Comparison of the Software Safety Criteria between IEC and IEEE Standards for the Digital Instrumentation and Control System

Jang-Soo Lee, Kee-Choon Kwon
KAERI: Korea Atomic Energy Research Institute,
Instrumentation and Control . Human Factors Division, Daejeon, Korea, 305-353
{jslee, kckwon}@kaeri.re.kr

1. Introduction

This paper describes the relationship between the overall safety lifecycle and the software safety lifecycle during the development of the software based safety systems of Nuclear Power Plants. This includes the design and evaluation activities of components as well as the system. The paper also compares the safety lifecycle and planning activities defined in IEC 61508 with those in IEC 60880, IEEE 7-4.3.2, and IEEE 1228. Using the Korean KNICS project as an example, software safety lifecycle and safety analysis methods applied to qualify the POSAFE-Q PLC system under the internal verification and validation by KAERI and independent 3rd party review by ISTec are demonstrated. KNICS software safety lifecycle is described by comparing to the software development, testing, and safety analysis process with international standards. The qualification of the software for the KNICS POSAFE-Q PLC is a joint Korean German project. The assessment methods applied in the project and the experiences gained from this project are presented.

2. Safety Lifecycles in IEC and IEEE Standards

The safety assessment of the software for the KNICS RPS and PLC is an ongoing joint Korean/German project. In the cases where the documents have been evaluated by KAERI, ISTec has checked the results of the evaluation by supplementing spot checks for the development documents according to the following IEC and IEEE standards.

- IEC 61508-1, Functional safety of electrical/electronic/programmable electronic safety-related systems –Part 1:General requirements [1]
- IEC 61508-2, Functional safety of electrical/electronic/programmable electronic safety-related systems –Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems [2]
- IEC 61508-3, Functional safety of electrical/electronic/programmable electronic safety-related systems –Part 3: Software requirements [3]
- IEC 60880, Nuclear Power Plants – I&C systems important to safety – Software aspects for computer-based systems performing category A functions [4]
- IEC 61513, Nuclear Power Plants – Instrumentation and control for systems important to safety – General requirements for systems [5]
- IEEE Std. 7-4.3.2-2003, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations [6]
- IEEE Std. 1228-1994, IEEE Standard for Software Safety Plan [7]

Table 1. Comparison of the Safety Lifecycles between IEC and IEEE standards

IEC 61513 system safety lifecycle	IEC 60880 software safety lifecycle	IEEE 7-4.3.2 computer system safety lifecycle (Annex D)	IEEE 1228 software safety lifecycle
System requirements specification	Software requirements specification	Hazards identification and evaluation plan	Software safety plan
System planning		Safety system hazard identification	Software safety analyses preparation
System specification		Computer system hazards identification	
System detailed design and implementation		Software requirements hazards identification	Software safety requirements analysis
System architecture	Software design	Software design hazards identification	Software safety design analysis
Design constraint requirements			
Defense against propagation of failures			
System architecture, self-monitoring and tolerance to failures	Implementation of new software in general		

	purpose language		
Selection of equipment	Implementation of new software in application-oriented language	Software implementation hazards identification	Software safety code analysis
Internal behavior of system	Configuration of pre-developed software and devices	Evaluation of hazards in previously developed systems	
System integration	Software aspects of integration	Computer system integration testing for hazards conditions	Software safety test analysis
System operation plan			
System validation	Software aspects of validation	Computer system validation testing	
System modification		Maintenance and modification hazard analysis	Software safety change analysis
System verification plan			

Most of the IEC and IEEE standards consist of three main phases, planning phase, realization phases according to the plan, and the validation phase. The safety lifecycles for the industry specific standards, for example, IEC 62279 for a railway, IEC 61513 for nuclear power plants, inherit the definition of phases from the generic IEC standard of IEC 61508. However, the detailed phases of the safety lifecycles for the specific industries are different from IEC 61508. Table 2 shows for instance the differences in the safety lifecycles between the IEC and IEEE standards. The safety lifecycles in the IEEE standards require a direct safety analysis at each phase of the lifecycle.

3. Software Safety Lifecycle for KNICS

In the KNICS project, a safety lifecycle was developed as shown in Fig. 1 with the quantitative approach for the reliability analysis of the system and hardware levels, but with the qualitative approach for the safety analysis of the software.

We used the software fault tree analysis (FTA) method for the design and coding phases of the lifecycle. After creating the software fault trees by using the procedure, they produced two groups of outcomes from the software FTA. One group is the recommendations to improve the fault tolerance, and the other is the influence on a testing.

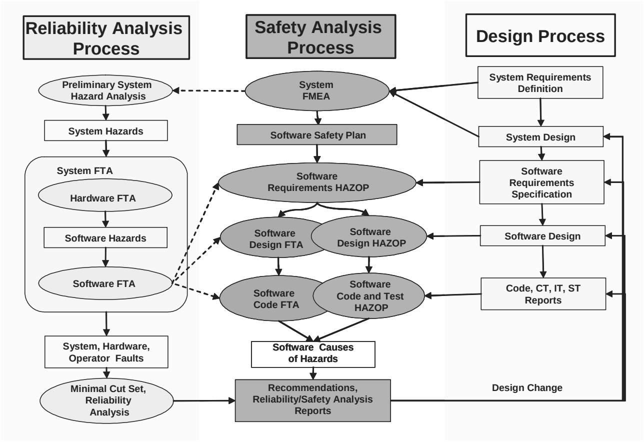
Reliability Analysis Process
Safety Analysis Process
Design Process
Preliminary System Hazard Analysis
System FMEA
System Requirements Definition
System Hazards
Software Safety Plan
System Design
System FTA
Hardware FTA
Software Requirements HAZOP
Software Requirements Specification
Software Hazards
Software Design FTA
Software Design HAZOP
Software Design
Software FTA
Software Code FTA
Software Code and Test HAZOP
Code, CT, IT, ST Reports
System, Hardware, Operator Faults
Software Causes of Hazards
Minimal Cut Set, Reliability Analysis
Recommendations, Reliability/Safety Analysis Reports
Design Change

Fig. 1. Software safety lifecycle for the KNICS RPS and PLC systems

4. Conclusion

This paper discusses the software lifecycle safety analysis tasks for the safety-critical software protection system in nuclear power plants. In order to meet the requirements from both the frameworks of the standards, IEC and IEEE, the safety lifecycles have been compared, and the differences of the frameworks have been identified.

REFERENCES

[1]IEC 61508-1, Functional safety of electrical/electronic/programmable electronic safety-related systems –Part 1:General requirements

[2]IEC 61508-2, Functional safety of electrical/electronic/programmable electronic safety-related systems –Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

[3]IEC 61508-3, Functional safety of electrical/electronic/programmable electronic safety-related systems –Part 3: Software requirements

[4]IEC 60880, Nuclear Power Plants – I&C systems important to safety – Software aspects for computer-based systems performing category A functions

[5]IEC 61513, Nuclear Power Plants – Instrumentation and control for systems important to safety – General requirements for systems

[6]IEEE Std. 7-4.3.2-2003, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

[7]IEEE Std. 1228-1994, IEEE Standard for Software Safety Plan