Digital Instrumentation and Control Systems for Safety System and Main Control Room Design in Japan Nuclear Power Station

December 2007

JNES

Preface

1. Digital Technology and Nuclear Power Plants

The purpose of this text is to describe instrumentation and control systems of a safety protection system and a main control room using digital technology that perform the centralized operation of a nuclear power plant. Before entering into the main subjects, the reason is shown first why it is necessary to make a point to the use of digital technology although products using digital technology are all over the place in our daily life.

Almost all of household appliances such as a cell phone and television that we use in our everyday life without any question make use of digital technology. It cannot be exaggerated to say that a personal computer (PC), which we use for convenience, such as Internet, cannot be realized without digital processing technology. It is good enough for us as users only to be able to use a television, cell phone etc. comfortably and conveniently, and we don't care what technology is used in them and don't have to. What can be said for sure is that today's convenient tools that we use every day, such as a cell phone, television and personal computer, were not realized without digital technology. A technology in contrast to digital technology is analog technology. Analog technology is the one to represent things in almost same ways as human senses. For example, like the ambient temperature indicated by a mercury-in-glass thermometer, the mercurial column goes up when the temperature is high, and thus the physical quantity of the temperature is represented in terms of the mercurial column height. At a nuclear power plant, many temperature measurements of steam and water are made. For example, the number of the temperature measurements of cooling water supplied to a reactor and steam generated in the reactor, etc. are as many as thousands. Generally, these temperatures once used to move indicating needles to show the temperature using continuous electrical signals (analogue signals) from thermometers with thermo-couples or resistance temperature sensors. When using digital technology for such temperature measurements, electrical signals from thermometers with thermo-couples or resistance temperature sensors are not continuous, but are converted to discrete signal of "0" and "1" inside the thermometers, namely, are digitized, and the digital signals are transmitted from those thermometers. These digital signals are transmitted through one cable and converted to indications of physical quantities of temperature. Such representations are given so as to help human beings understand the temperature, for example, 300°C. Since this is a simple example to indicate a temperature, digital advantages cannot be fully demonstrated. But for a case that a function is required to keep the temperature in a range by automatically turning off a switch for a heater when the temperature goes up to 250°C and turning on the switch when the temperature goes down below 200°C, or to shut off a power supply and make an alarm when the temperature rises abnormally to 400°C, a simple calculation of the physical quantities derived from digital signals can judge whether the temperature is higher or lower than these values. However, when trying to make this calculation in circuits using analog signals, a comparison processor is required for each calculation, thus requiring a large number of components for the circuits. There certainly was an analog-type mobile phone, but our vivid memory is that the phone was large and heavy, and worse still, it was expensive.

Thus, digital technology makes it possible to realize advancement and diversification of functions, miniaturization and weight saving, and low-pricing of devices, inevitably resulting in analog-type devices going out of production except for special-purpose applications. Consequently, production of analog-type devices for special-purpose applications cost a lot more. These days, it is very difficult to obtain an analog-type instrumentation and control device even if it is simple. It is natural that instrument manufactures are unwilling to produce unmarketable products. It is an unavoidable trend to shift from instrumentation and control devices using analog technology to those with digital technology. Therefore, the system to which digital instrumentation and control devices are applied will be introduced to nuclear power plants to be built. Application of digital technology to nuclear power plants is only decades old. General industry including thermal and hydroelectric power, petroleum, paper making and steel have preceded nuclear power industry in the utilization of digital technology, and the utilization for nuclear power plants has been promoted behind them. The reason is that the nuclear power industry has been conservative in introducing new technology because it gives an overriding priority to safety. It has been the concept that technology well proven in the general industry should be applied. In addition, since digital technology makes use of software for signal processing and operation, there are various technical issues to be solved such as quality control and maintenance management, which have not been experienced with analog instrumentation and control devices, and special considerations and measures are required for applying this technology. When applying it especially to instrumentation and control systems important to safety of nuclear power plants, solving the issues and the special considerations are essential requirements for safety.

2. Issue of Instrumentation and Control Systems of Nuclear Power Plants in Japan

Instrumentation and control systems using digital technology have many merits, compared with those of analog type, in realization of upgrade of control functions, reduction of components constituting the systems, design of circuits capable to make complicated logic judgment, and graphical information display easy to understand process parameters such as flow rates and pressures, and operational states of pumps and valves. On the other hand, as mentioned above, under the present circumstances it has been getting difficult to obtain analog type instrumentation and control devices. Because of these merits and circumstances, the utilization of digital instrumentation and control systems cannot be avoided and rather should be promoted. This is the situation as of this date.

The first nuclear power plant in Japan started its operation at the beginning of 1970. The instrumentation and control devices of all plants that started their operations by around 1985 were those with analog technology. The digital technology was applied to a part of control systems of the plants that started their operation in the 1990s. The above-mentioned history might give an impression that digital technology application in Japan was slower to nuclear power plants than the general industry including thermal and hydroelectric power, petroleum, paper making and steel. But taking into account the period for the regulatory review on a plan and establishment of a nuclear power plant in addition to its construction period of 5 to 6 years, its design must have been finalized ten years prior to its commissioning. This means that the application of digital technology to the nuclear power plant was determined in 1980. This was just about the time when the music compact disk (CD) came out to the market, so application of digital technology to nuclear power plants seems not to be so slow. It was for ABWR and APWR that digital instrumentation and control devices were applied to all the instrumentation and control systems including the reactor safety protection systems. In 1997, the first ABWR unit started its operation.

As it cannot be avoided nowadays to apply digital technology to the operational and signal processing of instrumentation and control devices, it is a major issue how digital technology is applied. Systems with functions to measure process parameters, such as reactor pressure and temperature and cooling water flow rate, and to control reactor power and steam pressure are instrumentation and control systems. A failure in the instrumentation and control devices could stop operation of a nuclear plant. A small instrumentation and control device that can be held with one hand governs operation of a nuclear power plant that generates 1350Mwe. Especially, instrumentation and control systems used for the safety protection system ensuring the reactor safety are required to have reliability not only in a single device, but also in overall systems. Since software is used for control operation, logic processing, signal conditioning, etc. to be performed in digital instrumentation and control devices, those operations and processing are invisible and not understandable from the outside in their nature. Analog instrumentation and control devices consist of resistors, capacitors, amplifiers etc., and logic processing circuits consisting of operational processing circuits, relay contacts, etc. are tangible and easy to check for their functional integrity. On the other hand, programmed software is invisible as called a black box. Therefore, while digital devices are superior in many ways to analog ones, special considerations and measures are required when using devices since there are many issues including technical, quality control, and maintenance matters to be solved in system design and operation, which is essential as safety requirements when applying digital devices especially to instrumentation and control systems important to safety. A digital safety protection system is subject to safety review in an application for nuclear plant establishment license.

Under the conditions mentioned above, when organizing the issues concerning instrumentation and control systems of nuclear power plants in Japan, they are summarized into the following two points.

(1) Instrumentation and control systems of existing plants

There is a nuclear power plant that has been already in service for 30 years since its commissioning. Maintenance of instrumentation and control devices has become very costly with an increase in service time. It is not possible to purchase the same analog instrumentations or control devices. The old instrumentation and control devices for systems except the safety protection system are, in general, replaced with digital devices. What is called modifications of instrument and control system has been conducted. Since modifications of the instrumentation and control devices for the safety protection system are related to the requirements for safety review, the change or modification to digital devices belonging to the safety protection system have not been made yet, and it is the current situation that conventional analog devices have been continuously used fixing and maintaining them.

Those systems other than the safety protection system govern plant availability factors, and inappropriate modification could result in plant shutdown and a loss of nuclear power credibility with the public. Therefore, modification of instrument and control systems has been made with the utmost care.

Such an issue is not limited only to Japan, but is the same also in U.S., EU etc. “SAFETY OF MODIFICATIONS AT NUCLEAR POWER PLANTS - The role of minor modifications and human and organizational factors - (Version 2.2, 2005, OECD/NEA)” points out the following: Operating experience repeatedly shows that changes and modifications at nuclear power plants (NPPs) may lead to safety significant events. At the same time, modifications are necessary to ensure a safe and economic functioning of NPPs. To ensure a safety in all plant configurations it is important that modification processes are given proper attention both by utilities and the regulators. The operability, maintainability and testability of every modification should be thoroughly assessed from different points of view to ensure that no safety problems are introduced.

This paper discusses problems and issues associated with all over the changes and modifications of mechanical systems. Modifications of instrumentation and control systems are important changes and modifications at nuclear power plants. In modifying instrumentation and control systems, devices are not only simply replaced but the operating principles, that is, change from analog to digital, are also changed to achieve their functions. Therefore, it should be noted that more cautious approaches and considerations are required for modifications of instrumentation and control systems.

(2) Instrumentation and control systems of newly constructed nuclear power plants

At existing nuclear power plants, digitization of instrumentation and control systems, i.e., modification to replace instrumentation and control devices with digital devices, of the safety protection system has not been performed yet. The digital reactor safety protection systems were introduced for the first time to the Kashiwazaki Kariwa Nuclear Power Station Unit 6 (ABWR) that started commercial operation in 1997. At this plant, according to digitization of the safety protection system, all the instrumentation and control systems consist of digital instrumentation and control devices and optical fiber cables, which replace the conventional electrical cables, for signal transmission.

In Japan, the digital application to the reactor safety protection systems was performed at the newly constructed plant. When comparing the difference between difficulties associated with an application of digital reactor safety protection systems to an existing plant and to a new plant, the difference is easy to understand when imagining the difficulties involved between a new-type engine installation to a newly designed car body and the one to a used car body. Although the efforts in developing the new-type engine are common to both cases, its installation to a used car involves different difficulties on how to install the engine harmonizing it with the existing car body and to obtain the best performance.

