XA9949627

Development of Digital Plant Protection System for Korean Next Generation Reactor

Suk-Joon Park
Managing Director
NSSS Engineering and Development Division
Korea Power Engineering Company
Taejon, Korea

Abstract

A Digital Plant Protection System (DPPS) for Korean Next Generation Reactor (KNGR) is being developed using the Programmable Logic Controller (PLC) technology. For the design verification, the development of the DPPS prototype is progressing at this time. The prototype hardware equipment is installed and software coding is started. DPPS software is being coded by strict software V&V activities and function block language that uses simple graphical symbols. By adopting the PLC technology, the design of DPPS is possible to take full advantages in areas such as automatic testing, simplified calibration, improved isolation between redundant channels, reduced internal and external wiring and increased plant availability.

I. Introduction

In recent, the application of analog technology for designing instrumentation and control (I&C) systems in Nuclear Power Plants (NPPs) is becoming more difficult because of its increasing obsolescence. One of the nuclear power industry goals is the continual modernization and improvement of plant equipment and systems to increase reliability and maintain public safety. Recent developments in electrical control technology, specifically, programmable logic controller (PLC) show promise in improving plant availability and enhancing performance of I&C system. [1) 5)]

PLC, which is one of the alternative to resolve the obsolescence problem in conventional I&C System, has been applied to Korean Next Generation Reactor Digital Plant Protection System (KNGR DPPS). PLC has the potential for additional benefits such as ease of maintenance, increased performance, and improvements in availability. Table 1 shows the design differences between Yonggwang Nuclear Power Plant Units 5&6 PPS and KNGR Prototype DPPS.

For designing a safety system, both conventional design criteria and newly issued design criteria have to be considered. Basically, the functional design requirement of the digital plant protection system is almost same as that of the conventional system. And the applicable criteria are also same as the conventional design criteria except for the digitalization. For the digitalization, new criteria for programmable digital computers in safety systems of NPPs, and new codes and standards [7)] which provide methods acceptable for designing software, verifying software, implementing software and validation in safety related system, should be considered. The defense in depth and diversity against Common Mode Failures (CMFs) should be also considered in the DPPS design.

The major licensing issue, to be considered seriously for the application of DPPS in KNGR, are listed in the followings.

- Common Mode Failure Prevention
- Software V&V including Software Classification for the Digital Computer based Safety System
- Commercial Dedication for off-the-self Hardware and Software
- EMI/RFI Qualification

Table 1. Comparison of Analog Type vs. Digital Type PPS

Item \ Plant	Yonggwang Units 5&6	KNGR Prototype
Type	Analog type PPS	Digital type PPS
Major Component	Analog Card Mechanical Relay	Programmable Logic Controller
Function Implementation	Hardware Based	Software Based
Test Method	Manual Function Test	Manual Initiated Automatic Function Test
The Number of Channels	4 Channels	4 Channels
The Number of Protection Processors	1 Analog Card per Trip Parameter	Programmable Logic Controllers per Channel
Operator Interface	Lamps, Indicators, Mechanical Switches	Flat Panel Display with Touch Screen Capability
Software V & V	Not Applicable	IEEE 7-4.3.2, 1993 R.G 1.152, 1996
Cabinet Structure	1 Cabinet with 4 bays	4 Separate Cabinets

II. DPPS Design Features

1. System Description

The DPPS consists of Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS). The functions of RPS are to protect the nuclear fuel design limits and reactor coolant system pressure boundary by tripping the reactor when certain plant conditions approach safety system setpoints. Reactor trip is provided through an interface with the reactor trip switch gear system. The PPS also provides assistance in mitigating the consequences of accidents through actuation of separate Engineered Safety Features (ESF) System.

The DPPS is comprised of four redundant channels (A, B, C and D as depicted on Figure 1. KNGR DPPS Basic Block Diagram) that perform the necessary bistable, coincidence, initiation logic and associated maintenance/test function. Four redundant channels are provided to satisfy single failure criteria and improve plant availability. The system includes four redundant Remote Control Modules located on the Main Control Room panels.

A Bistable Logic receives a separate measurement of the process variable in each channel. There is a separate bistable function per process variable. The bistable function determines the trip state by comparing the measured process variable to predefined limits.

