Journal of the Korean Nuclear Society
Volume 32, Number 4, pp.316~327, August 2000

A Study on Design of the Trip Computer for ECC System Based on Dynamic Safety System

Seog Nam Kim and Poong Hyun Seong
Korea Advanced Institute of Science and Technology
373-1, Kusong-dong, Yusong-gu, Taejon, 305-701, Korea
snkim21@hotmail.com

(Received October 29, 1999)

Abstract

The Emergency Core Cooling System in current nuclear power plants typically has a considerable number of complex functions and largely cumbersome operator interfaces.
Functions for initiation, switch-over between various phases of operation, interlocks, monitoring, and alarming are usually performed by relays and analog comparator logic which are difficult to maintain and test.
To improve problems of an analog based ECC (Emergency Core Cooling) System, the trip computer for ECCS based on Dynamic Safety System (DSS) is implemented.
The DSS is a computer based reactor protection system that has fail-safe nature and performs a dynamic self-testing. The most important feature of the DSS is the introduction of test signal that send the system into a tripped state. The test signals are interleaved with the plant signals to produce an output which switches between a tripped and health state. The dynamic operation is a key feature of the failsafe design of the system.
In this work, a possible implementation of the DSS using PLC is presented for a CANDU Reactor. ECC System of the CANDU Reactor is selected as the reference system.

Key Words : emergency core cooling (ECC), dynamic safety system (DSS), CANDU (CANada Deuterium Uranium)

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 Emergency Core Cooling system is one of four special safety systems in CANDU Reactor designed to limit the release of radioactivity to the public for postulated accidents. 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.

Current emergency core cooling system in

CANDU power plants typically has a considerable number of complex functions and largely cumbersome operator interfaces.

Functions for initiation, switch-over between various phases of operation, interlocks, monitoring, and alarming are usually performed by relay and analog comparator logic which is difficult to maintain and test.

The ECC System is an analog based system, therefore it has also some relative demerits, compared with a digital system, such as inflexibility, complexity, and instrumentation drift. The signal and setpoint drift is the most important problem in current reactor protection system. Also the periodic test of the reactor protection systems is required for maintenance, but this test is almost carried out only by human operators these days. Therefore a large amount of time and human effort is needed. In addition the risk of a spurious reactor trip always exists during the test.

In order to overcome these problem, the dynamic safety system (DSS) has been developed in this work.

2. Description of the Emergency Core Cooling System [1, 2]

The Emergency Core Cooling system is one of four special safety systems designed to limit the release of radioactivity to the public for postulated accidents. 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.

Supporting functions of steam generator crash cooldown (to cool down the secondary side of the coolant system) by opening the Main Steam Safety Valves (MSSVs) and isolation of the PHT loops interconnection valves (to prevent a blowdown of the intact loop) are also initiated by ECC.

The current ECC system consists of three stages: high pressure (HP), medium pressure (MP), and low pressure (LP) injection phases.

Following a heat transport system loss of coolant accident (LOCA), the emergency core cooling (ECC) system injection is triggered to allow emergency coolant injection into the primary heat transport (PHT) system to remove reactor core residual and decay heat.

Supportive functions of steam generator crash cooldown and closure of PHT interconnection valves are also initiated separately.

Detection of an LOCA and various stages of ECC operation are described below.

2.1. LOCA Detection

Automatic closure of the PHT interconnection valves is initiated if two out of three channels of "header pressure" measurements register at least one pressure within each channel as low.

A similar low header pressure signal AND-ed with two out of three channels of "high reactor building pressure" or "sustained low header pressure", or "high moderator level" presents a conditioned LOCA signal for automatic steam generator crash cooldown, ECC and associated functions. Low header pressure is conditioned by the above signals to minimize the possibilities of spuriously initiating light water injection and boiler crash cooldown. High building pressure provides conditioning for breaks into a functioning containment. Sustained low header pressure measurements provide conditioning for small breaks and moderator high level provides conditioning for pressure tube/calandria tube rupture into the calandria.

2.2. High Pressure Injection and Associated Functions

On a LOCA signal, the HP gas isolating valves

open and vent valves close respectively to pressurize the high pressure water accumulator tanks. The H_2O isolating valves and D_2O isolating valves also open. When the header pressure drops to approximately 4.14 MPa(g) HP injection commences. On low level in the HP accumulator tanks, HP injection is automatically terminated by closing the HP H_2O isolating and test valves.

