Transactions of the Korean Nuclear Society Spring Meeting
Chuncheon, Korea, May 25-26 2006

A Study on a Software Quality Assurance of a Process and a Product

KIM Hyun Tae
Korea Atomic Energy Research Institute
htkim@kaeri.re.kr

1. Introduction

Since nuclear plants and facilities have made increasing use of digital technology, the safety and reliability of software is a primary concern. Software errors are more difficult to detect and handle than hardware-related failures. It is crucial to consider the a process and a product of a software life cycle to increase the quality of a software.

This paper discusses the quality assurance of a process and a product of a software life cycle based on two prominent standards, ISO 9001:2000 and CMMI.

2. Standards

There are harmonization efforts being made on software life cycle process standards (IEEE Std 1074, ISO/IEC 12207 and IEEE/EIA 12207) and a systems life cycle process standard (ISO/IEC Std 15288) among organizations such as ISO, IEC, IEEE and EIA.

Relevant standards such as IEEE Std 730 (Standard for Software Quality Assurance Plans), IEEE Std 1012 (Standard for Software Verification and Validation), and ISO/IEC 15504 (Information Technology - Software Process Assessment) are based on these life cycle processes:

- IEEE Std 1074
- ISO/IEC Std 12207
  - ISO/IEC Std 12207
  - ISO/IEC Std 12207 Amendment 1
  - ISO/IEC Std 12207 Amendment 2
- IEEE/EIA Std 12207
  - IEEE/EIA Std 12207.0
  - IEEE/EIA Std 12207.1
  - IEEE/EIA Std 12207.2
- ISO/IEC Std 15288

In the case of IEEE Std 730-1998, many other standards should be used for further information. Two of them are listed below [1]:

- ASME NQA-1-1997, Quality Assurance Program for Nuclear Facilities,
- IEEE Std 7-4.3.2-1993, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.

IEEE Std 730-1998 was replaced by IEEE Std 730-2002, ASME NQA-1-1997 was replaces by ASME NQA-1-2004, and IEEE Std 7-4.3.2-1993 was replaced by IEEE Std 7-4.3.2-2003.

IEEE's *Standard Glossary of Software Engineering Terminology* (IEEE Std. 610.12-1990) defines the quality as "the degree to which a system, component, or process meets (1) specified requirements, and (2) customer or user needs or expectations."

Figure 1 shows a scheme of main ISO/IEC standards.

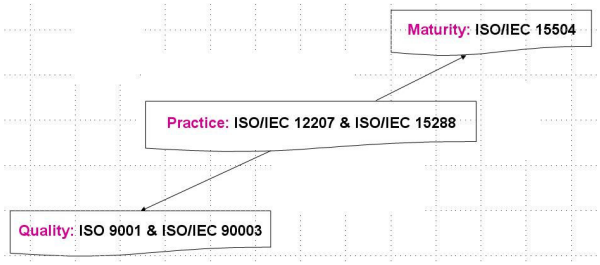

Figure 1. Main ISO/IEC Standards (adapted from [2])

SQA (Software Quality Assurance) covers all the phases of the software life cycle processes, including safety, reliability, independent verification and validation, and metrics.

SQA monitors and evaluates the process as well as the products. In a process assurance, SQA provides a management with objective feedback regarding compliance to approved plans, procedures, standards, and analyses. In a product assurance, SQA monitors the changing level of product quality within each phase of the life cycle, such as the requirements, design, code, and test plan. The objective is to identify and eliminate the defects throughout the life cycle as early as possible.

The KINS (Korea Institute of Nuclear Safety) recommended that the software life cycle should be based on IEEE (The Institute of Electrical and Electronics Engineers) Std 1074 with a supplementary requirement of a software safety analysis. The KINS also recommended that the IEEE standard should be used to perform the software development activities [3].

2.1 IEEE Std 1074

IEEE Std 1074-1997 is a standard for the generation of the process that governs a software development and the maintenance for a project. This standard allows for a continuing harmonization with IEEE/EIA 12207.0-1996 and its successors.

2.2 ISO/IEC Std 12207 and IEEE/EIA Std 12207 [4]

ISO/IEC Std 12207 for Software Life Cycle Processes was published in 1995, with Amendment 1 in 2002 and Amendment 2 in 2004, defining the requirements for an acquisition, supply, development, operation and maintenance of software. The processes specified in the standard cover the entire software life cycle. ISO/IEC Std 12207 includes some general processes which are also present in ISO 9001:2000 such

as the documentation, records, quality assurance, audits, management responsibility, infrastructure, improvement, and training.

