



Agenzia Nazionale per le Nuove Tecnologie,  
l'Energia e lo Sviluppo Economico Sostenibile



*Ministero dello Sviluppo Economico*

## RICERCA DI SISTEMA ELETTRICO

Analysis of the dynamics of supervision, control and protection  
systems in pressurized water reactors of evolutive generation

*Stefano Di Gennaro, Bernardino Castillo*



ANALYSIS OF THE DYNAMICS OF SUPERVISION, CONTROL AND PROTECTION SYSTEMS IN  
PRESSURIZED WATER REACTORS OF EVOLUTIVE GENERATION

Stefano Di Gennaro, Bernardino Castillo (Università dell'Aquila)

Novembre 2011

Report Ricerca di Sistema Elettrico

Accordo di Programma Ministero dello Sviluppo Economico – ENEA

Area: Governo, gestione e sviluppo del sistema elettrico nazionale

Progetto: Fissione nucleare: metodi di analisi e verifica di progetti nucleari di generazione evolutiva ad acqua pressurizzata

Responsabile Progetto: Massimo Sepielli, ENEA

**Titolo**

**Analysis of the dynamics of supervision, control and protection systems in pressurized water reactors of evolutive generation**

**Ente emittente** Università di L'Aquila – Centro di Eccellenza DEWS

## PAGINA DI GUARDIA

**Descrittori**
**Tipologia del documento:**

**Collocazione contrattuale:** ACCORDO DI PROGRAMMA Ministero dello Sviluppo Economico – ENEA sulla Ricerca di Sistema Elettrico PIANO ANNUALE DI REALIZZAZIONE 2010 Progetto 1.3.2.a: Fissione nucleare: Metodi di analisi e verifica di progetti nucleari di generazione evolutiva ad acqua pressurizzata.

**Argomenti trattati:** **Controllo dei reattori nucleari, reattori nucleari ad acqua.**



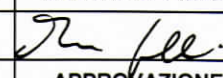
**Sommario**

Il presente lavoro, sviluppato dal gruppo del Prof. Stefano Di Gennaro del Centro di Eccellenza DEWS dell'Università degli Studi dell'Aquila, si concentra sui sistemi di controllo per i reattori nucleari ad acqua pressurizzata, e si articola secondo tre deliverables.

Il presente documento, dal titolo "Analisi della dinamica dei sistemi di supervisione, controllo e protezione in reattori ad acqua pressurizzata di generazione evolutiva", offre una presentazione dettagliata dei sistemi di supervisione, controllo e protezione per il circuito primario di reattori ad acqua in pressione di generazione III/III+.

Negli altri due rapporti sono descritti, rispettivamente, la modellizzazione matematica del circuito primario del reattore, allo scopo di individuare le proprietà dei controllori impiegati e valutarne le prestazioni anche in risposta a perturbazioni esterne o interne, e uno studio delle prestazioni dei sistemi di controllo in presenza di guasti e/o incidenti di riferimento nei reattori evolutivi ad acqua in pressione sulla base di un modello più accurato del pressurizzatore.

**Copia n.**
**In carico a:**

2			NOME			
			FIRMA			
1			NOME			
			FIRMA			
0	EMISSIONE		NOME	Mauro CAPPELLI	Emanuele NEGRENTI	Massimo SEPIELLI
			FIRMA			
REV.	DESCRIZIONE	DATA	CONVALIDA	VISTO	APPROVAZIONE	



CENTER OF EXCELLENCE DEWS  
DEPARTMENT OF ELECTRICAL AND INFORMATION ENGINEERING

UNIVERSITY OF L'AQUILA, V. G. GRONCHI 18, 67100, L'AQUILA, ITALY

DELIVERABLE 1

---

***Analysis of the Dynamics of Supervision, Control and Protection  
Systems in Pressurized Water Reactors of Evolutive Generation***

---

***Analisi della dinamica dei sistemi di supervisione, controllo e protezione in reattori  
ad acqua pressurizzata di generazione evolutiva***

---

*Authors:*  
Stefano DI GENNARO and Bernardino  
CASTILLO-TOLEDO

*Principal Investigator:*  
Prof. Stefano DI GENNARO

Project PAR 2010  
June 30, 2011

---

***Abstract***

In this deliverable the supervision, control, and protection systems for the primary circuit of pressurized water reactors of evolutive generation are described and analyzed. The main components of the primary circuit, the reactor, the pressurizer, and the steam generators, are analyzed. More in particular, the pressurizer is treated in more detail, due to its important role of maintaining the primary circuit pressure within a specified range. The pressurizer design objectives, its main characteristics, the thermal hydraulics, the connections to the reactor cooling system, the surge line, the water level and pressure controls, the pressure sensors, etc., are studied. Finally, the main control room and the satellite control rooms are described and analyzed, in particular with respect to the signals from/to the primary circuit and, mainly, from/to the pressurizer.

---

***Riassunto***

In questo lavoro sono descritti e analizzati i sistemi di supervisione, controllo e protezione per il circuito primario di reattori ad acqua pressurizzata di generazione evolutiva. Vengono analizzati i principali componenti del circuito primario, il reattore, il pressurizzatore, e generatori di vapore. Più in particolare, il pressurizzatore è trattato più in dettaglio, in considerazione del suo importante ruolo nel mantenere la pressione del circuito primario all'interno di un intervallo specificato. Vengono studiate le specifiche progettuali del pressurizzatore, le sue caratteristiche principali, l'impianto idraulico termico, i collegamenti al sistema di raffreddamento del reattore, la surge line, i controlli di livello dell'acqua e della pressione, i sensori di pressione, etc. Infine la sala di controllo principale e le sale di controllo satelliti sono descritte e analizzate, in particolare per quanto riguarda i segnali dal/al circuito primario e, soprattutto, dal/al pressurizzatore.

---

# 1 Introduction

A nuclear power plant is an electric generating station with one or more reactors. Like all conventional thermal power plants, it consists of a steam supply system that converts water into steam. The steam drives a turbine, which in turn drives a generator, producing electricity.

In Pressurized Water Reactors (PWRs), such as the EPR power plant, ordinary light water is utilized to remove the heat produced inside the reactor core by the nuclear fission phenomenon. This water also slows down, or moderates, neutrons. Slowing down neutrons is necessary to sustain the nuclear reaction.

The heat produced inside the reactor core is transferred to the turbine through the steam generators. Only heat is exchanged between the reactor cooling circuit (primary circuit) and the steam circuit used to feed the turbine (secondary circuit). No exchange of cooling water takes place.

The primary cooling water is pumped through the reactor core and the tubes inside the steam generators, in four parallel closed loops, by coolant pumps powered by electric motors. Each loop is equipped with a steam generator and a coolant pump.

The reactor operating pressure and temperature are such that the cooling water does not boil in the primary circuit but remains in the liquid state. A pressurizer, connected to one of the coolant loops, is used to control the pressure in the primary circuit.

Feedwater entering the secondary side of the steam generators absorbs the heat transferred from the primary side and evaporates to produce saturated steam. The steam is mechanically dried inside the steam generators then delivered to the turbine. After exiting the turbine, the steam is condensed and returned as feedwater to the steam generators. A generator, driven by the turbine, generates electricity.

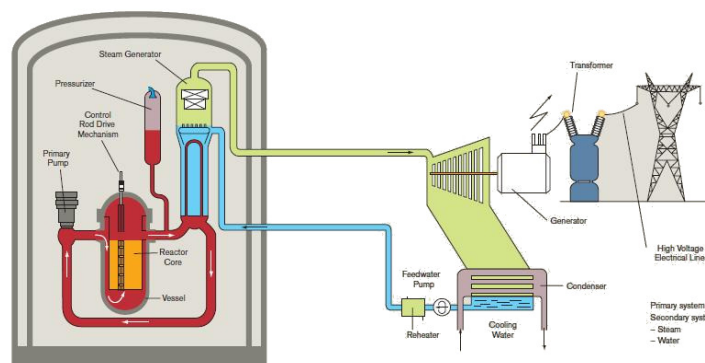


Figure 2: A Pressurized Water Reactor scheme

This work is focused on the supervision, control and protection of the primary circuit. The main components of the primary circuit are the reactor, the pressurizer, and the steam generators. More in particular, we will consider the pressurized whose main role, as it will be more widely explained in the following section, is to maintain the primary pressure within a specified range.

For the reader's convenience, in Table 1 the main abbreviations used in this deliverable are summarized.

ACC	accumulator	AOO	anticipated operational occurrence	AOP	abnormal operating procedure
APWR	advanced pressurized water reactor	BISI	bypassed and inoperable status indication	CCF	common cause failure
CCW	component cooling water	CCWS	component cooling water system	CFR	Code of Federal Regulations
CFS	condensate and feedwater system	COL	Combined License	COM	communication system
CPU	central processing unit	CRDM	control rod drive mechanism	CS	containment spray
CS/RHR	containment spray/residual heat removal	CSS	containment spray system	C/V	containment vessel
CVCS	chemical and volume control system	DAAC	diverse automatic actuation cabinet	DAS	diverse actuation system
DCD	design control document	DCS	data communication system	DHP	diverse HSI panel
DNB	departure from nucleate boiling	ECCS	emergency core cooling system	EFW	emergency feedwater
EFWS	emergency feedwater system	EOF	emergency operations facility	EOP	emergency operating procedure
EPG	emergency procedure guideline	ERDS	emergency response data system	ESF	engineered safety features
ESFAS	engineered safety features actuation system	ESWS	essential service water system	GDC	General Design Criteria
GTG	gas turbine generator	HEPA	high-efficiency particulate air	HFE	human factors engineering
HSI	human-system interface	HSIS	human-system interface system	HVAC	heating, ventilation, and air conditioning
I&C	instrumentation and control	IEEE	Institute of Electrical and Electronics Engineers	LDP	large display panel
LOCA	loss-of-coolant accident	LOOP	loss of offsite power	MCR	main control room
MELTAC	Mitsubishi Electric Total Advanced Controller	MFW	main feedwater	MOV	motor operated valve
MSS	main steam supply system	NIS	nuclear instrumentation system	NRC	U.S. Nuclear Regulatory Commission
NUREG NRC	Technical Report Designation (Nuclear Regulatory Commission)	OC	operator console	PA	postulated accident
PAM	post accident monitoring	PCMS	plant control and monitoring system	PRA	probabilistic risk assessment
PSMS	protection and safety monitoring system	QA	quality assurance	RCP	reactor coolant pump
RCS	reactor coolant system	RG	Regulatory Guide	RHR	residual heat removal
RHRS	residual heat removal system	RMS	radiation monitoring system	RPS	reactor protection system
RSC	remote shutdown console	RSR	remote shutdown room	RT	reactor trip
RTB	reactor trip breaker	RTP	rated thermal power	RV	reactor vessel
SBLOCA	small break loss-of-coolant accident	SG	steam generator	SGTR	steam generator tube rupture
SLS	safety logic system	SPDS	safety parameter display system	SRP	Standard Review Plan
SSA	signal selection algorithm	Tavg	average temperature	TSC	technical support center
UHS	ultimate heat sink	UPS	uninterruptible power supply	V&V	verification and validation
VDU	visual display unit				

Table 1: Acronyms and abbreviations list

## 2 The main components of a pressurized water reactor

In this section we briefly describe the principal components of the primary circuit of a PWR. To this aim, we will refer to the European Pressurized water Reactor (EPR). The main components of the EPR are described in [58]. The primary components and the loop arrangement, see Fig. 3, are very close to those of operating plants. Some changes have been introduced

1. to improve the economy of the project;
2. to better satisfy utility needs regarding operation and maintenance;
3. to comply with new recommendations from the Franco–German Safety Authorities.



Figure 3: EPR main primary components

The main components feature an increase in size compared to existing designs. This provides longer grace periods in a number of transients and postulated accident sequences.

The larger water inventory in the reactor pressure vessel between reactor coolant loops and the top of the core provides a longer grace period in Loss of Coolant Accident (LOCA) sequences and under shutdown conditions, in particular during mid-loop operation.



Enlarging the pressurizer volume provides benefits regarding smoothening transients and reduction of reactor trip probability. Under Anticipated Transient Without (reactor) Trip (ATWT) conditions, the large pressurizer volume reduces the pressure transient. A larger pressurizer volume enables a better staggering of pressure and water level limits, so that countermeasures actuated by one set–point are more effective.

Increasing the steam generator volume on the secondary side is beneficial with regard to steam generator tube rupture scenarios by extending the time when the affected steam generator is filled up by coolant transfer from primary to secondary side.

Furthermore, the dry out time in case of a loss of all feedwater supply is now significantly longer than 30 min, thus giving ample time for appropriate countermeasures.

