Preceeding of the Korean Nuclear Society Autumn Meeting
Seoul, Korea, October 1999

A study on design of the trip computer for ECC System based on Dynamic Safety System

Seog Nam Kim, Hee Hwan Han, Jai Bok Han
Korea Power Engineering Company Inc.
NSSS Power Division, Taejon, Korea
and
Poong Hyun Seong
Department of Nuclear Engineering
Korea Advanced Institute of Science and Technology

``

Abstract

Current emergency core cooling system in nuclear power plants typically have considerable numbers of complex functions and large cumbersome operator interfaces. Functions for initiation, switch-over between various phase of operation, interlocks, monitoring, and alarming are usually performed by relay and analog comparator logic which is difficult to maintain.

The Dynamic Safety System (DSS) is a computer based reactor protection system that has fail-safe nature and perform dynamic self-testing. In this paper, the implementation of the DSS in PLC is presented for CANDU reactor. ECC (Emergency Core Cooling) System of the CANDU Reactor is selected as the reference system.

1. Introduction

The reactor protection system is currently used in nuclear power plant for safety and efficiency. The reactor protection system receives the signals from the reactor and other components, and generates a trip signal with the coincidence logic. Then, the reactor protection system sends the trip signal for the reactor trip. The Dynamic Safety System (DSS) is a computer based reactor protection system that allows much more complex trip algorithm. It has fail-safe nature, and can perform dynamic self testing. The DSS is developed in AEA Technology of the UK and apply Protype Fast Reactor (PFR) at first. And then the DSS is applied to Advanced Gas-cooled Reactor (AGR) named Dungness B (1992) with great success.

The CANDU ECC System is selected as reference the reactor protection system using DSS technology is implemented in Programmable Logic Controller (PLC).

The Emergency Core Cooling System (ECCS) is one of four special safety systems designed to limit the release of radioactivity to the public for postulated accidents in CANDU Reactor. The ECC system is actuated following a Loss of Coolant Accident (LOCA) to inject coolant into the Primary Heat Transport (PHT) system to remove residual and decay heat from the core.

The ECC system is operated in of three stages: high pressure (HP), medium pressure (MP), and low pressure (LP).

2. Dynamic Safety System

In nuclear power plants, safety is a matter of great significance and most components used in nuclear power plant must be highly reliable. As shown in Figure 1, the typical DSS consists of several components such as, Trip Algorithm Computer (TAC), Voting Algorithm Computer (VAC), Pattern Recognition Logic (PRL), and Final Voting Logic (FVL). The test inputs are chosen to just exceed safe limits and therefore to cause transient excursions of the TAC (Trip Algorithms Computer) software into the tripped state.

The VAC receives signals from the TACs and performs voting logic. The PRL compares output pattern from VAC with expected output pattern, and if these two patterns are mismatched, the PRL generates trip signal. The FVL votes PRL output finally.

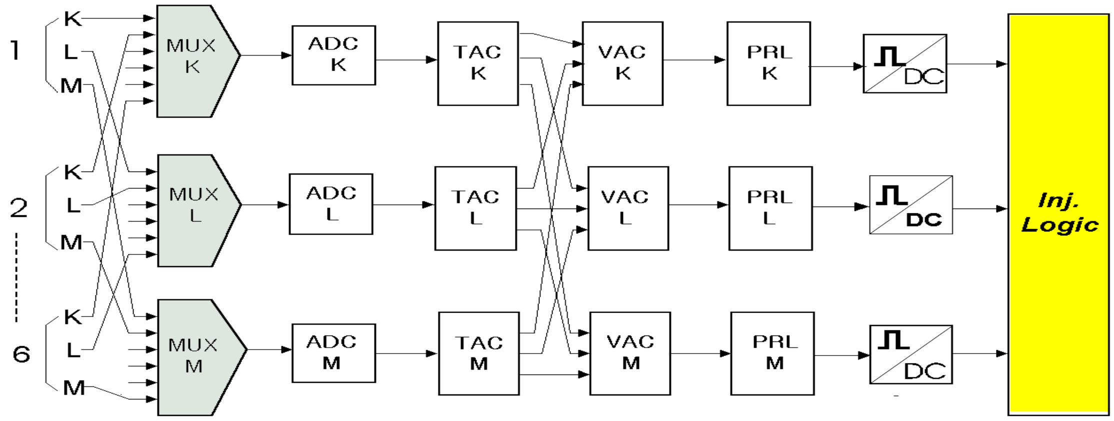

Figure 1 Schematic diagram of modified DSS for CANDU ECCS

2.1 Test Signal Generator

As shown in Fig. 2, Fig. 3 & Fig. 4, test parameter is chosen by one shifting, and then the test signal is interleaved among real plant signals as input to the DSS.

