Experience in the Selection of the CASE Tool for the Safety Critical Software

Do Young Oh*, Chang Ho Kim, Ji Hyeon Kim, Se Do Sohn
I&C System Engineering Department, KEPCO Engineering and Construction Co. Inc.
150 Duckjin-dong, Yuseong-gu, Daejeon 305-323
Corresponding author: grayo@Kepco-enc.com

1. Introduction

IEC 60880 [3] introduces detail requirements to apply model based software engineering tools which can generate qualified source codes in the safety critical software. These tools were already applied to the developments of safety critical software in the Nuclear Power Plant of European Union. However, in Korea, all of design works were performed by engineers where human errors can be introduced. This traditional approach is hard to verify and validate the function block diagrams.

KEPCO E&C develops PPS and QIAS-P software in SUN 1&2 and needs to adopt the efficient way of developing safety critical software and keeping same reliability of software with previous software. KEPCO E&C is planning to apply a software engineering tools in software development process. KEPCO E&C evaluated several tools in order to select the most appropriate tool in its new development environment.

2. The goal of tool selections

For the tool selection, KEPCO E&C focuses on the following essential characteristics needed during developing safety critical software.

- Model Based design and V&V tool
- Interface with requirements management tools and Software configuration tools
- Automatic document and reliable source code generation
- Simulation, Debugging, and Testing
- Satisfying IEC [3] and IEEE [1, 2] standards, and licensing requirements
- Experience in safety critical software field

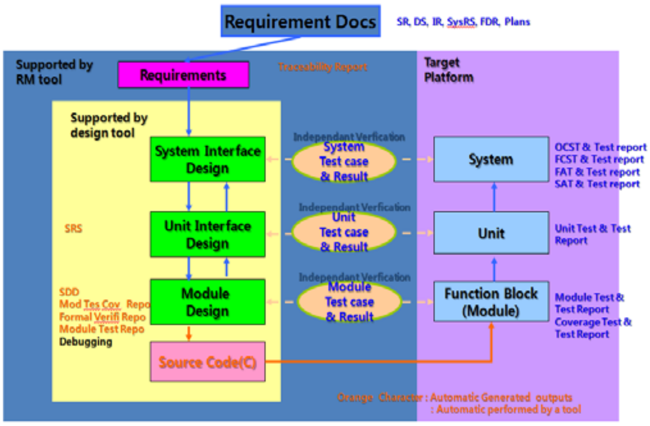


Figure 1. Target Software Development Procedure

Based on these functions, KEPCO E&C was planning to build up a new safety critical software development methodology like Figure 1.

KEPCO E&C contacted several companies providing software engineering tools and ask information about tools. After reviewing features of each tool, KEPCO E&C chose top three tools satisfying almost required major functions above, in order to perform detailed evaluation.

3. The procedure of the tool selection

In order to choose the most proper tools, KEPCO E&C divided the tool selection procedure to three phases by the purposes of them. All phases and their relationship are depicted in Figure 2.

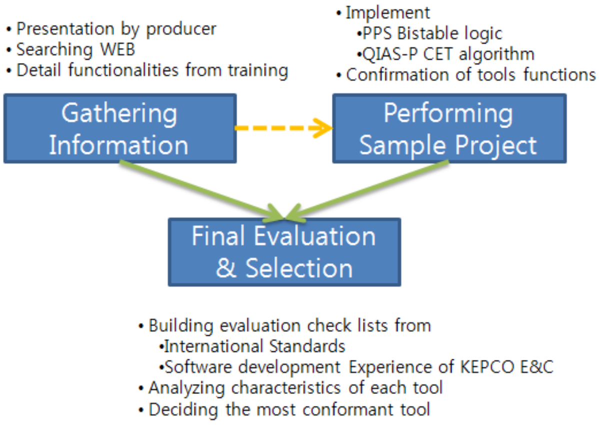

• Presentation by producer
• Searching WEB
• Detail functionalities from training
• Implement
•PPS Bistable logic
•QIAS-P CET algorithm
• Confirmation of tools functions
Gathering Information
Performing Sample Project
Final Evaluation & Selection
• Building evaluation check lists from
•International Standards
•Software development Experience of KEPCO E&C
• Analyzing characteristics of each tool
• Deciding the most conformant tool

Figure 2. Three Phases of the tool selection

3.1. Gathering Information

At the first phase, KEPCO E&C gathered information of three tools by a presentation of each tool producer, web searching, tool manuals, and so on. Additionally, KEPCO E&C took a training to learn the detail tool features and usages for the second phase. In this phase, KEPCO E&C clarified the major target fields, experiences, providing development method, interfaces with the other tools, and useful functions to development of each tool.

3.2. Performing Sample Projects

By implementing sample project, the testing of tools was performed for substantiation of collected features in phase 1. Important parts of PPS and QIAS-P logic were chosen as samples and implemented with candidates. Generating source codes and documentation, testing implemented model, applying formal verification, and simulating and debugging the models were performed. By this phase, almost of required features including merits, weakness, conformance of generated codes and documents, modeling convenience, and provided specific or special functions of tools were confirmed. Figure 3 shows the sample project implementation.