The steam generator tube rupture as well as the other accidental transients will be dealt with a physical state oriented approach which minimizes the risk of operator error.

## 2.1 Primary components

### 2.1.1 Reactor pressure vessel

The Reactor Pressure Vessel (RPV, see Fig. 4) is designed for a 241  $17 \times 17$  fuel assembly core and a lifetime of 60 years. The material is the standard Mn–Mo–Ni alloy but with a more stringent specification as far as impurities are concerned, to have a higher beginning of life toughness.

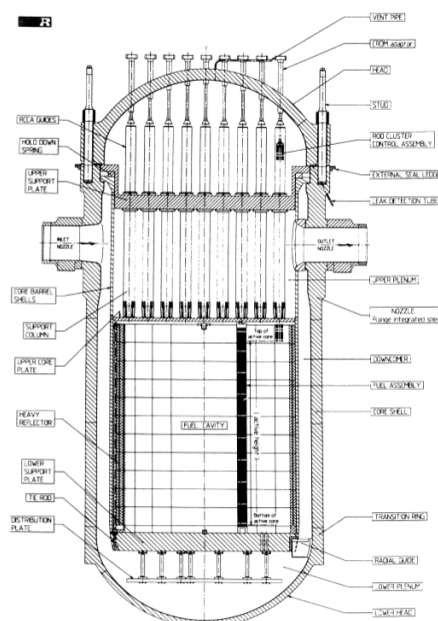


Figure 4: EPR reactor pressure vessel and RPV internals

The target for the core shell fluence after 60 years is  $1019 \text{ n cm}^{-2}$  to conservatively meet the  $RT_{\text{NDT}}$

end of life<sup>1</sup> specified at 30°C. This design objective meets the request of the Safety Authorities to have a low fluence.

This is achieved by a large downcomer between the reactor vessel coreshell and the core barrel.

The RPV upper part is made of a nozzle shell and a flange machined from one single forging. The inner diameter of the flange is machined to form the ledge supporting the internal structures of the reactor (internals and core). The flange contains threaded holes for the closure studs, and its top surface is clad with stainless steel, machined to provide a surface suitable for metal ring seals.

The nozzle shell has eight penetrations for the main coolant nozzles. At its lower end the nozzle shell is tapered to allow the nozzle/core shell weld to be made in a region of uniform thickness. The nozzles are separate forgings, welded onto the vessel according to a set-on design.

The nozzles are located as high as practicable above the core top in order to increase the hydrostatic pressure for reflooding, to maximize the water inventory above the core. The RPV rests on a support ring through support pads located underneath the nozzles. Radial expansion is free. As there is a need to prevent the vessel uplifting in an unacceptable manner in the event of a postulated severe accident, the support hardware is double-acting.

The RPV lower part is made of two core shells, a transition ring and the lower head dome. Radial guides are welded on the inside surface of the transition ring to center the lower internals and ensure the secondary support function of the internals.

The in-core instrumentation is top mounted. There is no penetration through the main body of the vessel below the main nozzles.

The closure head consists of two pieces welded to each other

1. The head flange is a ring forging with holes for the closure studs;
2. The dome head is a part-spherical form forged piece penetrated by adaptors for control rod drives, instrumentations, and the vent pipe.

The Control Rod Drive Mechanisms (CRDMs) are flanged to the adaptors and easily removable. The same principles are used for the instrumentation adaptors.

## **2.2 Reactor internals**

The Reactor Pressure Vessel Internals (RPVI) consist of two substructures (see Fig. 4)

1. The lower internals, which support the fuel assemblies from underneath. The core barrel flange at the upper end of the core barrel rests on a ledge machined from the RPV flange. The core support plate, on which the fuel assemblies are directly resting, is a thick perforated forging welded to the core barrel.

---

<sup>1</sup>RT<sub>NDT</sub> is the reference temperature for a reactor vessel material, under any conditions. For the reactor vessel bellline materials, RT<sub>NDT</sub> must account for the effects of neutron radiation.

The space between the polygonal outside shape of the core and the cylindrical inner surface of the core barrel is filled with a stainless steel structure to reduce the fast neutron leakage and to flatten the power distribution. This structure is called the heavy reflector (Fig. 5) and is an innovative feature, aimed at savings on fuel costs (3–5%). It contributes also to lower the vessel fluence.

The heavy reflector is made of thick forged plates stacked upon each other and keyed together and resting on the core support plate. There are no bolt or weld close to the core and submitted to a high fluence. The gamma heat generated inside the heavy reflector is taken away by small cooling channels patterned to limit the inside temperature of the material.

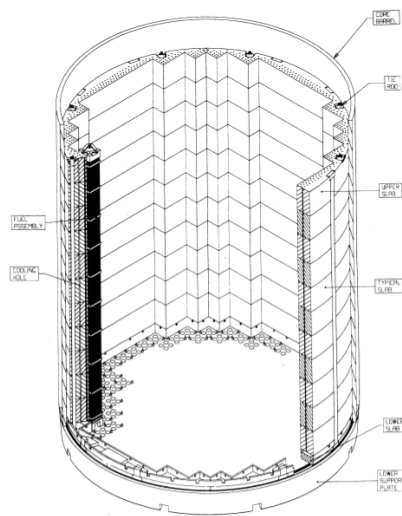


Figure 5: EPR heavy reflector

2. The upper internals, which preload the fuel assemblies from the top. Their function is also to guide the control rods and the instrumentation (thermocouples and in-core). The main parts are the forged upper support plate, the upper core plate and support columns connecting the two together. The support columns house the Rod Cluster Control Assemblies (RCCA) guides which are inserted inside the column and are removable. The upper and lower internals are aligned together and to the vessel head and body by a set of pins and preloaded by a hold down spring when the vessel is closed.

### 2.3 Steam generator

The European pressurized water reactor (EPR) steam generator (Fig. 6) encompasses the following main features

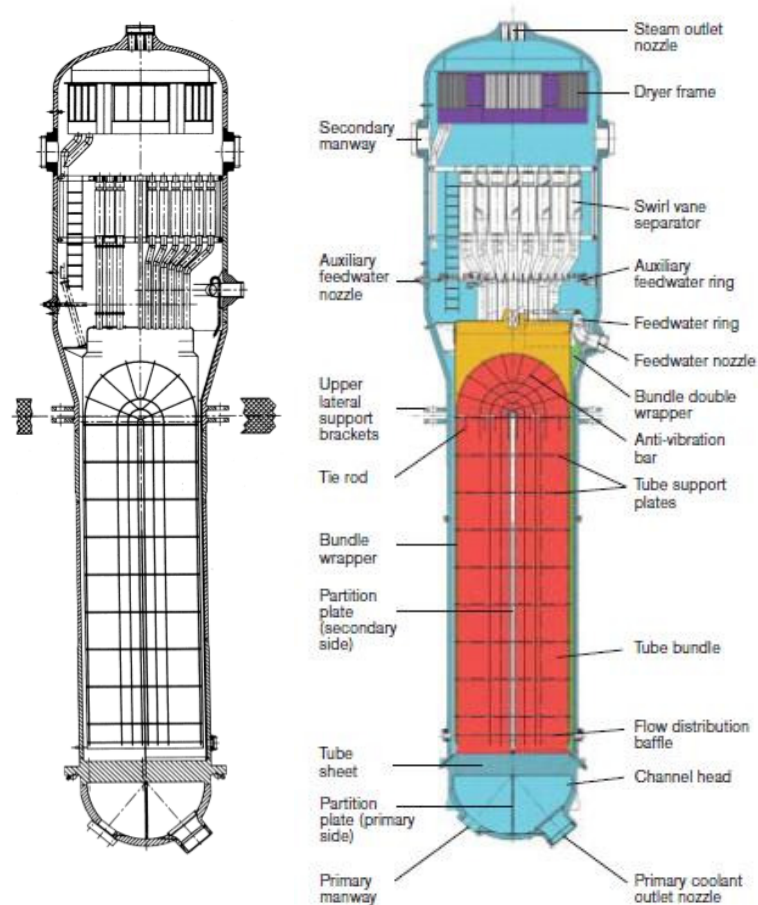


Figure 6: EPR steam generator

1. *Axial economizer* (Fig. 7). The benefit of the economizer is to increase the steam pressure increase at a low cost when compared with a boiler type SG with the same tube surface. It has no impact on the plant operating modes and the economizer is a purely internal system to the SG. The axial economizer principle consists primarily in directing all the feedwater to the cold leg of the tube bundle and 90% of the recirculated water to the hot leg of the tube bundle.

This is practically ensured by adding to the standard boiler design a wrapper in the cold leg of the downcomer to guide the feedwater to the cold leg of the tube bundle, and a partition plate (up to the sixth support plate) to separate the cold leg and the hot leg of the tube bundle. Moreover and in conjunction with the two above modifications, the internal feedwater distribution system (J-tubes) of the steam generator covers only the 180° of the wrapper.

This design enhances the heat exchange efficiency and increases by 3 bars the steam pressure output, as compared to a standard steam generator with the same heat exchange surface.

The axial preheater has several advantages over the cross flow preheater

- a. there is no cross flow on the tubes and no vibration risks;
- b. accessibility to the tube bundle for inspection and maintenance is not impaired.

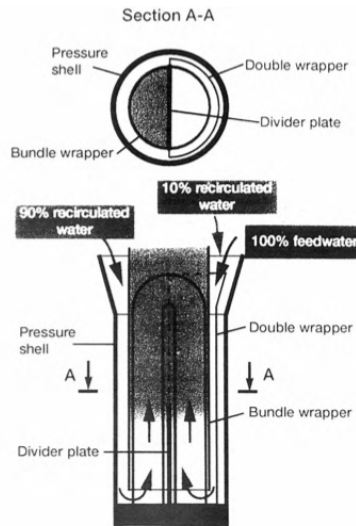


Figure 7: Axial economizer steam generator principle

2. *Tube bundle geometry.* The tube diameter is 19.05(O.D.), the triangular pitch is 27.43 mm. 19.05 is the international standard today and is a good compromise between compactness, vibratory behavior and manufacturing.
3. *Tube material.* Both Incoloy 800 and Inconel 690 are alternate materials for
  - a. corrosion resistance of both materials is very good;
  - b. both have the same yield strength and the same conductivity. They can be interchanged without any consequence on the design of the tube bundle and the size of the steam generator.
4. *Separators technology.* High efficiency separators have been developed and full scale tested simultaneously with the economizer on the MEGEVE loop. Results were excellent, carry under was too small to be measured, carry over very low.
5. *Dryers arrangement.* Dryers modules are arranged in the so called star arrangement. Benefit is clearly to save about 1.2 m on the SG total height. There is no difference between this arrangement and the standard two-stage system found more commonly as far as the total surface of dryers is concerned.
6. *Tube support plates.* Intermediate support of the tubes is provided by stainless steel (13% Cr) plates broached in a trefoiled scheme with flat contact surfaces with the tube (flat-land).

7. *Pressure boundary materials.* The tube sheet and the bottom head are forged parts made of the same grade of steel as the RPV, with two layers of cladding.

The mass of water on the secondary side for normal operating conditions is approximately 75 tons. This gives more thermal inertia to the steam generator and a longer dry-out time in the event of a total loss of feedwater when compared to existing plant of same power level. Although this is a major improvement from the operating and safety points of view, it does not impact the technology of the steam generator. The extra amount of water volume is essentially obtained by increasing the height of the steam drum and by stretching the risers which connect the top of the tube bundle wrapper to the cyclones.

8. *Supports.* The steam generator is vertically supported by pinned–pinned columns bolted to a ledge machined from the tube sheet plate or to brackets welded to the bottom head. It is guided at the tube sheet elevation by guide plates or key/keyways assemblies. Rocking is prevented by lateral supports located underneath the steam drum transition.
9. *Maintainability and inspectability.* The design minimizes the number of welds and optimizes their geometry in order to facilitate inservice inspection. Measures have also been taken to enhance inspectability and maintainability of the steam generator internals.

The pressurizer (Fig. 8) is of a conventional design but with enlarged free volume. To achieve a lifetime of 60 years and the plant power flexibility requirements, two spray lines for normal operation and one auxiliary spray line are completely separated from each other.