2.3. Medium Pressure Injection

On a LOCA the ECC pumps dousing tank isolating valves are automatically opened. On low HP water accumulator tank level, the MP H_2O isolating valves are automatically opened and the HP isolating and test valves are automatically closed.

2.4. Low Pressure Injection

During HP and MP ECC operation, the injected water is discharged to the reactor basement floor. On Low dousing tank water level, the recovery sump isolation valves and ECC heat exchanger RCW return isolation valves are automatically opened. The dousing tank isolation and test valves are automatically closed.

2.5. Manual Initiation

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.

2.6. Manual Block

The ECC System shall not be operated in the "BLOCKED" state when the PHT temperature is greater than 100℃.

ECC System is disabled when the PHT temperature is less than 100℃ using Manual Block Handswitch HS-502K/M.

3. Implementation of conventional ECC System logic to Trip Computer [6]

The Trip Computer (TC) houses all of the logic for detecting ECC trip conditions. It monitors

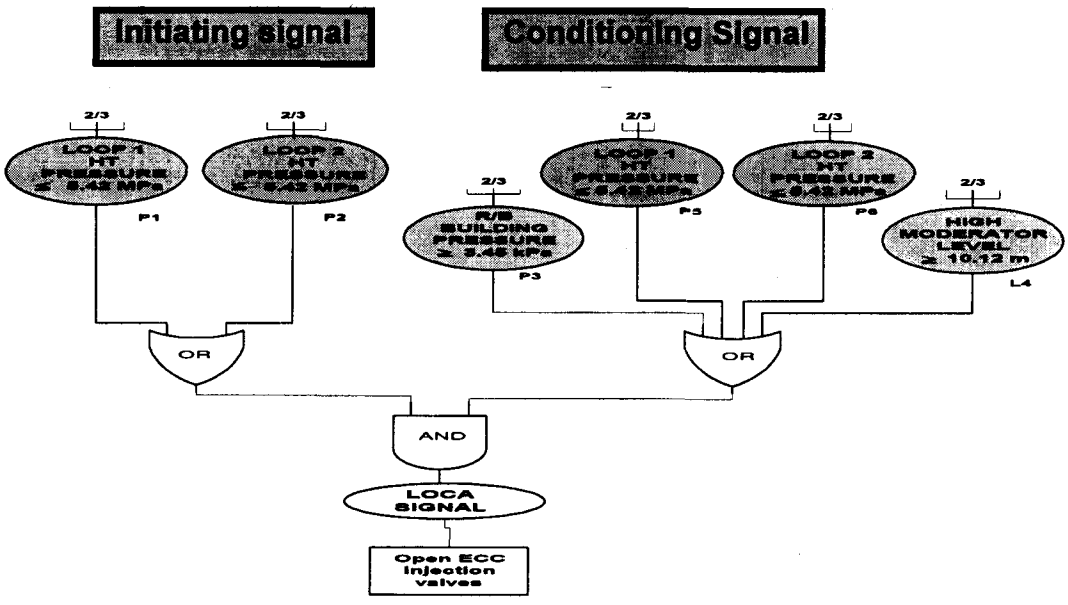


Fig. 1. Schematic of Logic to initiate ECC Injection Valves

sensor data coming in on the serial links and issues device controls for its 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 (TC) replaces the original current alarm units, analog comparators and relay logic for each process trip parameter they monitor/control as shown in Figure 1.

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. 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 Low differential 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 in 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