The trip outputs from the Bistable Logic are provided to the Local Coincidence Logic (LCL) and the three Cross Channel Communication (CCC) processors within the channel. The LCL provides RT and ESFAS logic for the individual channel. The three CCC processors provide a channel bistable trip status to the other redundant channels of the DPPS.

The LCL algorithm determines the state of the coincidence output based on the status of the four trip inputs and their respective trip channel bypass inputs. The LCL produces a trip signal if two or more of four inputs indicate a trip state. If a trip bypass is present, the LCL logic is converted from 2 out of 4 coincidence to 2 out of 3 coincidence. The trip channel bypasses are manually initiated in each channel from the Maintenance & Test Panel (MTP).

Each trip channel bypass initiated from the MTP is sent to the Integrated Test Processor (ITP) in the respective channel. Each ITP sends all its trip channel bypass status to the ITP in the other three redundant channels. The ITPs monitor initiated trip channel bypasses and perform verification as appropriate to determine which channel is bypassed for the same trip parameter. This algorithm is repeated in the LCL to ensure that an ITP failure can not cause an erroneous bypass condition and prevents the respective LCL being reduced to less than two out of three coincidence.

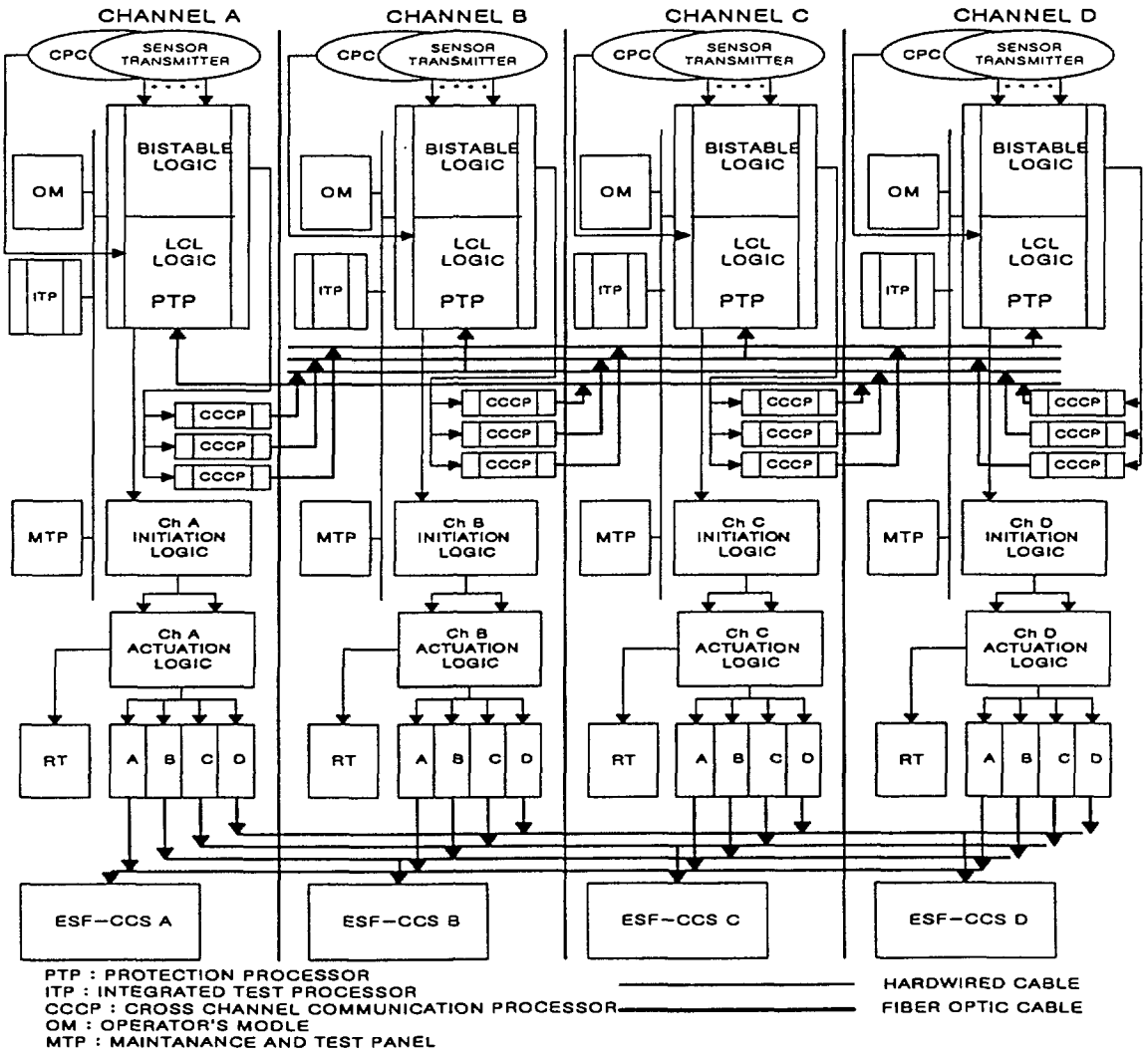

Fig 1. KNGR DPPS Basic Block Diagram

2. Functional Diversity Consideration

The "defense-in-depth" approach for functional diversity in the design of the overall KNGR DPPS is applied to address the potential for common mode failures. The trip parameters are typically assigned to different analog input cards, Core Protection Calculator System (CPCS) and Alternate Protection System (APS) based on functional diversity as shown in Table 2.

Table 2. Trip Parameter Assignments

Trip Parameters	DPPS (Protection Processor)		CPCS	APS
	AI Card 1	AI Card 2		
Excore Neutron Flux Linear Power	X		X	
Excore Neutron Flux Log Power		X		
Pressurizer Pressure (NR)	X		X	
Pressurizer Pressure (WR)		X		X
Steam Gen. 1 Level (WR)	X			X
Steam Gen. 1 Level (NR)	X			
Steam Gen. 2 Level (WR)		X		X
Steam Gen. 2 Level (NR)		X		
Steam Gen. 1 Pressure	X			
Steam Gen. 2 Pressure		X		
Hi Containment Pressure (NR)	X			X
Hi Hi Containment Pressure (WR)	X			
Steam Gen. 1 Delta P RCS Flow	X			
Steam Gen. 2 Delta P RCS Flow		X		
Refueling Water Tank Level		X		
CEA Positions			X	
RCS Temperatures			X	
