Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 10-11, 2007

State-of-the-Art: Evolution of Software Life Cycle Process for NPPs

Yong Suk Suh,[a] Heui Youn Park,[a] Ki Sung Son,[b] Ki Hyun Lee,[b] Hyeon Soo Kim [c]
a I&C and HF Div., KAERI, 150 Dukjin-dong, Yuseong-gu, Daejon, Korea, 305-353, yssuh@kaeri.re.kr
b Control Tech. Research Inst., SEC Co., Ltd.,974-1 Goyeon-ri Woongchon-myon, Ulju-gun, Ulsan, Korea, 689-871
c Dept. of Computer Science and Eng., Chungnam Nat'l Univ., 220 Gung-dong, Yuseong-gu, Daejon, Korea, 305-764

1. Introduction

This paper is to investigate the evolution of software life cycle process (SLCP) for nuclear power plants (NPPs) based on IEEE Std 7-4.3.2 which has been updated twice (namely 1993 and 2003) since it was published in 1982 and relevant software certifications. IEEE Std 7-4.3.2 specifies additional computer specific requirements to supplement the criteria and requirements of IEEE Std 603. It also specifies the software quality requirements as follows: computer software shall be developed, modified, or accepted in accordance with an approved software quality assurance (QA) plan. IEEE Std 7-4.3.2 has evolved to address specific standards to supplement the requirements as follows:

- IEEE Std 7-4.3.2-1982: ANSI/ASME NQA-1-1979 and IEEE Std 467-1980.
- IEEE Std 7-4.3.2-1993: ASME NQA-2a-1990 Part 2.7, IEEE Std 730-1989 and IEC Std Pub 880, 1986.
- IEEE Std 7-4.3.2-2003: IEEE/EIA Std 12207.0-1996, IEEE Std 730-1998 and IEC Std 60880.

IEEE Std 7-4.3.2-1982 specifies a minimum software development process as follows: plan, design and implementation. ANSI/ASME NQA-1-1979 is not directly related to software development process but to overall quality assurance criteria. IEEE Std 7-4.3.2-1993 addresses ASME NQA-2a-1990 Part 2.7 for software development requirements. ASME NQA-2a-1990 Part 2.7 which was interpreted into KEPIC QAP-2 II.7, specifies software development process in more detail as follows: requirements, design, implementation, test, installation and checkout, operation and maintenance, and retirement. Along with this, software QA plan is emphasized in IEEE Std 730-1989. In IEEE Std 7-4.3.2-2003, IEEE/EIA Std 12207.0-1996 replaces the ASME NQA as a requirement for software development. The evolution of SLCP from ASME NQA to IEEE/EIA Std 12207.0 is discussed in Section 2 of this paper. The publication of IEEE/EIA Std 12207.0 is motivated from industrial experiences and practices to promote the quality of software. In Section 3, three international software certifications relating to the IEEE/EIA Std 12207.0 are introduced.

2. The Evolution of SLCP for NPPs

ASME NQA-2a-1990 Part 2.7 describes a development-centric SLCP which adopts typical software engineering practices as shown in Fig. 1.

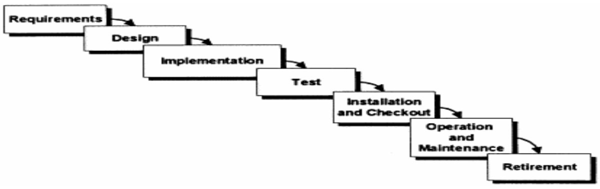

Fig. 1 SLCP in ASME NQA-2a-1990

The SLCP had evolved to present detailed activities as shown in Fig. 2, which is described in NUREG/CR-6101 and NUREG-0800(Rev.4) HICB BTP-14, and has become the acceptance criteria for software in the safety systems of NPPs. The SLCP has evolved through IEEE/EIA Std 12207.0-1996 which contains ISO/IEC Std 12207-1995.

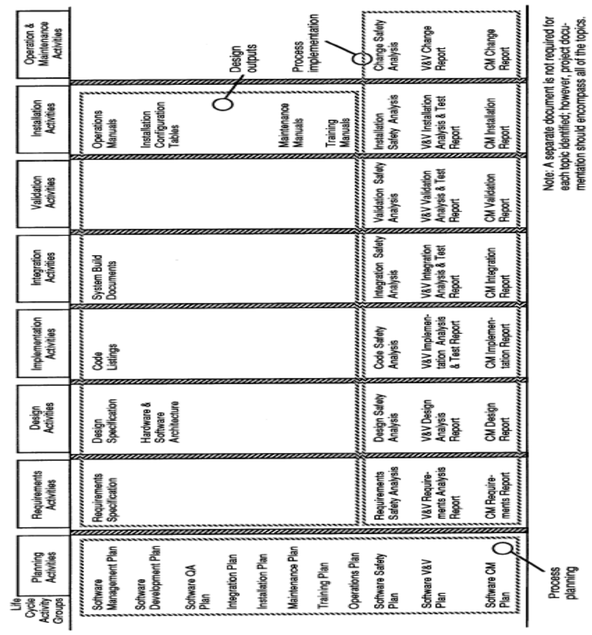

Fig. 2 SLCP in NUREG-0800(Rev.4) HICB BTP-14

ISO/IEC Std 12207-1995, as an international standard, establishes a common framework for SLCP that can be referenced by the software industry. It groups the activities performed during the software life cycle into five primary processes, eight supporting processes, and four organizational processes as shown in Fig. 3. IEEE/EIA Std 12207.0-1996 is to promote a better understanding and application of ISO/IEC Std 12207.

