Software Quality Evaluation of Non-safety Digital I&C System in NPPs

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 Company Ltd., Shenzhen, China

Abstract. As an important process control system in nuclear power plants, non-safety digital I&C system has the characteristics of numerous internal and external interface, complex functions and low development integrity level. Users pay more and more attention to the quality in each phase of its life cycle, such as design, equipment manufacturing, commissioning and verification, delivery, operation and maintenance. This paper studies the software quality evaluation process, and proposes a set of applicable regulations and standards system and quality evaluation model. The contents and key elements of quality evaluation in three important phases of life cycle process are discussed in detail, and the V&V technical requirements and quality management requirements are integrated, which provides a reference for the implementation of new building nuclear power plants and modernization projectsPer.

Keywords: Quality evaluation · Verification and Validation (V&V) · Nuclear power plant · Non-safety I&C system

1 Introduction

With the increasingly application of digital technology in nuclear power plant, the reliability of software is still one of the focuses of all parties. As software is a kind of logic product, its defects are mainly caused by design errors, which may exist in multiple redundant channels and components of I&C system at the same time, leading to the failure of the I&C system. System failure is closely related to its operating environment, and hardware failure often leads to software failure. For example, a fuel deformation event in a domestic nuclear power plant is caused by multiple logic errors in the upgraded nuclear fuel loading and unloading and storage system control software. The internal logic implementation of the local PLC of another nuclear power plant is unknown and frequently causes system function errors, and causes other problems such as communication interruptions, life monitoring for communication function errors.

Compared with the safety I&C system, the non-safety digital I&C system has more problems in the process of design, manufacture, commissioning, operation and maintenance, such as lack of systematic reliability quantitative analysis methods, risk analysis and control methods, insufficient testing and verification methods, and the complexity of

Y. Xu et al. (Eds.): SICPNPP 2020, LNEE 779, pp. 420–428, 2021.
https://doi.org/10.1007/978-981-16-3456-7_40

transient test control. Details, in the design phase, there is a lack of complete, reliable and clear measurement and control requirements, and the suitability of design parameters is difficult to evaluate. In the manufacturing phase, the research and development integrity level and the testing strictness of non-safety I&C platform is not high, can lead to many system defects. In the commissioning phase, the analysis of important control interlocking protection functions is insufficient, and the integrity of verification is not easy to confirm. In order to achieve the expected reliability and availability of non-safety digital I&C system, verification and validation throughout the whole life cycle are required in the process of software development. At the same time, process quality evaluation is carried out to form a closed loop with the system research and development process, which is an effective means of life cycle quality risk control.

2 Standard System

At present, the regulations and standards that the safety digital I&C system software follows are relatively complete, and there are many applications and practices in nuclear power plants at home and abroad. The main standards used to guide the research and development of software for non-safety digital I&C systems are also mainly focused on IEEE and IEC standards, which can be used. It is suggested to select lower level requirements for application. In addition, some requirements for common industrial standards and COTS related standards can be combined [1]. Based on the experience of safety V&V and the application practice of other industries, this paper proposes the following standard architecture to guide the software quality evaluation of non-safety digital I&C system, as shown in Table 1 below. It is suggested that in the quality evaluation activities of the life cycle process, the requirements of the following standards should be reasonably matched and selected in each phase, and compliance review and testing should be carried out.

Table 1. Standard architecture of software quality evaluation

Level	Type	Standard code	Application analysis
1	Plant	HAF102-2016	Evaluation of system and software design requirements
		HAD102/16-2004	
2	I&C System	IEC 61513-2011	Evaluation of I&C overall structure design requirements
3	Computerized System	IEC 61508-1 2010	Check system design and functional safety defect, like dangerous/risk/hazard points
4	Software Requests	IEC 62138-2004	Evaluation of compliance with software design requirements
		IEC 61508-3 2010	
	V&V Process	IEEE 1012-2004	process, tasks and contents of software V&V
		TRS-384-1999	

(*continued*)

Table 1. (*continued*)

Level	Type	Standard code	Application analysis
5	Quality Evaluation	GB/T 25000.51-2016	Evaluation of software quality requirements, quality model in life cycle
		GB/T 16260-2006	
	Configuration Management	IEEE 828-2012	Evaluation of software configuration management in life cycle
		IEEE 1042-1987	
	Review/Audit	IEEE 1028-2008	Review methodology used in software evaluations
6	Test Specification	GB/T 15532-2008	Guide the process of software testing, factory acceptance test, site acceptance test and site integration test
		NB/T 25040-2014	
	Test Documentation	IEEE 829-2008	Guide the writing of software test documents
7	Code Specification	GB/T 28169-2011	Check specification requirements in software programming
		GJB 5369-2005	
		NUREG/CR6463-1996	