The plant signals and test signals are sampled sequentially by the data acquisition system and transmitted to the Trip Algorithm Computer (TAC). The response of the trip algorithms to the test and plant signal inputs yields a sequential pattern of status bits, one for each input, in which a 1 represents the non-tripped "healthy" state, and a 0 the tripped state. Under normal "healthy" conditions, the trip algorithms will yield a 1 state from the plant signals and a 0 status from the test signals.

P1	P2	P3	L4	P5	P6
0	1	0	1	1	1
1	0	1	0	1	1
0	1	1	1	0	1
1	0	1	1	1	0

<NOTE> 0: test signal, 1: plant signal

Figure 4 Test Set

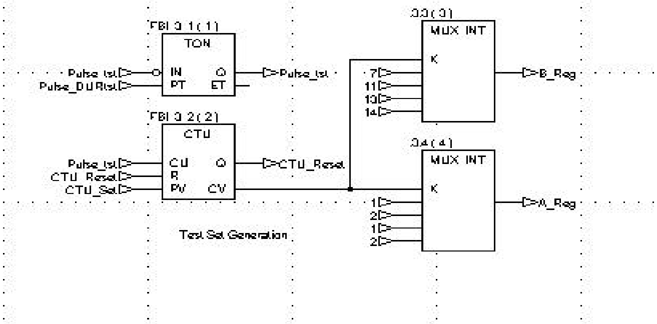

Figure 3 Test Signal Generator

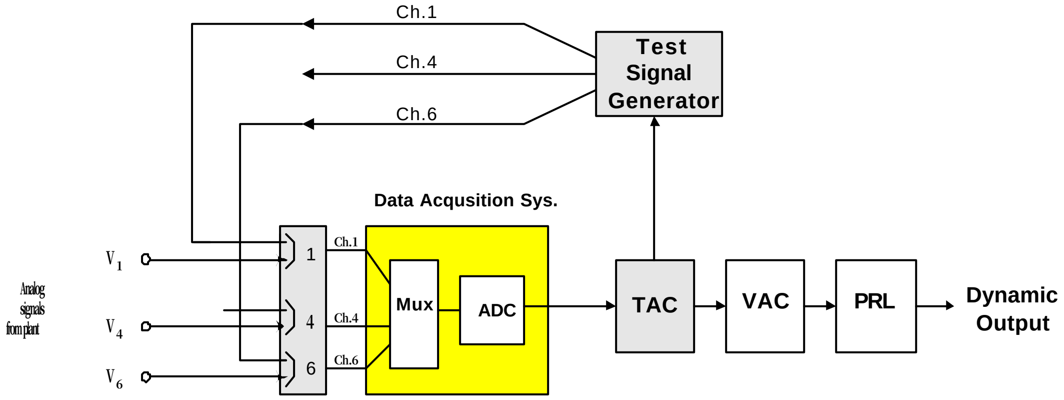

Figure 4   Schematic of Test Signal Generator

2.2 Data Acquisition System

Plant signals are inputs to the multiplexer with interleaved test signals. The multiplexer performs input sampling, and sends sampled input to TAC accordingly to the command of TAC.

The addresses of the test inputs are chosen to exercise every digit of the multiplexer address code on every scan of the multiplexer inputs.

2.3 TAC (Test Algorithm Computer)

The trip algorithm is implemented in TAC. The TAC performs two tasks. The first task is the determination of reactor trip using trip algorithms, and the second task is the control of MUX and the test signal generator. To maintain segregation of signal flow channels up to the stage where they are combined by voting, each channel of a group monitoring any plant parameter must be sampled by a separate multiplexer and processed by a separate TAC. This ensures that a failure of a single multiplexer or TAC affects only one measurement of any one parameter and does not constitute a common mode failure. The function of the test signal generator is the generation of trip test signal for each trip parameter according to trip algorithms and setpoints.

