Research of Software V&V Technology in the Non-safety DCS of NPPs

Sheng-Chao Wang(✉), Wang-Ping Ye, Jian-Zhong Tang, and Tao Bai

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, China

Abstract. As the nerve center of nuclear power plant (NPP), distributed control system (DCS) has been widely used with perfect control function, flexible system configuration, safe and reliable operation state and strong applicability. The relevant modification or upgrade of DCS is the focus of NPP's digital modification or upgrade. The reliability of the computerized system or equipment of DCS depends to a large extent on the reliability of the software, and systematic failure may be introduced in the development process of the software. Software verification and validation (V&V) technology is recognized as one of the key technologies in the field of nuclear power that can effectively ensure and improve the quality of software. Software V&V technology for safety DCS system has been widely studied and applied, but software V&V technology for non-safety DCS system has not attracted attention from all parties. Based on this, through studying NPP's non-safety DCS software V&V related standards and technical reports, combining with the analysis of NPP's operating experience in operating event reports, a V&V scheme based on system engineering method is proposed, and the activities and tasks of each phase of the scheme V&V process are preliminarily summarized, and the detailed guiding standards or technical reports that can be referred to when executing V&V tasks are expounded. At last, the research results are expected to provide technical reference for the modification or upgrade of non-safety DCS in software.

Keywords: Modification or upgrade · Non-safety DCS · Software V&V

1 Introduction

Many nuclear power plants (NPP) based on analog technology in the world are facing the challenge of digital modification or upgrade. In the past, the engineering process focusing on fluid and mechanical systems has proved insufficient to solve the problem of integrating new digital technology and software-based technology into existing NPP facilities. As the nerve center of NPP, distributed control system (DCS) has been widely used with perfect control function, flexible system configuration, safe and reliable operation state and strong applicability. The relevant modification or upgrade of DCS is the focus of NPP's digital modification or upgrade. However, the reliability of the computerized system or equipment depends to a large extent on the reliability of the software,

Y. Xu et al. (Eds.): SICPNPP 2020, LNEE 779, pp. 444–451, 2021.
https://doi.org/10.1007/978-981-16-3456-7_43

and systematic failure may be introduced in the development process of the software. In the process of digital modification or upgrading of NPP DCS system, how to ensure the software reliability of computerized system or equipment is an urgent problem to be solved in the process of digital modification or upgrade. Software verification and validation (V&V) technology is recognized as one of the key technologies in the field of nuclear power that can effectively ensure and improve the quality of software.

DCS system is divided into safety level (1E) and non-safety level (NC) according to different safety levels, and is functionally divided into safety function 1E, safety related function SR and non-Safety function NC. Safety function 1E and safety related function SR are implemented by nuclear safety level (1E) DCS system, while non-safety function NC is implemented by non-safety level (NC) DCS system. Software V&V technology for safety DCS system has been widely studied and applied, but software V&V technology for non-safety DCS system has not attracted attention from all parties.

Based on the above contents, the research on relevant standards and technical reports of software V&V for non-safety DCS system in the process of digital modification or upgrade of NPP will be carried out. At the same time, the software V&V scheme and process of non-safety DCS system and key activities in the V&V process will be sorted out and formed in combination with the operating experience of non-safety DCS in NPP of China.

2 Requirements of Standards or Reports

IEEE 1220 introduces the application and management of systems engineering process [1], in which systems engineering process spans multiple disciplinary fields, mainly to create an interdisciplinary process and implement it to ensure that requirements are met in a high-quality, reliable, low-cost and timeline manner throughout the system life cycle. The systems engineering process usually includes the following seven tasks: state the problem, investigate alternatives, model the system, integrate, launch the system, assess performance, and re-evaluate. It should be reminded that the systems engineering process is not a sequential seven tasks that can be executed in parallel and iteratively.

IEEE 1012 is a general software V&V process standard which matches specific V&V activities and tasks according to software integrity level [2], and defines the attributes, inputs and outputs of tasks in each stage of V&V process. The V&V process provides objective evaluation of products and processes throughout the life cycle to prove whether the requirements are correct, complete, accurate, consistent and measurable, and to determine whether the development product of a given activity meets the requirements of the activity and whether the final product meets its intended use and user requirements.