RCP Speed			X	

A. Protection Processor Functional Diversity

Each DPPS channel includes redundancy and diversity for assignment of plant signals to Protection Processor. For example, diverse channelized analog input signals are assigned to independent analog input cards in a DPPS channel. Thus, single failure of an analog input card will only affect a limited number of analog input signals.

B. CPCS Functional Diversity

The CPCS calculates the following trip demand signals:

- Lo Departure From Nucleate Boiling Ratio (DNBR)
- Hi Local Power Density (LPD)

The DNBR and LPD calculations in the CPCS are performed by industrial VME bus computer (Xycom XVME-655). These computers are diverse from the Programmable Logic Controllers (PLCs) used for the Protection Processors. Functional diversity exists between the trip algorithms of the Protection Processor and the CPC. The CPC algorithms are programmed in "C" language while the Protection Processor algorithms are programmed in function block language.

C. Alternate Protection System (APS) Functional Diversity

The APS is a two-channel Non-Safety related system that augments the Plant Protection System (PPS) function by providing alternate means to trip the reactor and to initiate a turbine trip and Auxiliary Feedwater System actuation which are diverse from DPPS. The APS is originally designed for ATWS event and also can perform its function by DPPS postulated failure such as common mode failure. Therefore, APS is another protection barrier.

3. Common Mode Failure Consideration

The potential for common mode failure has become an important issue as the software component of protection systems. This potential was not present in earlier analog type protection systems because it could be usually assumed that common mode failure, if it did occur, was due to slow process such as corrosion or premature wear-out. This assumption is no longer true for systems containing software in the protection system.

The KNGR DPPS is PLC-based system that share processing functions (software) and process equipment (hardware). Therefore, a hardware design error, a software design error, or a software programming error may cause redundant equipment to fail. The use of digital computer technology could result in safety-significant common mode failure. The common mode failure could defeat the redundancy achieved by the hardware architectural structure and result in the loss of more than one echelon of defense in depth provided by the I&C system.