2.4 VAC (Voting Algorithm Computer)

The VAC performs voting of the status (trip or normal) input yielded by TACs and this function is equivalent to the ECCS Injection logic of currently used reactor protection system. The VAC generates output pattern also. This pattern is built by voting each group of channel output for all parameters. The voting logic of the CANDU ECC System is two-out-of-three.

2.5 PRL (Pattern Recognition Logic)

PRL compares the output pattern from VAC with expected output pattern, and shifts the expected pattern after comparison. If these two patterns are mismatched, the PRL generates trip signal as shown in Fig. 5. Then the reactor trip breaker is de-energized and reactor trip occurs. A pattern mismatch occurs in two cases as follows : The first is the case of any one of the plant signals beyond the prescribed limits. The second is the case of system faults, such as hardware fault, software fault, and wiring error.

Therefore, it is also possible to ensure the correctness of the DSS during normal operation and the DSS becomes fail-safe. For redundancy, separated VACs and PRLs are used and the FVL votes the PRL outputs finally.

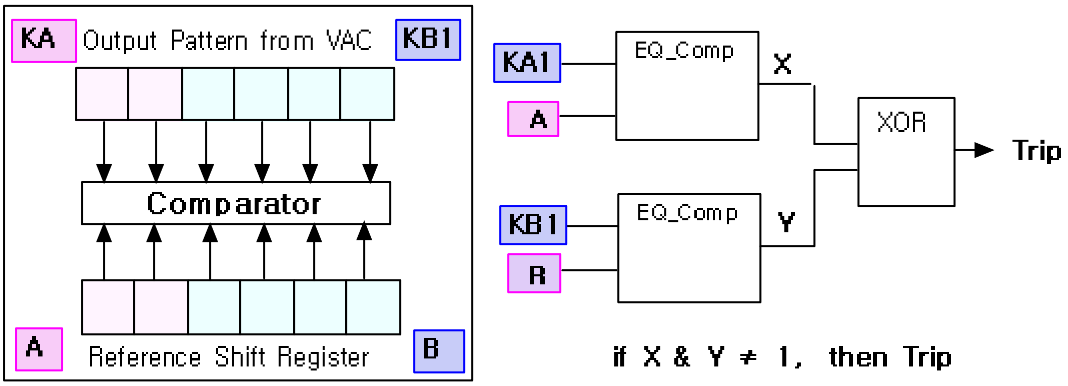

Figure 5 Pattern Recognition Logic

3. Implementation of conventional ECC System logic to Trip Computer

The Trip Computer (TC) houses all of the logic for detecting ECC trip conditions. It monitors sensor data coming in on the serial links and issues device controls for it's own actions and for display. Upon detecting a trip condition, this computer will communicate back to the display. As the Trip Computer is the only computer, which receives the sensor information, this information must be relayed to display at regular intervals.

The Trip Computer will require a database to store all signals needed for operation of all phases of ECC. (More details described in Ref. [2])

3.1 Injection Logic

The Trip Computer (TC) replaces the original current alarm units, analog comparators and relay logic for each process trip parameter they monitor/control. (Refer to Fig. 6)

The TC software is written such that the operation is continuous, i.e., if a trip condition is detected, the software opens the relevant trip Digital Output (D/O) and then continues on to the next task in the TC program.

3.1.1 Trip Computer Trip Variables

Trip computer is used to execute the trip logic. The assignment of trip parameters is as follows ;

1) PHT Low Pressure 2) HP Water Tank Low Level 3) ECC Pumps Differential Low Pressure 4) Dousing Tank Low Level 5) Reactor Building High Pressure trip parameters.