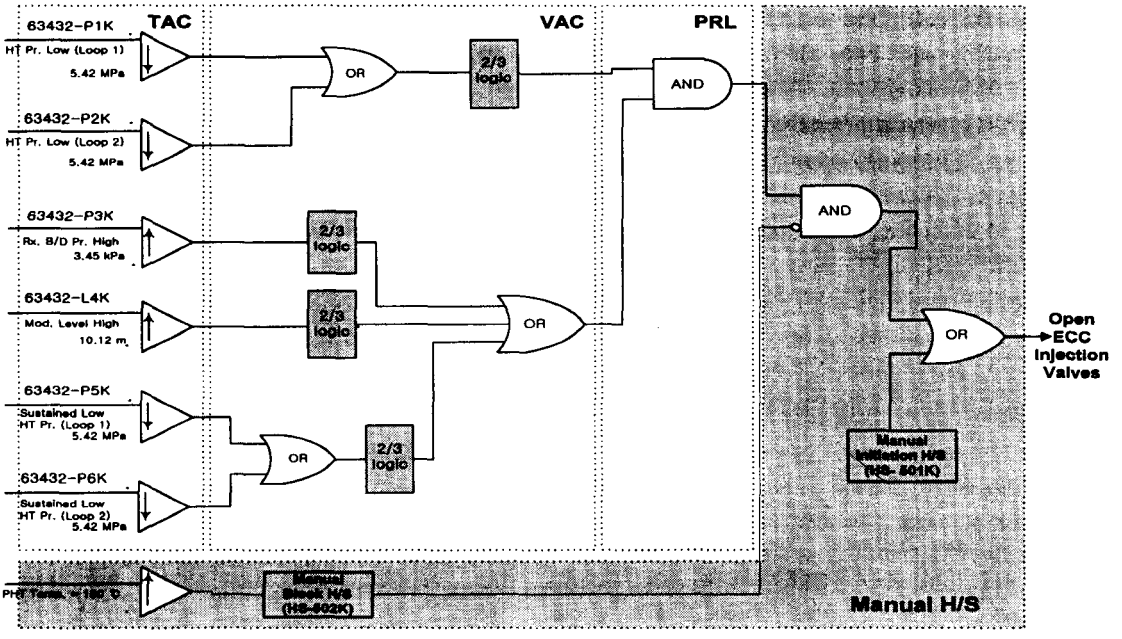


Fig. 2. Overall Injection Logic with Manual Hand Switches (Typical for Ch. "K")

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 2.

3.1.1. 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.

3.1.2. 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 HP Injection valves, then open window alarm on the display.

3.1.3. 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 (0.45m), switch to low pressure ECC operation.

4. Dynamic Safety System [3,4,5,8]

The basic arrangement of the typical DSS is shown in Figure 3. The main components are multiplexer, Trip Algorithm Computer (TAC), Voting Algorithm Computer (VAC), Pattern Recognition Logic (PRL), and Final Voting Logic (FVL). 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 trip algorithm is implemented in TAC. The test inputs are chosen to just exceed safe limits and therefore to cause

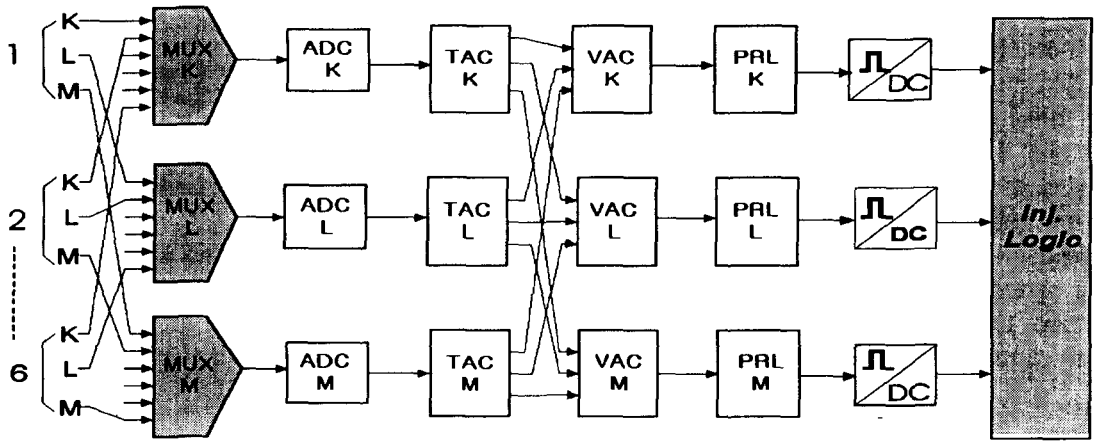


Fig. 3. Schematic Diagram of Modified DSS for CANDU ECCS

transient excursions of the TAC (Trip Algorithms Computer) software into the tripped state. 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.

