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

Experience on the COTS Software Dedication of the PROFIBUS FMS-Driver

Jang Yeol Kim, Young Jun Lee,
Kyung Ho Cha, Se Woo Cheon, Jang Soo Lee, Kee Choon Kwon

Address : I&C and HF Div. Korea Atomic Energy Research Institute (KAERI)
P.O. Box 105, Yuseong, Daejeon, 305-600, Republic of Korea
E-mail : jykim@kaeri.re.kr

1. Introduction

From the middle of the 1980's, the field bus has been developed for the network system which supports the real-time communication of various controls and automation equipments. It is known for PROFIBUS in the field of a production automation environment. The PROFIBUS architecture uses open communication (ISO 7498) based on the ISO/OSI model. The PROFIBUS standard uses layer 1 (physical layer : PHY), layer 2, (data link : FDL) and layer 7 (application). Layer 7 of PROFIBUS FMS(Fieldbus Message Specification) provides a information level communication service to a communication and the user of a station. The Field, the Cell and Factory Level among the Cell Level portion of Figure 1 correspond to the PROFIBUS-FMS.

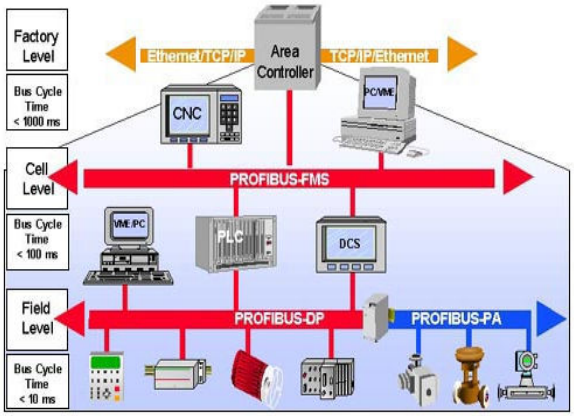

Figure 1. PROFIBUS Architecture

The high-level communication of the safety-grade PLC (POSAFE-Q) developed through the KNICS projects is the FMS. The PROFIBUS FMS software consist of the CPB (Communication Processor Board) and the Driver Software. The CPB software is a self–developed software following the software life cycle which is exempted from the COTS Dedication. Therefore, the PROFIBUS FMS Driver software is the portion of the COTS Dedication. Third party test as a special test by the TTA (Telecommunication Technology Association) has been performed for the goal of a reliability and safety

2. The COTS item of PROFIBUS-FMS

The PROFIBUS FMS communication module consist of a Processor Module, two Dual Port Memory(DPM-CPB, DPM-DRV), a Communication Processor Board(CPB) and the Driver module. PROFIBUS FMS communication Driver board portion (COTS module) is composed of 2 communication ports.

The driver board portion is shown in the right side block named COTS module of Figure 2. COTS module is the scope of the COTS dedication.

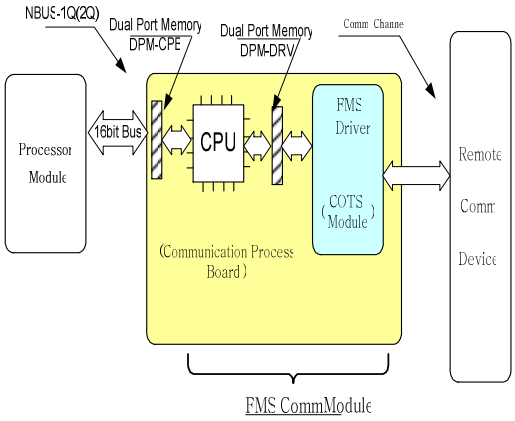

Figure 2. Hardware configuration for PROFIBUS FMS communication module

3. COTS Software Dedication Effort

The Commercial-Off-The-Shelf(COTS) software used in the safety software should be subjected to the same level of verification as the software to be developed for a nuclear plant safety software system. Basically, the Commercial Off-the-Shelf(COTS) software dedication is the responsibility of the Software Safety Verifier.