Two out of three channels of low header pressure signal are **AND-ed** with two out of three channels of high reactor building pressure, sustained low header pressure or high moderator level and the result presents a LOCA signal for automatic Steam Generator (S/G) crash cooldown, ECC injection and associated functions. The three main functions of the ECC System are opening injection valves, PHT loop isolation and S/G crash cooldown. Among the three main functions of ECCS, only ECC Injection is described by this paper. If the parameter trip is not blocked out, then the D/O related injection valves is opened by the TC. Odd/Even circuit blocking is to be controlled by Handswitch HS-502K/M. The ECC System shall not be operated in the "BLOCKED" state when the PHT temperature is greater than 100 ℃.

All manual device controls override automatic device control by the trip computer before, at the instant of and after a LOCA using Manual Initiation Handswitch HS-501K/M as shown in Figure 6.

3.1.1.1 PHT Pressure Low

The PHT Low Pressure trip requirements are ;

a. Read the 2 PHT Pressure (64332-P1K, -P1L, -P1M / 63432-P2K, -P2L, -P2M) signals.

b. If any PHT Pressure signals is irrational, annunciated via the TC abnormal signals window alarm and PHT Pressure signal abnormal message on the display.

c. If the PHT Pressure signal is below the trip setpoint (5.42 MPa), open the appropriate trip message and window alarm on the display.

3.1.1.2 Reactor (Rx) Building Pressure High

Rx. Building High Pressure trip requirements are ;

a. Read the Reactor Building Pressure (63432-P3K, -P3L, -P3M) signal.

b. If Reactor Building Pressure signal is irrational, annunciated via the TC abnormal signals window alarm and Rx. Building Pressure signal abnormal message on the display.

c. If Reactor Building Pressure signal exceeds 3.45 kPa(d), open the appropriate trip message and window alarm on the display.

3.1.1.3 Moderator Level High

Moderator Level High trip requirements are ;

a. Read the Moderator Level (63432-L4lK, -L4L, -L4M) signal.

b. If Moderator Level signal exceeds 10.12 m, open the appropriate trip message and window alarm on the display.

3.1.1.4 Sustained Header Pressure Low

The Sustained Header Pressure trip requirements are ;

a. Read the 2 PHT Pressure (64332-P5K, -P5L, -P5M / 63432-P6K, -P6L, -P6M) signals.

b. If the PHT Pressure signal is below the trip setpoint (5.42 MPa), open the appropriate trip message and window alarm on the display.

3.1.1.5 Coincidence Logic

The coincidence logic requirements are ;

a. Two out of three channels of 'Low Header Pressure' signal are AND-ed with two out of three channels of 'High Reactor Building Pressure' or 'Sustained Low Header Pressure' or 'High Moderator Level' Trip

b. If the above parameter trip is conditioned in, open (NC→open)/ close (NO→close) D/O activate HP injection [Refer to Table 4 in Ref. [2]).

3.1.1.6 High Pressure (H.P) Water Tank Level

The H.P Water Tank (TK1, TK3) Low Level trip requirements are ;

a. Read the HP Water Tank level (63432-L23K, -L23L, -L23M) signals.

b. If the signal is irrational, then annunciate it via the TC abnormal signals window alarm and the HP Water Tank level signal abnormal message on the display.

c. If the HP Water Tank level signal is below switch-over setpoint, open the trip appropriate message and the D/Os related to ECC MP injection valves and close D/Os related to HP Injection valves, then open window alarm on the display.

3.1.1.7 Dousing Tank Level

The Dousing Tank Low Level trip requirements are ;

a. Read the Dousing Tank level (63432-L8K, -L8L, -L8M) signal.

b. If the signal is irrational, then annunciate it via the TC abnormal signals window alarm on the display and the Dousing Tank level signal abnormal message on the display.

c. If the Dousing Tank level signal is below switch-over setpoint, close the D/Os (MP Dousing Tank isolation valves & MP H_2O Test valves), and open the appropriate trip message and the D/Os (Recovery Sump Isolation valves & ECC Heat Exchanger RCW return isolation valves), then open window alarm on the display.

3.2 Switch-over on ECCS Operation

3.2.1 Switch-over from High Pressure to Medium Pressure ECCS Operation

If the H.P water tank level signal is low (1.97 m/ 1.35 m), switch to medium pressure ECC operation.

3.2.2 Switch-over from Medium Pressure to Low Pressure ECCS Operation

If the Dousing tank level signal is low (0.45 m), switch to low pressure ECC operation.