The reactor safety protection systems are classified as the system most important to the safety of a nuclear power plant, and digitization of the systems leads to digitization of all instrumentation and control systems. Following digitization of instrumentation and control systems, substantial changes has occurred to detectors to measure process parameters, such as pressure and flow rate, cables to transmit signals of measurements, indicators to display process parameters, operating devices, and control panels to mount indicators and operating devices, which had been conventional analog devices. Because one optical cable can transmit a great number of signals, indicators have changed from meters to flat displays or cathode-ray tubes for digital values of pressures and flow rates, bar charts, trend displays, etc. on screens, which realized easy-to-understand indications. Operating devices can also use touch screens where a finger touches the icons displayed on flat displays for operation, replacing operating switches. One flat display can provide a wide range and number of information by switching the display screens. These changes in indicators and operating devices have permitted the reduction of their physical outline sizes, and the miniaturization of control panels. Thus, digital technology application to nuclear power plants has revolutionized main control rooms that perform the centralized plant operation management.

Next, let us take a look at the historical transitions of main control rooms.

3. Historical Transitions of Main Control Rooms of Nuclear Power Plants in Japan, which Digitization Brought about

Following the technical progress in instrumentation and control devices, transitions of main control room of nuclear power plants have taken place in Japan in response to needs to reduce operators' workload and to prevent human errors. The digital technology application have been progressed and realized miniaturization of control panels along with flat displays presenting information and devices with multi-operating functions, etc., which has changed the main control rooms. The transitions can be divided into three phases.

Phase 1: Nuclear power plants that started their operations in from 1970 to 1985.

As shown in Picture-1, the indicators for process parameters such as pressures and flow rates are vertically-installed ones with indicating pointers. The operating devices are switches with handle. Control panels in the main control room are provided with indicators and switches for the reactor cooling system, reactor power control system, turbine-generator system and plant power supply system, and they are in L-shape-arrangement of approximately 2 m high and approximately 17 m long. The instrumentation and control systems were ones using analog technology.

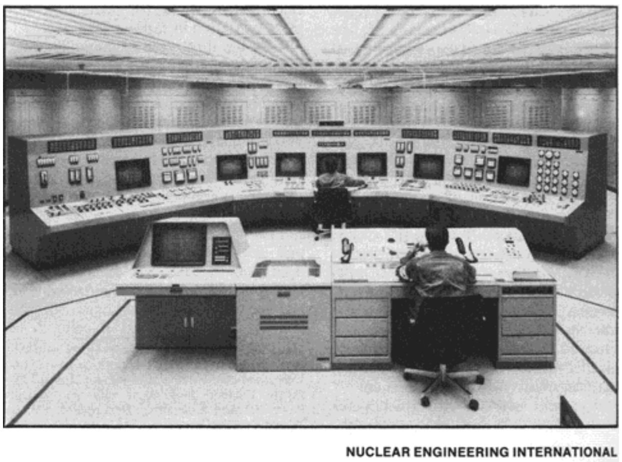
Picture-1: 1st generation control panel

Phase 2: Nuclear power plants that started their operations in from 1986 to 1996.

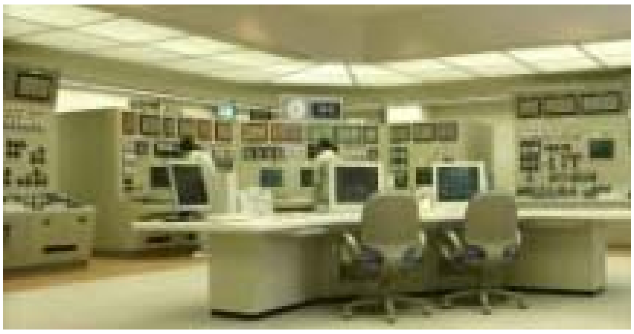
As shown in Pictures-2A and 2B, the indicators for process parameters are divided into two groups, one for safety systems and another for non-safety systems, and only the indicators for safety systems remain as hardware devices, while ones for non-safety systems were replaced with seven sets of cathode ray tubes (shown in the pictures) to show process parameters. Furthermore, the indicators and operating devices for safety systems are mounted on control panels dedicated for those systems, while the indicators and operating devices to be used for normal plant operation are on the main console in the center of the picture. Thus, the size of the main console was reduced to approximately 7 m, and the area for normal operation shrank substantially.

Although the operating devices are mainly switches attached with handle, they were changed to smaller ones or push-button types. A large process computer performs display control of process parameters on CRTs. As explained above, digital technology was applied to normal instrumentation and control systems on the phase 2 control panel except for those to monitor and control safety systems. The instrumentation and control systems for safety systems used analog technology.

And, each indicators and switches for the reactor cooling system, reactor power control system, turbine-generator system and plant power supply system are arranged from the left side of the control panels in the same manner as those on Phase 1. These arrangements are common to the control panels of Phase 1 to 3. Changes in the arrangements of devices for fundamental operation and monitoring could lead to human errors.



Picture-2A: 2nd Generation Control Panel (an example of BWR)



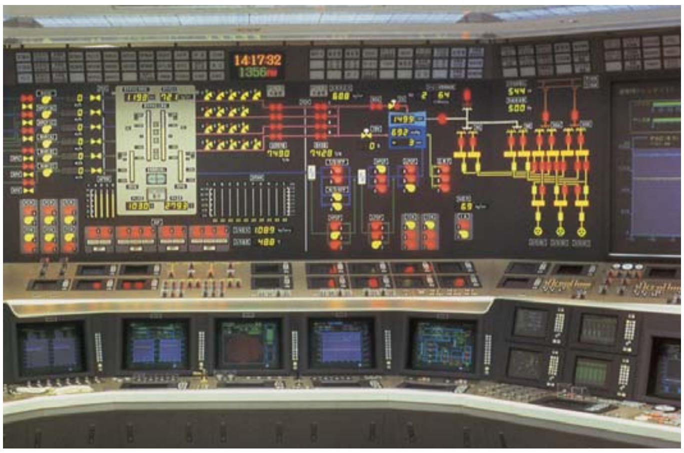
Picture-2B: 2nd Generation Control Panel (an example of PWR)

Phase 3: Nuclear power plants that started their operations after 1997.

Control panels shown in Picture-3 are arranged with short-in-height consoles in the front and large panels in the back. The console is for performing plant operation and monitoring during plant start-up, normal power operation, and shutdown. Seven CRTs and 17 flat displays are arranged on the console. There is no instrument like the conventional indicator, and all information such as pressures, temperatures, and flow rates are displayed on the CRTs and flat displays. All switching actions are performed by touching on the flat displays except for those to change reactor operation modes, scram buttons to perform reactor emergency manual shutdown, and those to switch for start-up and shutdown of large-sized equipment. The console is approximately 5 m wide. Large panel in the back displays, on a large scale, overall conditions of the reactor power, turbine-generator system, and feedwater and condensate system, so that all members of an operation team can monitor whole plant operating conditions. The left-hand side of the panel shows the equipment conditions of safety systems, such as the emergency core cooling system, and on the right-hand side, is a screen installed to show important information, such as reactor power and pressure. In the upper part, are alarm indication window provided.

Reactor emergency shutdown and actuation of the emergency core cooling system are, of course, performed automatically, but operating actions which operators conducted on Phase-2 control panels, such as reactor power control by control rod operation and recirculation flow control, turbine-generator start-up and shutdown, and switching action of feedwater pumps, were automated with digital control systems. With the first directive given by an operator to a control system, the function to automatically operate the control system up to a target operating point is provided.

Picture-3(A): 3rd Generation Control Panel



Picture-3(A): Center part of 3rd Generation Control Panel

4. Application Status of Digital-Type Safety Protection System

It is Kashiwazaki Kariwa Nuclear Power Station Units 6 and 7 of the Tokyo Electric Power Co., Inc., which applied digital technology to instrumentation and control systems of the safety protection system for the first time in Japan. These are the first ABWR plants that started operation in 1997. Following these, the same application was made to Hamaoka Nuclear Power Station Unit 5 (commissioned in 2005, ABWR) of the Chubu Electric Power Co., Inc. And, the same application was made to the Tomari Nuclear Power Station Unit 3 (PWR) of the Hokkaido Electric Power Co., Inc. under construction.

In foreign countries, Canadian CANDU plants have computerized shutdown systems (Ichiyen and Joannou. 1995). French N4 PWR plants have microprocessor based reactor protections systems (Burel 1995). Microprocessor based safety systems have also been installed in a newly constructed PWR plant in the United Kingdom (Daily and Orme. 1992).

Table of Contents

1. Instrumentation and Control Systems in the Most Advanced Nuclear Power Plants

The 3rd phase instrumentation and control systems put in service since1997 and afterwards use digital data processing technology. The role of the instrumentation and control systems is to achieve stable and reliable plant operation by measuring the operational states of many mechanical systems constituting a plant, and appropriately controlling them. In this section, the instrumentation and control system is defined as a system including the instrumentation system to measure process parameters such as flow rates, pressures and reactor power, optical information transmission system to send measurement signals to controllers, controllers to adjust process parameters such as reactor power and reactor pressure, and control panels to bring these information to a main control room and perform an operation monitoring. On the other hand, the instrumentation and control systems can be roughly categorized into the following four categories in terms of functions. Hereinafter, the instrumentation and control systems will be discussed taking for an example the advanced BWR plant that started its operation in 1997.

a) Safety protection system to ensure the reactor safety (Reactor Protection System)

b) Power control system to monitor and control reactor power (Power Control System)

c) Nuclear steam supply system (NSSS) to control components such as pumps and valves which adjust steam generation and cooling water, and electrical house power system to control power supplies (Electrical House Power System)

d) Turbine generator system to adjust a rotating speed and generator output (Turbine Generator System)

All of the above information is displayed on the control panels of a main control room. Fig. 1-1 shows schematically the overall configuration of the instrumentation and control systems. The main control room is shown in the upper part of the figure. The equipment in the main control room consists of an operating console and a large-screen display. In the main control room, many control panels housing digital controllers of the reactor protection system, the power control system, etc. are located. The lower part of the figure shows mechanical systems that consist of various components represented by the nuclear reactor and the turbines and generator. The detector signals that have measured the operational states of the mechanical systems are converted to digital signals at RMU (Remote Multiplexing Unit), and are transmitted to the control panels in the main control room via optical cables. RMU assigns identification code number to each signal, and transmits many measured signals using a single optical cable. Conventional analog technology requires one metal cable for one signal, but one optical cable can transmit many measured signals. Some signal transmissions between the mechanical systems and control panels use partly metal cables. For example, the cables that send important signals to command an emergency reactor shutdown and to control the turbines and generator are metal cables. However, portions using metal cables are very few, compared with those using optical cables. The cables for all the signals from the control panels housing digital controllers to the operation console and large display panel are optical cables. The external view of control panels is shown in Fig. 1-2. There are printed circuit boards containing central processing units (CPU), operational state display panels, maintenance panels, power supply units, and signal transmission devices, etc. inside of the control panels.