In the current KNGR design, manual initiation switches are provided on the Main Control Board. It is assumed that a common mode failure of PLC hardware and/or software occurs in the ESF-CCS, the actuation of the ESF equipment may not occur. Therefore, an additional set of manual actuation switches should be provided in the main control room to interface directly with the downstream of ESF-CCS as shown in Figure 2. This will ensure that manual actuation of ESF equipment is available even with a common mode failure of the DPPS and/or ESF-CCS.

Based on above descriptions, KNGR DPPS can meet the SECY-93-087 [8] requirements which address the defense against common mode failure in digital I&C system.

4. Advantages

The advantage of DPPS is enhanced testability, rapid fault identification, easy configuration, improved MMI, and expandability. These features will provide an improvement in plant availability. Summary of advantages is listed in the followings.

- Easy Configuration
- Simplified Calibration and Scaling
- Simplified Testing
- Improved MMI
- Reduced Spare Part
- Flexibility

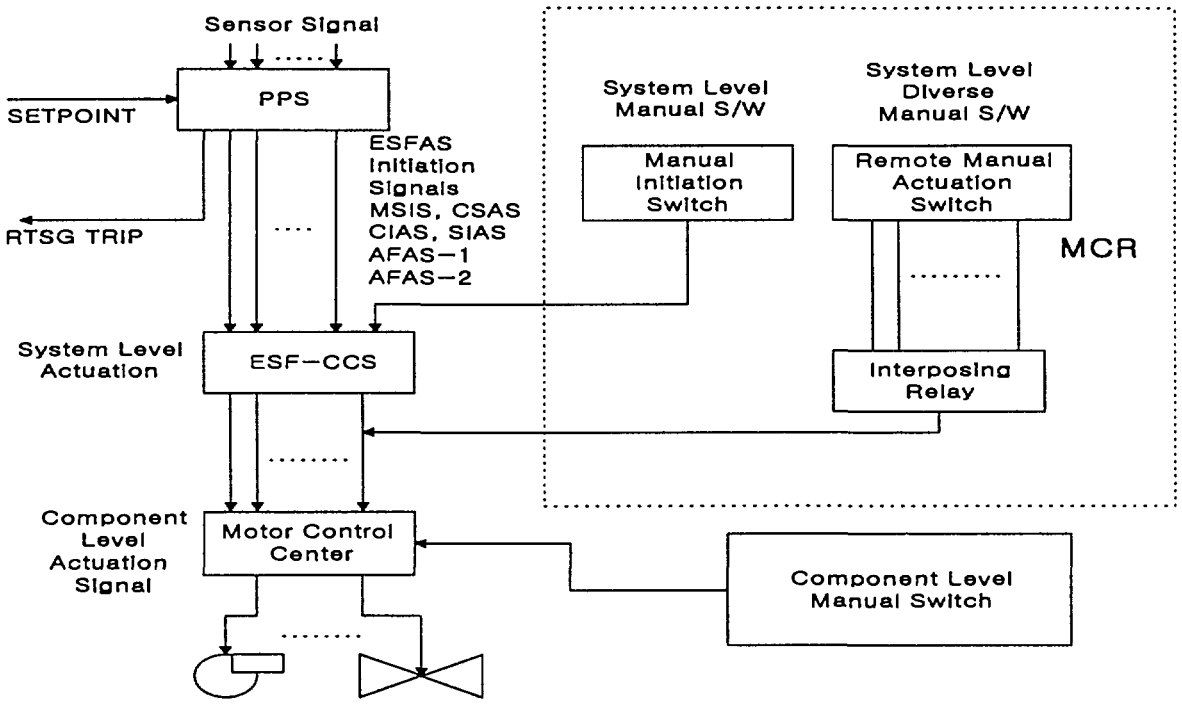

Figure 2. Diverse Manual ESF Control Function Block Diagram

III. PLC based DPPS Prototype

To demonstrate the design function of DPPS, single channel of DPPS prototype is being developed as shown in Figure 3. And the development staging area and coding example are shown in Figure 4. The DPPS prototype uses the ABB Master Advant Controller 110 product line of PLC equipment.[6] A detailed description of this equipment is in reference 6.

1. Hardware Description

One channel of DPPS prototype includes Protection Processor, LCL processor, CCC processor, Integrated Test Processor, Maintenance and Test Panel and Operator's Module with Flat Panel Display.

- Backplane Chassis
  PLC equipment chassis is designed to be panel mounted inside cabinet. It has provisions for distribution of power and data bus signal transmission to and from its installed modules. It contains slots for up to 10 modules.