4. Implementation in PLC

In PLC the function of the DSS is implemented with the CONCEPT. The CONCEPT developed by GROUPE SCHNEIDER. is a graphic user interface programming tool for the Quantum PLC.

As shown in Figure 7, a MMI display for ECCS based on DSS is implemented with LOOKOUT developed by National Instruments Inc. The LOOKOUT is a object driven programming tool.

The trip logic of the DSSs tested in the UK is two-out-of-four, however the trip logic of the CANDU ECC System is two-out-of-three.

5. Conclusion

The application of the DSS to CANDU ECCS has many advantages. The inherent self-testing feature and fail-safe design provide a high level of reliability and low spurious trip rate. The convenience in software modification makes it possible to use more complex trip algorithms.

To meaningfully show how the DSS can enhance a current reactor protection system, the verification is needed. we will verify the correct operation of the DSS based ECC logic implemented in PLC using Computerized ECCS prototype.

It is expected that the use of DSS technology will offer a lot of merits in the upgrade of PWR reactor protection system as well as digital computer based CANDU emergency core cooling system.

Nomenclature

CANDU	: CANada Deuterium Uranium
D/I	: Digital Input
D/O	: Digital Output
ECCS	: Emergency Core Cooling System
HP	: High Pressure, MP : Medium Pressure, LP : Low Pressure
Mux	: Multiplexer
PHT	: Primary Heat Transfer
TC	: Trip Computer

Reference

[1] Fully Computerized ECCC Prototype Design Requirement, 69-63432-DR-001

[2] S. N. Kim, PFS for Trip Computer on ECCS

[3] Ung Soo Kim, "A Study on Implementation of Dynamic Safety System in Programmable Logic Controller for Pressurized Water Reactor"

[4] A.B. Keats, "Fail-safe Design Criteria For Computer Based Reactor Protection Systems," Nuclear Energy, Vol. 1, No. 6, pp. 423-429, December 1980.

[5] G. Adams, D. Miller, B. Hajek, A. Kauffman, G. Toth, J. Fluhrer, "Emulation of a Dynamic Safety System Reactor Protection System for a US Light Water Reactor," ANS International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human Factor Interface Technologies (NPIC&HMIT'96), May 6-9,1996, State College, PA.