As shown in Figure 4, the test parameter is chosen by one shifting, and then the test signal is interleaved among real plant signals as input to the DSS. The VAC performs voting of the status (trip or normal) input yielded by TACs and this function is equivalent to the SSPS logic of currently used reactor protection system. The VAC receives signals from the TACs and performs voting logic.

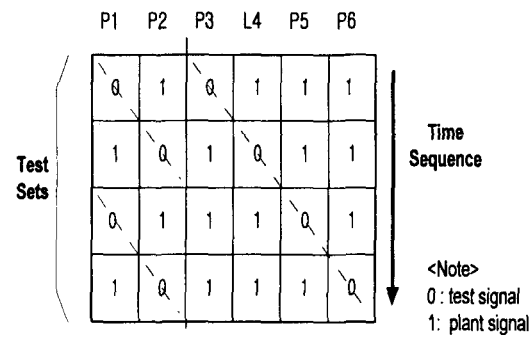


Fig. 4. Test Signal Set

The VAC generates output pattern also. This pattern is built by voting each group of channel output for all parameters. The PRL compares 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 Figure 7. Then the reactor trip breaker is de-energized and reactor trip occurs. A pattern mismatch occurs in two cases as follows: The first case is about deviation of any one of the plant signals beyond the prescribe limits. The second case is about system faults, such as hardware fault,

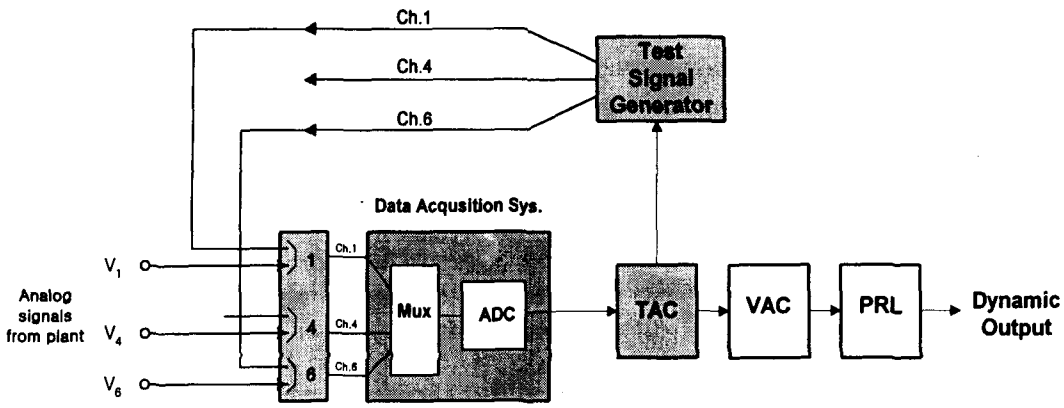


Fig. 5. Schematic of Test Signal Generator

software fault, and wiring error. Therefore ensuring the correctness of the DSS, during normal operation, is also possible and the DSS becomes fail-safe. For redundancy, separated VACs and PRLs are used and the FVL votes the PRL outputs finally. This operation of the DSS is described in Figure 6.

4.1. Test Signal Generator

As shown in Figure 4 & Figure 5, 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.

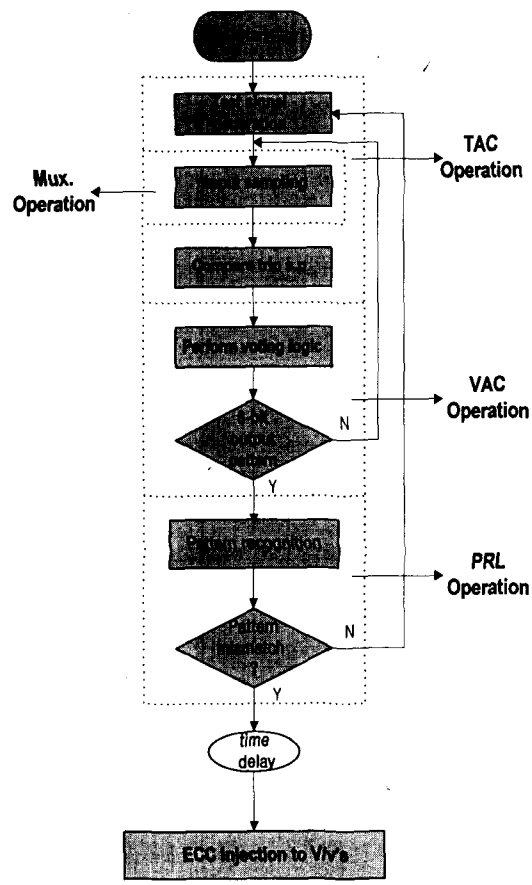
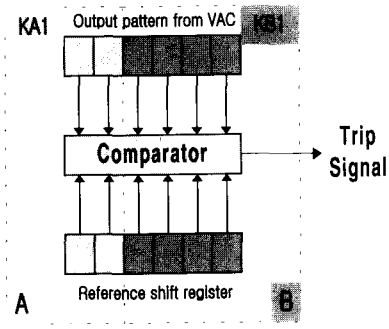


