*Transactions of the Korean Nuclear Society Spring Meeting*
*Chuncheon, Korea, May 25-26 2006*

# New Design of Engineered Safety Features-Component Control System to Improve the Performance and Reliability

SeongTae Kim [a], SungJin Lee [a], DongHoon Kim b, Ho Kim [c]
*a. R&D Center Production Division, Doosan Heavy Industries & Construction Co., Ltd.*
*b. Dept. of MMIS, Korea Atomic Energy Research Institute*
*c. R&D Center, BNF Technology Co., Ltd.*

## 1. Introduction

The Engineered Safety Features-Component Control System(ESF-CCS) is to control the engineered safety features of NPP like SOVs, MOVs, pumps, and dampers etc, for the purpose of mitigating the effects of DBA(Design Basis Accident) or abnormal operation. ESF-CCS is designed to be composed of fault tolerant GCs(Group Controller), LCs(Loop Controller), ETIP(ESF-CCS Test & Interface Processor), COM(Cabinet Operator Module), and so on.

For the increase of safety, reliability and availability compared to an existing system, in the first place, GCs in each division are designed to be fully independent triple configuration so that it can make possible to be tested one by one for GCs during normal operation. Secondly, the design change is made for the safety-related plant component control part to be included in LCs, and to be developed according to the safety-critical system development procedures. And lastly, the test and diagnosis capabilities of ETIP and COM are reinforced.

ESF-CCS consists of four independent divisions(A, B, C, and D) in APR1400, but one division as the prototype is being designed and will be tested in this stage.

## 2. System Perspective

ESF-CCS serves as an interface system between the Plant Protection System(PPS) and remote actuation devices. Also ESF-CCS performs monitoring function for all of the safety-related components.

ESF-CCS receives ESF initiation signals from PPS and Radiation Monitoring System(RMS), and performs system level NSSS and BOP ESFAS logic(2-out-of-4 logic and 1-out-of-2 logic, respectively) independently, so that generates component level control signals finally.

ESF actuation signals generated by NSSS ESFAS logic are CIAS, CSAS, MSIS, SIAS and AFAS-1, 2. ESF actuation signals generated by BOP ESFAS logic are FHEVAS, CPIAS and CREVAS. And the ESF-CCS generates D/G load sequencer control signal. Among these ESF actuation signals, NSSS ESF actuation signals except AFAS in conjunction with valve cycling function and BOP ESF actuation signals are latched and not reset automatically. Latched ESF actuation signals are reset manually in compliance with the status of plant.

ESF-CCS shall provide the methods to monitor the status of ESF-CCS itself and ESF components, and to test the functions of ESF-CCS.

ESF-CCS is required to have methods to actuate the system level ESFAS functions manually and to control the ESF components manually in conjunction with Main Control Room(MCR) or Remote Shutdown Room(RSR).

Figure 1 shows the configuration of the division A of full ESF-CCS, which of other divisions is identical.

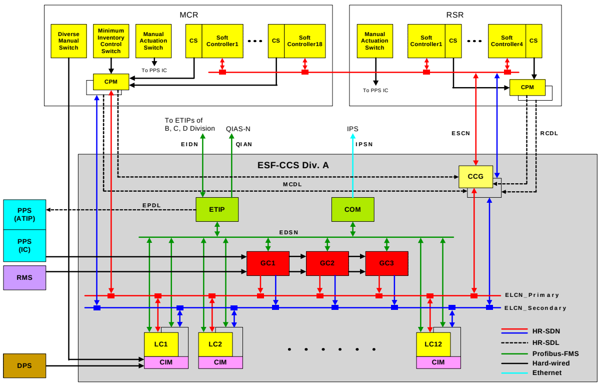

Figure 1. The configuration of the division A of full ESF-CCS

## 3. Prototype Configuration

The full design of LCs must be in accordance with the real configuration of ESF components in the target nuclear power plant, therefore in this paper, the prototype design of ESF-CCS that is to be tested and verified in this phase is introduced.

One division is made for the prototype. The hardware scope of the prototype includes fully independent triple GCs, single CCG, ETIP, COM and six LCs(note that twelve LCs in one division of the full ESF-CCS in figure 1). All platforms are nuclear safety-critical Programmable Logic Controllers(PLC) which are being developed in this project. The ESF functions embodied in the prototype are SIAS and AFAS-1, 2.

All components of the prototype are fabricated in class-1E cabinets, which are three group cabinets and six loop cabinets. In each loop cabinet, one loop controller with hot backup processing redundancy and Component Interface Modules(CIM) are established.