Application of digital technology to almost all instrumentation and control systems including the reactor safety protection systems has made it possible to realize such advanced instrumentation and control systems for plant control. And also, establishment of the specifications and control methods, meeting the stringent safety requirements for design, quality control, management control, etc. imposed on the instrumentation and control systems for the reactor safety protection systems, has led to the realization of such instrumentation and control systems.

Then, the following Chapter outlines the safety requirements for the instrumentation and control systems of the reactor safety protection systems, and the advantages and disadvantages of digital technology, and discusses measures, methods etc. taken in Japan in order to comply with the safety requirements.

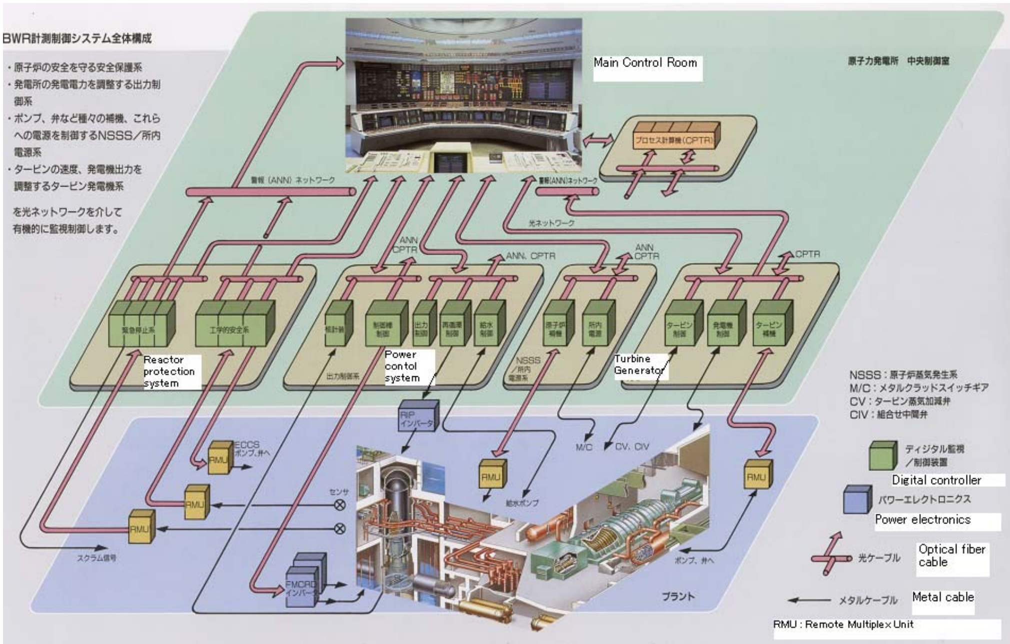


Fig. 1-1 Configuration of fully digitalized instrumentation and control system

Fig. 1-2 One group of typical digital control panel

2. Digital Safety Protection Systems

2.1 Safety Requirements for Instrumentation and Control Systems Important to Safety

The instrumentation and control systems for the systems important to safety, typified by the systems to perform emergency reactor shutdown and emergency core cooling have been subject to the safety requirements for design, quality control, and maintenance during plant service life since the analog instrumentation and control systems. When digital instrumentation and control systems had begun to be applied, specific requirements for digital systems came to be added to the conventional safety requirements. For example, IAEA Safety Guide NS-G-1.3 (Reference 5) on the instrumentation and control systems important to safety, which was revised in 1980 and 1984, was revised in 2002 to be applicable to systems using a digital computer to the instrumentation and control systems important to safety. "Instrumentation and control systems using a digital computer" has the same meaning as "instrumentation and control systems using digital technology", or "digitization of instrumentation and control systems" in this text.

(In 2002, the revision took account of developments in instrumentation and control systems important to safety since the earlier Safety Guides were published in 1980 and 1984. The main changes result from the following: in this Safety Guide, developments in the use of computer based instrumentation and control systems important to safety are considered.)

Advantages and disadvantages of digital computers, and matters to be taken into account described in Safety Guide NS-G-1.3 are provided in the following. (For details, go to References.) In addition, see Reference 5 for the IAEA safety requirements and design base for the instrumentation and control systems important to safety.

<u>Digital Computer Systems</u>

5.43. Digital computer systems are used in instrumentation and control systems important to safety to perform functions of protection, data acquisition, computation, control monitoring and display. If properly designed, they can offer the advantages of improved reliability, accuracy and functionality in comparison with analog systems. The computer system may take many forms, ranging from a large processor supporting many functions to a highly distributed network of small processors devoted to specific applications.

5.44. Computer systems may be used to advantage in detecting and monitoring faults internal and external to plant systems and equipment important to safety.

5.45. Hardware and software for computer systems should be configured so that the system operates in a predefined safe manner in conditions of credible failures of hardware and software.

5.46. With computers it is possible to have one set of equipment perform several system functions. A disadvantage of this is that if one component goes out of service, several functions may fail simultaneously. Consequently, this factor should be addressed in the design and analysis of the systems.

5.47. When the use of a computer involves two or more functions that fall into different safety classes, the computer system should meet the requirements of the higher safety class.

5.48. Start-up and reset of a digital system (e.g. after a temporary loss of electric power) should initialize the system to a predefined state that ensures continued safe operation.

5.49. The software for the digital system should be well documented and should be developed through a controlled engineering process.

5.50. An IAEA Safety Guide [IAEA, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, Safety Standards Series No. NS-G-1.1, IAEA, Vienna (2000)] provides additional guidance on the use of digital computer systems.

Maintenance

5.51. Adequate technical expertise in the original technology for the hardware and software should be preserved over the lifetime of the plant. Contrary to what is typical for other plant systems, maintenance of computer systems is not routine. Maintenance staff should have in-depth knowledge of the requirements of the computerized systems and of the development process used for the digital retrofit.

Upgrades to digital systems

5.52. It should be recognized that computerized instrumentation and control systems in new power plants will also age, become obsolete and eventually need replacement. Given that suppliers of digital equipment change their product lines frequently, it becomes difficult to maintain an inventory of spare parts for the lifetime of the plant. The user has to stock a substantial quantity of digital components and, in doing so, should consider the possible deterioration of electronic products that are stored for a long period of time.

Data communication

5.53. Data communication as defined for the purposes of this Safety Guide is the transmission from one location to another of two or more signals or messages over a single data channel by the use of time division, frequency division, technology of pulse coding or the like. Data communication encompasses a wide range of technical solutions varying from simple hardware only multiplexing to complex self-correcting and multilayer communication protocols controlled by software.

5.54. Data communication channels important to safety should satisfy the recommendations for independence given in Section 4, particularly Para. 4.36 to 4.48.

5.55. The design of the data communication system should provide for detection and, to the extent practicable, for correction of errors and for the status of data in the information transmitted.

5.56. Checking of data communication may be done periodically as an automatic self-check function. The chosen frequency of this self-check should be appropriate for the use of the data and the frequency of demand for the safety functions being performed by the system. Features for the detection and correction of errors can be used to improve the reliability of signal transmission to meet reliability goals.

5.57. The communication technology should be chosen and suitably configured to ensure that it is capable of meeting the requirements for time response under all possible conditions of data loading.

5.58. Where the reliability of the data and the data link are of great importance, suitable communication technology should be selected. The selection and use of more complex technology may offer functional advantages but may also introduce additional failure modes and validation difficulties. Appropriate consideration should be given to the use of redundancy in the data link, to the appropriate level of reliance on the data link in general, and to the ability of the sending and receiving systems to withstand failure by all possible modes. The use of data communications should not defeat the physical or functional channelization of processing or logic elements within the system architecture.

5.59. Data flow from systems of lower safety class to systems of higher safety class should generally be avoided as far as practicable. Where such data flows are essential, measures (such as data validation or data range checks) should be taken to ensure that data from the lower class system cannot jeopardize functions important to safety.

Moreover, refer to Reference 6 (NS-R-1) for the requirements for the safety design of nuclear power plants. These requirements provide those for overall mechanical and electrical systems constituting the plants. Many safety requirements for digital safety protection systems have been issued by NRC. As it is not the intention of this text to explain these safety requirements, please see the documents issued by IAEA, IEC and NRC.

In order to apply digital safety protection systems to nuclear power plants in Japan, software development and its verification and validation (V&V) were conducted in accordance with JEAG Standard 4609, which was established basically based on the IEC 880 (Software for Computers in the Safety Systems of Nuclear Power Stations, 1986), and then the software were applied to the nuclear power plants. The details are discussed below.

2.2 Digital Safety Protection Systems in Japan

2.2.1 Features and technical issues of digital instrumentation and control systems

Digital systems have the following advantages over analog systems:

1) Fewer characteristics change due to aging.
2) Easier configurability as a redundant system.
3) Easier modification and addition of new features by changing the system software.
4) Easier use of optic fiber data transmission which improves immunity against external electro-magnetic and radio-frequency noise.
5) Improved maintainability by introducing self-diagnosis, self-calibration, event and data recording, and so on.

However, they also have the following disadvantages:

1) Because signal processing is done by software, it is difficult to observe the system status directly, as it is possible in analog systems by watching the relay operations.
2) Signal processing is performed sequentially, so that processing time and timing constraints must be considered.
3) Microprocessors performing signal processing halt due to software or hardware failure, which leads to the loss of signal processing capability.
4) Signal processing is based on digitized (i.e. discrete) data, so that the effects of digitization, such as accuracy, aliasing and so on must be considered.
5) Detection of failures in software design and development may be more difficult and complex.