The Commercial Off-the-Shelf(COTS) software dedication have four methods; Method 1(special test and inspection), Method 2(Commercial grade survey), Method 3(Source verification), Method 4(Qualification Vendor List and operational history record). We have applied Method 1, Method 2 and Method 4. The special test(Method 1) is performed by the TTA(Telecommunication Technology Association). In order to site audit for Commercial Grade Survey(Method 2) visits HilScher company located in

Germany. It can be acquired from the experience record(Method 4) from HilScher Company during site audit. The combined methods are applied for the COTS dedication. Especially, it received a PNO(Profibus National Organization) certificate as an additional effort.

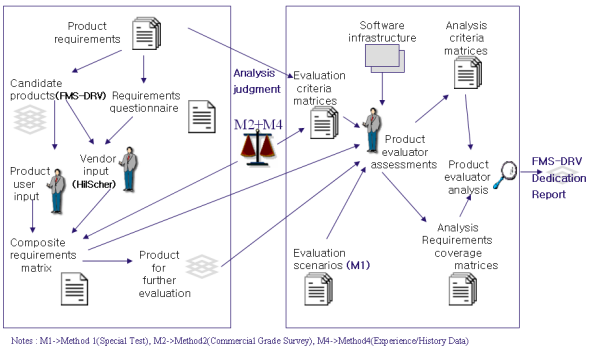

Figure 3 Combined COTS Dedication process

4. Conclusion

The PROFIBUS FMS Driver (PNDOS1) is a commercial business software and is operated with a high-level communication over the POSAFE-Q.

At the beginning of the COTS dedication, we have tried to apply a combination of Method 2 (commercial grade survey method) and Method4 (Experience history record) but, which is not enough. We have to choose Method1 (special testing) by TTA as a compensation factor. The PNO is an abbreviation of the PROBIBUS National Organization. The PNO stands for a national PROFIBUS user organization. The reason for a PNO Certificate which is very important leads to the sharing hardware board between Physical Layer 1 and Data Link Layer 2. It was needed for a integrity of this portion to make sure of its reliability. PNO certification was acquired from Germany after several on-site testing processes. Actually, we used three combination methods which are Method 1, Method 2 and Method 4. From the above combination method, there was no problem in using the software Driver of PROFIBUS FMS. From an objective viewpoint, it has a significant meaning to have the reliability of PROFIBUS FMS by TTA and an additional PNO certification. Figures 4 and 5 are the TTA certification and PNO certification respectively

Figure 3. TTA Certification for PROFIBUS FMS communication module

Figure4. PNO Certification for PROFIBUS FDL communication module

REFERENCES

[1]USNRC, NUREG-0800/BTP-14, "Guidance on Software Reviews for Digital Computer-based I&C Systems," 1997.

[2]USNRC, Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computers used in Safety Systems of Nuclear Power Plants," 2004.

[3]USNRC, Regulatory Guide 1.152, "Criteria for Programmable Digital Computers System Software in Safety Related Systems of Nuclear Power Plants," 1996.

[4] IEEE Std. 603-1998, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

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

[6] NUREG/CR-6421, "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications."

[7] Electric Power Research Institute (EPRI) NP-5652, Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications

[8] EPRI Topical Report, TR-106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications

[9] J.Y. Kim, S.W. Cheon, J.S. Lee, Y.J. Lee, K.H. Cha, and K.C. Kwon, "Software V&V Methods for a Safety Grade Programmable Logic Controller," Proceedings of the International Conference on Reliability, Safety and Hazards-2005, Dec. 1, 2005.

[10] SeoRyong Koo, PoongHyun Seong, JunBeom Yoo, Sung Deok Cha, Cheong Youn and HyunChul Han, "NuSEE An Integrated Evvironment of Software Specification and V&V for PLC based Safety-critical Systems", Nuclear Engineering and Technology, Vol 38 No 3 April 2006.