Fig. 6. Flow Chart of DSS Operation

4.2. 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.



4.3. 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.

4.4. 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.

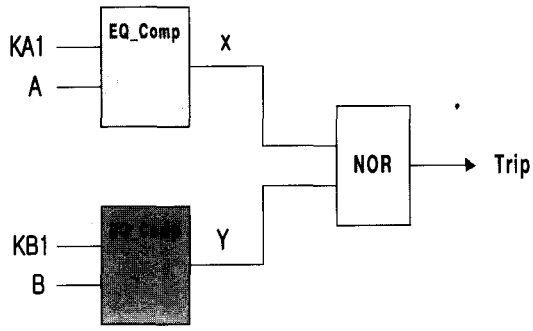


Fig. 7. Pattern Recognition Logic

4.5. 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 Figure 7. 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,

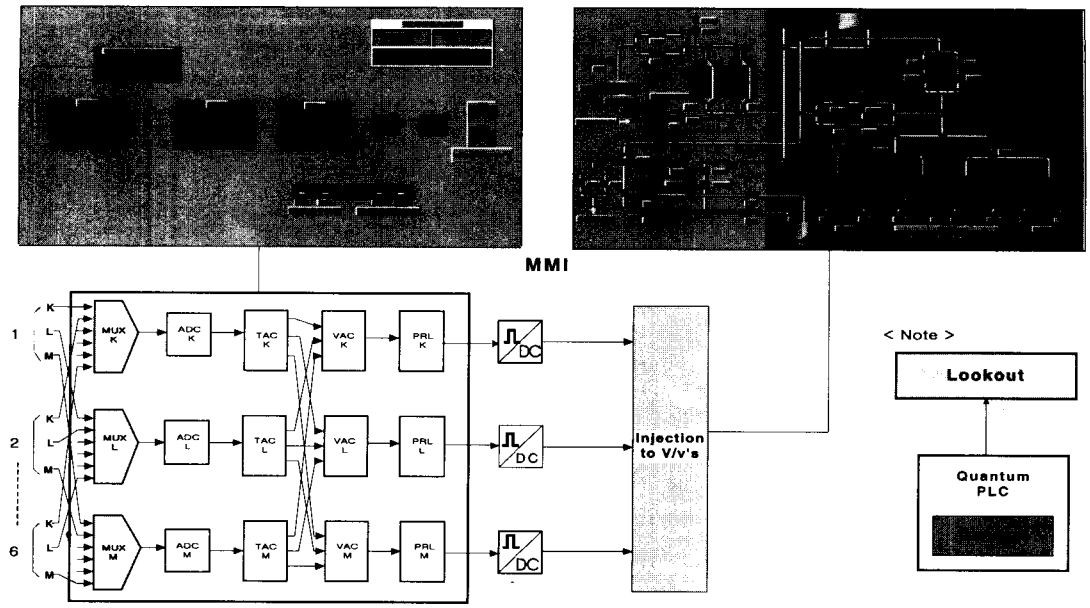


Fig. 8. MMI Display for DSS Based ECC System

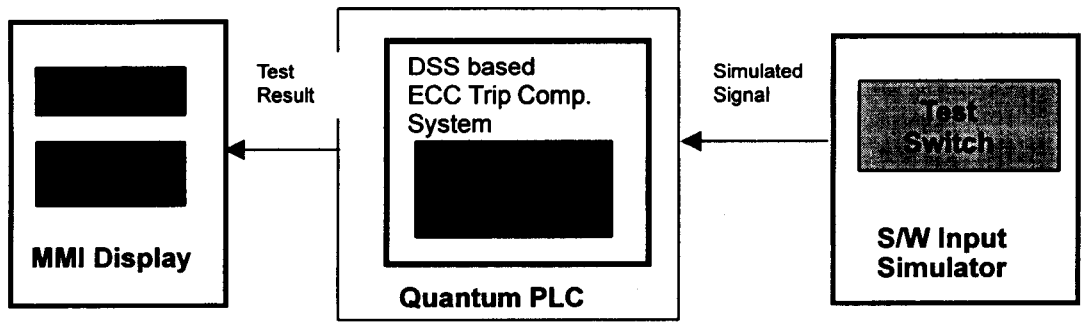


Fig. 9. Typical Validation Test Setup

separated VACs and PRLs are used and the FVL votes the PRL outputs finally.

4.6. Implementation of ECC System Logic with Dynamic Safety Features

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

As shown in Figure 8, a MMI display for ECCS based on DSS is implemented with LOOKOUT developed by National Instruments Inc. The LOOKOUT is an object driven programming tool. The trip logic of the DSSs tested in the UK is two-out-of-four logic, however the trip logic of the CANDU ECC System is two-out-of-three logic.

Table 1. Validation Checklist for Valves Open/Close Status for Each Mode to ECCS Operation by LOCA Signals

Valve	Normal State	Operating Modes			Remarks
		HP	MP	LP	
3432-PV81	NC	OPEN	OPEN	OPEN	HP Gas Inj. V/v's
3432-PV82	NC	OPEN	OPEN	OPEN	
3432-PV83	NO	CLOSE	CLOSE	CLOSE	HP Gas Vent V/v's
3432-PV84	NO	CLOSE	CLOSE	CLOSE	
3432-MV79	NC	OPEN	CLOSE	CLOSE	HP H_2O Inj. V/v's