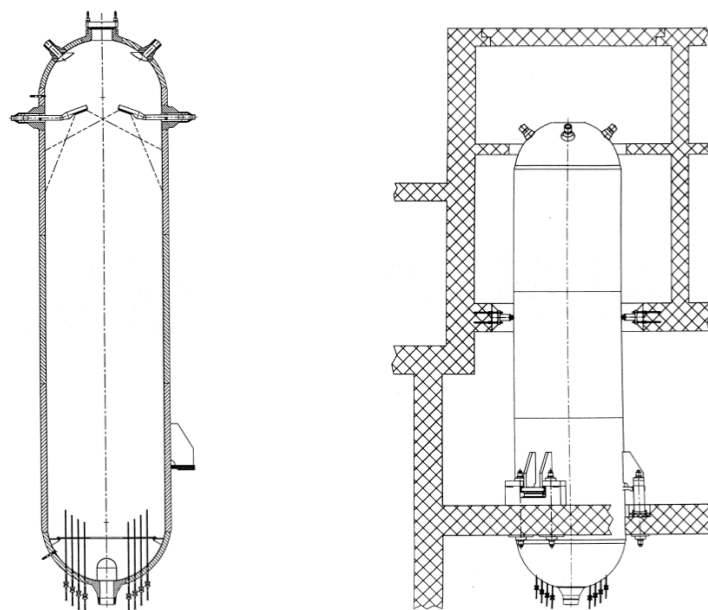


Figure 8: EPR pressurizer and its support



Figure 9: The pressurizer

The spray lines are connected laterally to the upper cylindrical shell, and equipped with a spray head each. The spray system delivers a permanent flow to minimize thermal transients upon valve fast opening.

All pressure boundary parts, except the heater penetrations, are made of ferritic steel with two layers of stainless steel cladding. The steel grade is the same as for the reactor pressure vessel. The penetrations are in stainless steel.

The pressurizer is supported by three brackets integrally welded on the cylindrical shell in its lower part (Fig. 8). The brackets rest on the supporting floor by means of an intermediate supporting structure which allows free radial thermal expansion.

These supports block horizontal vessel displacements. Eight radial stops fixed on the civil work at an upper level insure vessel stability during accident conditions. These upper lateral supports allow free thermal expansion of the vessel.

In November 29, 2010, the EPR nuclear power plant under construction at the Olkiluoto site in Finland has taken a major step in the assembly of the primary circuit major components. After the reactor vessel, its head and the reactor coolant pumps, the pressurizer has been successfully introduced into the reactor building and placed in its final location.

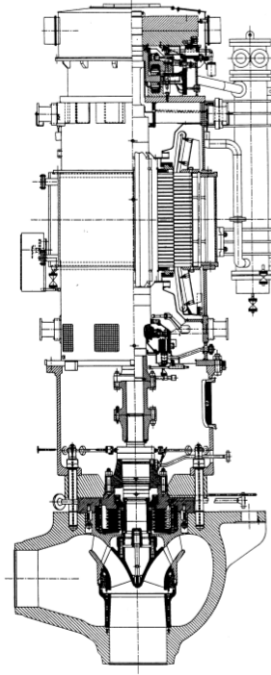


Figure 10: EPR-J.I. pump

The role of the pressurizer is to regulate (create and maintain) the water pressure in the reactor coolant system, at a level designed to prevent the primary cooling water from reaching the boiling point.

This nuclear reactor key component consists of a steel cylindrical tank. It is connected to the hot leg of one of the four loops of the primary circuit and equipped with electric heaters enabling water pressure adjustment in the reactor coolant system.

Pressurizing the coolant system at 155 bar keeps the water in the liquid state and maximizes the efficiency of heat exchange.

The EPR pressurizer sizes are

- Weight of 150 metric tons;
- Height of more than 14 meters;
- Diameter of nearly 3 meters.

## **2.4 Reactor coolant pumps**

Framatome-Jeumont Industrie (Fig. 10) and KSB are the suppliers of the reactor coolant pumps for the EPR. The pumps will be based on the design already operating in France and Germany. The reactor coolant pumps are equipped with a standstill seal in order to assure leak-tightness along the shaft seal, should the normal shaft seals fail.



## 2.5 Main coolant lines

The main coolant lines are made of low carbon stainless steel. Each leg is forged in one piece including the elbows which are induction bent. The loop layout (Fig. 11) is also compatible with clad ferritic steel main coolant lines.

The break preclusion concept is applied. Credit is taken for the high quality of design, construction and surveillance measures, to exclude a catastrophic failure of the main coolant line with regard to its possible mechanical effects.

Double-ended guillotine breaks of the main coolant line are still assumed for the design of the emergency core cooling system and the containment.

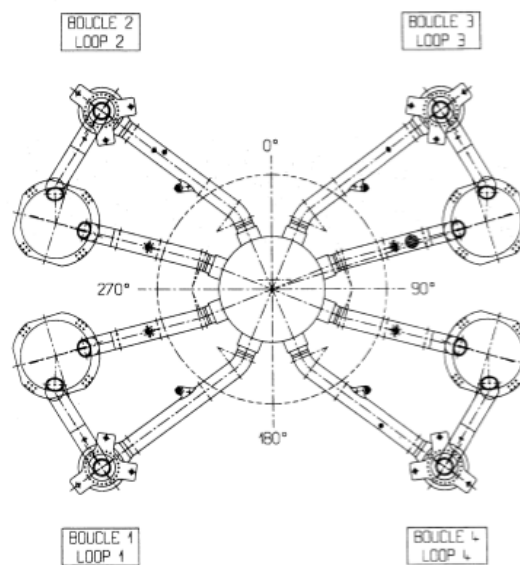


Figure 11: EPR loop layout–plan view

### ***3 The pressurizer in a pressurized water reactor nuclear power plant***

The pressurizer is the component in the reactor coolant system which provides a means of controlling the system pressure. Pressure is controlled by the use of electrical heaters, pressurizer spray, power operated relief valves, and safety valves.

It is equipped with

- Three nozzles connected to the pressure relief valves;
- One nozzle connected to the dedicated bleed valve line;
- The first three nozzles are each equipped with a scoop inside the pressurizer in order to maintain a water seal below each valve seat;
- A manhole providing access inside the pressurizer;
- A vent nozzle.

The forged cylindrical shell consists of three sections. It is equipped with

- Upper (steam phase) instrument nozzles;
- Lateral bracket supports;

The pressurizer operates with a mixture of steam and water in equilibrium. If pressure starts to deviate from the desired value, the various components will actuate to bring pressure back to the normal operating point. The cause of the pressure deviation is normally associated with a change in the temperature of the reactor coolant system. If reactor coolant system temperature starts to increase, the density of the reactor coolant will decrease, and the water will take up more space. Since the pressurizer is connected to the reactor coolant system via the surge line, the water will expand up into the pressurizer. This will cause the steam in the top of the pressurizer to be compressed, and therefore, the pressure to increase.

The opposite effect will occur if the reactor coolant system temperature decreases. The water will become more dense, and will occupy less space. The level in the pressurizer will decrease, which will cause a pressure decrease. For a pressure increase or decrease, the pressurizer will operate to bring pressure back to normal.

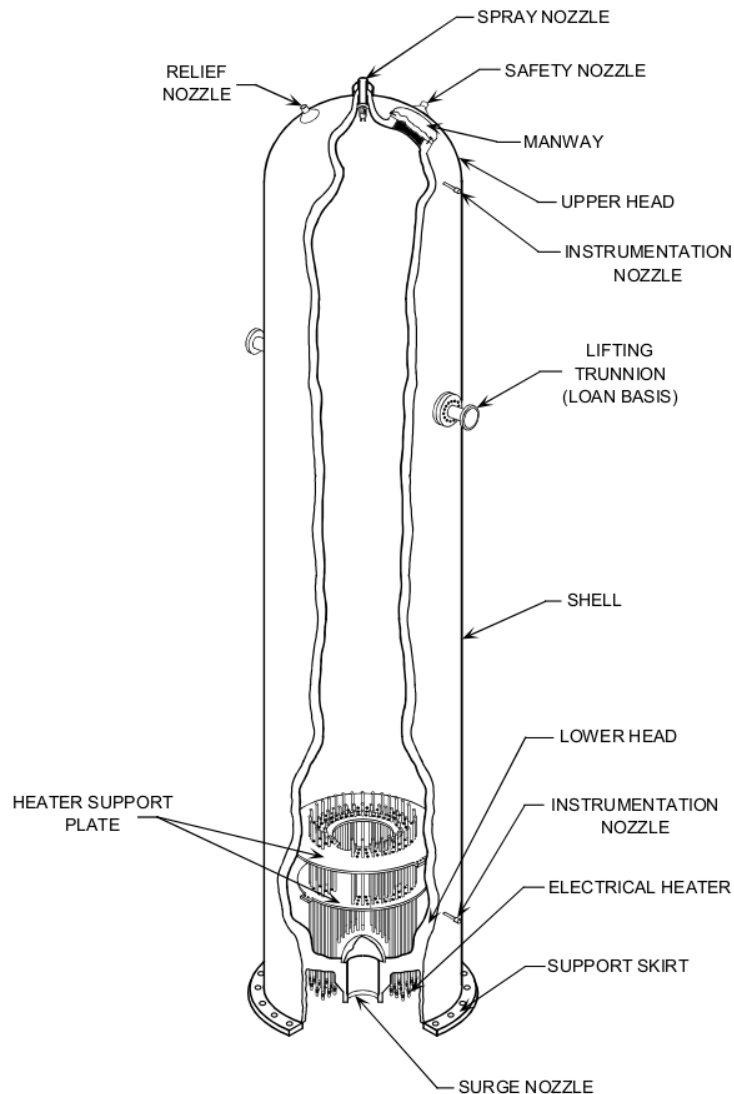


Figure 12: Cutaway view of a pressurizer

For example, if pressure starts to increase above the desired setpoint, the spray line will allow relatively cold water from the discharge of the reactor coolant pump to be sprayed into the steam space. The cold water will condense the steam into water, which will reduce pressure (due to the fact that steam takes up about six times more space than the same mass of water). If pressure continues to increase, the pressurizer relief valves will open and dump steam to the pressurizer relief tank. If this does not relieve pressure, the safety valves will lift, also discharging to the pressurizer relief tank.

If pressure starts to decrease, the electrical heaters will be energized to boil more water into steam, and therefore increase pressure. If pressure continues to decrease, and reaches a predetermined setpoint, the reactor protection system will trip the reactor. The pressurizer relief tank is a large tank containing water with a nitrogen atmosphere. The water is there to condense any steam discharged by the safety

or relief valves. Since the reactor coolant system contains hydrogen, the nitrogen atmosphere is used to prevent the hydrogen from existing in a potentially explosive environment.

The lateral spray system consists of three separate nozzles welded laterally near the top of the upper cylindrical shell

- Two nozzles for the main spray lines (connected to two cold legs);
- One nozzle for the auxiliary spray line, connected to the RCV (Reactor Coolant Volume) [CVCS]).

The three spray nozzles have integral welded thermal sleeves. Each thermal sleeve is extended by a lance. The end of each lance holds a spray box with screwed spray heads which inject spray flow into the pressurizer steam space. The lower hemispherical head is a hot-formed single-piece unit. It is equipped with

- Axial surge line nozzle;
- Lower (water phase) instrument nozzles;
- Heater sleeves equipped with connecting flanges.

A screen installed at the surge line nozzle in the bottom head which prevents the passage of loose parts from the pressurizer to the reactor coolant pipework. The pressurizer is equipped with 116 heater rods, including 8 spare heaters, arranged vertically, inserted into the heater sleeves. There are no spare sleeves without heaters. The heaters are mounted using flanged connections for easy replacement. They are similar in manufacture to spare heaters currently produced for existing plants.

The heater flanged connections are comprised of the following parts

- Heater sleeves, welded to the inner cladding of the bottom head after the final post weld heat treatment of the pressurizer;
- Open flanges of austenitic stainless steel with threaded holes (replaceable);
- Slip-on flanges (upper flange) of austenitic stainless steel, installed prior to welding the heater sleeves;
- Heater flange attachments, welded on the heater sheath, containing grooves for O-ring seal;
- Metal O-ring seals;
- Slip-on flanges (lower flange) of austenitic stainless steel;
- Studs and nuts.

Two areas are free of heater penetrations, these being the central area around the surge line nozzle and the area located above the surge line routing. This allows access to the heaters for maintenance and replacement. The pressurizer has thermal insulation on the outside surface.

The major secondary systems of a pressurized water reactor are the main steam system and the condensate/feedwater system. Since the primary and secondary systems are physically separated from each other (by the steam generator tubes), the secondary system will contain little or no radioactive material. The main steam system starts at the outlet of the steam generator. The steam is routed to the high pressure main turbine. After passing through the high pressure turbine, the steam is piped to the moisture separator/reheaters (MSRs). In the MSRs, the steam is dried with moisture separators and reheated using other steam as a heat source. From the MSRs, the steam goes to the low pressure turbines. After passing through the low pressure turbines, the steam goes to the main condenser, which is operated at a vacuum to allow for the greatest removal of energy by the low pressure turbines. The steam is condensed into water by the flow of circulating water through the condenser tubes.

