Qualification Strategy of a Software Development Tool for PLC Programming in KNICS

Kyung H. Cha, Yeong J. Lee, Jang Y. Kim, Jang S. Lee, and Kee C. Kwon
Instrumentation and Control·Human Factors Research Division, KAERI,
P.O. Box 105, Yuseong, Daejeon, 305-600, Republic of KOREA
{khcha, ex-yjlee426, jykim, jslee, kckwon}@kaeri.re.kr

1. Introduction

The IEC 61131-3 [1] deals with the programming aspect of industrial programmable controllers, defining the logical blocks and languages such as Structured Text (ST), Instruction List (IL), Sequential Function Charts (SFC), Ladder Logic (LD), Function Block Diagrams (FBD). A software development tool for the IEC 61131-3 programming, namely pSET (POSCON Software Engineering Tool), has been prototyped for developing safety software for the Korea Nuclear Instrumentation and Control System (KNICS) since 2001. Figure 1 shows the pSET architecture.

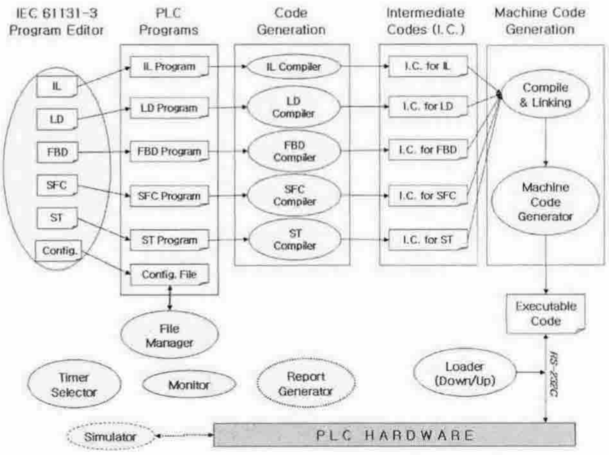

Figure 1. The pSET architecture (The dotted lines mean the unimplemented components in the current pSET.)

Software and their development tools for nuclear Instrumentation and Control (I&C) systems should be qualified in accordance with the nuclear codes and standards. The recent ones include the code generation and type testing for Teleperm XS [2] and the TriStation system for Triconex TRICON PLC (Programmable Logic Controller) [3].

The pSET qualification strategy has been established and featured for the criteria and requirements, the qualification processes, the qualification of the code generation, and the qualification techniques and tools.

2. The pSET Qualification Strategy

The pSET qualification strategy is generated by considering reliability requirements, analysis of the pSET development process, adequacy of the pSET documentation, and life cycle testing of the pSET. Specially, the pSET qualification strategy is focused on the code generation and the Integrated Development Environment (IDE) for the IEC 61131-3 programming because they may affect to the quality of software to be embedded into the target PLC system. Figure 2 shows the qualification strategy of the pSET for developing the embedded software in the KNICS.

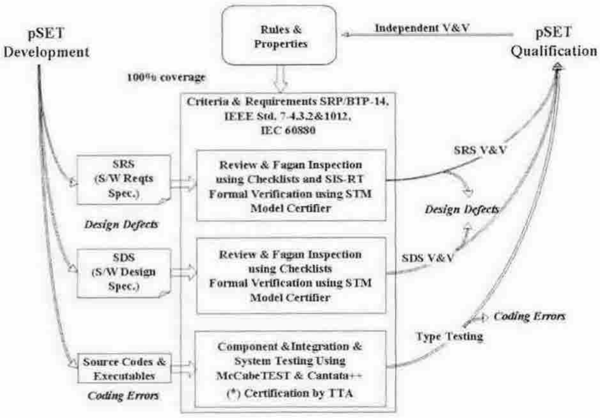
pSET Development
Rules & Properties
Independent V&V
pSET Qualification
100% coverage
Criteria & Requirements SRP/BTP-14, IEEE Std. 7-4.3.2&1012, IEC 60880
SRS (S/W Reqts Spec.)
Review & Fagan Inspection using Checklists and SIS-RT Formal Verification using STM Model Certifier
SRS V&V
Design Defects
Design Defects
SDS (S/W Design Spec.)
Review & Fagan Inspection using Checklists Formal Verification using STM Model Certifier
SDS V&V
Coding Errors
Type Testing
Source Codes & Executables
Component & Integration & System Testing Using McCabeTEST & Cantata++ (*) Certification by TTA
Coding Errors

Figure 2. The pSET qualification strategy

2.1 Qualification Criteria and Requirements

The pSET shall be qualified for the review criteria and the tool requirements in the Software Review Plan (SRP)/BTP-14 [4], the IEEE Std. 7-4.3.2 [5], and the IEC 60880 [6]. The IEEE Std. 1012 [7] is also applied for the life-cycle verification and validation (V&V) of the pSET.