These disadvantages seem to be the background factors leading to discussions on the reliability of software based safety systems. It is generally discussed that deliberate and elaborate efforts are required to cope with design errors which may result in a common mode failure. The reliability of software based safety system is a significant issue. Guidelines or standards such as IEEE 7-4.3.2 (1993), IEC88O (1986) and JEAG4609 (1989, Japan Electric Association Guide) have been published for applying software based digital safety systems to nuclear power plants. These documents address the issues on reliability of software based safety systems and define requirements for hardware software design, manufacturing, verification and validation (V&V) procedures, documentation, maintenance and so on.

2.2.2 Digital safety system

The digital safety systems, which have been implemented at Kashiwazaki Kariwa Unit 6 of the Tokyo Electric Power Co. Inc. as the first ABWR plant, are discussed.

The newly developed digital safety systems for ABWR consist of a reactor protection system (RPS) and an engineered safety feature (ESF). Fig. 2.2-1 shows its primary configuration of RPS and ESF. The RPS controls the scram function if abnormal events occur. The ESF controls the activation of emergency core cooling systems, containment isolation and cooling system and so on.

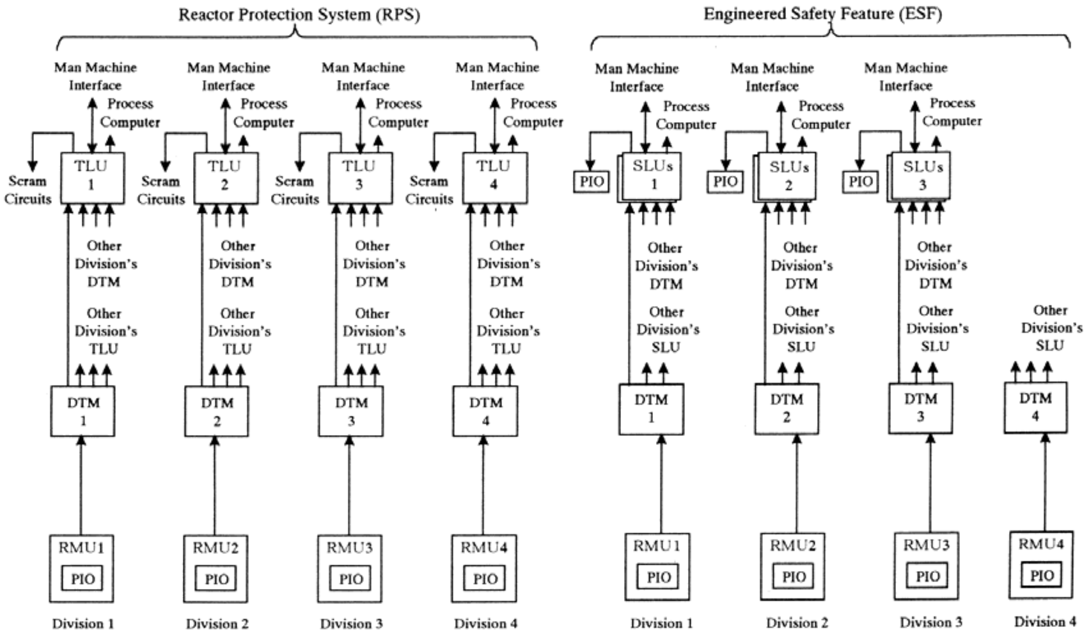


Fig. 2.2-1 Primary system configuration of the digital safety systems

2.2.2.1 Reactor protection system (RPS)

Fig. 2.2-2 shows the system configuration of the RPS. The RPS has four independent divisions, each provided with sensors for measuring process parameters. Signals from sensors are supplied to multiplexing units at local panels where they are digitized and sent to a digital trip module (DTM). The DTM compares the input signals with pre-defined set points and sends the results to a trip logic unit (TLU) as logic (1 or 0) signals. Each TLU in each division receives the results of the DTMs of the four divisions and performs '2-out-of-4' logic to validate the activation of the plant protection function (if two or more DTMs detect the violation of the set point, scram is validated by the TLU.). The outputs from the TLU are sent to a hard-wired scram circuit via an output logic unit (OLU). The hard-wired scram circuit consists of two sets of scram solenoids to form '2-out-of-4'logic circuits so that the reactor scram occurs only when two sets of the scram solenoids are de-energized at the same time. A data communication unit (DCU) is provided to receive signals from the DTM and the TLU in the division and display them on the flat display (color liquid crystal display). A dual redundant interface unit (IFU) is provided to perform alarm processing and send the results to an annunciator system and the process computer. Regarding diversity, a pair of independent hardwired switches is provided, as in the conventional system, to allow the scram solenoid power to be cut off directly. Also, hardwired indications of important safety related parameters such as reactor pressure, reactor water level, containment pressure and so on are provided.

DTM, TLU, DCU and IFU use a 32-bit fast microprocessor for signal processing. Multiplexed data transmission via optical fibers is used as shown in Fig. 2.2-2.

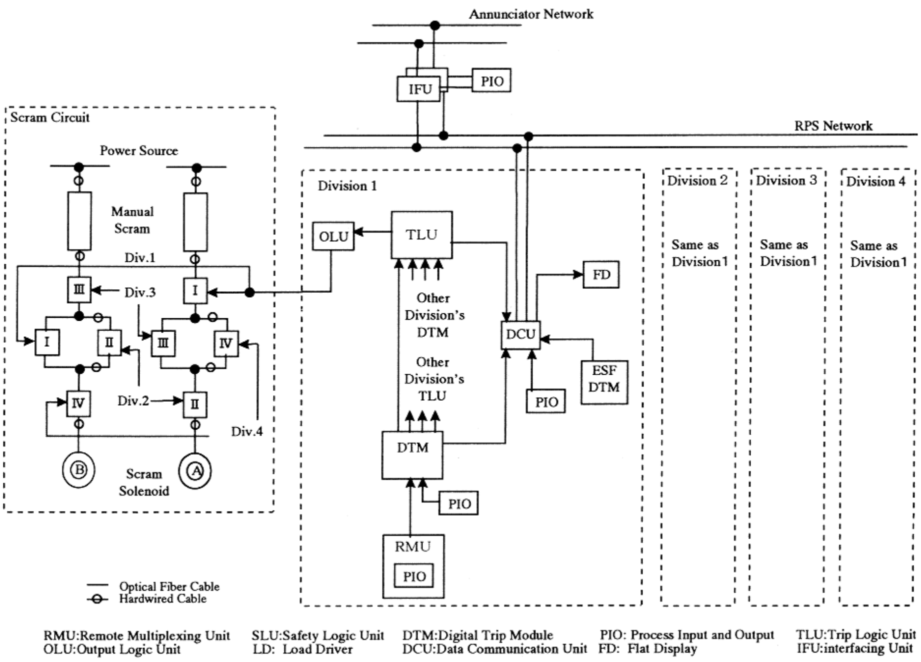


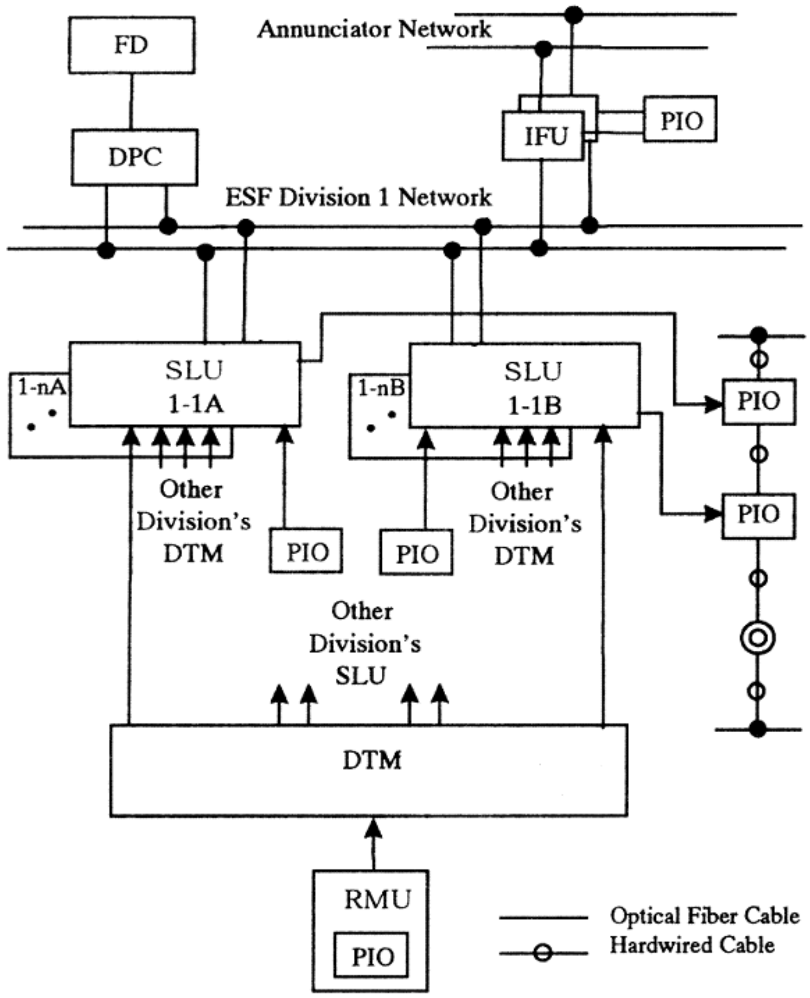
Fig. 2.2-2 System configuration of RPS

2.2.2.2 Engineered safety feature (ESF)

The ESF consists of three divisions of several pairs of safety logic units (SLU) and four DTMs. Control functions of one or several digital safety systems such as emergency core cooling systems are assigned to each SLU in each division. The SLU activates the assigned functions if necessary based on the "2-out-of-4" logic. The DTM performs the same functions as the DTM in the RPS. Fig. 2.2-3 shows the configuration of a typical division of ESF. A pair of SLUs performs the same control logic redundantly and asynchronously. Each SLU in a pair has its own process input and output module (PIO) and sends the processing results to respective PIOs. The two PIOs are connected in series to form '2-out-of-2' logic. Several sets comprising a data processing controller (DPC) and a flat display (color liquid crystal display) are provided with each division. The DPC displays system status on the flat display and processes a touch operation signal from the flat display. A dual redundant IFU is provided to perform alarm processing as in the case of RPS.