At this point, the condensate/feedwater system starts. The condensed steam collects in the hotwell area of the main condenser. The condensate pumps take a suction on the hotwell to increase the pressure of the water. The condensate then passes through a cleanup system to remove any impurities in the water. This is necessary because the steam generator acts as a concentrator. If the impurities are not removed, they will be left in the steam generator after the steam forming process, and this could reduce the heat transfer capability of the steam generator and/or damage the steam generator tubes. The condensate then passes through some low pressure feedwater heaters. The temperature of the condensate is increased in the heaters by using steam from the low pressure turbine (extraction steam). The condensate flow then enters the suction of the main feedwater pumps, which increases the pressure of the water high enough to enter the steam generator. The feedwater now passes through a set of high pressure feedwater heaters, which are heated by extraction steam from the high pressure turbine (heating the feedwater helps to increase the efficiency of the plant). The flow rate of the feedwater is controlled as it enters the steam generators.

The Chemical and Volume Control System (CVCS) is a major support system for the reactor coolant system. Some of the functions of the system are to:

- Purify the reactor coolant system using filters and demineralizers;
- Add and remove boron as necessary;
- Maintain the level of the pressurizer at the desired setpoint.

Purify the reactor coolant system using filters and demineralizers, Add and remove boron as necessary, and Maintain the level of the pressurizer at the desired setpoint. A small amount of water (about 75 gpm) is continuously routed through the chemical and volume control system (called letdown). This provides a continuous cleanup of the reactor coolant system which maintains the purity of the coolant and helps to minimize the amount of radioactive material in the coolant.

The reactor coolant pump seals prevent the leakage of primary coolant to the containment atmosphere. The chemical and volume control system provides seal injection to keep the seals cool and

provide lubrication for the seals. This water has been cooled by the heat exchangers and cleaned by the filters and demineralizers. There is also a path (not shown) to route the letdown flow to the radioactive waste system for processing and/or disposal.

During normal operation, the heat produced by the fission process is removed by the reactor coolant and transferred to the secondary coolant in the steam generators. Here, the secondary coolant is boiled into steam and sent to the main turbine.

Even after the reactor has been shutdown, there is a significant amount of heat produced by the decay of fission products (decay heat). The amount of heat produced by decay heat is sufficient to cause fuel damage if not removed. Therefore, systems must be designed and installed in the plant to remove the decay from the core and transfer that heat to the environment, even in a shutdown plant condition. Also, if it is desired to perform maintenance on reactor coolant system components, the temperature and pressure of the reactor coolant system must be reduced low enough to allow personnel access to the equipment. The auxiliary feedwater system and the steam dump system (turbine bypass valves) work together to allow the operators to remove the decay heat from the reactor. The auxiliary feedwater system pumps water from the condensate storage tank to the steam generators. This water is allowed to boil to make steam. The steam can then be dumped to the main condenser through the steam dump valves. The circulating water will then condense the steam and take the heat to the environment.

If the steam dump system is not available (for example, no circulating water for the main condenser), the steam can be dumped directly to the atmosphere through the atmospheric relief valves. By using either method of steam removal, the heat is being removed from the reactor coolant system, and the temperature of the reactor coolant system can be reduced to the desired level.

At some point, the decay heat being produced will not be sufficient to generate enough steam in the steam generators to continue the cooldown. When the reactor coolant system pressure and temperature have been reduced to within the operational limits, the Residual Heat Removal System (RHR) will be used to continue the cooldown by removing heat from the core and transferring it to the environment. This is accomplished by routing some of the reactor coolant through the residual heat removal system heat exchanger, which is cooled by the Component Cooling Water System (CCWS). The heat removed by the component cooling water system is then transferred to the service water system in the component cooling water heat exchanger. The heat picked up by the service water system will be transferred directly to the environment from the service water system. The residual heat removal system can be used to cool the plant down to a low enough temperature that personnel can perform any maintenance functions, including refueling.

### **3.1 Operating conditions and interfaces**

The operating functions of the pressurizer and its associated equipment are

- RCP (Reactor Coolant Pressure) [RCS (Reactor Coolant System)] pressure boundary function as

a part of the reactor coolant system and the second barrier;

- RCP [RCS] volume control (coolant expansion vessel of the RCP [RCS]);
- RCP [RCS] pressure control, overpressure protection and depressurization functions.

These functions are provided by

- Presence of water and steam phases in the pressurizer vessel;
- Normal and auxiliary spray systems;
- Heaters;
- Pressurizer pressure relief valves.

The interfaces providing these functions are

- Interface with the RCP [RCS] hot leg: the pressurizer is connected to hot leg of the RCP [RCS] through the surge line. This connection allows continuous adjustment of the volume and pressure between the reactor coolant system and the pressurizer;
- Interface with the reactor coolant system cold legs: Two main spray nozzles are connected to two spray lines from two cold legs of the reactor coolant system. One of the cold legs belongs to the same reactor coolant system loop as the one connected to the surge line. The spray water is injected into the steam volume as fine droplets, creating an instantaneous condensing surface;
- Interface with the RCV [CVCS]: an auxiliary spray pipeline is connected to the RCV [CVCS]. The auxiliary spray water has a much lower temperature than the normal spray water;
- Interface with the pressurizer relief tank: three nozzles are connected to the pressurizer relief valves which discharge into the pressurizer relief tank and into the reactor building if the pressurizer relief tank rupture disc fails. An additional nozzle is connected to the dedicated bleed line in the event of a severe accident.

### **3.2 Design principles and objectives**

The design objectives and main characteristics of the pressurizer are as follows

- Reliable operation and suitability for all operating conditions and loading, by choosing an appropriate structural design which minimizes as far as possible the stress levels and the stress distribution;
- Reduced fatigue in all loaded points for the EPR requirement of 60 years design life;
- Selection of acceptable and proven materials;
- Use of good manufacturing practice, following industrial techniques used by traditional manufacturers and complying with manufacturing and in-service inspection requirements;

- Design which allow easy access for maintenance and in-service inspections;
- Design which reduces personnel radiation exposure.

### **3.2.1 Main characteristics**

#### **3.2.1.1 Surge line**

The surge line is connected to the pressurizer via the surge line nozzle which is located vertically in the centre of the bottom head.

This design limits the effects of excessive thermal loads on the nozzle under normal operations and excursions. The surge nozzle is equipped with a thermal sleeve opened at the lower end to avoid the accumulation of radioactive particles.

Loads resulting from thermal expansion of the pressurizer vessel are minimised by the short distance between the nozzle and the lateral supports, the vertical position and the surge line route.

The axial location of the nozzle at the lowest point of the pressurizer helps continuous sweeping of the pressurizer bottom area to avoid stagnant areas and the deposition of radioactive particles.

The surge line nozzle is made of ferritic forged steel, and provided with an austenitic safe end. The welding metal used for the bimetallic weld is Inconel 52. The nozzle is clad with austenitic stainless steel on all surfaces in contact with the primary coolant

#### **3.2.1.2 Spray system**

The spray system is located at the top of the pressurizer upper shell and comprises three spray nozzles:

- Two lines are connected to two of the reactor coolant system cold legs (one of these two loops being the surge line loop) and provide the normal spray function in the pressurizer;
- One line is connected to the RCV [CVCS] system.

In order to protect the spray pipelines against excessive thermal loads and to reduce fatigue damage as much as possible, the spray nozzles are fitted with thermal sleeves. Each spray lance is extended with a water box equipped with screwed spray nozzles, which provide a fine droplet spray.

The distance between the spray nozzles and the area where spray fluid hits the pressurizer wall is relatively large. The size of droplets is relatively small due to the choice of small spray nozzles and ensures good heat transfer to the droplets before they reach the pressurizer wall. This design limits the risk of thermal fatigue in the spray/pressurizer wall contact area.

The spray system and its component parts are easily accessible for inspection and maintenance. The entire replacement of a spray lance with its spray nozzles can be carried out.



### 3.2.1.3 Relief valve and dedicated bleed valve connections

Three nozzles are connected to the pressure relief valves. An additional nozzle is connected to the dedicated line used in the event of a severe accident. They are located on the upper hemispherical head of the pressurizer on which are also provided three taps for the safety valve pilots. The relief valves are shielded from spray pipeline radiation by a concrete floor.

The sealing elements are an expanded graphite type gasket or some other proven seal.

The manway opening provides access to the interior of the pressurizer for inspection and maintenance.

A small degassing tap is provided in the manway nozzle as a complement to the venting nozzle to allow the complete removal of non-condensable gases.

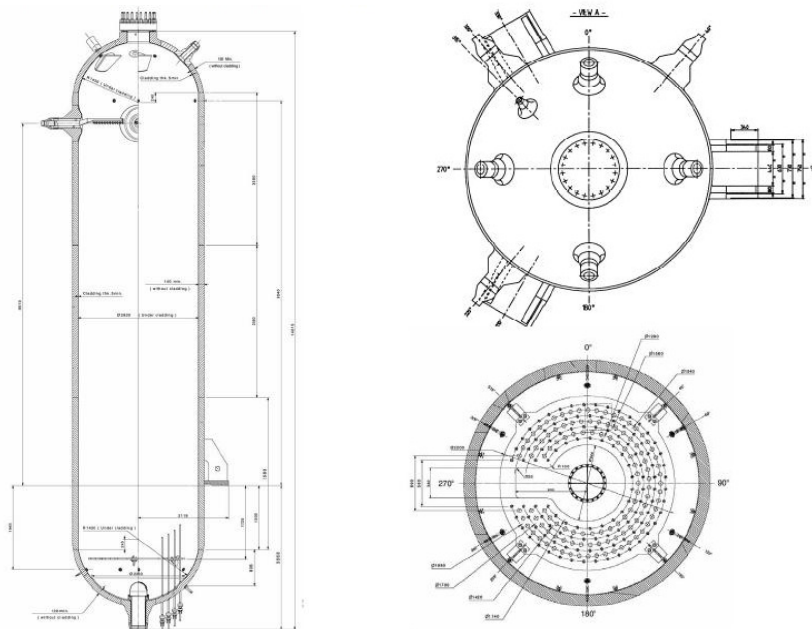


Figure 13: Frontal and upper view of a pressurizer

### 3.2.2 Main dimensions

The main dimensions, characteristics, and nozzles connected to the pressurizer are listed in Tables 1 and 2.

### 3.2.3 Functional requirements

The functional requirements for the pressurizer are

- Design pressure: 17.6 MPa;
- Design temperature: 362°C;

<i>Feature</i>	<i>Value</i>	<i>Unit</i>
Internal volume at 20 °C	75	m <sup>3</sup>
Internal diameter measured at the ferritic wall	2820	mm
hline Spherical heads inside radius at the ferritic wall	1430	mm
Cylindrical shell thickness	140	mm
Upper head thickness	120	mm
Lower head thickness	120	mm
Cladding thickness	5	mm
Heaters sleeves thickness	3.6	mm
Cylindrical shell length	10740	mm
Pressure retaining body (internal) length	13103	mm
Total (overall) pressurizer length	about 14400	mm

Table 2: The main dimensions and characteristics of pressurizer

<i>Nozzles</i>	<i>Quantity</i>	<i>Diameter</i>
Surge line nozzle internal diameter	1	325 mm
Safety valve nozzle internal diameter	3	132 mm
Normal spray line nominal diameter	2	DN 100 mm
Auxiliary spray line nominal diameter	1	DN 100 mm
Dedicated bleed valve nozzle	1	132 mm
Venting nozzle	1	66.9 mm
Manway diameter	1	533 mm
Number of heater sleeves	116	23 mm
Total weight: tare, as delivered		150000 kg
Total weight filled with water (hydrostatic test)		225000 kg

Table 3: Nozzles connected to the pressurizer

- RCP [RCS] volume control: The pressurizer volume is sufficient to meet the following requirements
  - ◇ The volumes of water and steam combined are sufficient to meet the desired pressure response caused by changes in RCP [RCS] system volume;
  - ◇ The water volume is large enough to prevent the heaters being uncovered in PCC-2, PCC-3, and PCC-4 conditions and at the same time large enough to accommodate coolant expansion between 0% and 100% of the power level under PCC-1 conditions;
  - ◇ The steam volume is large enough to accommodate overpressure protection requirements in respect of the RCP [RCS] overpressure criteria in PCC-2 to PCC-4 conditions;
  - ◇ Fluctuation in steam pressure during normal operation should avoid frequent actuation of the pressure regulation devices;
  - ◇ The pressurizer will not empty following reactor trip or turbine trip;
  - ◇ The safety injection signal will not actuate during reactor trip or turbine trip.
- Pressuriser pressure regulation
  - ◇ Three spray nozzles are located in the upper section (two separate nozzles for normal spray, and one for auxiliary spray);

- ◇ The heaters are located in the lower section of the pressurizer (water volume);
- ◇ Three nozzles for the relief valves connection and one for the dedicated bleed valves connection are located in the upper part of the pressurizer head (steam volume).
- Surge line requirements
  - ◇ The surge line connects the pressurizer to a reactor coolant system hot leg;
  - ◇ The surge line is connected vertically to the nozzle at the bottom of the pressurizer;
  - ◇ The surge line differential pressure  $\Delta P$  during overpressure transient conditions (rising flow) is within the maximum allowable pressure loss;
  - ◇  $\Delta P < 2$  bar for an insurge of up to 2500 m<sup>3</sup>/h (from reactor coolant pump to PZR water volume), and  $\Delta P < 5$  bar for an insurge of up to 5000 m<sup>3</sup>/h (from reactor coolant pump to PZR water volume).