2.2 Qualification Procedure

The qualification procedure to be applied for the IDE and the code generation is generated for the following activities.

1. Specifying software requirements and design
2. Verifying the code generation against the IEC 61131-3 programs by the Program Editor
3. Automated life cycle testing of the pSET, including type testing
4. Testing and validating the generated C codes (This activity may be performed by the software tester of the RPS or the ESF-CCS.)

2.3 Qualification of Code Generation

The code generation is the core part of the pSET because the generated code shall be compiled and loaded into the target PLC system.

Therefore, the followings are considered for the qualification procedure 3 in Section 2.2.

1. Formal verification by model checking or theorem proving
2. Quality evaluation by Software Testing Center of TTA (Telecommunication Technology Association)

2.4 Techniques and Tools for the pSET Qualification

Representative qualification techniques [8] include checklists-based Review and Inspection (R&I), the certification of the code generation and the programming environment for the IEC 61131-3 programming languages, and automated software testing.

Checklists are structured with the qualification criteria and requirements listed in Section 2.1 and they are used for the life-cycle software V&V of the pSET. In addition to the life-cycle V&V, an interactive verification technique such as model checking or theorem proving is considered for qualifying the code generation.

These qualification techniques are supported by their tools, including the SIS-RT (Software Integrated Support and Requirements Traceability) [9] for supporting the checklist-based R&I, the McCabe for structured testing, the Cantata++ for dynamic software testing, and the Statemate MAGNUM Model Certifier for formal verification.

In addition to the qualification tools, a reverse engineering tool like the SPACE system for Teleperm XS is being studied for validating the generated code against the IEC 61131-3 PLC programs.

3. Conclusions

The pSET, as a software development tool for the IEC 61131-3 programming in the KNICS, shall be qualified in accordance with the criteria and requirements in the SRP/BTP-14 [4], the IEEE Std. 7-4.3.2 [5], the IEC 60880 [6] and the IEEE Std. 1012 [7].

The pSET qualification strategy, emphasizing on the code generation and the IDE for the IEC 61131-3 programming, is featured for the qualification criteria and requirements, the qualification procedures, the type testing or the certification of the pSET components, and the techniques and tools for qualifying the pSET.

The generated qualification strategy shall be refined for reflecting a design change of the pSET and applied to qualify the pSET for the KNICS.

ACKNOWLEDGMENTS

This work is being performed for "Development of the Licensing Technology for Digital I&C" which is a part of the KNICS project and is supported by the Korean Ministry of Science and Technology (MOST) from 2001 to 2008.

REFERENCES

[1] IEC 61131-3, Programmable Controllers – Programming Languages(2nd Ed.), Dec. 10, 2001.

[2] Hulbert C. Li, Regulatory Review of Siemens Teleperm XS: A Digital Reactor Protection System, Proceedings on NPIC&HMIT 2000, Washington, DC, Nov., 2000.

[3] J. Troy Martel, P.E., Generic Qualification of the Triconex TRICON Fault Tolerant PLC-Based Platform for Safety-Related Applications, Proceedings on NPIC&HMIT 2000, Washington, DC, Nov., 2000.

[4] NUREG-0800, SRP/BTP-14: Guidance on Software Reviews for Digital Computer-based I&C Systems, USNRC, Washington D.C., July, 1997.

[5] ANSI/IEEE Std. 7-4.3.2-2003 (Revision of IEEE Std 7-4.3.2-1993), IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.

[6] IEC 60880 (Ed.2.0) Committee Draft (CD), Nuclear Power Plants-I&C systems important to safety – Software aspects for computer-based systems performing category A functions, Dec. 12, 2003.

[7] IEEE Std. 1012-1998(Revision of IEEE Std 1012-1986), IEEE Standard for Software Verification and Validation Plans.

[8] KAERI, Software Verification and Validation Plan (SVVP) for the Safety PLC (Programmable Logic Controller), Aug.26, 2004. (In Korean)

[9] Seo R. Koo, et al., Development of Software Requirement Analysis Tool for NPP Software Fields Based on Software Inspection and Formal Method, Proceedings of International Symposium on the Future I&C for NPP (ISPFIC 2002), Seoul, Korea, pp.159-164, Nov. 7-8, 2002.