- Central Processing Unit Module (PM)
  This Module includes controller using 32bit Motorola Processor, with built in RAM and flash PROM. The application program is stored in PROM. A battery is provided for RAM backup power. Two front mounted serial port interfaces (9600 baud) are provided to connect a programming workstation and exchanging data with personal computer.
- Communication Interface Module (CI)
  It is designed to interface with the other PLC controller processors using a proprietary bus mastering, serial and high performance data transmission network with a speed of 1.5 Mbit/s.
- Analog Input Modules (AI)
  This accepts up to 16 analog differential inputs per module, with 12 bit resolution. Ranges from 0 – 20 mA and +/- 10 V.
- Digital Input Modules (DI)
  This accepts up to 32 digital inputs (24Vdc) per module. It includes input opto isolation, contact bounce filtering, front module input status indicators.
- Digital Output Modules (DO)
  It provides up to 32 digital outputs (24Vdc) per module. It includes output opto isolation, front module output status indicators.
- Analog Output Modules (AO)
  It provides up to 16 analog outputs per modules, with 12 bit resolution. Ranges from 0 – 20mA and 0 –10 V. It includes output opto isolation.

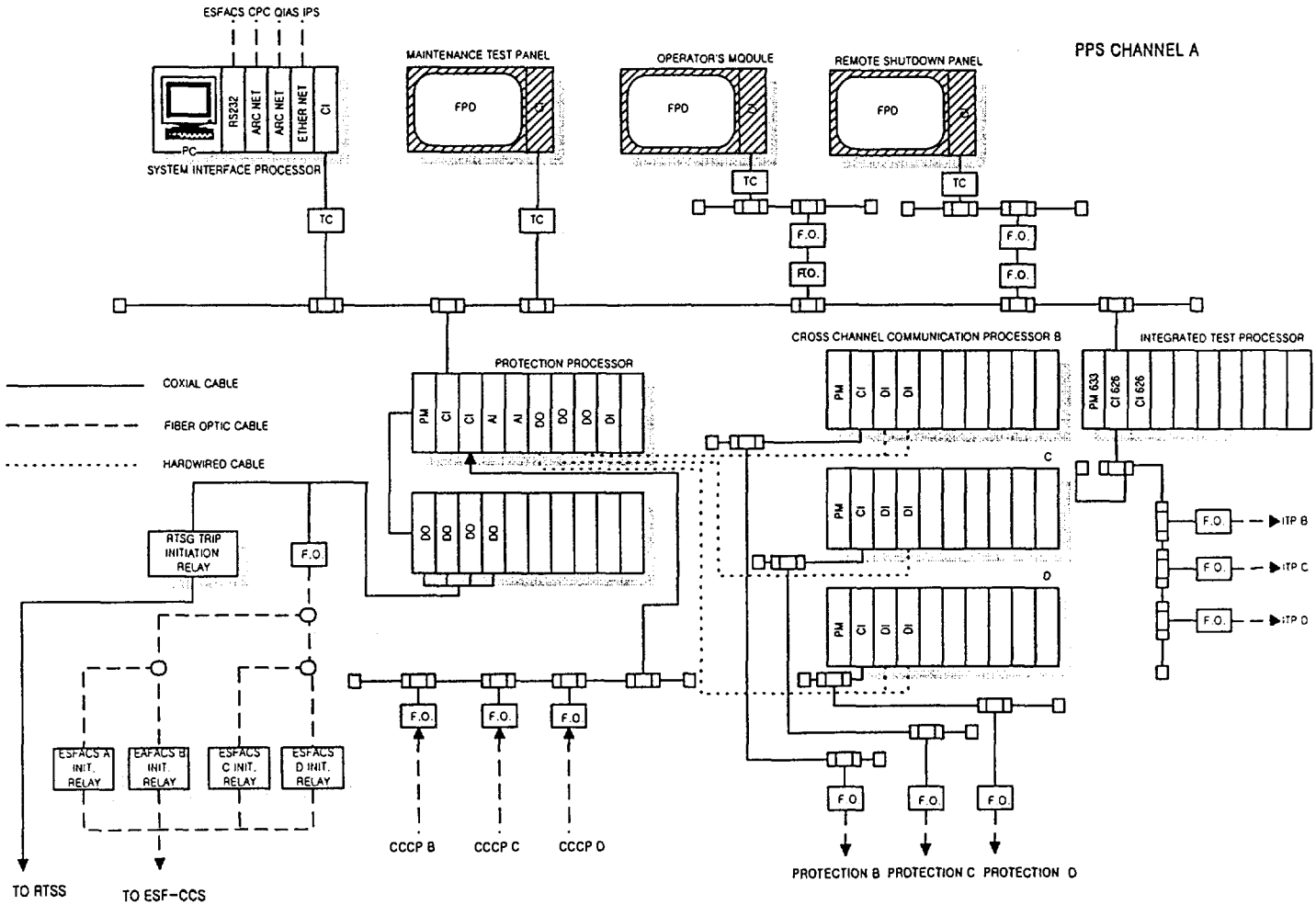

Fig 3. Prototype Configuration of KNGR DPPS

The local DPPS man-machine interface is MTP and OM. It used to monitor DPPS status, perform DPPS control functions. The MMI display equipment is typically composed of the following equipment.

- Flat Panel Display (FPD)
  It has color VGA, 11.6 ″ TFT, with touch screen. Serial Port, RS-232 and parallel port are provided for the FPD interfaces.
- Industrial PC chassis
  PC equipment chassis is designed to be panel mounted in the cabinet.

2. Software Description