### **3.2.4 Requirements for inspection, repair and replacement**

#### **3.2.4.1 Inspection**

The outer surface of the pressurizer around the butt welds can be fully inspected. The shape and slope of welded parts, including safe-end-to-nozzle welds, allow both radiographic and ultrasonic examination. The thermal insulation can be removed from all areas subject to in-service inspection such as

- circumferential welds on the body of the pressurized vessel (there are no longitudinal welds);
- nozzle welds on hemispherical heads;
- lateral support bracket welds.

The nozzle-to-head welds are sufficiently remote from other welds to allow performance of required ultrasonic examination. Inspection of heater sleeve welds can be carried out through the sleeve after heater removal. The inner cladding inspection may be performed from the outside by a remote-controlled camera. Access is via the manway opening.

The pressurizer design does not require the presence of personnel inside the pressurizer to carry out in-service inspections. All inspections are possible from the outside and some may be accomplished using automatic inspection tools.

#### **3.2.4.2 Repair**

The repair of the pressurizer is made possible for the following components or areas where fatigue, corrosion-erosion, seizing or aging may occur

- Manway threads (mechanical damage, threading tearing): repair by threaded inserts;
- Manway sealing surfaces (scratches, tearing or corrosion): the flat surface design of the sealing surface and cladding extra thickness allow easy repair by machining.

### **3.2.4.3 Replacement**

The following components or parts can be replaced if necessary

- Manway studs and nuts;
- Spray lances;
- Spray heads;
- Heater rods (flanged connection);
- Heater rods studs, nuts and threaded open flange.

## **3.3 Material properties**

All materials used in the pressurizer pressure vessel construction comply with RCC–M requirements<sup>2</sup>.

### **3.3.1 Basic materials**

Low alloy ferritic steel 18MND5 is the base material used for the shells, hemispherical heads, main nozzles and the lateral bracket supports. The RCC–M specification gives the chemical compositions and mechanical properties specified for the base materials. The determination of the initial RTNDT is based on both Pellini and Charpy V notch tests. The initial RTNDT for the pressurizer shells and nozzles is less than  $-20^{\circ}\text{C}$ .

### **3.3.2 Studs and nuts**

The pressurizer studs are small diameter studs ( $D < 60$  mm) made of high-strength bolting steel. Pressurizer safe ends, heater wells and instrument nozzles The safe ends are welded to the pressurizer nozzles during manufacture in the factory. The safe ends are manufactured from austenitic stainless steel forged bars. The welding of safe ends onto the nozzles is carried out with a Ni–Fe–based alloy without previous buttering. The internal cladding of the pressurizer is applied in two successive layers using austenitic stainless steel welding strips. The heater wells and instrument nozzles are welded to the internal cladding. The cladding thickness is locally increased in the weld area.

## **3.4 Mechanical design**

This section presents the main results of sizing calculations for the main parts and sub-assemblies, primarily the pressurized vessel and closure parts. For mechanical design, the pressurizer is a class 1 RCC–M–component. The design life is 60 years.

---

<sup>2</sup>RCC–M is a set of diagram and construction rules for mechanical component of a power nuclear island.

### **3.4.1 Sizing calculations**

- The thicknesses of the pressure retaining walls are determined on the basis of the design pressure and design temperature.
- The manway closure assembly is sized taking into account the design conditions (pressure and temperature) and the mechanical characteristics of the gaskets, as provided by the gasket manufacturer: a graphite expanded type gasket or other proven design is used for the manway assembly (relatively frequent openings).

### **3.4.2 Design of sub-assemblies**

Analysis of the surge nozzle behaviour A fatigue evaluation of the surge nozzle was performed in order to verify the acceptability of usage factors for the 60-year design life. The fatigue calculation was based on the most onerous dimension changing transients (during heat-up and shutdown of the plant unit). The results demonstrate that the usage factor is acceptable at each point in the nozzle. Pressure relief valve nozzles The relief valves nozzle loads were calculated considering the discharge forces. Safe end calculations have been carried out; this area being considered to be the most stressed due to the geometry and materials properties. The stresses in nozzle safe ends have been calculated for pressure, temperature and external moments (using the set of loads given for second category conditions and for accident conditions) resulting from the pipework calculations. The calculated stresses are acceptable with very large margins in the weakest points of the structure. Lateral fastening support welds The stresses in brackets support welds on the pressurizer shell were calculated based on the loads given by the loop analysis results. Stresses induced in the welds are acceptable for all operating conditions and accident situations.

## **3.5 Manufacturing and procurement**

The pressurizer vessel is manufactured from the following parts

- Forged cylindrical shells;
- Hot-formed hemispherical heads;
- Forged nozzles;
- Forged plates for covers;
- Forged safe ends;
- Forged bars for small diameter branch pipes;
- Plates for lateral supports;
- Plates for heater support.

Cladding of parts in the pressurized vessel utilises stainless steel strips which are deposited using automatic welding with manual finishing of the circumferential welds. The safe ends are welded to the ferritic forged parts using a narrow groove welding process using a Ni-Fe-based alloy with 30% Cr welding material.

Pre- and post-welding heat treatment and final heat treatment of welds must comply with RCC-M requirements. During the final stage of the manufacturing process, the weld surfaces and transitions must be prepared in order to allow a surface inspection to be carried out (liquid penetrant testing, magnetic particle inspection) and volume inspections (radiographic, ultrasonic).

The final surface finish of the cladding must be suitable to allow inspection by liquid penetrant and ultrasonic tests. Pressuriser shell and ends have no longitudinal welds.

## **4 Control and protection of the pressurizer in a PWR power plant**

### **4.1 The pressurizer**

The pressurizer is a vessel containing primary water in the lower part, and steam in the upper part. It maintains the pressure of the primary circuit inside prescribed limits. It is part of the primary circuit, and is connected through a surge line to the hot leg of one of the four loops of that circuit.

The pressurizer has two main functions

1. *Pressure control.* During normal operation the pressurizer is the only component of the primary system that contains vapor. The compressible vapor volume shall prevent pressure spikes in case of increase or decrease of the medium primary system temperature. The pressurizer is usually a stagnant volume connected to the hot leg of a nuclear power plant by the surge line. During normal operation, the pressurizer is in saturated conditions. Two third of the pressurizer are filled with saturated liquid, one third with saturated vapor. To keep the pressurizer saturated, heaters, which are located in the liquid part, are constantly kept on – to compensate for heat losses by the pressurizer wall. In addition, a small amount of additional vapor is produced. This additional vapor is condensed by a continuous flow the pressurizer spray. To control the pressure heaters and spray can be regulated. To limit excessive pressure increases, safety valves on top of the pressurizer can open.
2. *Mass control.* During normal operation the liquid level of the pressurizer is an indication for the amount of fluid mass that is contained in the primary system of the nuclear power plant. Therefore, the make-up and let-down system (to control the primary system mass, chemistry, and for fluid purification), which constantly exchanges a part of primary system liquid, regulates its outflow and inflow according to the pressurizer level. The level set point keeps track of the average liquid temperature. If the fluid is colder than nominal, the set point for the pressurizer level is lower than nominal, and the other way around. The goal of the system is to keep the liquid mass constant (instead of the liquid volume).

Although the water in the pressurizer is the same reactor coolant as in the rest of the reactor coolant system, it is basically stagnant, i.e. reactor coolant does not flow through the pressurizer continuously as it does in the other parts of the reactor coolant system. Because of its incompressibility, water in a

connected piping system adjusts equally to pressure changes anywhere in the connected system. The water in the system may not be at the same pressure at all points in the system due to differences in elevation but the pressure at all points responds equally to a pressure change in any one part of the system. Hence, the pressure in the entire reactor coolant system, including the reactor itself, can be controlled by controlling the pressure in a small interconnected area of the system, the pressurizer. The pressurizer is small vessel compared to the other two major vessels of the reactor coolant system, the reactor vessel itself and the steam generator(s).

Pressure in the pressurizer is controlled by varying the temperature of the coolant in the pressurizer. Water pressure in a closed system tracks water temperature directly; as the temperature goes up, pressure goes up and vice versa. Hence, to accommodate some primary coolant volume variation, the pressurizer is equipped with (large) electric heaters at the bottom to vaporize more liquid, and with a spray system at the top to condense more steam. To increase the pressure in the reactor coolant system, the electric heaters in the pressurizer are turned on, raising the coolant temperature in the pressurizer and thereby raising the pressure. To decrease pressure in the reactor coolant system, sprays of (relatively) cool water are turned on inside the pressurizer, lowering the coolant temperature in the pressurizer and thereby lowering the pressure.

The pressurizer has two secondary functions

1. to provide a place to monitor water level in the reactor coolant system. Since the reactor coolant system is completely flooded during normal operations, there is no point in monitoring coolant level in any of the other vessels. But early awareness of a reduction of coolant level (or a loss of coolant) is important to the safety of the reactor core. The pressurizer is deliberately located high in the reactor containment building such that, if the pressurizer has sufficient coolant in it, one can be reasonably certain that all the other vessels of the reactor coolant system (which are below it) are fully flooded with coolant. There is therefore, a coolant level monitoring system on the pressurizer and it is the one reactor coolant system vessel that is normally not completely full of coolant.
2. to provide a “cushion” for sudden pressure changes in the reactor coolant system. The upper portion of the pressurizer is specifically designed to do not contain liquid coolant and a reading of full on the level instrumentation allows for that upper portion to do not contain liquid coolant. Because the coolant in the pressurizer is quite hot during normal operations, the space above the liquid coolant is vaporized coolant (steam). This steam bubble provides a cushion for pressure changes in the reactor coolant system and the operators ensure that the pressurizer maintains this steam bubble at all times during operations. Allowing this steam bubble to disappear by filling the pressurizer to the top with liquid coolant is called letting the pressurizer “go hard” meaning there is no cushion and any sudden pressure change can provide a hammer effect to the entire reactor coolant system.



Part of the pressurizer system is an over–pressure relief system. In the event that pressurizer pressure exceeds a certain maximum, there is a relief valve called the Pilot Operated Relief Valve (PORV) on top of the pressurizer which opens to allow steam from the steam bubble to leave the pressurizer in order to reduce the pressure in the pressurizer. This steam is routed to a large tank (or tanks) in the reactor containment building where it is cooled back into liquid (condensed) and stored for later disposition. There is a finite volume to these tanks and if events deteriorate to the point where the tanks fill up, a secondary pressure relief device on the tank(s), often a rupture disc, allows the condensed reactor coolant to spill out onto the floor of the reactor containment building where it pools in sumps for later disposition.

Compared to previous designs, the volume of the pressurizer in a PWR of new generation, such as the EPR, is significantly increased to smooth the response to operational transients. This improvement increases equipment life duration and time available to counteract potential abnormal situations in operation.

Relief and safety valves at the top of the pressurizer protect the primary circuit against overpressure. Compared to previous designs, the EPR features an additional set of motorized valves. In case of a postulated accident with a risk of core melting, these valves would provide the operator an additional efficient means of rapidly depressurizing the primary circuit and avoiding a high-pressure core melt situation.

A number of design features have been incorporated to improve maintainability. In particular, a floor between the pressurizer head and the valves eases heater replacement and reduces radiological dose during valve service.

All the pressurizer boundary parts, with the exception of the heater penetrations, are made of forged ferritic steel with two layers of cladding. The steel grade is the same as that for the reactor pressure vessel. The heater penetrations are made of stainless steel and welded with Inconel.

The pressurizer is supported by a set of brackets welded to the main body. Lateral restraints will preclude rocking in the event of a postulated earthquake or accident.

The description of the instrumentation of the pressurizer will be given in a future deliverable.