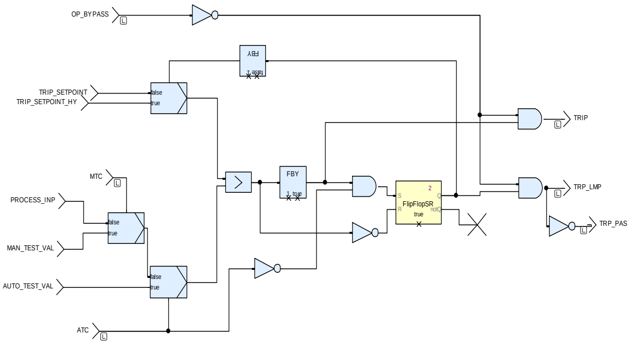
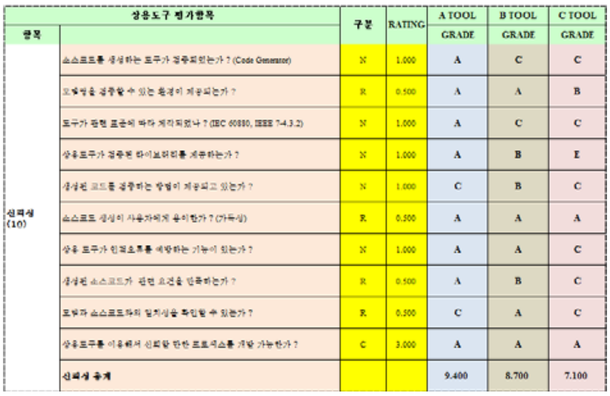


Figure 3. PPS sample software

3.3. Final Evaluation and Tool Selection

Based on the international standards [1, 2, 3] and experience of KEPCO E&C in safety critical software, the evaluation sheet was developed. The major points were Functionality, Reliability, Efficiency, Maintainability, Testability, Licensing effort, Resources, Rigor of the Quality, Vendor Tool History, and Economical Efficiency. Each point had weights in accordance with its importance and divided into specific items. Figure 4 shows the sample evaluation sheet for the Reliability.



상용도구 평가항목		구분	RATING	A TOOL	B TOOL	C TOOL
항목				GRADE	GRADE	GRADE
신뢰성 (10)	소스코드를 생성하는 도구가 검증되었는가 ? (Code Generator)	N	1.000	A	C	C
	모델링을 검증할 수 있는 환경이 제공되는가 ?	R	0.500	A	A	B
	도구가 관련 표준에 따라 제작되었나 ? (IEC 60880, IEEE 7-4.3.2)	N	1.000	A	C	C
	상용도구가 검증된 라이브러리를 제공하는가 ?	N	1.000	A	B	E
	생성된 코드를 검증하는 방법이 제공되고 있는가 ?	N	1.000	C	B	C
	소스코드 생성이 사용자에게 용이한가 ? (가독성)	R	0.500	A	A	A
	상용 도구가 인적오류를 예방하는 기능이 있는가 ?	N	1.000	A	A	C
	생성된 소스코드가 관련 요건을 만족하는가 ?	R	0.500	A	B	C
	모델과 소스코드와의 일치성을 확인할 수 있는가 ?	R	0.500	C	A	C
	상용도구를 이용해서 신뢰할 만한 프로세스를 개발 가능한가 ?	C	3.000	A	A	A
	신뢰성 총계			9.400	8.700	7.100

Figure 4. Sample Evaluation Sheet

The sub-clauses were defined for the detail evaluations of each major point. Some of them came from requirements described in the international standard. In order to apply new tools to traditional development process and to select tools the users can easily use, the opinions of users were also considered. Each sub-clause had its weigh decided by the committee consisting of experienced engineers and future users for considering opinions of groups taking part in whole development process.

Based on the results coming from two previous phase, conformances of candidates were evaluated by the committee with a grade which consists of A, B, C, D, and E. By adding these score, the final score of each tool was calculated and the tool getting the highest score was selected.

This tool provides powerful model based design and various validation and verification functions. It was used to develop safety critical software in nuclear and aero space. The code generator makes the same codes with model and it is qualified by testing with highest level of the software. European standards [3] request automatic code generation when developing safety critical software, so it is vital to enter European market.

4. Future Plan

Each tool has its own characteristics and does not provide enough features which can cover whole development process, because of the various target platforms, legacy development procedure, and so on. So KEPCO E&C is customizing the selected tool for adopting it to own development process and developing PPS and QIAS-P with it. The uncovered area of the selected tool will be covered by the other tools or V&V effort in order to meet the international standards and licensing requirements.

5. Conclusion

The tool selection process took 1 year, but this work is very important process for a new development procedure, because the software development tool affects all of the software life cycle. The procedure was developed for the new tool selection, because tools applied to safety critical software requires very high reliability and it affects the whole software engineering process. For this evaluation, the qualitative and quantitative analyses are applied. And the survey based selection may have high risk, because the quality of provided function varies according to application characteristics developed by each tool. Hence, it is essential to test and confirm all required features over whole tool selection process. The evaluation sheet should be developed considering the purpose and scope of a developed software type and given circumstance of software development.

REFERENCES

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

[2] IEEE Std. 1012-2004, IEEE Standard for Software Verification and Validation.

[3] IEC Std. 60880, Software aspects for computer-based systems performing category A functions.