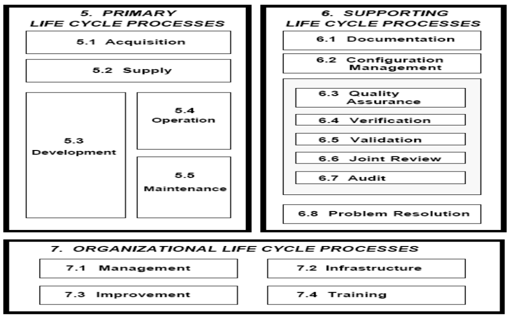

Fig. 3 SLCP in ISO/IEC Std 12207-1995

As seen in Figs 1, 2 and 3, the SLCP has evolved to encompass all activities necessary to produce software and to increase the quality of it. This evolution reflects the experiences and practices of software industry.

3. Software Certification Relating to IEEE/EIA Std 12207.0

Software certification is actually not a mandatory but a voluntary process, which aims to assure that software products are reliable and safe. There are three international certifications which assess a conformance to the ISO/IEC 12207-1995 contained in IEEE/EIA Std 12207.0-1996: 1) SPICE (Software Process Improvement and Capability dEtermination), 2) CMMI-SW(Capability Maturity Model Integration-SoftWare), and 3) ISO 9001.

The SPICE, which was developed by the ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) as ISO/IEC 15504, focuses on a software process assessment and improvement, as well as a supplier's software development capability determination. It specifies a framework for the assessment of the processes and categorizes six capability levels: 0) incomplete process, 1) performed, 2) managed, 3) established, 4) predictable, and 5) optimizing process. The certified SPICE assessors appraise an organizational capability as one of the six levels. A previous study suggested that the safety-critical software processes should achieve a third or above capability level of the SPICE [1].

The CMMI-SW which was developed by SEI (Software Engineering Institute) in U.S. CMU (Carnegie Mellon University) specifies twenty-five key process areas and classifies the capability and the maturity of a software development organization into six and five levels, respectively. The capability levels are classified as: 0) incomplete process, 1) performed, 2) managed, 3) defined, 4) quantitatively managed, and 5) optimizing process. The maturity levels are classified as: 1) initial, 2) managed, 3) defined, 4) quantitatively managed, and 5) optimizing process. The SEI authorized lead assessors appraise an organizational maturity as one of the levels. U.S. DoD requires an applicant who wishes to participate in major military software projects to achieve at a minimum CMMI-SW level 3 or its equivalent [2].

The ISO 9001 specifies requirements for a quality management system applicable to every industry. The ISO 90003 provides guidance for organizations in the application of ISO 9001 to the acquisition, supply, development, operation and the maintenance of a software and related support services. The ISO 90003 is strongly related to the ISO/IEC 12207.

4. Conclusion

We recognized IEEE Std 7-4.3.2-2003 adopts IEEE/EIA Std 12207.0-1996 instead of ASME NQA and IEEE/EIA Std 12207.0-1996 adopts ISO/IEC Std 12207-1995. There are three international certifications which assess a conformance to the ISO/IEC 12207-1995: SPICE, CMMI-SW, and ISO 9001. These three certifications can be used as the means to objectively assess a compliance with the IEEE/EIA Std 12207.0-1996 and also to ensure a high quality of software. Due to its voluntary characteristics and high cost, many companies that want to develop the safety-critical software are not encouraged to achieve the certificate. As KEPIC (Korea Electric Power Industry Code) certificate is required for a safety systems development for NPPs and MIC (Ministry of Information and Communication) gives an advantage to a company which achieves the CMMI-SW certificate for government software development projects, these three certifications will have attract attention from the companies relating to the NPPs in the future. The authors have proposed that a nuclear regulatory body should require the three software certifications as a part of the safety-critical software acceptance criteria [3]. However, the reliability of safety critical software for NPPs cannot be credited only with the three certifications because they specify a lack of software safety analysis requirements.

REFERENCES

[1] O Benediktsson, R B Hunter, A D McGettrick, Processes for Software in Safety Critical Systems, *Software Process: Improvement and Practice*, John Wiley and Sons Ltd., 2001, Vol. 6, issue 1, pp. 47-62.

[2] Memorandum for Component Acquisition Executives Director of Ballistic Missile Defense Organization, Software Evaluations for ACAT 1 Programs, U.S. DoD, 1999.

[3] Yong Suk Suh, et al., A Method to Improve the Software Acceptance Criteria for Nuclear Power Plants, Transactions of the KNS Autumn Meeting, Busan, Korea, Oct 2005.