Regarding diversity, independent hardwired controls for the manual activation of high pressure core flooding systems and for the manual isolation of main steam lines, cleanup water system and reactor core isolation cooling system are provided. SLU, DTM, DPC and IFU use a 32-bit fast microprocessor. Multiplexed data transmission via optical fiber cables is utilized as shown in Fig. 2.2-3.

Table 1 summarizes the elements and the scope of the digital safety system.



RMU:Remote Multiplexing Unit SLU:Safety Logic Unit DTM: Digital Trip Module
PIO: Process Input and Output FD: Flat Display DPC:Data Processing Unit
IFU: interface Unit

Fig. 2.2-3 Configuration of a division of ESF

Table1 Elements and scope of the digital safety system

System element	RPS	ESF
DTM	4	4
TLU/SLU	4	Div. 1 6×2, Div. 2 6×2, Div. 3 3×2
DCU/DPC	4 (DCU)	Div. 1 3, Div. 2 3, Div. 3 2 (DPC)
IFU	1×2	3×2
FD	4	Div. 1 3, Div. 2 3, Div. 3 2
PIO	About 1500 points	About 5000 points
Transmission data	About 4500 points	About 30 000 points

2.2.2.3 Logic of the digital safety system

The signal processing of the digital safety system is basically logic signal processing (i.e. and/or logic calculation). Fig. 2.2-4 shows the RPS logic. The information on whether or not a process parameter exceeds its predetermined set point is represented and processed logically using and/or logic combinations to determine the activation of the RPS. The activation of digital safety systems by ESF is determined similarly to RPS. The DTM checks the violation of set points, while the TLU (for RPS) or SLU (for ESF) performs the rest of the logic calculation. These units are controlled by POL. Other units such as DTM, IFU, DCU and DPC are also controlled by POL.

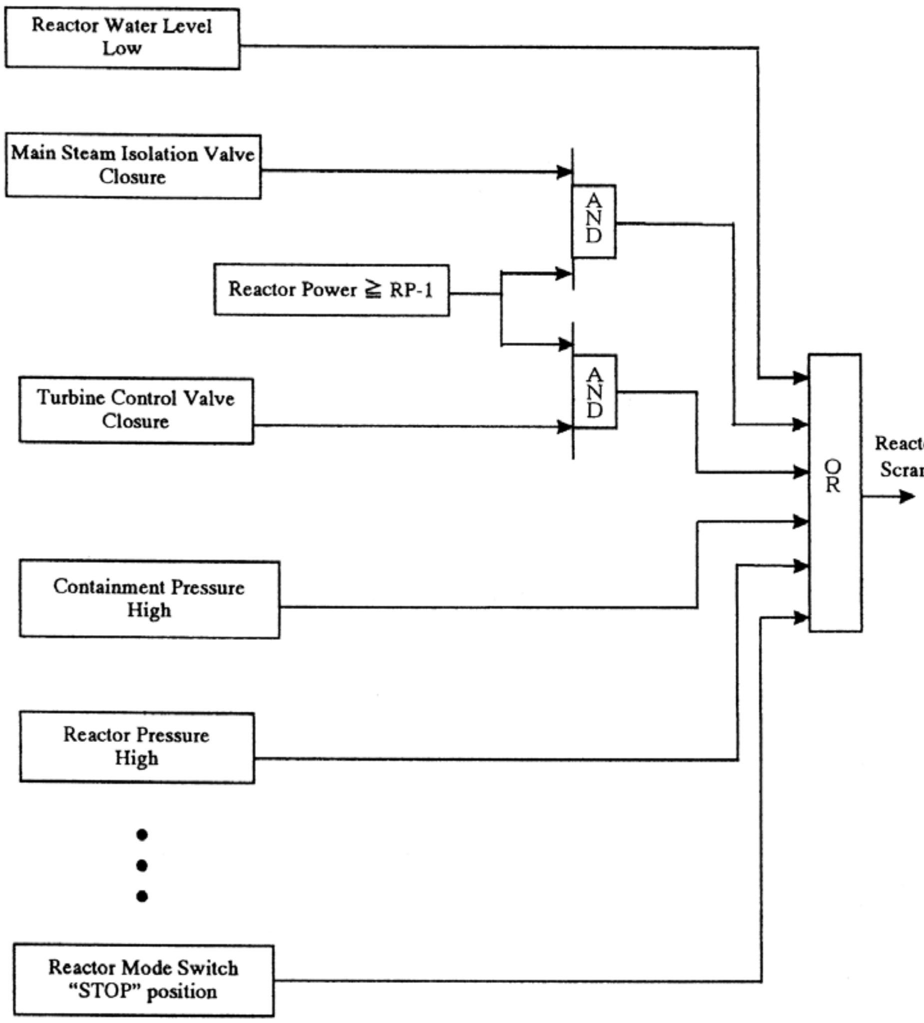


Fig. 2.2-4 logic of RPS

2.2.3 Basic software technology of digital safety systems

Basic software technology for the digital safety systems of the Kashiwazaki Kariwa Unit 6 of the Tokyo Electric Power Co., Inc. is discussed.

In the development of the digital safety system, the following technologies are used to make the system reliable, traceable and transparent, which helps make V&V feasible and reliable.

2.2.3.1 Logic processing by single task

To avoid complexity and maintain software traceability, and to simplify V&V of processing timing and response time, the logic calculation by POL is executed as a single program, generally called a task in real time application. POL is a kind of software language but does not require software coding which is generally required when using software languages like C, PL/M, ADA, etc. POL directly interprets or compiles graphically represented logic charts that define the required logic calculation, and executes it. This feature enables visual software design, programming and verification, and makes these processes transparent as for analog systems in which logic charts and relay circuit diagrams are used for design and verification.

2.2.3.2 Avoidance of external interrupts

To avoid complexity and maintain software traceability, there is no signal processing by external interrupts.

2.2.2.3 Logic representation for fail-safe

The fail-safe concept is applied to RPS (Reactor Protection System) and ESF (Engineered Safety Feature). In this concept, loss of control signal to the actuator leads to initiation of protective action of the actuator. To maintain fail-safe capability, reverse logic representation is used, where the state which leads to the activation of the target system is represented as ‘0' i.e. 'FALSE', while the state which does not lead to the activation is represented as ‘1' i.e. 'TRUE'. In this representation, for example, 'OR' logic in normal representation is calculated by 'AND', and 'AND' logic is calculated by 'OR'. If the result of the logic calculation is 'TRUE', control signal to the actuator is kept 'ON'. Control signal is set to 'OFF' if the result is 'FALSE', which initiates the activation of the protective action.

For logic processing in ESF, the fail-as-is concept is applied and normal logic representation is used. A control signal causes activation when it is 'ON', and holds as is when a failure occurs.

2.2.3.4 Graphical program language: POL

The graphical program language or Problem Oriented Language called POL is used for the software of the digital safety system. POL enables graphical description of the software using a logic diagram. Fig. x shows the outline of POL. The logic diagram used in POL is called Software Diagram (SD) and has the form shown in the top of Fig. 2.2-5.

The SD can be built or edited on a CRT display using CAD. It contains information on input/output signals and their logic combination required for determining whether protective action should be initiated. In building the SD, variable numbers are assigned for signals, and operation numbers and operation codes are assigned for logic operations (i.e. AND OR, NOT, etc.). Variable numbers, operation numbers, operation codes and their connections are stored in a storage device as program data. Once the SD is drawn by CAD, POL directly reads out the data and understands which logic operation should be carried out to which signals. Before executing the logic calculation, POL rearranges the data so that the calculation is consistently performed from input to output. After rearranging the order of the calculation, POL stores the rearranged data and executes the calculation. Thus, POL does not require logic program coding as when using program languages such as C, PL/M, etc. In POL, software coding means building a SD visually using CAD. The CAD function for building and editing the SD can be installed together with POL to the digital safety systems or can be separately installed in a different computer system. The maintenance tool hooked up to the digital safety system can be used on-line display and editing of the SD. POL can display the running status of the software in the SD displayed on the terminal of the maintenance tool. POL enables visual programming and checking of the software, which helps maintain software traceability and transparency and makes the V&V feasible and reliable. The feature makes design and verification similar to those of analog systems in which logic charts and relay circuit diagrams are used for design and verification. PLO was selected based on this feature and fossil power plants, in the belief that the possibility of design errors and common mode failures can be reduced.

Logic calculation by POL is performed as a single task. This task runs periodically for short time intervals. An independent self-diagnosis function is installed to monitor execution of the task and to detect failures such as memory error, communication error, microprocessor error and so on. If the task cannot run for a pre-determined time or a failure is detected, the self-diagnosis function brings the system to a safe-state: i.e. the output signal is forced into the state in which protective action takes place. In V&V, to assure the system response time, the time from the change of input signal to the change of output signal was measured and confirmed.