IEEE/EIA Std 12207 is the product of cooperative efforts exerted by several major standards organizations for the purpose of developing a global software life cycle process standard. The main contributors were:

- US DOD (MIL-STD-498:1994)
- ANSI, IEEE and EIA (J-Std-016-1995)
- ISO and IEC (ISO/IEC Std 12207)

2.3 CMMI and ISO 9001:2000 [5]

CMMI (Capability Maturity Model Integration) of SEI (Software Engineering Institute) CMU (Carnegie Mellon University) was upgraded from CMM to harmonize several capability maturity models: systems engineering, software engineering, acquisition, and integrated product development. CMMI has a close relationship with ISO/IEC 15504.

IEEE software engineering standards are closely related to CMMI-SW Level 2 compliance [6].

CMMI and ISO 9001:2000 have more similarities than differences. We can use the strengths of one standard to counter the weaknesses of the other, thus further unifying the process improvement approach.

Both documents are based on the following:

- Process approach,
- Full life cycle,
- Integration of management and production process,
- Systematic planning,
- Extensive process and product measurements,
- Explicit requirements for the resources needed to implement the process,
- Educated and well-trained workforce,
- Need for stakeholder involvement and customer satisfaction.

2.4 ISO/IEC 90003 [7]

The international standard ISO/IEC 90003 provides guidance for organizations in the application of ISO9001:2000 for the acquisition, supply, development, operation and maintenance of a computer software. It is independent of the technology, life cycle models, development processes, sequence of activities and organizational structures. ISO/IEC 90003 has the following five areas:

- Quality Management System
- Management Responsibility
- Resource Management
- Product Realization
- Measurement, Analysis and Improvement

Organizations with quality management systems for developing, operating, and maintaining software based on this standard may choose to use processes from ISO/IEC 12207 to support or complement the ISO 9001:2000 process model.

Figure 2 shows harmonization efforts and relationships among various frameworks (standard, model, …).

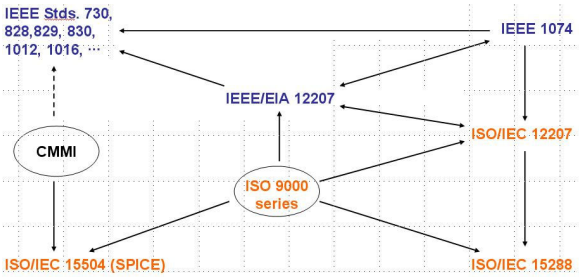

Figure 2. Harmonization among Frameworks (adapted from [5], [6], [8] and [9])

3. Conclusion

Integrated implementation of ISO 9001:2000 and CMMI is regarded as possible and may result in a synergy effect. Since using IEEE standards is recommended by the KINS and it could ensure a CMMI-SW Level 2 compliance, applying the combined approach of ISO-CMMI could give us a good software quality assurance of a process and a product.

REFERENCES

[1] Jang Yeol KIM, et. al., Methods of Software Quality Assurance under a Nuclear Quality Program, Proceedings of Korean Nuclear Society 2005 Spring Meeting, Korea, May 2005.

[2] http://www.15288.com/15288%20relations.htm

[3] Yong Suk Suh, et. al., SMART-P MMIS Software Development by Considering the Software License for Nuclear Power Plants and Development Cost, Proceedings of Korean Nuclear Society 2005 Spring Meeting, Korea, May 2005.

[4] Daniel Galin, Software Quality Assurance, Pearson Education Limited, 2004, Chapter 24.

[5] Boris Mutafelija, Harvey Stromberg, Systematic Process Improvement Using ISO 9001:2000 and CMMI, Arctech House, Inc., 2003, Figure 1.1, pp. 8~9.

[6]http://standards.computer.org/sesc/s2esc_conferences/SSTC_2004/SSTC04-Land-IEEE.ppt

[7] http://profs.logti.etsmtl.ca/wsuryn/research/SQE-Publ/ISO_IEC90003%20(IMS4_2004).pdf.

[8] http://www.software.org/quagmire/

[9] G. Gordon Schulmeyer, James I. McManus, Handbook of Software Quality Assurance, 3rd Ed., Prentice Hall PTR, 1999, Figure 4-2.