3432-MV80	NC	OPEN	CLOSE	CLOSE	
3432-MV71	NO	OPEN	CLOSE	CLOSE	HP H_2O Test V/v's
3432-MV72	NO	OPEN	CLOSE	CLOSE	(Closed during testing & on low HP water tank level)
3432-MV39,40,4142 43,44,45,46,5960,61 62,63,64,65,66	NC	OPEN	OPEN	OPEN	D_2O Isolation V/v's
3432-PV87	NO	CLOSE	CLOSE	CLOSE	HP Vent V/v's
3432-PV88	NO	CLOSE	CLOSE	CLOSE	
3432-PV78	NO	CLOSE	CLOSE	CLOSE	Disc H_2O Vent V/v's
3432-PV73	NO	CLOSE	CLOSE	CLOSE	RD1 D_2O Vent V/v's
3432-PV74	NO	CLOSE	CLOSE	CLOSE	RD2 D_2O Vent V/v's
3432-CP1	Cycled ON/OFF	STOP	STOP	STOP	Compressor
3432-P3	Non	STOP	STOP	STOP	Recir. Pump
3432-HR3	Cycled ON/OFF	OFF	OFF	OFF	Heater
3432-P1	NAUTO	On a LOCA, one pump should be started. If the AUTO Pump fails or does not start following a LOCA, after a 10 s delay the STBY pump starts automatically			ECC Pump (e.g, If one is AUTO mode, the other is STBY mode.)
3432-P2	or NSTBY				
3432-PV10	NC	OPEN	OPEN	CLOSE	MP Dousing TK Isol. V/v's
3432-PV11	NC	OPEN	OPEN	CLOSE	
3432-MV31	NC	CLOSE	OPEN	OPEN	MP H_2O Isol. V/v's
3432-MV50	NC	CLOSE	OPEN	OPEN	
3432-PV8	NO	OPEN	OPEN	OPEN	MP H_2O Test V/v's
3432-PV9	NO	OPEN	OPEN	OPEN	(Closed during Testing of ECC Vaves
3432-PV1	NC	CLOSE	CLOSE	OPEN	Recovery Sump Isol.
3432-PV2	NC	CLOSE	CLOSE	OPEN	V/v's
3432-PV162	NO	OPEN	OPEN	CLOSE	MP Dousing TK Test
3432-PV163	NO	OPEN	OPEN	CLOSE	V/v's
3432-PV23	NO	OPEN	OPEN	OPEN	Pumps Recir. V/v's
3432-PV24	NO	OPEN	OPEN	OPEN	
7134-PV569	NC	CLOSE	CLOSE	OPEN	ECC Hx RCW Iso. V/v
7134-PV570					

