Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 22, 2009

Safety Evaluation of Full Digital Plant Protection System of Shin-Kori 3&4 in Korea

J.S. Koh, D.I. Kim, C.H. Jeong, H.S. Park, S.H. Ji, Y.D. Kang, G.Y. Park
Korea Institute of Nuclear Safety(KINS)

Instrumentation & Control Department, Korea Institute of Nuclear Safety, 19 Gusung-dong,Yuseong, Daejeon, Korea,
(k080kjs, dikim, chjeong, k394phs, k350jsh, k407kyd, k703pgy) @kins.re.kr

1. Introduction

Keeping pace with the emerging trend of digital computer technologies, KHNP has utilized full digital plant protection system into the design of I&C systems at SKN 3&4.

This paper presents safety review activities and results related to digital plant protection systems during the licensing of construction permit for the Shin-Kori 3&4(SKN 3&4) in Korea. The major licensing issues regarding the digital systems were software quality & cyber security during planning stage, system integrity with fail-safe design, EMI equipment qualification of digital systems, FPGA qualification and communication independence between safety and non-safety System. This paper addresses our approach to evaluate full digital protection systems with revised safety review guidelines and the resulting discussion to resolve the licensing issues.

2. System Functional Description

The SKN 3&4 PPS/ESF-CCS systems are designed with a totally computerized digital system in the instrumentation and control system important to safety including soft controllers. The PPS, the Plant Protection System, consists of four safety channel cabinets (A, B, C & D). The ESF-CCS, the Engineered Safety Features - Component Control Systems, is comprised of four safety train cabinets. Each train of the ESF-CCS shall receive initiating signals that are generated by ESFAS from all four channels of the plant protection system (PPS) and shall perform selective 2/4 logic to automatically actuate Engineered Safety Features (ESF) Systems. The major components of each channel and train in PPS/ESF-CCS are comprised of the Bistable Processor(BP), Local Coincidence Processor(LCP), Interface Test Processor(ITP) and Maintenance and Test Panel(MTP), Minimum Inventory Switches, ESCM(ESF-CCS Soft Control Module), Group Controller, Loop Controller, etc.

Bistable Processor(BP) ; monitoring the process variable and comparing it to a setpoint and generating a bistable trip signal
Local Coincidence Processor(LCP) ; comparing the bistable trip signals from the four channels and initiating an output initiation signal based on a 2/4 coincidence.
Interface Test Processor(ITP) and Maintenance and Test Panel(MTP) ; conducting PPS periodic maintenance and automatic testing.
Communications Networks ; It consists of Soft Control Network, Intra-Channel Network, QIAS(Qualified Indication & Alarm System)-N Network, etc.

3. Safety Evaluation And Results

The SKN 3&4 PPS/ESF-CCS systems are digital-based systems using ABB Advant PLC. It is said that such systems could result in safety significant common cause failures due to hardware and software design errors, or software programming errors which may cause redundant equipment to fail. And also, these digital-based systems are also vulnerable to electromagnetic environments.

During the licensing of construction permit for the SKN 3&4 in Korea, The major licensing issues regarding the digital systems were software quality & cyber security during planning stage, system integrity with fail-safe design, EMI equipment qualification, FPGA qualification and communication independence between safety and non-safety system. etc.

3.1 Software Quality & Cyber Security during planning stage

It was evaluated that the development process for the PPS/ESF-CCS software was based on the software program manual(SPM) for SKN 3&4. The SPM describes the requirements for the software design and development process and consists of several basic elements; software quality assurance plan, software verification and validation plan, software configuration management plan, etc[1].

After evaluating software quality including cyber security during planning stage, KINS required the utility to establish a strong interface between the software development group and quality assurance group. And also KINS required KHNP to submit key documents related with the safety systems (PPS, ESF-CCS, CPCS, Soft Controller and so on) in order to assure software quality including cyber security.