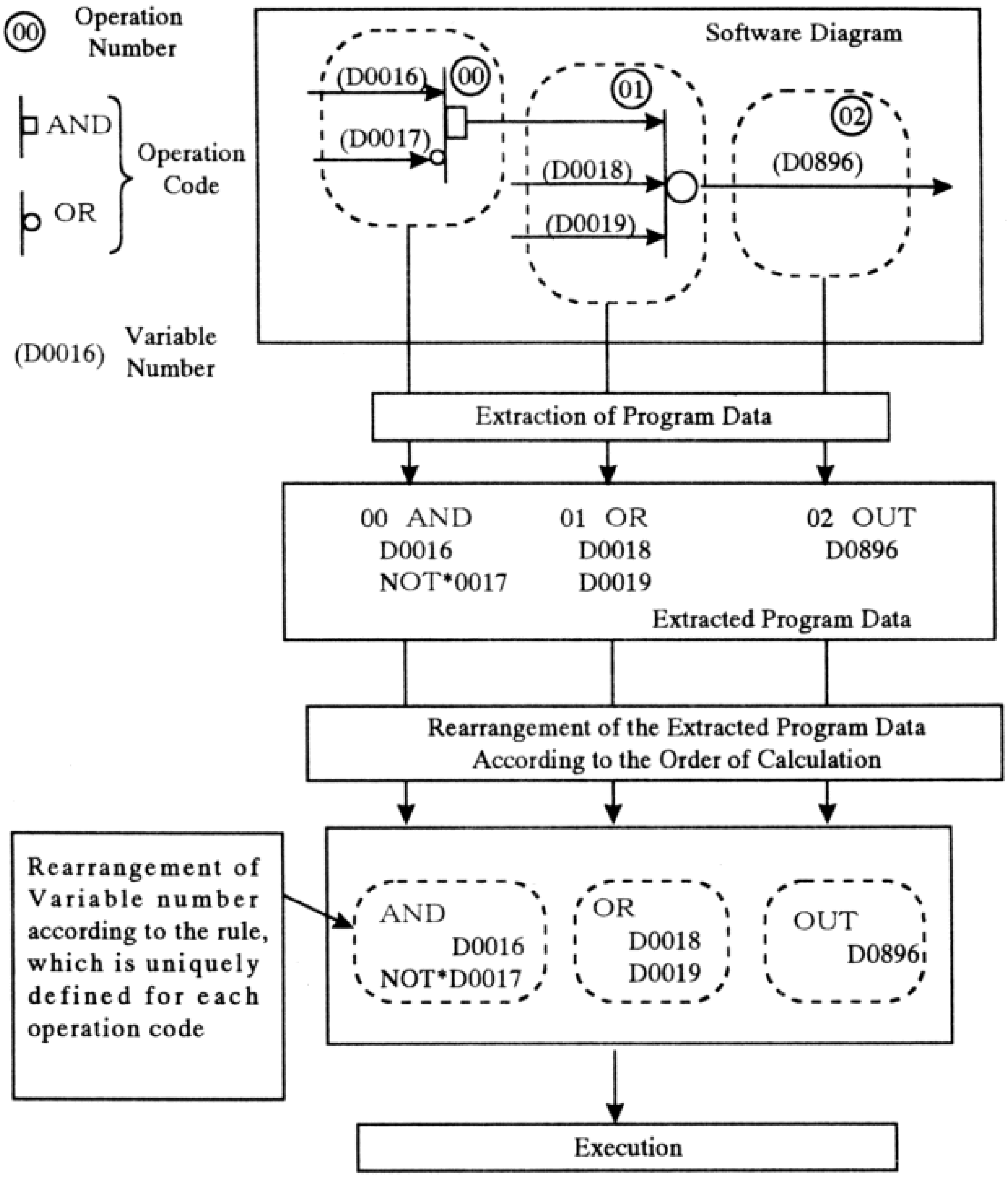


Fig. 2.2-5 Outline of graphical program language POL

2.2.4 Verification and validation (V&V) of digital safety systems

V&V performed for the digital safety systems of the Kashiwazaki Kariwa Unit 6 of the Tokyo Electric Power Co., Inc. is discussed.

The reliability of software based safety system is a significant issue. Guidelines or standards such as IEEE 7-4.3.2 (1993), IEC88O (1986) have been published for applying software based digital safety systems to nuclear power plants. These documents address the issues on reliability of software based safety systems and define requirements for hardware software design, manufacturing, verification and validation (V&V) procedures, documentation, maintenance and so on. In Japan, JEAG4609 (1989) requires V&V as a measure of software based safety system reliability.

The basic requirements for V&V in JEAG4609 are summarized as follows.

(a) Verification and Validation (V&V) procedures should be performed and the results should be well documented in an auditable manner.
(b) V&V should be performed by a team or personnel independent of the design and manufacturing team.
(c) V&V should cover all steps in system design and manufacturing from design to final test.
(d) A V&V plan should be prepared and the V&V should be carried out on that basis.

Fig. 2.2-6 shows basic flow of V&V procedures. Verification should be carried out at each step in system design and manufacturing. At each verification step, it should be verified that the results of that step meet the requirements.

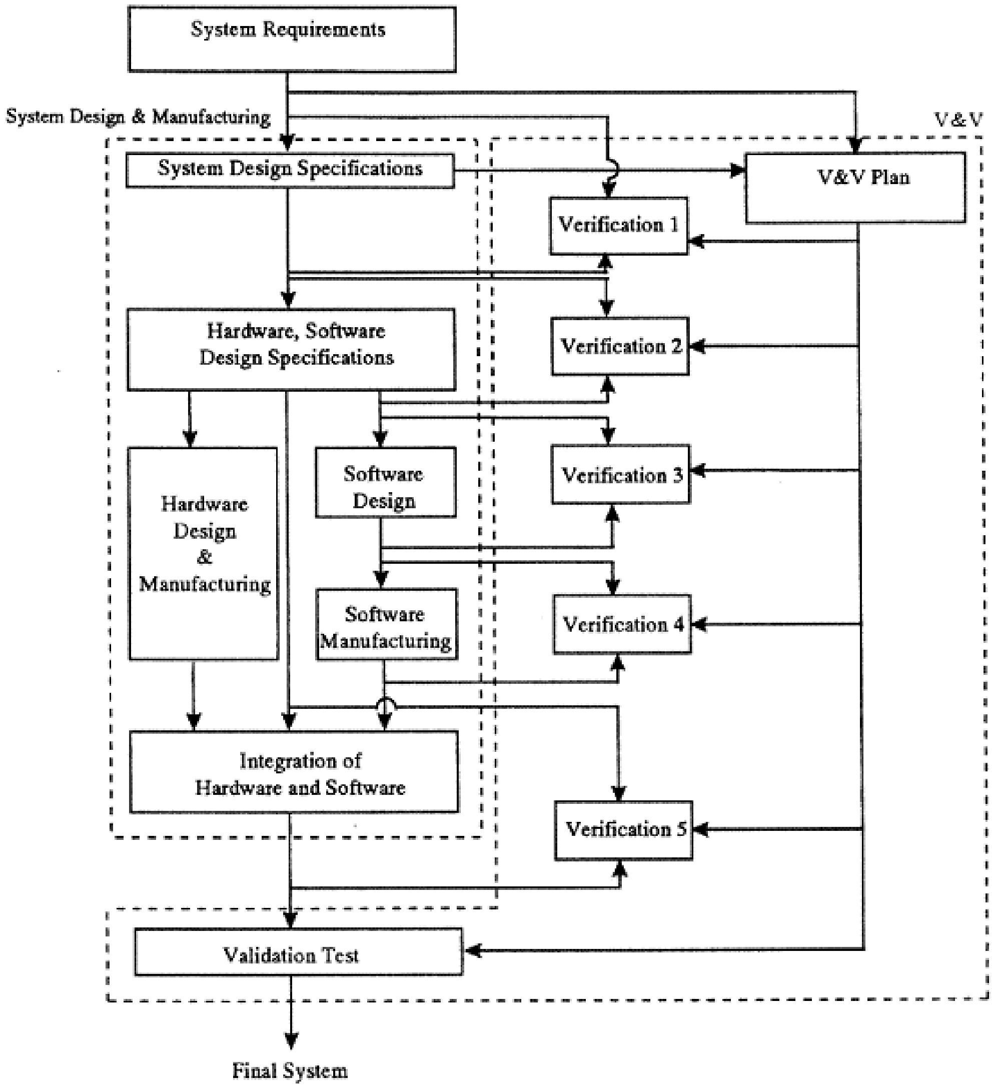


Fig. 2.2-6 Basic flow of V&V

Table 2 summarizes the steps, documents and methods used in the V&V of the digital safety system. According to the basic outline of the V&V defined by the guideline (JEAG4609), the following steps were taken.

<u>Step I: Verification of the system specification (verification 1)</u>

The system specification is the most basic document, defining the principal specifications of the digital safety system. The first step of V&V is to verify the system specification. This is done by examining the consistency of the system specification with upper documents such as Safety

Analysis Report and various regulatory standards and guidelines.

Step 2: Verification of the software design specification (verification 2)

The second step of V&V is to verify the software design specification, that is, the logic design specification. A document called interlock block diagram (IBD) is used to specify the primary logic required for the digital safety system. The IBD has the form shown in Fig. 2.2-7. The logic design is verified by confirming that the logic described in the IBD meets the requirements of the system specification.

Step 3: Verification of the software design and manufacturing (verification 3 and 4)

With POL, software can be designed and manufactured using the SD (Software Diagram). Once the SD is designed, POL understands the program data defined by the SD and executes them. POL also displays the logic status inside the system in the SD. Therefore, verification steps 3 and 4 for software design and manufacturing can be integrated as single verification step, which helps simplify the verification of software design and manufacturing. The software design and manufacturing is verified by checking that the SD displayed by POL has no discrepancy with the IBD. All passes in the SD are verified by visually marking every pass in the displayed SD one by one.

Step 4: Verification of software installation (verification 5)

The verification at this step is to verify that the software is properly installed in the target system. In POL, the software, i.e. rearranged program data, is stored in ROM. The verification is performed by comparing binary bit patterns of the ROM with the original data for the SD.

Step 5: Validation test

The validation test is the final V&V step and aims to validate that the system works correctly and reliably. The validation test consists of the following:

I/O matrix test;
Instrumentation loop test;
System logic test;
System failure test; and
System response time test.

In the validation test, each unit of the safety system is first tested independently using signal simulators and the maintenance tool. For test inputs, the response of each unit is confirmed step by step, checking all passes in the SD that is displayed on the screen of the maintenance tool. After the independent test, the total system test is carried out using the automatic test tool. In this test, the response of the whole system (i.e. the status of initiation signal for protective action) is confirmed against test input signals.