5. Trip Software Validation and Test [7]

The purpose of the validation test is to exercise all inputs in as few combinations as practical, and observe the corresponding outputs to verify that the Trip Computer (TC) program performs correctly. The formal validation tests are black box tests designed to ensure that the trip computer meets the functional requirements for the design. In essence, while the preceding white box tests were looking for errors in software coding and execution of the design, the validation tests go back to basics and look for errors in conceptual understanding of the design.

TC Software modules for ECCS shall be tested in accordance with the Validation Test Procedure as per Reference [7].

All inputs are set as per Table in Reference [7] and ensure that the outputs are normal.

The test has been performed by S/W Input Simulator as shown on Figure 9. The result of the test was checked and displayed on the MMI display as shown in Figure 8.

The functional requirements for the TCs used in ECCS are specified in the followings.

1) Test for each trip parameters : 2/3 local coincidence logic
2) Injection to open/close valves test by LOCA Signals

Each ECCS Operating mode (HP→MP→LP) was tested by the following steps.

- When 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 is conditioned-in, open (NC→open)/ close (NO→close) D/O activate HP injection as per Table in Reference [7].
- If the HP Water Tank level signal is below switch-over setpoint, open the trip appropriate message and the D/Os related ECC MP injection valves and close D/Os related HP Injection valves, then open window alarm on the display as per Table in Reference [7].
- the Dousing Tank level signal is below switch-over setpoint, close the D/Os (MP Dousing Tank isolation valves & MP H2O 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 as per Table in Reference [7].

3) ECC Pumps Low differential pressure trip test : On a LOCA, one pump should be started.

If the AUTO Pump fails or does not start following a LOCA, the STBY pump starts by Manual Test Switch as per Table in Reference [7].

5.1. Results of Test

Using S/W input simulator as shown in Figure 9, the software validation and test are done. The test results shows that the modified DSS for digital based ECC System provides correct trip/ injection output for all test cases for trip parameters. Test results show that the modified DSS operates correctly in all conditions as per Tables in Reference [7]. Above all, In the LOCA based test, the result shows that activated components operate correctly as per operating modes in Table 1, there is no spurious trip in normal conditions.

6. Summary and Conclusions

In this study, we suggest the application of the DSS algorithm to current CANDU ECC System and implement the modified Dynamic Safety Features in a PLC. Applying the Dynamic Safety Features to a reactor protection system has a great number of advantages. However, the DSS needs modification to be applied to CANDU Reactor

because there are many differences between CANDU and UK AGR systems.

In addition, the modified DSS has the flexibility for handling several types of voting logics. The modified DSS algorithm is implemented in a PLC and the tests of the modified DSS are carried out using S/W Input Simulator as per Validation Test Procedure. Test results show that the modified DSS operates correctly in all conditions as per Tables in Reference [7].

This study confirms that the upgrade of current PWR & CANDU reactor protection system using DSS technology offers a number of merits. It is confirmed that this technology is very useful and can be applied to advanced Nuclear Power Plants through further enhancement.

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.

It is expected that the use of DSS technology will offer a number of merits in the upgrade of PWR and CANDU reactor protection system including current analog based ECC System.

References

1. Design Manual of the Emergency Core Cooling System, 86-63432-DM-000
2. Fully Computerized ECCS Prototype Design Requirement, 69-63432-DR-001 December, (1995).
3. Ung Soo Kim and Poong Hyun Seong, "An Application of Dynamic Safety System to Pressurized Water Reactor", Annals of Nuclear Energy, Vol. 25, No. 15, p.1221-1233, (1998).
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, Penn. State University, PA.
6. S. N. Kim, Program Functional Specification for Trip Computer on ECCS, RD-63432-PFS-000, July (1999).
7. S. N. Kim, Validation Test Procedure for Trip Computer on ECCS, RD-63432-VTP-000, November (1999).
8. AEA Technology, "ISAT promises fail-safe computer based reactor protection Systems", Nuclear Engineering International, pp. 53-55, December (1989).