## **4.2 *Pressurizer thermal hydraulics***

This section reports the geometry of the pressurizer and its connection to the reactor cooling system (RCS), the surge line.

## **4.3 *RCP [RCS] pressure control***

Control of RCP [RCS] pressure contributes to

- The RCP [RCS] overpressure protection safety function by preventing the activation of the pressurizer relief valves

- The reactor heat transfer safety functions, core cooling and reactivity control by maintaining the RCP [RCS] pressure above saturation pressure.

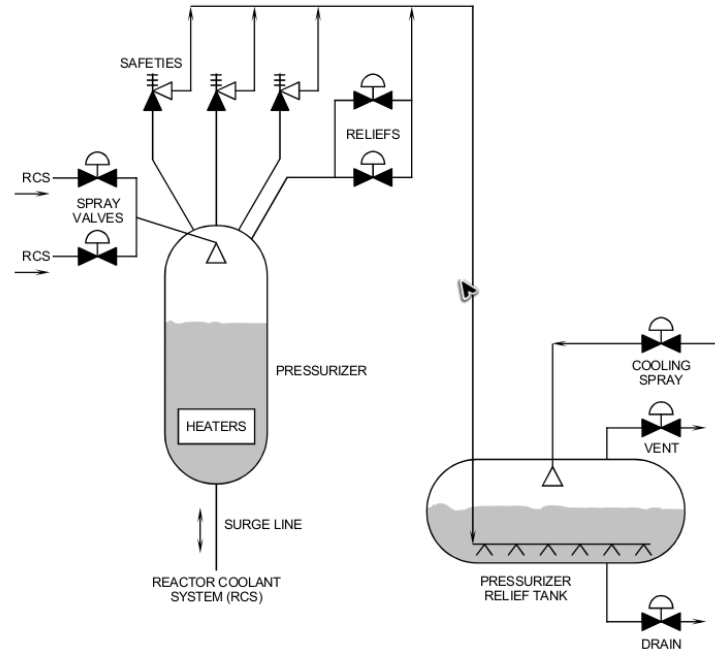


Figure 14: Pressurizer and relief tank

Control of RCP [RCS] pressure is achieved by operation of the pressurise heaters and water spray. A control signal derived from the comparison between the measured pressurizer pressure and the reference pressure setpoint, leads the control actuators to:

- Activate the pressurizer heaters to increase pressure by heating the liquid phase of the pressurizer. Introduce spray water in the steam phase of the pressurizer to reduce pressure. When set in automatic mode, the pressurizer (continuously controlled) heaters and spray control valves, control the RCP [RCS] pressure during minor variations relative to the reference pressure setpoint.

On/off heaters and spray control valves in on/off mode are activated only in the event of a significant variation compared with this pressure setpoint. RCP [RCS] pressure measurements contribute to the establishment of alarm set-points and automatic actions. Upper and lower RCP [RCS] set-points generate automatic alarms or limitation measures such as

- Actuation or switch-off of the pressurizer heaters
- Opening or isolation of the normal and/or auxiliary spray
- Isolation of the RCV [CVCS] charging flow or switch-off of the RCV [CVCS] charging pump (high pressure).

RCP [RCS] pressure measurements are also used to activate the protection instrumentation and control functions.

#### **4.4 Pressuriser level control**

Control of the pressurizer level contributes to the safety function of maintaining the RCP [RCS] water inventory. Pressuriser level control is based on the comparison between the measured pressurizer level and the pressurizer reference level. The level control provides a demand signal to the RCV [CVCS] high pressure letdown flow control valve. The pressurizer reference level is a function of the RCP [RCS] temperature and is calculated to keep a constant reactor coolant mass for pressure levels between 0 and 100%. Pressuriser level measurements contribute to the establishment of alarm set-points and automatic actions, thereby preventing the actuation of automated instrumentation and control protection functions. The upper and lower pressurizer level set-points generate automatic alarms or limitation measures such as:

- Opening or closing of the RCV [CVCS] high pressure letdown flow rate control valve
- Start up of the second RCV [CVCS] charging pump (low level)
- Isolation of the RCV [CVCS] charging flow (high level)
- Isolation of the pressurizer normal and/or auxiliary spray (high level)
- Switching off the pressurizer heaters (low level). Pressuriser level measurements are also used to activate the protection instrumentation and control functions.

During normal operation, a constant letdown flow is sucked from the intermediate leg of RCS loop 1 to the volume control tank of chemical and volume control system (CVCS).

The centrifugal charging pump (CCP) is a component of CVCS. The pressurizer level control system regulates the charging flow rate through a control valve to maintain the pressurizer level to the setpoint. Due to a constant letdown flow rate, 4 kg/s, it causes pressurizer level to decrease at the beginning. The measured pressurizer level is compared with its desired level, hence an error signal is generated. The error signal passes through a proportional and integral controller, which is used to regulate the charging flow rate through control valve.

The pressurizer level setpoint is a function of average RCS temperature. For full load, this temperature is about 309.2°C (582.25 K) and the pressurizer level high limit is 56.5% of level span. The level program between 291.7°C and 309.2°C is linear from 22.4% to 56.5% of level span.

#### **4.5 Protection against internal and external hazards**

In addition to the special requirements applied to the pressurized equipments, the whole Reactor Coolant System (RCP) [RCS] is subject to protection against internal and external hazards. The following external hazards have been considered from the point of view of their effects upon the RCP [RCS] lines:

- Seismic event
- Aircraft crash
- External explosion
- Lightning and magnetic interferences
- Underground water
- Extreme meteorological conditions (temperature, snow, wind and rain)
- External flooding
- Offsite hazardous substance

The reactor building protects the RCP [RCS] against most of these external hazards. The reactor building cooling system protects the RCP [RCS] from extreme ambient temperature. The reactor building and the RCP [RCS] have been assigned seismic category 1. The RCP [RCS] is designed to maintain structural integrity during a Safe Shutdown Earthquake (SSE) event. The following internal hazards have been considered from the point of view of their potential effect on the RCP [RCS]:

- Fire
- Missiles
- Failure of pressurized components
- Main turbine disintegration
- Dropped loads
- Explosive gas mixtures
- Hazardous materials
- Explosive effects of electrical faults
- Radio-frequency interference
- Flooding

The primary system pipework is located inside bunkers that protect it from missiles arising inside the containment. As it is all located inside the containment, it is protected from missiles arising in the auxiliary building. The design of the polar crane, which is not operational whilst the plant is at pressure, limits the probability of dropped loads.

#### **4.6 Pressurizer sensors**

In [66] a strain measurement procedures, applied to a compact nuclear reactor pressurizer, during a hydrostatic test, using strain gage technology, is presented. The Pressurizer is one of the equipments that

belong to the CS-1 nuclear safety class of the primary circuit of the Nucleoelectric Generation Laboratory Reactor (facilities of the Navy Technological Center in São Paulo, Brazil).

The materials and the equipments used were the following

- Strain Gage: Rectangular Rosette, mark Kyowa, model KFG-5-120-D17-11;
  - ◇ Nominal Resistance:  $120,04 \pm 0,4 \Omega$ ;
  - ◇ Sensor Length: 5 mm;
  - ◇ Gage Factor K:  $2,11 \pm 1\%$ ;
  - ◇ Thermal Coefficient Expansion:  $11,7 \text{ ppm}/^\circ\text{C}$ ;
  - ◇ Temperature compensation: Steel.
  
- Rectangular Rosette, mark Kyowa, model KFG-5-120-D17-16;
  - ◇ Nominal Resistance:  $120,04 \pm 0,4 \Omega$ ;
  - ◇ Sensor Length: 5 mm;
  - ◇ Gage Factor K:  $2,18 \pm 1\%$ ;
  - ◇ Thermal Coefficient Expansion:  $16,2 \text{ ppm}/^\circ\text{C}$ ;
  - ◇ Temperature compensation: Stainless Steel.
  
- Adhesive: Resin cyanoacrylate, mark Kyowa, model CC33A. Operation temperature:  $-196^\circ\text{C}$  a  $120^\circ\text{C}$ .

For treating a test submerged (the strain gage is immersed in water) and under pressure it was necessary to use a protection on the internal strain gages. A protection was also used on the due to external strain gages by virtue of the risk to wet during the test. For protecting the internal strain gages, the protection AK22 was selected due to be efficient in cases of immersion in water under pressure up to 400 bar. For the protection of the external strain gages, the protection ABM75 was selected due to be efficient for situations where immersion can occur on the strain gages.

The internal points were protected with two varnish layers, mark EMEME (Vishay), model MCoat A; a thick layer of mass, mark HBM, model AK-22; an aluminum foil leaf and adhesive tape mark 3M, model silver tape.

The external points were protected with two varnish layers, mark EMEME (Vishay), model MCoat A; a mass layer with leaf of aluminum, mark HBM, model ABM75 and adhesive tape mark 3M, model silver tape.

Each gage (the rectangular rosette possesses 3 gages) was connected through a cable with 3 armored threads to the Wheatstone bridge as presented in Fig. 15. The Wheatstone bridge was set up, being strain gages of type rectangular rosette model CEA-06-250-UR-120 manufactured by Measurements Group

protection ABM75 was selected to be efficient for situations where

The internal points were protected with two varnish layers, mark EMEME

The external points were protected with two varnish layers, mark EMEME

**Connection:**

Each gage (the rectangular rosette possesses 3 gages) was connected to the Wheatstone bridge as presented in Figure 1. The Wheatstone bridge was set up being strain gages of type rectangular rosette model CA-06-250-UK-120 manufactured by Measurements Ltd. The Wheatstone bridge was installed close to the rosettes to minimize the size of the threads of the strain gage connection.

19	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor
20	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor
21	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor
22	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor	Fluor

Screen of result typical of the acquisition program and data treatment.

With the Pressurizer full of water and being submitted to pressure, it was made a series of readings of the points scored for the determination of the zero reading system.

**2.2 Location of Strain Gages Rosettes in the Pressurizer**

The strain gages of the rectangular rosettes are numbered from 1 to 3 in the counterclockwise sense as presented in Figure 3. The final orientation of the strain gages 1, 2 and 3 of the rectangular rosettes are suitable in bounded areas of steel original not submitted to mechanical efforts. The Wheatstone bridge was installed close to the rosettes to minimize the size of the threads of the strain gage connection.

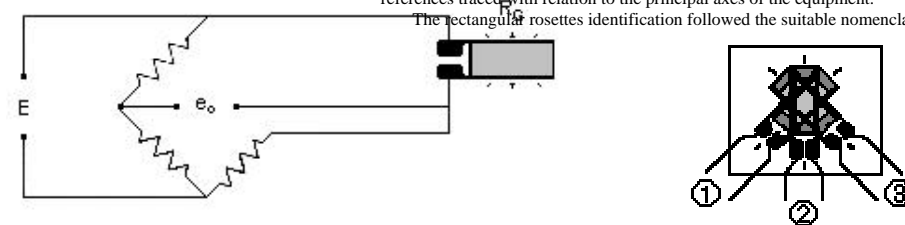


Figure 1 – Connection of the strain gage to the Wheatstone bridge. Figure 3 – Numbering and orientation of the rectangular rosette gages.

2800 Copyright © 2005 by SMiRT18  
A cable with 4 armored threads was used to connect the bridge of Wheatstone to the data acquisition system and the feeding source. To the data acquisition system were connected the terminals suitable  $e_0$  in Fig. 15 and the terminals  $E$  were connected to the power supply. The Wheatstone bridge was fed with 2 V, and this value was monitored by the data acquisition during the measurements. The connection of the internal points was done through the use of the Wheatstone bridge was installed close to the rosettes to minimize the size of the threads of the strain gage connection.

The acquisition and data treatment system was composed by

- a system with 48 channels, mark Agilent, model 34970A, with 3 modules of switch, model 34902A.
- a system with 60 channels, mark Agilent, model 34970A, with 3 modules of switch, model 34901A.
- a microcomputer type notebook, mark Texas Instruments, Extensa model 610CD, pentium 133 Mhz.

Internal pressure measurement was not accomplished by the data acquisition system. The pressurizer internal pressure can be accomplished through manual reading in two manometers with calibration and certification both valid and updated, with a reading every ten minutes.

Strain gages bounded in the internal surface are exposed to the flowed or pressurized gas, which acts directly in the strain gage element. Under such conditions, the resistance of the strain gages suffers a small increase due to the pressure that acts perpendicular to its grade and it should be taken into account for the strain gage readings analysis. Hence a the correction/compensation has to be considered. The global uncertainty of the measured values can be evaluated in 4% of the read values.

