as required by IEC 60880 [4].

In each phase of software life cycle, software fault or failure is inevitable because of human error, systematic design fault and tools failure. Software reliability qualitative analysis and quantitative analysis methods have not been accepted universally. Therefore, the feasible and practical measures are used to focus on the product quality of each phase. V&V activities should be performed to ensure that the product meets the requirements of its input of each phase and no new errors are induced, so that the reliability of final product is limited within the acceptable level.

As the most basic requirement, each I&C function documentation should be traceable throughout the software life cycle. Traceability analysis should be performed to demonstrate that each I&C function integrated in the digital I&C systems are complete with respect to their system design specification. That is, neither any extra function is allowed, nor is any necessary function missed. However, the granularity of itemized I&C function requirements would affect the quality of V&V activities, especially of traceability analysis directly. Therefore, how to effectively itemize I&C functions is an important issue.

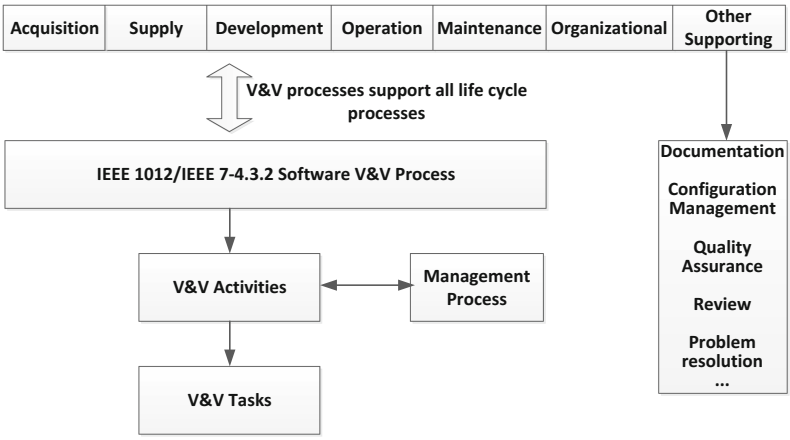

Fig. 1. Software life cycle processes according to IEC 12207

3 Necessities of Itemized Requirements

IEEE has published a series of standards on recommended practice for software development documentation, such as IEEE std. 1233, IEEE std. 830 and IEEE std. 1016 [7–9]. However, development teams do not comply with these standards rigidly and do not develop their software documents according to software quality characteristics hierarchically.

Shown in Fig. 2 as an example, it describes the maintenance tool design of digital protection system for a CPR1000 NPP in software concept phase. On one hand, the design description of functions, interface, separation and isolation for the maintenance tool is mixed in one paragraph. On the other hand, the function interfaces with on-line monitoring, diagnosis and parameter calibration are not given, which need to be searched for and checked by the V&V team from the other parts of the documents. As a result, it will burden the traceability analysis and may decrease the quality of V&V activity.

Maintenance tool performs on-line monitoring, diagnosis and parameter calibration throuth maintenance network for the safety-critical distributed control system. Due to the maintenance tool is non-safety related, the physical separation and electrical isolation from the safety-critical systems are realized by the following measures (where detailed information are omitted).

Fig. 2. Snapshot of maintenance tool design description

4 Discussions on Itemized I&C Requirements

Learning from some NPPs project experience, difficulties of itemized I&C requirements are discussed and key points are proposed for implementation of itemized I&C function requirements.

4.1 Difficulties of Itemized I&C Requirements

According to our practical experience, the following difficulties are summarized.

(1) Granularity of itemized I&C function requirements

As the example shown in the previous section, if one paragraph is defined as a traceable item, one-to-many mapping will exist in the traceability matrix, where some slight but important information may be overlooked among the traceable items. It means the itemized I&C function requirements are coarse and are difficult to be managed effectively.

However, the finer granularity of itemized I&C function requirements is, the easier the potential software failure is found, and the higher quality the traceability analysis could be increased. It would increase the workload of V&V team.

(2) Identification number coding rules for itemized I&C function requirements

It is necessary to define well-defined and readable identification number coding rules for itemized I&C function requirements. Unfortunately, the traceable items are not coded or are coded without uniform coding rules for different projects in practice. It should be studied what kinds of key information be given, such as information of system, sub-system or components, quality characteristics and so on.

(3) Itemized requirements for I&C diagrams

Compared with the language description of I&C functions, diagram description is more accurate, more intuitive and easier to be understood. Usually, there are all kinds of I&C diagrams used in project practice, including Logic Diagrams (LD), Analog Diagrams (AD), Function Diagrams (FD) and Configuration Diagrams. There are nearly 10 thousands pages of I&C diagrams for the safety-critical I&C system. Each page of I&C diagrams may contain large amounts of data, such as functions, interfaces, setting values and etc.…If one page is defined as a traceable item, too much data may be ignored easily. The pages of I&C diagrams are also strongly correlated with each

other. As a result, it would be hard to analyze the traceability among those I&C diagrams. Moreover, it would also be very hard to trace the relationship between documents and diagrams due to their completely different ways of expression.