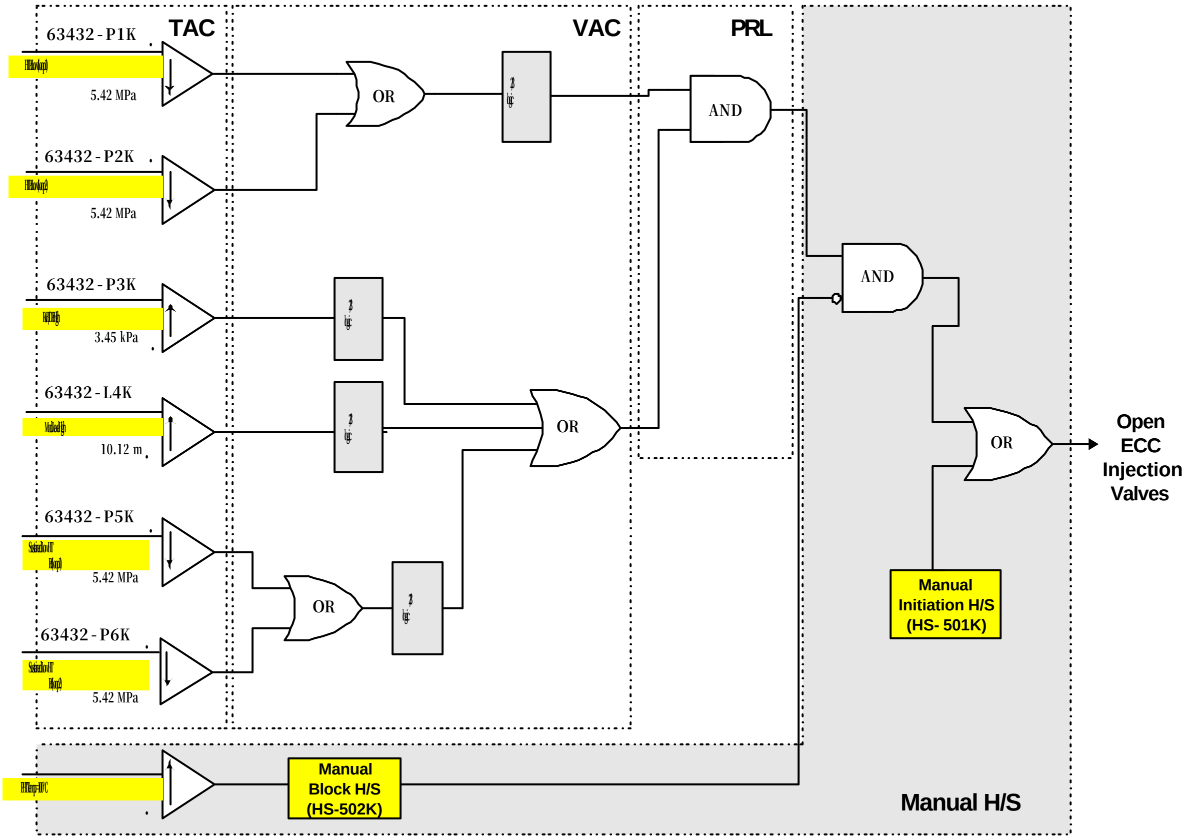

Figure 6 Overall injection logic (typical for K Ch.)

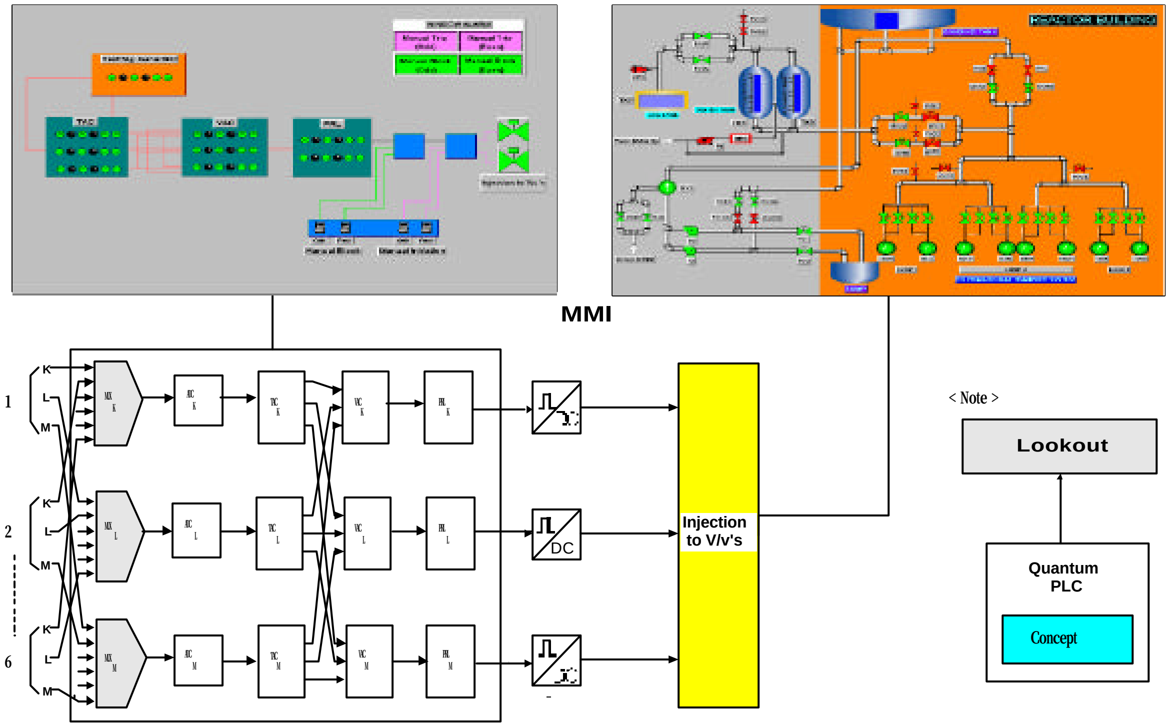

Figure 7 MMI display for DSS based ECC System