### *3.1 Triple Configuration of Group Controllers*

Main function of each GC's software is to determine whether to actuate ESF functions by system level NSSS and BOP ESFAS logic(2-out-of-4 logic and 1-out-of-2 logic, respectively) independently. And the test logic is performed using test signals from ETIP for all functions of GC's software, step by step.

GCs in each division are designed to be fully independent triple configuration, and to perform so that it can make possible to be tested one by one for GCs during a normal operation. While one of three GCs is tested automatically or manually, other two GCs perform the normal functions. So the output signals of three GCs are generated at an interval of the PLC scan time(50ms) irrespective of an operational mode. In a normal operational mode of GCs, each LC determines whether to generate component level control signals by component control logic, 2-out-of-3 logic, using three output signals from GCs. Then in a test mode of one GC, 2-out-of-3 logic is converted to 2-out-of-2 logic using two output signals from GCs in a normal operational mode, excepting for one signal from GC in a test mode. Therefore the LC's function can be executed stably even during a test mode of GC.

Figure 2 shows the functional diagram of GC's and LC's software.

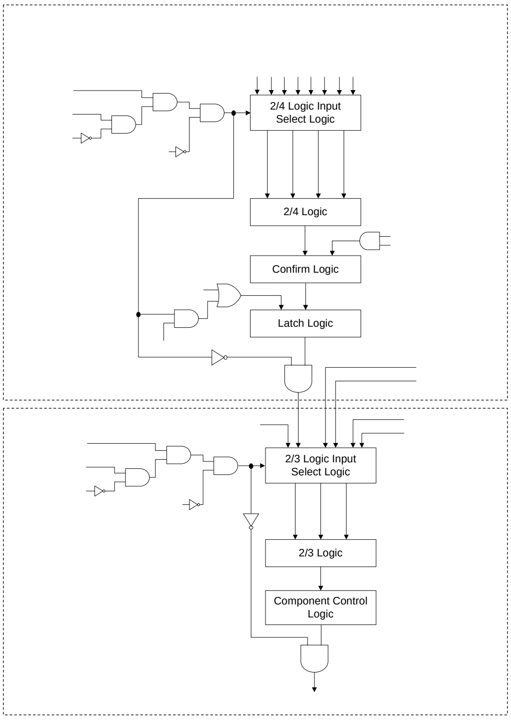

Figure 2. The functional diagram of GC and LC software

### 3.2 Unified Configuration of Component Control Part

In an existing system, the safety-related plant component control part has belonged to the Plant Control System(PCS), non-safety system. For the increase of safety and reliability, the design change is made for this part to be included in LCs, and to be developed according to the safety-critical system development procedure.

By the software life cycle, the design documents which are system requirement, interface requirement, design specification and software requirement specification for the LC's logic, have been made out till now. The separate V&V team has reviewed the above products. The LC's logic shown in figure 2, is verified by the formal method using the statechart tool.

### 3.3 Reinforcement of the Test Functions

The test and diagnosis capabilities of ETIP and COM are reinforced. By means of an automatic periodic test for all main functions of the system, it is possible to find out the abnormal status of the system quickly, and to decrease the elapsed time for tests, thus availability can be enlarged effectively.

The kinds of tests are the manual test and the automatic test, and these tests to be complementary and be overlapped can cover the whole system's functions.

| Test type | | Test scope |
|---|---|---|
| Manual test | | Fan, door and temp. sensor test |
| | | Manual actuation & reset test |
| | | Individual component output test |
| Automatic test | Passive test | H/W self-diagnosis,<br>Heartbeat error check |
| | | GC ESF initiation signals comparison test |
| | | LC ESF actuation signals comparison test |
| | Active test | GC logic test |
| | | LC actuation logic test |
| | | LC component control logic test |

Table 1. Test functions of ESF-CCS

## 4. Conclusion and Future Works

For the localization of ESF-CCS, the plan, requirement and design phase processes are being conducted in cooperation with KAERI and BNF Technology Co., Ltd. To increase the safety, reliability and availability in comparison with an existing system, the design changes are made for the system configuration and test functions. Hereafter one division as the prototype will be manufactured and tested to acquire the authorization lastly.

## REFERENCES

[1] H. Kim, and D. H. Kim, Design Specification for the Engineered Safety Features-Component Control System, 2005.

[2] H. Kim, and S. T. Kim, Software Requirement Specification for the Engineered Safety Features-Component Control System, 2006.

[3] IEEE Std. 603-1998, Standard Criteria for Safety Systems for NPGS.

[4] IEEE Std. 7-4.3.2-2003, Standard Criteria for Digital Computers in Safety Systems of NPGS.

GC

PPS A Init
PPS A Test Init
PPS B Init
PPS B Test Init
PPS C Init
PPS C Test Init
PPS D Init
PPS D Test Init

GC 1
Test Start