**4.7 Measurement procedure**

For the reading of the 22 installed rectangular rosettes, 66 reading channels were used, being 30 channels read in the system 34970A with 48 channels and the other 36 channels read in the system 34970A with 60

channels. The two systems were controlled by a program developed by CDTN (Center of Development of the Nuclear Technology), presenting the following data in real time

- Strain of the three rectangular rosette gages;
- Principal strains, maximal, minimal and angular;
- Principal stresses, maximal, minimal and shear;
- Angle and direction of the principal strains.

With the pressurizer full of water and before being submitted to pressure, it was made a series of readings of the points scored for the determination of the zero reading system.

#### **4.8 Location of Strain Gages Rosettes in the Pressurizer**

The strain gages of the rectangular rosettes are numbered from 1 to 3 in the counterclockwise sense as presented in Fig. 15. The final orientation of the strain gages 1, 2 and 3 of the rectangular rosettes are given in Table 4.

Point	Gages		
	1	2	3
SG1	Circunferencial	45	Longitudinal
SG2	Longitudinal	45	Circunferencial
SG3	Circunferencial	45	Longitudinal
SG4	Longitudinal	45	Circunferencial
SG5	Circunferencial	45	Longitudinal
SG6	Circunferencial	45	Longitudinal
SG7	Longitudinal	45	Circunferencial
SG8	Circunferencial	45	Longitudinal
SG9	Longitudinal	45	Circunferencial
SG10	Circunferencial	45	Longitudinal
SG11	Circunferencial	45	Longitudinal
SG12	Longitudinal	45	Circunferencial
SG13	Longitudinal	45	Circunferencial
SG14	Circunferencial	45	Longitudinal
SG15	Longitudinal	45	Circunferencial
SG16	Circunferencial	45	Longitudinal
SG17	Longitudinal	45	Circunferencial
SG18	Longitudinal	45	Circunferencial
SG19	Circunferencial	45	Longitudinal
SG20	Longitudinal	45	Circunferencial
SG21	Circunferencial	45	Longitudinal
SG22	Longitudinal	45	Circunferencial

Table 4: Gages orientation of the rectangular rosettes

The final position of the 22 rectangular rosettes installation is indicated in Fig. 16. The identification of the rectangular rosettes positions was accomplished by the Jaraguá team through references traced with relation to the principal axes of the equipment.

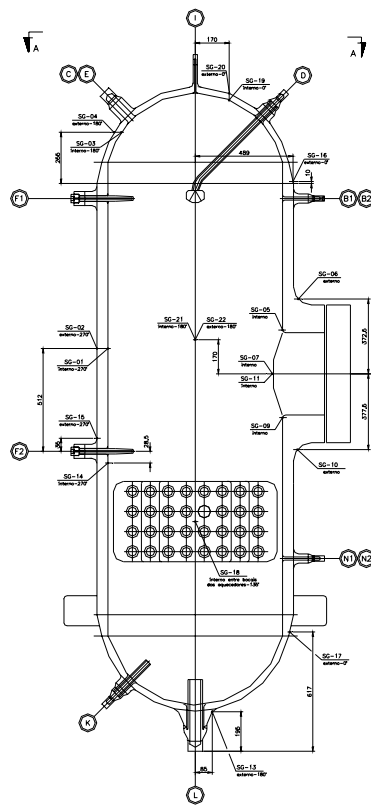


Figure 4 – Location of the rectangular rosettes in PZ of II

Figure 16: Location of the rectangular rosettes on the pressurizer

2804

Copyrig

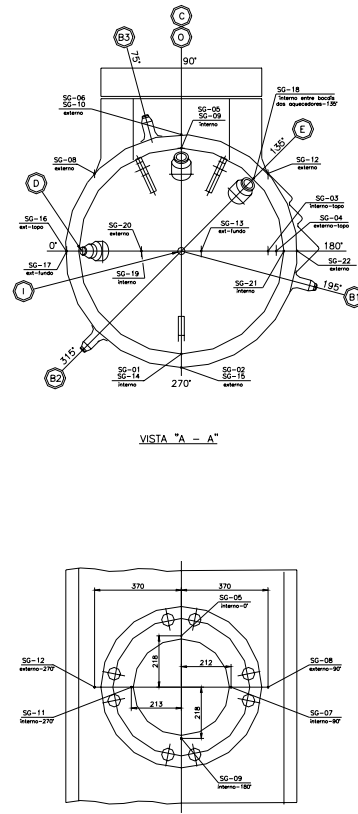


Figure 5 – Location of the rosettes rectangular views A-A and B-B.

**2.3 Pressurization and Depressurization of PZ**

The pressurization and depressurization of PZ were commanded and operated by the Jaraguá team and done according to the document NEQ184 Rev.. 05 of the Quality Program of Warranty of Jaraguá Industrial

Figure 5 – Location of the rosettes rectangular views A-A and B-B.

2805

Copyright © 2005 by SMiRT18

**2.3 Pressurization and Depressurization of PZ**

The pressurization and depressurization of PZ were commanded and operated by the Jaraguá team and done according to the document NEQ184 Rev.. 05 of the Quality Program of Warranty of Jaraguá Industrial

2805

Copyright © 2005 by SMiRT18



## **5 The control rooms**

### **5.1 Importance of the human factor and of the communications in off-normal conditions in a control room of a nuclear power plant**

In the following we will illustrate the importance of human performance issues in every aspect of control systems [46], [44], [11]. The survey results are necessary to identify the error categories in terms of interrelationship among the error casual factors. The focus is on the communications because, according to the survey results, it has been revealed that maintaining good communication is one of the essential parts of securing the safety of a large and complex process system.

#### **5.1.1 Human performance in control rooms**

Human performance and reliability are integral to the safe and efficient operation of nuclear power plants. Investigation of past nuclear power plant abnormal events, ranging from minor incidents to serious accidents, such as the Three Mile Island (TMI) and Chernobyl accidents, has pointed out that the events “have so often been the result of incorrect human actions” [19]. Reflecting on the causes of the TMI accident, [42] stated that “The most serious ‘mindset’ is the preoccupation of everyone with the safety of equipment, resulting in the downplaying of the importance of the human element in nuclear power generation. We are tempted to say that while an enormous effort was expended to assure that safety related equipment functioned as well as possible, and that there was backup equipment in depth, what the Nuclear Regulatory Commission (NRC) and the industry have failed to recognize sufficiently is that the human beings who manage and operate the plants constitute an important safety system”.

Although the Human–System Interfaces (HSIs) of all operating nuclear power plants in the United States have gone through an industry–wide re–evaluation after the TMI accident, and many human factors design guidelines for nuclear power plants (such as NUREG–0700; U.S. Nuclear Regulatory Commission, 2007b) have been put in place, incidents caused by human errors continue to occur. Interestingly, most post–accident human errors occur in control rooms [75]. A review by the authors in August 2008 of the Institute of Nuclear Power Operations (INPO) Operating Experience (OE) database revealed 146 human error plant incidents between December 3, 1990, and April 24, 2008; 18% of the incidents resulted in either a plant trip/transient or technical specification violation, the cost of which could be as high as one million dollars per day for repairs and rework. It should be noted that approximately 70% of the incidents did not lead to any immediate corrective actions. Among those that led to immediate cor-

rection actions, measures were confined to merely trending HSI-related errors instead of taking steps for extensive investigation. Three decades after TMI, the boom in the nuclear industry worldwide is driven by the increasing demand for reliable and clean energy. New technologies are used not only to build new generations of nuclear power stations, but also to upgrade existing power plants. The applications of the new technologies have greatly improved productivity and plant reliability. The introduction of new technology, however, also has the potential to negatively impact human performance, spawning new types of human errors, and thus possibly reducing human reliability. For example, computerized information and control devices have been introduced to process control and monitoring. Analog instrument and control (I&C) technology, and hardwired controls and displays, which are predominantly used in currently operating nuclear power plants, are being replaced by digital I&C technology and computer-based HSIs used in next generation plants [21]. The transition in technology raises many important human performance issues in every aspect of control systems, ranging from low-level physical design of equipment and control rooms to high-level human decision making and communication. Moreover, as computer technology increases the amalgamation level of process control in control rooms, human performance becomes more critical because operators face more responsibilities due to the increased economic value of what is controlled [55]. One may argue that because the impact of human performance on the safety and efficiency of nuclear power plants will decrease as the automation level of the plants increases, we can eliminate human errors by using advanced automation technology. It is true that increased automation levels normally reduce the number of nuclear power plant personnel; however, the reduction in staffing levels decreases as automation levels increase because a certain number of personnel are required to handle potential disruptions or emergencies [3], [71]. Furthermore, manning levels may even increase with automation levels beyond a certain level of automation. This means that human performance issues cannot be eliminated by merely using advanced automation technology, and it supports our earlier statement that new technologies have the potential to spawn new types of human errors. Through a statistical approach, this study examined the causal factors of HSI-related human errors in nuclear power plant control rooms. The results can help us to identify error categories in terms of the interrelationships among the error causal factors. Moreover, an investigation of the error causal factors can enable us to better understand the nature of the errors and then propose effective corrective action guidelines to mitigate their consequences and enhance human reliability.

### **5.1.2 Human Operators in Process Control**

The interaction between operators and processes can be described by the model shown in Fig. 17 as one of the components of a complex process control system, an operator acts as an information processor. A dynamic mental model of the actual process under supervision is developed through training and stored in the operator's long-term memory. Actual process information is first received through the operator's sensory, mainly visual and auditory, receptors. Next it is interpreted and organized by the

operator's perceptual processors to update the operator's mental model. The synchronization takes place continually at a subconscious level during process monitoring. When there is a disagreement between the actual process and the mental model, the operator's attention will be focused on the discrepancies, and conscious cognitive activities will take over to select an action to respond with inputs retrieved from the operator's long-term memory. The selected action will be executed by the operator's motor processors. Finally, the response of the process to the operator's action will be captured by the operator's sensory receptors through the feedback loop to initiate a new information processing cycle [37]. As illustrated in Fig. 17, the whole information-processing cycle can be generally divided into two stages: cognitive information processing, which consists of information reception, identification, interpretation, and decision making, and manual task execution actions.

Liao and Chang

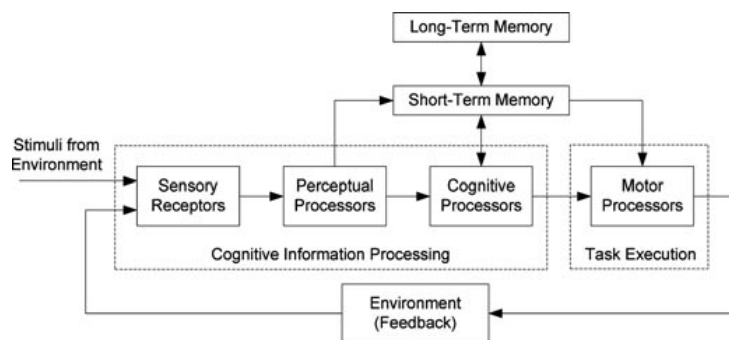


Figure 1 Human information processing model (Based on Card, Moran, & Newell, 1983; Ivergård & Hunt, 2008).

Figure 17: Human information processing model [7], [37]

information-processing cycle can be generally divided into two stages: *cognitive information processing*, which consists of information reception, identification, interpretation, and decision making, and *manual task execution actions*.

## 2.2. Human Error

Human error can be defined as an inappropriate or undesirable human action or behavior that reduces or has the potential to reduce system effectiveness, safety, and system performance, which may or may not result in an accident or injury [65]. The nature of human error is complex. First, it occurs at different levels. For example, it may be caused by humans operating a system, those who designed the system, and/or those who supervise, train, or advised the operator. Second, understanding human error for many reasons, such as fatigue, distraction, inattentiveness, poor work habits, insufficient training, poor work environment, social pressure, poor decision making, and personal traits.

Various schemes for human error classification have been developed in an effort to design "fail-safe" systems or to improve human performance and reliability. For example, [47] divided human errors into four types in terms of where they originate: *operating errors*, *design errors*, *manufacturing errors*, and *installation and maintenance errors*. In probabilistic safety assessment (PSA) and human reliability analysis (HRA) for high consequence industries (e.g., the nuclear and aviation industries), human errors are often classified into three categories based on the relative timing of the errors and a certain accident sequence. The first category is *pre-initiator human errors*, which are faults that occur before the beginning of an accident sequence.

The second category is *initiator human errors*, which are human actions contributing to the initiating event of an accident sequence. The third category is *post-initiator human errors*, which are faults that occur after an incident or accident to aggravate the incident and human error [96].