Standard IEC 61513 specifies the objectives, required inputs and outputs of system and software life cycle development activities. It also specifies basic requirements for system configuration management plan, system security plan, system integration plan, system installation plan, system operation plan and system maintenance plan. IEC 61508 puts forward the requirements to effectively predict and evaluate the risks of controlled equipment during the design process and adopt the necessary safety related systems to reduce the risks. IEC 62138 stipulates the basic requirements of computer software development activities for I&C systems to carry out class B and class C functions, and supplementing and improving the relevant requirements of IEC 61513. Software of non-safety DCS suggests to refer to class C requirements of this standard. IEEE 1012 stipulates the whole implementation process of software V&V activities. GB/T 25000.51 and GB/T 15532 specify the quality requirements and evaluation requirements of software products. IEEE 828 (RG1.169) and IEEE 829 (RG1.170) respectively stipulate the requirements and guidance for the software configuration management and development documentation. NB/T 25040 specifies the guidelines for non-safety digital I&C system factory acceptance tests (FAT), site acceptance test (SAT) and site integration test (SIT).

3 Quality Evaluation Model

The development process of non-safety digital I&C system in nuclear power plant is divided into requirements analysis phase, design phase, implementation phase, appraisal/finalization phase, delivery, operation and maintenance phase [2]. The requirement analysis phase includes system operation, parameters, design restrictions, instrument control, human-machine interface, system boundary, and other analysis contents, and the output file is the system requirement specification. The design phase includes regulations and standards analysis, overall architecture, function allocation, software and hardware design, etc. The output file is system design manual, which is completed by the overall design unit together with the system requirement specification. The implementation phase includes system platform design, software and hardware development, application function design, source code design, software and hardware integration, system testing and confirmation testing. The output files are the delivered equipment, supporting documents and records, which are completed by the equipment manufacturer. The appraisal/finalization phase includes independent evaluation by a third party, site installation test, commissioning, etc., which is completed by the installation and commissioning unit. The output files are the systems and equipment that have passed the commissioning, supporting documents and records.

Software quality management activities run through the entire system development process described above. Implement complete quality management including the determination of quality indicators, the design and implementation of quality indicators, and the testing and verification of the satisfaction degree of quality indicators. Comprehensively demonstrate the suitability and sufficiency of various activities of system development, focusing on whether the equipment provided by the equipment manufacturer can meet the reliability requirements of the target application. The specific quality evaluation model is shown in Fig. 1 below.

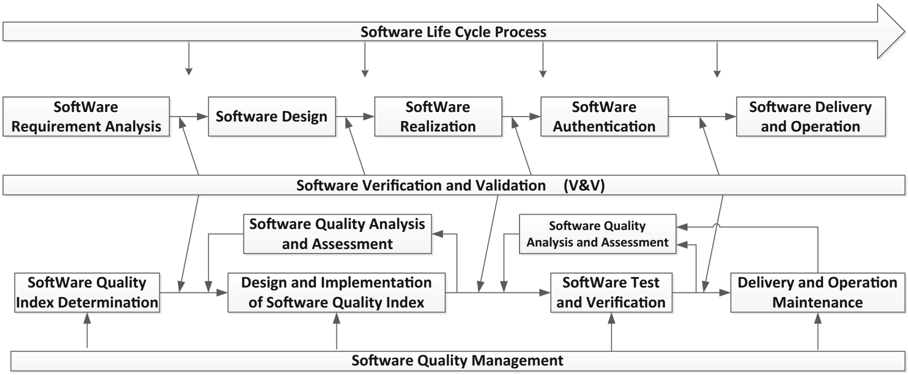
Software Life Cycle Process
SoftWare Requirement Analysis
Software Design
SoftWare Realization
SoftWare Authentication
Software Delivery and Operation
Software Verification and Validation (V&V)
Software Quality Analysis and Assessment
Software Quality Analysis and Assessment
SoftWare Quality Index Determination
Design and Implementation of Software Quality Index
SoftWare Test and Verification
Delivery and Operation Maintenance
Software Quality Management

Fig. 1. Quality evaluation model of software

4 Evaluation Key Points

4.1 Design Phase

The design phase is the source of the life cycle of the software. The design requirements are converted into the detailed design of each finished product, including the control logic diagram, I/O list and set point manual. The correctness, completeness and consistency of control logic and requirement allocation directly affect the development of I&C system software and the use of end users. Therefore, carrying out design quality evaluation is the key activity to ensure the correct realization of user requirements. The purpose of quality evaluation activities in the design phase is to verify that I&C design is the correct, accurate and complete transformation of design requirements, and no unexpected features are introduced to ensure the correctness, completeness, accuracy, readability and consistency with upstream input of design documents.