IAEA TRS 384 is a software V&V standard in NPP instrumentation and control (I&C) system [3]. It introduces the organization and management of the V&V process, safety classification and types of software including devices containing software and software tools, and different types of software related activities and documents, verification by phase and validation.

EPRI TR 3002011816 is mainly aimed at the modification and upgrade of digital I&C systems or components of existing nuclear facilities [4]. These activities involve the whole life cycle of design, installation, testing and end-of-life. This guidance is also

fully applicable to new nuclear power development, including initial design, licensing, installation and start-up, and provides a graded approach with an appropriate amount of rigor, which results in reducing the likelihood and severity of consequential operating experience events. The process of this graded approach includes technology configurability, potential consequences of error, determining the configurability of the applied technology, determining the applicability of digital engineering systems (DEG) activities and determining the potential consequences of error. The EPRI TR 3002011816 provides a basic system engineering process, shown in Fig. 1, which is described in detail in EPRI TR 3002008018.

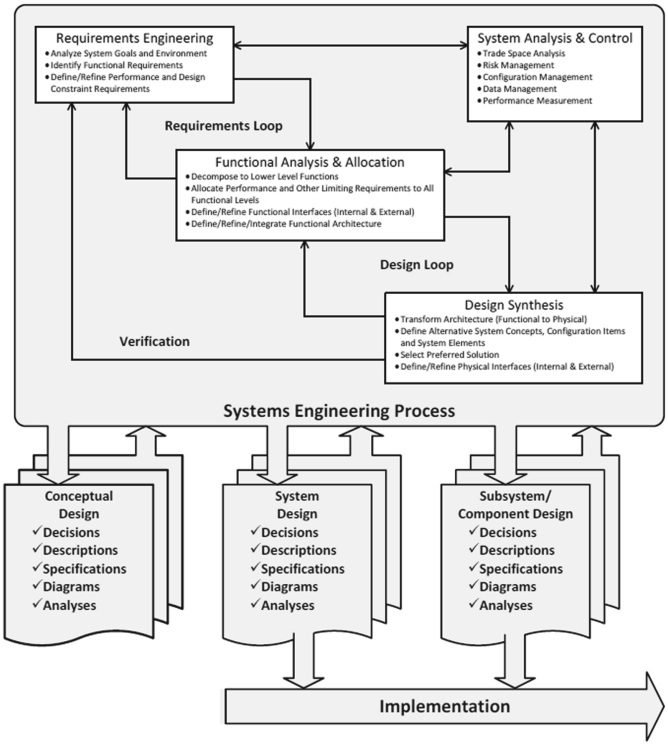

Fig. 1. The systems engineering process [4].

The system engineering process includes four activities, including requirements engineering, functional analysis & allocation, design synthesis and system analysis & control, which are applied on successive iterations of system decomposition, from the concept level, to the system level, then the subsystem/component level. Besides, EPRI TR 3002011816 also provides a series of activities in the system engineering process.

EPRI TR 3002008018 introduces the methods and tools related systems engineering process for digital I&C projects [5]. The systems engineering methods mainly include requirements analysis, trade Studies, function analysis and allocation, design synthesis, hazard analysis, human factors engineering (HFE) analyses, system optimization,

modeling and simulation and V&V. The V&V methods and activities are described in several guides and standards, and are most often applied in the context of software engineering and human factors engineering. EPRI guidance on software V&V is available via *TR 103291* [6]. EPRI TR 3002008018 also illustrates the basic V&V activities used in the systems engineering process. In addition, systems engineering tools include static tools (e.g., physical, virtual models), dynamic tools (modeling & simulation), and administrative tools (e.g., requirements management).

3 Operating Experience

An important activity of NPP's non-safety DCS modification or upgrade is the problem statement. An important source of the problem is the operating events in in-service or new NPP under construction. Through the problem occurrence, cause analysis and solutions of operation events, the valuable operating experience formed is conducive to the digital modification or upgrade of the NPP non-safety DCS.

Operating experience from 61 Operational Event Reports of 9 Nuclear Power Bases in China from February 2015 to January 2020, shows 39.32% of events are caused by software defect such as setting error of adjusting valve control mode in software, cross-processor network communication problem, hold and reset problem of pulse control-command [7]. 19.70% of events are caused by human errors like interface installation error and 40.98% of events are due to hardware faults like hardware aging. The causes of operational events are shown in Fig. 2.