Software is divided into two major categories: operating system software and application software. Operating system software consists of PLC processor operating system, input/output (I/O) handling, communications, and equipment self-test software.

Application software is programmed in ABB Master Programming Language (AMPL). AMPL is based on software implemented by function blocks which are combined with each other into programs which form a complete control function.

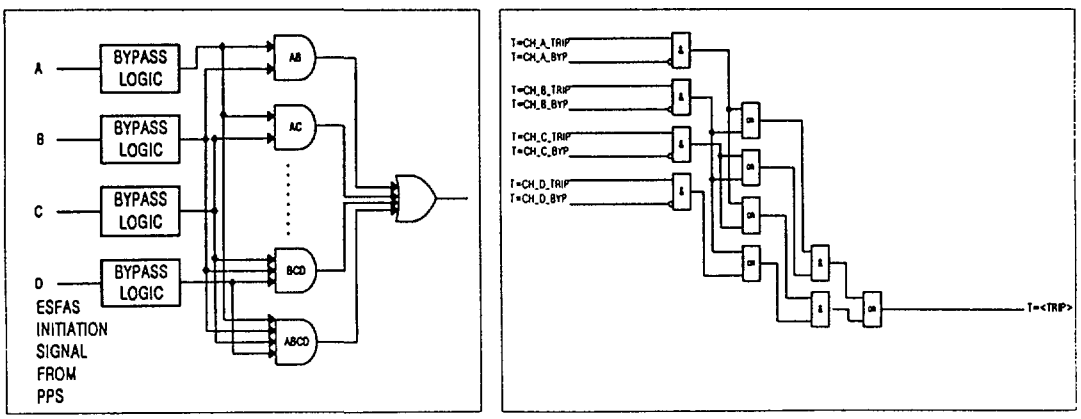

Fig 4. The View of Development Staging Area and Coding Example

3. Communication Networks

The data communication in DPPS prototype consists of PLC network, CCC network and ITP network.

- CCC Network
  There is one CCC network per redundant DPPS channel. The network employs coaxial cable, three fiber optic transmitters, and associated fiber optic cables to each of three CCC processors. Fiber optic communications is used for the CCC network as shown on Figure 3. It is a PLC proprietary high performance, 1.5 Mbit/s, serial data transmission network with bus mastering called AF 100 Field Bus.
- PLC Internal Network
  The PLC internal network connects all of the PLC stations in one channel. It allows status and testing information to be provided from each station. Failure of this internal network does not prevent the operation of the safety channel from performing its intended safety function. The PLC internal network has no interconnection to any of the other three redundant safety channels.
- ITP Network
  The Integrated Test Processor (ITP) network is another network employing an independent communication interface card which is capable of supporting 80 stations. The ITP network is connected to the other DPPS channels through the use of dual redundant fiber optics cables. ITP network provides the communication interface for exchange of non-safety information between the PLC stations.