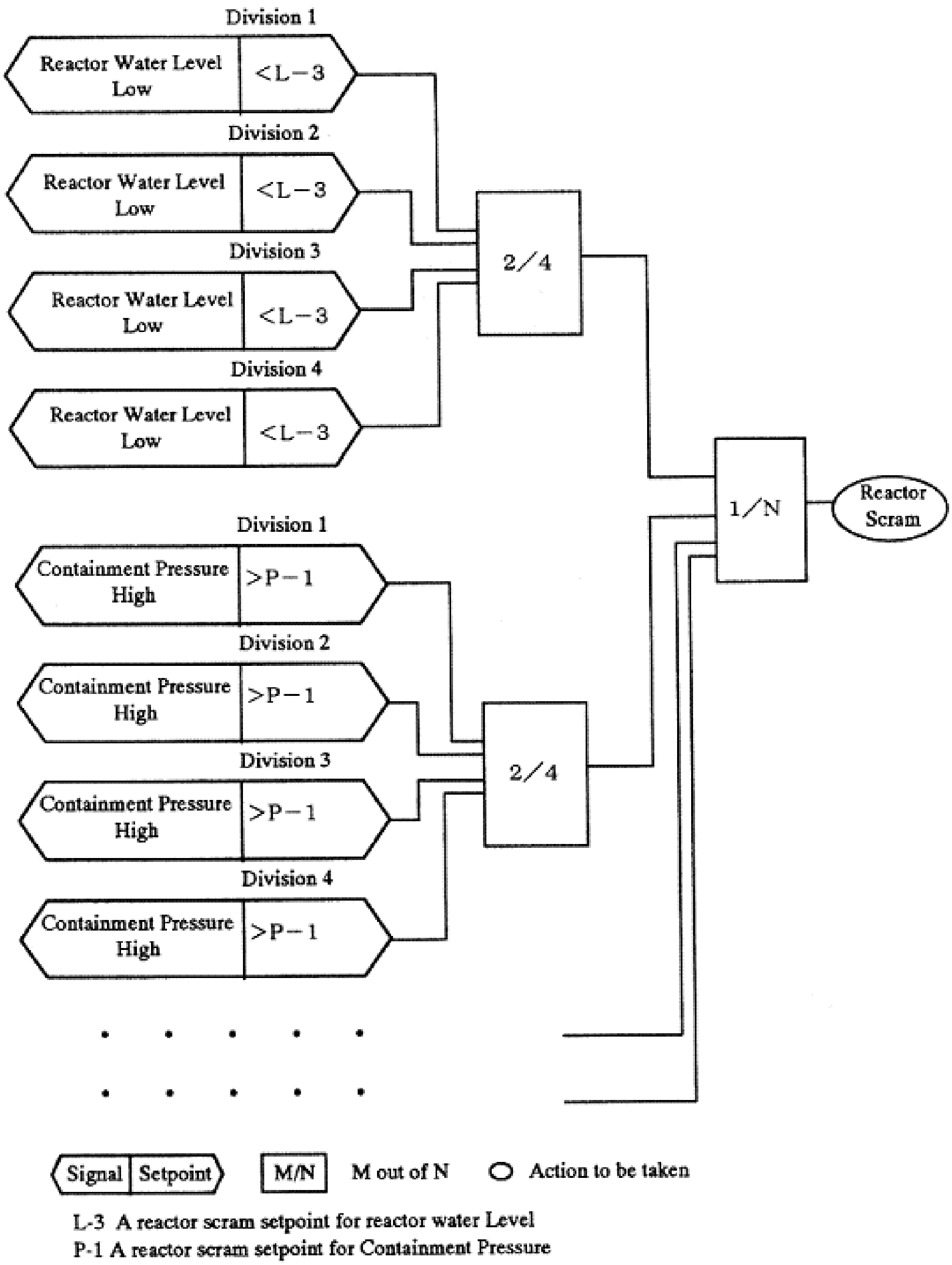
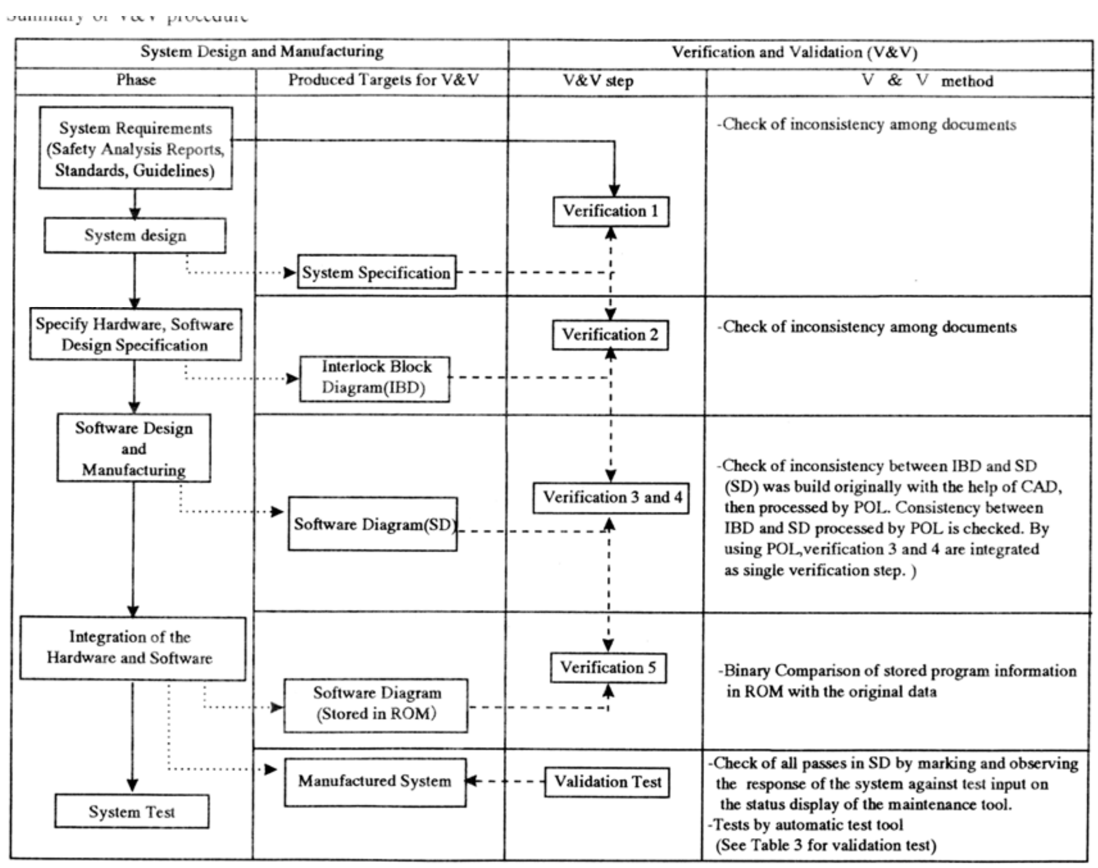


Fig. 2.2-7 Outline of interlock block diagram

Table 2 Summary of V&V activities



2.2.5 Summary

The digital safety protection systems for which the above-mentioned measures to improve the software reliability were taken have been applied to the Kashiwazaki Kariwa Nuclear Power Station Unit 6 (commercial operation started in 1997) and Unit 7(commercial operation started in 1998) of the Tokyo Electric Power Co., Inc., and the Hamaoka Nuclear Power Station Unit 5 (commercial operation started in 2005) of Chubu Electric Power Co., Inc. All of these are ABWR. In addition, for PWR, the digital safety protection systems have been applied to the Tomari Nuclear Power Station Unit 3 (under construction) of Hokkaido Electric Power Co., Inc. It is obvious that digital safety protection systems will be applied to nuclear power plants to be built in the future. It is because safety protection systems using circuits composed of analog instruments and relays with relay contacts is difficult to realize from various reasons, such as securing their parts, cost, and preservation of manufacturing and maintenance personnel. And, an application of digital technology can be said a logical conclusion also in the light of its functional superiority. Therefore, it is necessary to make efforts to solve the issues in applying digital technology to safety protection systems. And, as there exist its actual performance, it is necessary to closely study the application processes, related standards and experiences, and make efforts to apply them to nuclear power plants in your own country.

3. Main Control Room

3.1 Background of Main Control Room Improvement

The shock of the Three Mile Island (TMI) accident which took place on March 28, 1979, at unit 2 of the American nuclear power plant, was considerable, and many lessons were learned. As one of the important lessons learned, we shall mention the control room improvement. At the accident the operators were very confused and it led into errors of judgment on plant operation status. Core temperature indicators whose range wasn't wide enough went to their limit and held there. The operators thought they were broken. The operation computer, saturated with data, blocked and was inoperable for 2 hours. Finally, the control room itself was described as looking like a Christmas tree or a fairground. Very many alarms were lit or flashing. The various pre-alarms, alarm and alert sound signals were operating.

At first, the reactor was operating at nominal power. Its emergency shutdown, plus the difficulties of the secondary system, caused status change in many systems and parameters, all of which set off an alarm. There was no prioritization enabling initial alarm-provoking conditions to be distinguished from their normal consequences. This situation was of no helps to the operators.

The observations made at the TMI plant have an essential role in the design of future control rooms, but the most important points have also been corrected on operating plants or those being constructed.

Information presentation was improved, including in particular the elimination of command rather than state indications. Certain measurement or indication ranges were widened. New indicators were added, such as the primary coolant boiling monitors (showing the difference between the actual temperature of primary coolant and the boiling point at primary system pressure). Alarms have been prioritized. The most essential information is now shown on the safety panel.

As one of lessons learned from the TMI-2 accident, the NRC has recommended upgrading of a control room with NUREG-0700 "Human-System Interface Design Review Guidelines". NUREG-0700 provides detailed human-system interface upgrading measures in a control room based on the root cause analysis on the confusion which occurred in the main control room of TMI-2. This is the document that persons engaged in design and evaluation of a control room should look over.

3.2 Control Room Upgrade in Japan

Prompted by the TMI-2 accident, a control room design to improve information displays which might give misunderstanding to operators and controllers making operators susceptible to a mistake, that is, human-centered human engineering design has been taken up as a key issue, and the improvements have been made to the plants in operation and under construction in Japan.