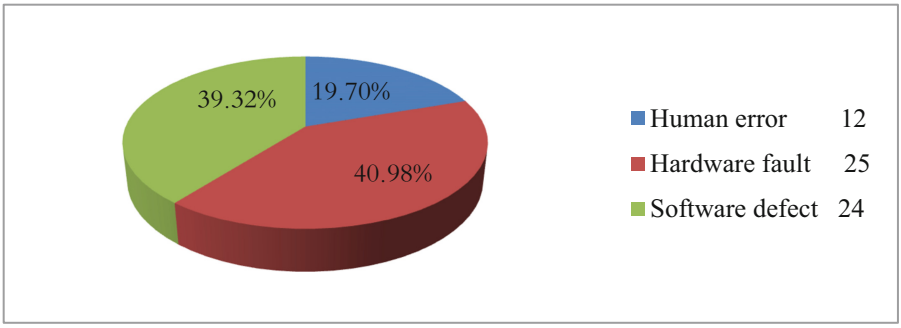

Fig. 2. The causes of operational events.

According to the types of event causes counted in NPP's operating event reports, the percentage of software defects is close to the percentage of hardware faults. Attention should be paid to software in the process of digital modification or upgrade. In addition, operating events caused by human errors cannot be ignored.

4 Software V&V Scheme

4.1 V&V Model

According to the research of above standards, technical reports and operating experience, a V&V scheme for NPP's non-safety DCS software is proposed, which includes V&V model and process, key activities and tasks (Fig. 3).

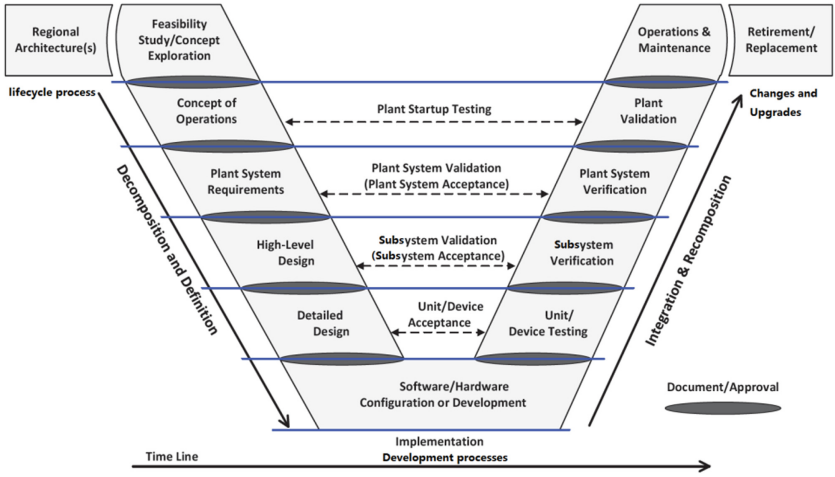

Fig. 3. The software V&V model [5].

Before adopting the model, it is necessary to measure the level of the engineering change in the model by using the A/B/C/D/E five-level differentiation scheme to determine the system or component of interest. Engineering changes can occur at multiple levels. To determine the level of change and the appropriate level of solution alternatives, the following issues or topics need to be considered:

1. Function, performance changes (e.g. supporting power increases) or new function (e.g. meeting new regulatory requirements)
2. Network Security Issues
3. Availability and quality of information on structures, systems, and components at the change level
4. New or emerging regulatory or design constraints
5. Change interfaces
6. Device difference
7. Data communication (network, fieldbus, media type, etc.)

4.2 V&V Activities and Tasks

After determining the scope of the changed system or component, the V&V activities and tasks of each phase are determined according to the graded approach and the change

level. According to the issues or topics to be considered in the main phases, inputs and outputs are adopted to match V&V activities and tasks. The V&V activities and tasks of main phases are shown in Table 1.

Table 1. V&V activities and tasks.