IV. Software Design

1. Software Program Manual

Reliable computer software is essential to the design and operation of the DPPS equipment. The KNGR DPPS software is being designed, developed, tested and qualified in accordance with Software Program Manual (SPM) for KNGR DPPS. The SPM is based on a Software Life Cycle model consistent with industry standards, that includes the following phases:

- Requirements Analysis/Definition
- Design
- Implementation/Coding
- Testing
- Site Installation and Check out
- Operations and Maintenance
- Retirement

The SPM includes and describes the following basic elements:

A. Software Quality Assurance Plan (SQAP), which describes the process and practice of developing and using software. The SQAP addresses standards, conventions, reviews, problem reporting and other software quality issues.

B. Software Verification and Validation Plan (SV&VP), which describes the method of assuring correctness of the software.

C. Software Configuration Management Plan (SCMP), which describes the method of maintaining the software in and identifiable state during its generation and implementation.

D. Software Operations and Maintenance Plan (SO&MP), which describes recommend software practices after delivery to the user organization.

2. Commercial Dedication

The PLC operating system and application programming tool software are procured from the PLC hardware vendor. The quality of this existing software is assured via a commercial dedication process and the V&V program established by the SPM. The commercial dedication process is composed of three phases:

A. A technical evaluation of the commercial grade component's ability to meet DPPS functional and performance requirements.

B. Following procurement, an acceptance process is conducted, verifying that the received components meet the requirements developed specifically for the component to be dedicated.

C. Additional modifications, testing, analysis and controls may be performed as needed for the DPPS Application.

3. Software Classification

For the purpose of describing software generation processes and methods, KNGR SPM identifies systems and subsystems as one of the following classes:

- Protection (Safety Critical)
  Software whose function is necessary to directly perform RPS functions, ESFAS functions and/or safe shutdown functions
- Important to Safety
  Software whose function is necessary to monitor or test protective functions
- Important to Availability
  Software whose function is necessary to maintain plant operation
- General Purpose
  Software that performs other than that described above previous classifications. This class include tools that are used to develop/generate software in the other classifications, but is not installed in the on-line plant system.

Throughout the SPM, distinctions are made based on the methods applied to each of the above classes. Specific parts of the software in a system may be assigned to different classes. DPPS software is classified as Table 3.

Table 3. Software Classification

DPPS	Software Class
Protection Processor	Protection
CCC Processor	Protection
MTP	Protection/Important to Safety
ITP	Important to Safety
Portable Engineering Work Station	General Purpose

V. Summary

The PLC based KNGR DPPS is being developed and hardware prototype is installed and software coding is started at this time. To increase the system reliability, hardware functional diversity and strict software V&V activities are considered during the development phase. For the common mode failure prevention, system level manual Engineered Safety Features (ESF) initiation switch will be provided in the main control board, and Alternate Protection System (APS) function may be expanded after completion of defense in depth and diversity analysis. For the software classification, technical discussions are continuing with Korean Regulatory Body.

The prototype development will be completed in the first half of 1999, and then detail technical discussions will be conducted with Korean Regulatory Body, but a lot of difficulties are expected in the software V&V activities.

After completion, KNGR DPPS will offer the enhanced surveillance test capability, rapid fault identification, easy configuration, improved MMI and easy expandability.

References

[1] NUREG-1462, vol. 1, "Final Safety Evaluation Report related to the Certification of the System 80+ Design", 1994

[2] Hung-Jun Kim et al, "PLC Based Prototype Digital Plant Protection System", ANS Proceeding NPIC & HMIT, 1996

[3] EPRI "Integrated Instrumentation and Control Upgrade Plan" EPRI NP-7343, 1992

[4] Y. Yamamoto et al, "Planning and Specifying of Digital Based Reactor Protection System for Next Stage PWR Plants in Japan", OECD/NEA, CSNI-CNRA, International Work Shop on Licensing Issues of Computer Based Systems Important to Safety, munich, Germany 1996

[5] EPRI TR-103699-V2, "Programmable Logic Controller Qualification Guideline for Nuclear Applications", 1994

[6] ABB "Advant® Controller 110 Reference Manual" Advant® Power Plant Control, 1997

[7] IEEE std 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations", 1993

[8] SECY-93-087, "Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor [ALWR] Design", NRC, April 2, 1993