The control rooms in Japan in 1997 when the accident took place were equipped with indicators for instrumentation and control devices using analog technology and switches with handle as described in “Phase 1 of Part 3, Historical Transitions of Main Control Rooms of Nuclear Power Plants in Japan, which Digitization Brought about” of the introductory section. The design of the details is unique to Japan, but as a whole they belong to the almost same type as that of TMI-2, and if the same event as one occurred at TMI-2 had happened in Japan, the same situation could have occurred in the control room. Also in Japan, the control room upgrade has been made incorporating lessons learned from the TMI-2 accident. For example, various upgrades such as better alarm layout to distinguish important alarms from general ones to improve alarm situation like a Christmas tree, rearrangement of the instruments to display important parameters such as reactor power and reactor pressure, making them easy to notice, and additional functions to graphically display operating status of safety systems using a computer, have been applied to the operating plants during periodical inspections. The instrumentation and control systems of the control room belonging to Phase 1, to which analog technology was originally applied, have been upgraded with the human engineering design prompted as one of lessons learned from the TMI-2 accident as much as possible, and those upgraded plants are performing satisfactorily nowadays.

For nuclear power plants which started their commercial operations in 1986 to1996, described in “Phase 2 of Part 3” of the introductory section, upgrades with human engineering design submitted as one of lessons learned from the TMI-2 accident were reflected in the plants at their plant design stage. That is, the upgrades were applied from the beginning such that, even if a difficult situation like the TMI-2 case occurred, operators could make their coolheaded judgment and perform well-informed operational actions. At the Phase 2, systems to display the information processed with a plant computer (process computer) on cathode ray tubes were applied substantially. The plant computer mainly served as a simple data logger at the early stage, but according to the computer processing speed improvement, it came to perform general information display functions other than safety system control functions, and to perform the functions monitoring plant operation conditions. In addition, at this phase, analog technology remained for the safety system control functions.

Digital systems for safety system control functions were applied to the plants that started operations in 1997 and afterwards, described in “Phase 3 of Part 3” of the introductory section. With digital system application to safety system control functions, digitization of all instrumentation and control systems was achieved. The introductory section explained that the control room configurations have changed substantially by this application. Control rooms of nuclear power plants to be built from now on will be designed based on the Phase 3 type. So, the latest control room will be discussed below.

3.3 The Latest Main Control Room

The ABWR control room is introduced as an example of the latest main control rooms. The nuclear power plant is centrally controlled in the main control room, and the panel layout of the control room where operators perform monitoring and operational actions is given in Fig. 3-1.

The operator console (1) is designed so that operational actions at normal plant start-up and shutdown and monitoring and operational actions during plant steady-state operation can be performed there. When starting or shutting down a plant, many actions, such as start and stop of systems and components including control rods operation, are required, and one operator will concentrate on those actions. On the other hand, when the operator concentrates on those actions, it is necessary to prevent the operator from paying scant attention to monitoring the whole plant. Therefore, the monitoring large panel (2) for monitoring the plant as a whole in a balanced manner is provided. Plant operation crews vary depending on the operation management system of each electric utility, but in general, 3 shifts of crews consisting of about 7 or 8 persons per crew perform plant operation.

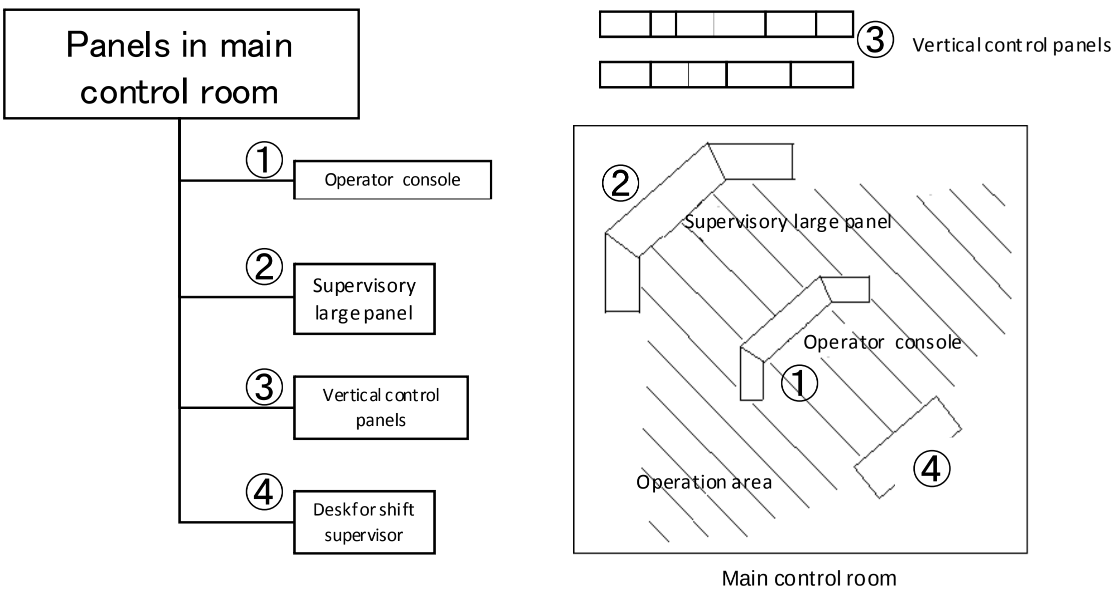
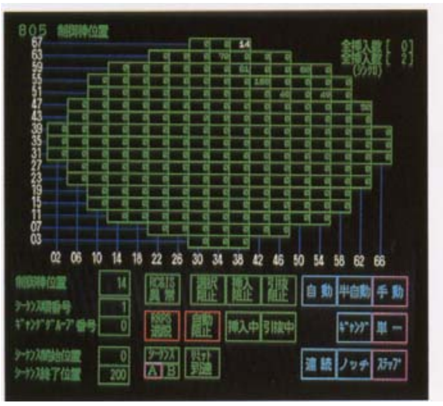


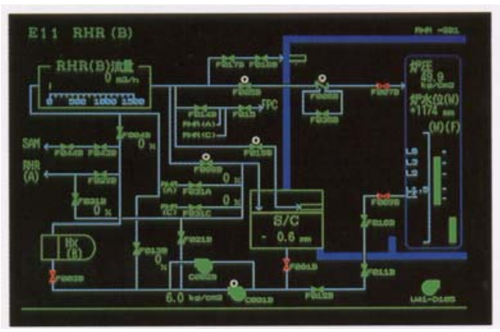
Fig. 3-1 Panel layout in main control room

The operator console (refer to Pictures 4 and 5 in the introductory section) is approximately 5 m wide and approximately 1.5 m high, and an operator can perform operational actions sitting down there. The monitoring large panel can be looked at from the sitting position. Seven CRTs (image display devices), 17 FDs (flat displays) of color liquid crystal, and hard switches are arranged on the operator console. Information necessary for operation is organized on approximately 500 screens, which is possible to look at on any CRT, in such a hierarchical and easy way to understand, and touch operation is possible on CRTs and FDs for individual operation of pump or valve. The upper part of Picture 6 shows the CRTs. The display screens of CRTs are given in Picture 7 and 8. Picture 7 is a screen to display an insertion and withdrawal state of control rods, and conditions for operating control rods. Picture 8 is a screen to display the operating state of the residual heat removal system, as an example.

Picture 6 Overall view of operator console (upper: CRT, lower: FD)



Picture 7 Display for operation interlock and control rod positions



Picture 8 Display of the Residual Heat Removal system

The monitoring large panel is intended to permit all members of an operation crew to always share the information of plant operating conditions. It consists of an important alarm display board to display important alarms at the plant level, a large mimic panel to display the plant conditions as a whole with LEDs in an easy way to understand, and a large-screen display to show the major parameters and trend of the plant. In addition, the alarm summary to display the conditions (serious failure / minor failure / change of state) of 120 or so systems constituting the plant in three colors (red / yellow / green) is provided on the upper part of the large mimic panel. On the right-hand side, the large-screen display using a 110-inch high-definition backlight-type projector is provided, on which trends of plant major parameters are automatically displayed at a plant abnormal event. During normal operation, operators can freely switch the screen to look at system drawings or various parameters to monitor plant-operating conditions.

Vertical control panels housing controllers to perform control and signal transmission functions consist of more than 100 control panels. As an example, a picture of a panel to control the turbines and generator and perform protective functions is shown in Fig. 1-2. Thus, there are various control panels ranging in functions for an emergency reactor shutdown to air-conditioning in the main control room.

3.4 Summary

The latest control rooms in Japan are explained as in the above. When newly planning and designing a control room, it is necessary to at least understand the design requirements for the control room. In Japan, the lessons learned from the TMI-2 accident were seriously taken, and the upgrading of the control rooms of operating plants was conducted first. In parallel to the upgrade, design changes to the control rooms of plants under construction, incorporating human-system interface with the maximum utilization of computer technology were made. To the control rooms of the plants under planning, user-oriented and newly planned designs reflecting the operational experiences and operators' opinions till then were performed together with digitization of safety protection systems. Plant operations were reproduced with full-scale control panels connected to a simulator to simulate plant behaviors, and the control rooms were designed reflecting the results. When a country builds a new power plant, it is considered that these experiences in Japan are useful.

Based on these experiences, it is necessary to proceed the planning and design according to the conditions of each country. It is necessary to plan a control room based on comprehensive perspective instead of merely seeking the latest control room. For example, it should be also taken into consideration how operator training should be conducted. That is, the point is to recruit and train personnel to be engaged in nuclear power plants.

References

１） Nuclear Engineering International, January 1988

２） Toshiba brochure on nuclear power plants

３） BWR Operator Training Center Web Site

４） Nuclear Power Training Center Ltd. Web Site

５） Safety Standards Series No. NS-G-1.3 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants IAEA

６） Safety Standards Series No. NS-R-1 Safety of Nuclear Power Plants: Design IAEA

７） "A Verification and Validation Method and Its Application to Digital Safety Systems in ABWR Nuclear Power Plants", A. Fukumoto, T. Tomizawa, Nuclear Engineering and Design (1998)

８） Japan Electrical Society, 1989. JEAG4609, Guidelines for Application of Digital Computer to Safety Protection System

９） International Electrotechnical Commission, 1986. IEC Standard Publication 880, Software for Computers in the Safety Systems of Nuclear Power Plants

１０） Institute for Electrical and Electronics Engineers, 1993. IEEE Std. 7-4.3.2-1993, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Plants

１１） Human-System Interface Design Review Guidelines (NUREG-0700, Rev. 2)