Phase	Activities	Tasks	Inputs	Outputs
Conceptual/ common design	Verify & validate or confirm V&V of the conceptual/common requirements, architecture, design and implementation	1. Traceability analysis 2. Criticality analysis 3. Identify improvement opportunities in the conduct of V&V 4. Management review of the V&V effort 5. SVVP generation	1. Plans and/or procedures 2. V&V processes Methods 3. Scenarios and test cases 4. Success criteria and expected results 5. Tools 6. Roles and responsibilities 7. Actions to be taken when anomalies are discovered	Report that provide the results and conclusions of V&V activities
Detailed design	Verify & validate or confirm V&V of the detailed requirements, architecture, design, and implementation	1. Traceability analysis 2. Criticality analysis 3. Identify improvement opportunities in the conduct of V&V 4. Integration V&V test procedure/plan/design/case generation 5. Management review of the V&V effort 6. Software requirements/design evaluation System V&V test case generation		
Installation planning and test	Verify and validate or confirm V&V of the integrated installed system or component	1. Traceability analysis 2. Identify improvement opportunities in the conduct of V&V 3. Integration V&V test execution 4. Management review of the V&V effort 5. System V&V test execution		

In addition, the closeout information of the closeout phase shall be documented under user specified procedures, and the operation and maintenance phase of the system or component lifecycle includes supporting system or component operations and maintenance activities, performing or confirming corrective actions, initiating engineering changes as needed, controlling bounded configuration changes via administrative procedure and performing or confirm disposal of system or component elements. The corresponding V&V tasks of operation and maintenance phase include criticality analysis, identifying improvement opportunities in the conduct of V&V, management review of the V&V effort, SVVP revision, and tasks iteration.

The purpose of the V&V process in the conceptual/generic design phase of the facility change project is to provide or determine objective evidence that the results of the conceptual/generic design phase activities are complete, correct and consistent. The V&V methods or tools of this phase include inspection, analysis (including modeling and simulation), demonstration, or test. Detailed requirements traceability analysis and verification process can be found respectively in EPRI 3002002843 section 4.8 and ISO/IEC/IEEE 15288 section 6.4.9 [8, 9].

During the detailed design phase of the facility change project, the purpose of the V&V process is to provide or determine objective evidence to prove that the detailed requirements, structure, design and implementation conform to the conceptual/generic requirements, architecture and design. The V&V methods or tools of this phase include inspection, analysis (including modeling and simulation), demonstration, or test. Detailed requirements traceability analysis and design review can be found respectively in EPRI 3002002843 section 4.8 and 5.2 [8], verification process and validation process can be found respectively in ISO/IEC/IEEE 15288 section 6.4.9 and 6.4.11 [9].

The purpose of the V&V process in the installation planning and test phase of the facility change project is to provide or identify objective evidence that the integrated system or component has correctly realized its detailed requirements, architecture and design, and that the installed and debugged system or component has correctly realized its detailed requirements, architecture and design throughout NPP. Detailed requirements traceability analysis and design review can be found respectively in EPRI 3002002843 section 4.8 and 5.2 [8], verification process and validation process can be found respectively in ISO/IEC/IEEE 15288 section 6.4.9 and 6.4.11 [9].

5 Conclusions

Based on the research of NPP's non-safety DCS software V&V related standards and technical reports, combined with the analysis of NPP's operating experience in operating event reports, a V&V scheme based on system engineering method is proposed, and the activities and tasks of each phase of the scheme V&V process are preliminarily summarized, and the detailed guiding standards or technical reports that can be referred to when executing V&V tasks are expounded.

Through the research on software V&V technology of non-safety DCS in NPP, it can provide technical reference for NPP V&V in the process of modification or upgrade of non-safety DCS in software, and effectively ensure the software quality in the process of digital modification or upgrade of non-safety DCS.

References

1. IEEE 1220-2005 IEEE Standard for Application and Management of the Systems Engineering Process
2. IEEE 1012-2004 IEEE Standard for Software Verification and Validation
3. IAEA TRS 384-1999 Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control

4. EPRI TR 3002011816-2018 Digital Engineering Guide: Decision Making Using Systems Engineering
5. EPRI TR 3002008018-2016 Systems Engineering Process: Methods and Tools for Digital Instrumentation and Control Projects
6. EPRI TR 103291-1998 Handbook for Verification and Validation of Digital Systems
7. Zhong, L., Ming-Liang, S., Jia-Jie, W.: Analysis of typical problems of DCS non-safety class software. Nucl. Power Eng. **38**(3) (2017)
8. EPRI 3002002843-2014 Requirements Engineering for Digital Instrumentation and Control Systems
9. ISO/IEC/IEEE 15288-2015 Systems and Software Engineering - System Life Cycle Processes