The following contents must be considered in the design quality evaluation: the completeness and clarity of I&C function requirements specification, the consistency between I&C function requirements and I&C platform, the compliance of I&C function requirements specification with corresponding engineering requirements (e.g. codes, symbols, etc.), the correctness and completeness of requirements as design inputs, the correctness of each I&C function module, and the consistency between each I&C function. We should focus on the verification and validation of digital I&C system regulate functions, regulate parameter settings and other important matters that are easy to cause turbine and reactor jumping events, verify the suitability of control logic and design parameters.

The main tasks of design quality evaluation include: design function and interface verification, parameter verification, requirement sorting and itemization, and requirement traceability analysis [3]. Focus on checking the integrity of LD/AD, that is, ensure that each line, each function block, each interface and each note in LD/AD are covered and verified. The input and output files of design phase evaluation are shown in Table 2 below.

Table 2. Input and output of design phase evaluation

Work tasks	Items	Foundation documents	Verification ddocument
Diagram verification	Forward	Control measurement requirements contract technical appendix	LD/AD I/O List
	Backward	LD/AD I/O List	Control measurement requirements Contract technical appendix
Parameter validation	/	Control measurement requirements LD/AD	Set point manual

Design quality evaluation methods mainly include static verification methods and dynamic verification methods. The static verification method does not need to use verification tools, and is completed by static inspection and analysis of design documents based on personnel with design review qualifications. The verification method based on dynamic experimental test refers to using software or hardware to simulate the design behavior, and then finding the problems existing in the design through dynamic operation. It is to set a certain scene for the testers to carry out actual operation and give evaluation conclusions according to the test results. The simulation platform should have the functions of process model simulation, control model simulation and human-machine interface. It adopts the method of analyzing configuration diagram data package and reconstructing control diagram, then import LD/AD into the simulation verification platform, and dynamically integrate the power plant process model and human-machine interface. According to the power plant operation conditions and relevant design requirements, test cases are designed to implement dynamic verification.

4.2 Equipment Manufacturing Phase

In the equipment manufacturing phase, the equipment supplier completes the software and hardware realization activities, that is, converting the software design into source code, database structure and related executable machine representations. The software quality evaluation involves software coding testing and simulation testing to verify that these conversions are correct, accurate and complete.

The main tasks of equipment manufacturing quality evaluation include: system document conformity review, control station configuration document review, requirement traceability analysis, interface analysis, experience feedback issue review. Focus on verification and review of diagrams and signals. The other part is application algorithm block review and software confirmation testing [4]. The methods involved include static testing methods and dynamic testing methods. The input and output files are shown in Table 3.

Table 3. Input and output of equipment manufacturing phase evaluation

Work tasks	Items	Foundation documents	Verification documents
Diagram tracing	Forward	Logic/Analog Diagram	Typical Functional Configuration Diagram Source Code
	Backward	Typical Functional Configuration Diagram Source Code	Functional Diagram
Signal tracing	Forward	Set point Manual I/O List	Cabinet Detailed I/O List
	Backward	Cabinet Detailed I/O List	Set point Manual I/O List
Algorithm block test	Forward	Software Function Block Requirements Specification Coding specification	Function Block Source Code
	Backward	Function Block Source Code	Software Function Block Requirements Specification Coding specification

(*continued*)

Table 3. (*continued*)

Work tasks	Items	Foundation documents	Verification documents
Confirmation Test	Forward	System/Scheme Description Requirements Specification Contract Technical Appendix	Test Plan, Test Procedure, Test Report Computer Integration System
	Backward	Test Plan, Test Procedure, Test Report Computer Integration System	System/Scheme Description Requirements Specification Contract Technical Appendix

The evaluation of equipment manufacturing quality should focus on the pure software problem, including the important logic that is easy to cause common cause failure (CCF) or turbine and reactor jumping, the engineering applicability of non-safety digital I&C platform, and the testing of software algorithm block that as the basis of the application software function realization. Like the software test of safety digital I&C system, the test methods of non-safety I&C system mainly include document review, code walkthrough, code analysis, unit test, integration test and system test. The test requirements are shown in Table 4.

4.3 Commissioning Phase

Commissioning verification is to conduct a comprehensive inspection of the equipment and system after installation, so as to ensure that the individual equipment and overall performance of the non-safety digital I&C system meet the design requirements and relevant operation criteria. The aim is to verify the output results of the previous phase such as design and manufacturing, further investigate the potential and legacy software and hardware or system interface problems after FT/FAT, and finally ensure that all control protection system meet the functional design requirements.