3.2 System Integrity with Fail-Safe design

We discussed how a protective function actuates in case of hardware or software failure detected by self-diagnosis, and what the fail-safe status is in case of failure or acceptable status in case of loss of energy[2]. We reviewed appropriateness of design concept that

ESFAS actuation state goes to non-actuate and alarm is generated in the case of failure of data transmission between PPS and ESF-CCS. It was asked to submit analysis result to evaluate the influence of it on the plant safety. KHNP answered that the consequences of an inadvertent ESFAS actuation, such as containment isolation, containment spray actuation, or main steam isolation, can be more harmful than the possible loss of ESFAS function in one division. It is a reason why SKN 3&4 adopts "fail-to-non-actuate", on the contrary, UCN 5&6 adopts "fail-to-actuate". As a result of reviewing analysis, the original trip logic algorithm was changed to meet system integrity with fail-safe design such that the selective 2/4 trip leg((A & C) or (B & D)) for ESFAS goes to trip state in the case of "bad" signal of both LCL.

3.3 EMI equipment qualification

As the electromagnetic environment could cause redundant digital-based systems to fail, KINS required the designer to perform RS-103 test with 10GHz according to the method of Reg. Guide 1.180 (Rev. 1). RS-103 test is applicable in the frequency range 1 GHz to 10 GHz, covering the unlicensed frequency bands where much of the high-frequency communications activity is taking place (2.45 GHz and 5.7 GHz) [3,4].

3.4 FPGA Qualification

The FPGA(Field Programmable Gate Array) technology is used in Component Interface Module (CIM) of the ESF-CCS. FPGA such as EPM7128SL84, A54SX16, and A54SX16P is used in the CIM. We discussed what a minimum documentation would be enough to assure good quality of FPGA-based CIM design. As a result of discussion, KINS required the following documentation to meet IEEE Std. 7-4.3.2.

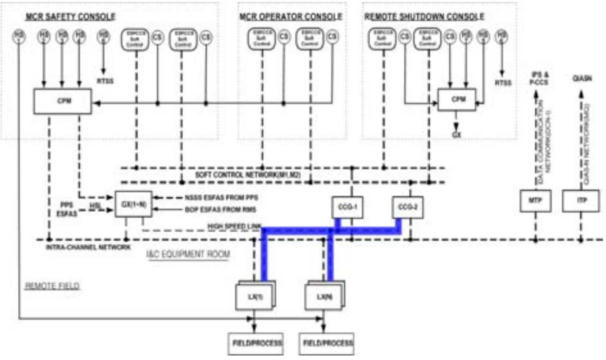
1) H/W function requirement, H/W specification, application specification (logic definitions), v&v plan
2) I/O definition and schematic diagrams
3) Simulation Waveform (Test Bit Stream)
4) Map/Place/Route: Fuse File
5) Test Vector File with Simulated Waveforms
6) JTAG File (Fuse File)
7) Board Level Functional Testing

3.5 Communication Independence between safety and Non-safety System

The independence between safety systems and non-safety systems shall be maintained as required[1,2]. We have discussed that manual ESF component control signal goes to loop controller via intra-channel network from soft controller. And also, test and indication signal are transmitted by the same intra-channel network. To meet data communication independence between safety systems and non-safety systems, modification in intra-channel network is required.

As a result of analysis of intra-channel network, communication architecture was changed to have additional communication network[4]. Manual ESF component control signals are communicated with HSL(High Speed Link) implementation which is uni-directional and safety-critical grade. Manual ESF component control signals are transmitted from the soft control networks to the appropriate intra-channel HSL via the CCGs shown as figure-1. These communications were reviewed as complying with communication independence.

Figure-1: Intra Channel Network (After modification)



4. Conclusions

The staff reviewed digital-based PPS/ESF-CCS system focusing on the assessments for the following fields ; software quality control including cyber security, system integrity with fail-safe design, EMI equipment qualification, FPGA qualification, communication independence between safety and non-safety system.

During the licensing of the construction permit for SKN 3&4 PPS/ESF-CCS systems, some design changes were accomplished such as trip logic algorithm to enhance system integrity and communication architecture to meet independence between safety and non-safety system as required by KINS. It is concluded that the SKN 3&4 PPS/ESF-CCS comply with the requirements and criteria of relevant standards.

REFERENCES

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

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

[3] USNRC Reg. Guide 1.180, Revision 1, "Guideline for Electromagnetic and Radio-Frequency Interference in Safety Related I&C System", 2003

[4] The 1st, 2nd, 3rd, 4th and 5th round questions and reponses on the SKN 3&4 PSAR provided by KHNP

[5] SKN 3&4 Preliminary Safety Analysis Report, Chapter 7, Revision 1, 2008