4.2 Key Points of Itemized I&C Requirements

Good practice on itemized I&C requirements can be learned from some new generation NPP projects. Their document architecture is defined and I&C requirements are itemized, refined and marked by specific identification numbers. Itemized I&C requirements in upstream documents are inherited by downstream documents explicitly, which makes it easy for V&V team to trace and review I&C requirements.

Based on the above discussion, an itemized scheme for I&C requirements is proposed. Its key points are listed as follows.

(1) To specify new document architecture, where I&C requirements are itemized according to quality characteristics defined in NUREG-0800 BTP-7-14 shown as Table 1 [10].
(2) To define four-segment identification number coding rules as shown in Fig. 3. The first segment is used to identify different I&C systems, such as RPR for reactor protection system in CPR1000 NPPs. The second segment is used to mark the documents produced in different development phases, as shown in Table 2. The third segment is used to identify the quality characteristics in Table 1, and the last segment is the serial number according to the specific quality.
(3) To define four-segment identification number coding rules for signals and parameters of each I&C function requirement, which is also very critical and should be checked and traced during V&V. Similarly, a four-segment identification number should be defined, as shown in Fig. 4. The first segment is used to identify different systems or equipment, which the signal is generated or the parameter is used by. The second segment is used to define signal types, such as input signal (AI, DI), output signal (AO, DO) or parameter (PAR). The third segment is used to identify the signal characteristics, such as FLW for flow, MT for temperature measurement, PP for primary pump and so on. The last segment is the serial number according to the specific signal characteristics.

Table 1. Quality characteristics in NUREG-0800 BTP-7-14

Quality characteristics	Quality identifier
Accuracy	QACC
Capacity	QCAP
Functionality	QFUN
Reliability	QREL
Robustness	QROB
Safety	QSAF
Security	QSEC

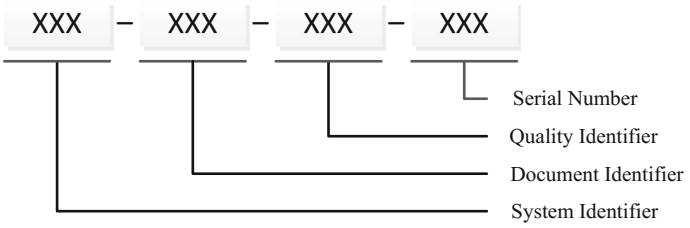

Fig. 3. Identification number coding structure of itemized I&C requirements

Table 2. Definition of document identifier

Phase of development process	Document identifier
Concept	SyREQ, SyDES
Requirements	SfREQ
Design	SfDES
Implementation	CmTST
Test	SfTST, SyTST

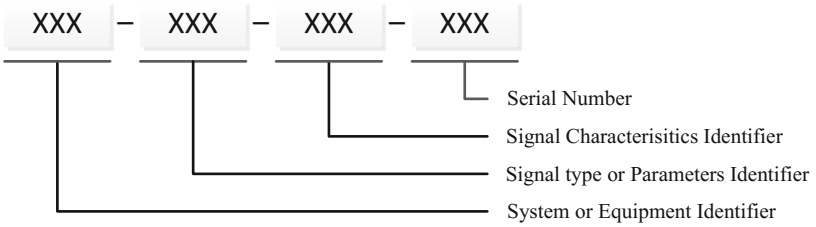

Fig. 4. Identification number coding structure of signals and parameters

(4) To use the special tools like DOORS. It is capable of developing itemized I&C Requirements and generating identification number coding number automatically.

5 Conclusions

With the digital technologies are used in NPPs, software reliability and V&V quality have caused widespread concerns around the world. Traceability is the basic requirement on I&C functions during the life cycle V&V activities. How to effectively itemize the I&C functions is an important question for traceability analysis. From the viewpoint of V&V, necessity of itemizing requirements on I&C function is discussed and key points of itemized requirements are proposed by learning from CPR1000 NPPs' project experience to ensure the software V&V quality with proper workload.

References

1. HAD 102/16: Computer-based safety-critical system software of nuclear power plants (in Chinese), National Nuclear Safety Administration (2004)
2. IEEE Std. 1012: IEEE standard for software verification and validation (2004)
3. IEEE Std. 7-4.3.2: IEEE standard for digital computers in safety systems of nuclear power generating stations (2010)
4. IEC 60880: Nuclear Power Plants-Instrumentation and Control Systems Important to Safety-Software Aspects for Computer-based Systems Performing Category A Functions (2006)
5. EUR: European Utility Requirements for LWR Nuclear Power Plants, Rev. E (2016)
6. ISO/IEC 12207: Information Technology-Software Life Cycle Processes (1995)
7. IEEE Std. 1233: IEEE Guide for Developing System Requirements Specifications (1998)
8. IEEE Std. 830: IEEE Recommended Practice for Software Requirements Specifications (1998)
9. IEEE Std. 1016: IEEE Recommended Practice for Software Design Specifications (1998)
10. NUREG-0800 BTP-7-14: Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems, Rev. 5 (2007)