Because of the use of CPU, complex communication and network technology, a large number of tests are allowed in the factory environment. Functions that have been fully tested in the factory tests do not need to be retested during commissioning. The main tasks of site commissioning verification quality evaluation include I/O inspection, interface verification, actuator transmission or partial function testing. The input and output files of commissioning evaluation are shown in Table 5 [5].

Simulation technology is recommended for commissioning non-safety digital I&C system. Research and develop of semi-physical testing equipment or other portable commissioning and verification tools. The commissioning device is connected to the cabinet of the target I&C system in the way of hard-wired; complete the site functional test or transient simulation analysis before the unit starts. After the unit fuel loading is

Table 4. Test requirements of algorithm block

Method	Type	Requirements
Static	Document review	Review the accuracy, non-ambiguity, standardization and readability of the document. Review of consistency with upstream design documents
	Code Walktthrough	Check in terms of traceability, logic, data, interfaces, comments, exception handling, memory, etc.
	Code analysis	Use code analysis tools, check the array cross-border, pointer, security vulnerability, variable uninitialized, data flow, annotation rate and coding specification
Dynamic	Unit test	Unit tests of all algorithm blocks and calling functions. Complete the test and analysis of statements, branches and MC/DC coverage, and analyze and explain with coverage less than 100%. Test cases need to involve logic testing, functional testing, performance testing, interface testing and boundary testing
	Integration Test	Through the incremental step-by-step integration method, each algorithm block that has passed the unit test is gradually combined for testing. Test cases need to involve functional testing, interface testing, data structure testing, resource testing, priority conflict testing, performance and stability testing, etc.

Table 5. Input and output of commissioning phase evaluation

Work tasks	Items	Foundation documents	Verification documents
Commissioning verification	Forward	Design documents (System design manual, set point manual, Equipment operation and Maintenance manual), Installation documents, Test Documents (Commissioning plan, Commissioning procedures)	Integrated System (Hardware, Software source code, user documents, configuration data, etc.)
	Backward	Integrated System (Hardware, Software source code, User documents, Configuration data, etc.)	Design documents (System design manual, Set point manual, Equipment operation and Maintenance manual), Installation documents, Test documents (Commissioning plan, Commissioning procedures)

started to the 100% power platform, closed-loop response tests and transient operation verification based on actual working conditions are repeatedly arranged. Finally, hidden and potential configuration design, parameter setting and interface problems of digital I&C system are investigated through iterative testing and complex operation conditions verification in different stages.

The dynamic response test of control parameters and the test of process control parameters cannot be completely carried out in factory testing and single system testing. Full scale simulator also seldom carries out verification on system interlock, network signal transmission and equipment interface, and cannot effectively verify the process control logic of analog quantity. Therefore, the commissioning verification should identify the important control interlock protection functions of the unit, analyze the related measurement control channel function design and interface influence of the I&C critical components (CCM1). Sorting out the verification items that factory test (FT)/factory acceptance tests (FAT) in the design phase and equipment manufacturing phase based on simulation technology or full scale simulator virtual DCS system (FSS) that cannot be implemented (such as verification of the first operation condition, the verification that real equipment actions or acceptance criteria have time requirements for loop system response). Sorting out the verification items that mandatory required of regulations and standards or regional power grid supervision, and other special verification (such as EMC, performance assessment, etc.).

5 Conclusions

With the increasing number of new nuclear power building projects and in service power plant modernization projects, safety regulators and power plant owners are paying more and more attention to the software quality of non-safety digital I&C systems. Quality control means gradually transition from equipment supplier factory verification to third-party independent verification. The quality evaluation strategy of non-safety digital I&C system proposed in this paper can provide a working and planning idea for all parties.

References

1. IAEA-TECDOC-1016: Modernization of instrumentation and control in nuclear power plants
2. IEEE 1012–2004: IEEE Standard for Software Verification and Validation
3. Guang-Xin, Z., Zhi-Yong, L.: Non-safety I&C system control logic design verification based on design analyzer of CAP1400 Nuclear Power Plant. Chem. Autom. Instrum. (43) (2016).
4. Lei, C., Miao, T., Song, W.: Non-safety DCS testing of nuclear power plant, China Computer & Communication, No. 24 (2016)
5. NB/T 25040-2014: Non-safety classified digital control system in nuclear power plants factory acceptance test (FAT), site acceptance test (SAT), and site integration test (SIT)