The schemes vary considerably depending on whether it has been developed from a theoretical psychological approach or based on an empirical practical approach. It should be noted that, due to the complex nature of human error, it is difficult for a scheme to capture all the complexity and facts; therefore, the selection of human error classification should be based on the goal of a specific study. Three well-known human error classification schemes are briefly described. For instance, [47] divided human errors into three categories: *operating errors*, *design errors*, and *manufacturing errors*, and into *errors of omission* (EOOs), which are instances in which operators fail to perform one or more procedural steps that are necessary for the particular circumstance they are facing, and *errors of commission* (EOCs), which refer to errors in which operators perform certain steps that are incorrect or performs a step incorrectly (Swain & Guttman, 1983; Wickens, Gordon, & Liu, 1998). EOOs are often caused by distraction or diversion of attention and are particularly prevalent in maintenance tasks. In contrast, EOCs are often caused by inadequate training of procedures, poor instruction, or unawareness of hidden hazards. Although the scheme was expanded by Swain and Guttman (1983) with two other categories (*sequential errors*, which are actions performed out of the correct order, and *time errors*, which are actions performed too slow, too fast, or

The second category is initiator human errors, which are human actions contributing to the initiating event of an accident sequence. The third category is post initiator human errors, which are faults that occur after an incident or accident to aggravate the incident and accident [20]. The schemes vary considerably depending on whether it has been developed from a theoretical psychological approach to understanding human error or whether it has been based on an empirical practical approach. It should be noted that, due to the complex nature of human error, it is difficult for a scheme to capture all the complexity and facts; therefore, the selection of human error classification should be based on the goal of a specific study. Three well-known human error classification schemes are briefly described. One frequently used scheme classifies human errors into Errors Of Omission (EOOs), which are instances in which operators fail to perform one or more procedural steps that are necessary for the particular circumstance they are facing, and Errors Of Commission (EOCs), which refer to errors in which operators perform extra steps that are incorrect or performs a step incorrectly [75], [84]. EOOs are often caused by distraction or diversion of attention and are particularly prevalent in maintenance tasks. In contrast, EOCs are often caused by inadequate training of procedures, poor instruction, or unawareness of hidden hazards. Although the scheme was expanded by [75] with two other categories (sequential errors, which are actions performed out of the correct order, and time errors, which are actions performed too slow, too fast, or too late), only the first two categories have been widely used in HRA, such as Technique for Human Error Rate Prediction (THERP) [75], since the 1980s. A second widely used classification scheme is the distinction between operators' intentions and their actual behavior [54], [63]. Under this scheme, human errors are classified into either slips (or lapses), which are instances in which the intention is correct but a failure occurs when carrying out the activities required, or mistakes, which arise from an incorrect intention, which leads to an incorrect action sequence, although this may be quite consistent with the wrong intention. Slips are normally results of inattention, misperceptions, losing track of one's place, and so on [62]. In contrast, mistakes result from human processing limitations, incorrect knowledge, or inadequate analysis to formulate a correct decision [61]. Skills, rules, and knowledge (SRK) taxonomy provides another framework for human error classification based on the different types of information processing involved [61]. According to the SRK taxonomy, operators' behavior in control rooms can be classified into three categories based on the levels of cognitive control: Skill-Based Behavior (SBB), Rule-Based Behavior (RBB), and Knowledge-Based Behavior (KBB). SBB consists of smooth, automated, and highly integrated patterns of action that are performed without conscious attention. It is usually based on feed forward, rather than feedback, control. A typical example of SBB is operators typing on a keyboard without visual support. RBB consists of stored rules derived from procedures, experience, instruction, or previous problem-solving activities. It is goal oriented but does not require reasoning. Actions are directly triggered merely by familiar perceptual cues in the environment. KBB requires analytical reasoning and consists of deliberate and serial search based on an explicit representation of goals and a mental model of the functional properties of the environment. The SRK

taxonomy-based scheme classifies human error into skill-based, rule-based, and knowledge-based errors. It should be noted that the slips/mistakes classification discussed earlier in text is closely related to the SRK classification.

Slips are skill-based because they are highly skilled and well-practiced activities and because they are caused by misapplied competence. Mistakes, in contrast, are largely confined to the rule- and knowledge-based domains. In the rule-based mode, an incorrect diagnostic rule leads to incorrect intention. In the knowledge based mode, incorrect intention results from considerable demands on operators' information-processing capabilities.

#### **5.1.4 Hypothetical factor structure for human errors related to HSI**

In an effort to develop a hypothetical factor structure for human errors related to HSI, the INPOOE database was first reviewed. A search in the database revealed 146 human error plant events listed under the categories of Control Room Operator Work Group and Man-Machine Interface Causal Factor between December 3, 1990, and April 24, 2008. Of those events, 106 can be classified as HSI related. Each of the HSI-related plant events was then analyzed to identify the causal factors.

The categorization proposed by the NRC in Human Factors Engineering (HFE) Guidelines [80], [81] was used as a starting point for the hypothetical factor structure development in this study.

This categorization classifies human factors issues in both advanced and conventional control rooms into eight categories: Information Display, User-System Interface, Process Control and Input Devices, Alarms, Analysis and Decision Aids, Inter-Personnel Communication, Workplace Design, and Local Control Stations. The categories and items in each category were expanded or deleted based on the actual plant events found in the INPO OE database. In addition, categories developed for control centers in nuclear or other industries were also examined. Examples of these categories include the discussion in [13] on factors important for structuring review criteria and the research on the control center of the railway traffic in Yugoslavia [16].

As listed in Table 5, the hypothetical factor structure developed in this study first classifies HSI-related human errors into four categories based on their causes: Operation Based, Controller Design Based, Deficient Indication Based, and Ambiguous Indication Based. The four categories are then broken down into 30 human error contributing items based on the analysis mentioned earlier in text. For most of these items, one representative source is listed for each of them in Table a. Items that do not have a reference source listed are simplified or paraphrased from the literature review and cannot be pinpointed into a single source document.

#### **5.1.5 Decision-action model**

Human activities in control rooms can be divided into two stages: cognitive information processing and manual task execution actions. Any incorrect activity occurring in this cognitive versus manual coupling

Event	Item	Source
Operation based	1. Operation movements. Operation requires small movements or jerkin/unsmooth motion.	[28]
	2. Simultaneous operation. Operator required to multitask.	[70]
	3. Control room/simulator discrepancies. Trained actions are not applicable to real scenarios.	[35]
	4. Operate equipment incorrectly. Due to inattention to details/distractions.	[31]
	5. Inappropriate compensation. From lack of trust in equipment.	[23]
	6. Overreliance. From overtrusting equipment.	[70]
	7. Defeated safety features. Manual override of safety features.	[26]
	8. Inexperience. From lack of operating hours on equipment.	[24]
Controller design based	9. Operate on wrong equipment. Due to similarity.	[36]
	10. Controls too far apart. Need excess movement to operate consecutive actions.	[10]
	11. Controls too close together. Poor design leads to inadvertent operation.	[29]
	12. Incorrect function allocation – Manual actions designed to be automated.	[18]
	13. Incorrect function allocation – Automated actions designed to be manual.	[18]
	14. Equipment allowing failures. Allowing operation outside of design parameters.	[34]
	15. Work-arounds. Known defects that require operators to take less direct action.	
16. Time limit to operation. Operation cannot be completed within the allowed time.	[22]	
17. No operator intervention allowed. To abort or assume control as necessary.	[53]	
Deficient indication based	18. No alarmnoting abnormal conditions and/or failures.	[30]
	19. Insufficient plant information.	[25]
	20. Boolean indication. Indication without level of severity.	[27]
	21. Unreliable indication. Indication known to reflect plant condition imperfectly.	[27]
	22. No feedback. Action is performed with no confirmation.	[6]
	23. No projection. No indication on anticipated result from action.	
	24. No trending. No indication on equipment failing over a prolonged time period.	[53]
Ambiguous indication based	25. Control panel visually crowded. Cannot take in presented information at a glance.	[16]
	26. Color/Sound coordination. Many indications of the same color/sound or all indications having different colors/sounds.	[32]
	27. Overindication. A single failure represented by more than one alarm.	
	28. Non-intuitive control.	
	29. Display challenges. Display font size/color or inconsistency in acronyms/labeling/terminology.	[33]
	30. Data searching. Extensive navigation needed to look for known existing.	[53]

Table 5: Hypothetical factor structure of HSI-related human errors in control rooms of nuclear power plants

will potentially lead to human errors. Inspired by [9], [72], a decision-action model was created to offer corrective action guidelines for current operating plants based on the stage at which a human error occurs. In the decision-action model, the decision represents the outcome of the cognitive information-processing stage, and four groups are considered as described in the following along with the suggested corrective action guidelines

1. Group I (no incident): Correct Decision + Correct Action. This group represents correct cognitive and manual action activities, hence no correction action is required;
2. Group II: Incorrect Decision + Correct Action. This group represents situations in which diagnosis is incorrect but the subsequent manual actions are correct under the wrong diagnosis. This type of human error can be prevented by improving operations procedure and general guidelines and by pre job briefing;
3. Group III: Correct Decision + Incorrect Action. This group represents circumstances in which manual actions are executed incorrectly with correct diagnosis. This type of human error can be prevented by additional operator training, peer checks, and management oversight;
4. Group IV: Incorrect Decision + Incorrect Action. This group represents situations in which diagnosis is incorrect and the subsequent manual actions are carried out incorrectly even under the wrong diagnosis. This type of human error can be prevented by control room modifications with human factor re-evaluation to the extended condition (cfr n. 1).

Incorrect decisions are cognitive errors that pertain to knowledge and judgment of the operator and are similar to the concept of “mistakes” described in [54]. Action represents manual task execution. Incorrect actions are similar to “slips”.

## **5.2 Characteristics of communications observed from the off-normal conditions of Nuclear Power Plants**

On July 30, 2006, cockpit crews took off from Incheon international airport at 1:56 p.m. after checking the boarding of crews. Since ground crew had confirmed that all flight crews were on board, the cockpit expected that all cabin crews were also on board because they understood flight crews as all the crews including the cockpit and the cabin crews. Accordingly the cockpit crews took off and flew for about 30 minutes. However, the cockpit crews realized that cabin crews were not on board. Consequently the airplane returned to Incheon international airport to take in the cabin crews. This brief reconstitution of an event that occurred at one of the international airports in the Republic of Korea is based on an article from a newspaper [17]. Although this event happened without any injured people or financial losses, there is no denying the fact that a communication, including an oral and/or a written communication, is one of the essential parts of everyday life. Communication is one of the decisive ways to exchange information among individuals [1]. Without communication, it is difficult to ask what we want to know as well as to provide what other people want to know.

As a result, many people (e.g., the cockpit crews of the airplane mentioned earlier) come across unanticipated situations when inappropriate communication has occurred. Unfortunately, the result of inappropriate communication is not always tolerable, especially when it has occurred among team members who operate a safety critical system. In other words, inappropriate communication will engender

unexpected consequences, because team members conduct many crucial activities (such as exchanging key information or coordinating shared resources) based on their communication [1], [69]. Actually, the statistical result of The National Aeronautics and Space Administration's (NASA's) Aviation Safety Reporting System (ASRS) revealed that the percentage of communication-related problems was more than 70% [4]. Similarly, it was revealed that approximately 92% of railway maintenance incidents were caused by communication-related problems [52]. In addition, it has been reported that communication related problems were twice as frequent as clinical skill errors in hospital deaths in Australia [88]. Accordingly, as many researchers have pointed out, the reduction of inappropriate communications is one of the prerequisites to securing the safety of any human-involved safety-critical systems, such as commercial airplanes, railway systems, off-shore oil platforms, and nuclear power plants [1], [15], [38], [69], [74], [77]. It should be emphasized, however, that the possibility of inappropriate communications would increase in proportion to the increase in workload. For example, the results of an existing study showed that, even under a stressful situation, highly experienced operating teams actively changed their communication patterns to maintain an average level of performance [68]. Similarly, it has been recognized that team members decreased the amount of communications when the level of their workload increased [79]. In addition, it has been observed that short-cut communications were frequently used when team members had to accomplish a task requiring a long task performance time [83]. Their results strongly indicated that team members seem to adaptively change the amount as well as the pattern of communication according to the nature of a situation at hand. If this is true, then it is necessary to investigate the characteristics of communication patterns under a stressful environment, because inappropriate communications that were caused by the stressful environment would be regarded as a novel source of human errors [48], [85]. For example, if human operators who are working in the Main Control Room (MCR) of a nuclear power plant reduce the amount of communication to cope with a high level of workload caused by off-normal conditions, then it is expected that the possibility of a human error, such as a misunderstanding, would increase due to a lack of communication. For this reason, the characteristics of communications observed under simulated off-normal conditions in nuclear power plants were investigated in this study. To this end, off-normal training sessions that have been conducted in the full scope simulator of the reference nuclear power plants were recorded by using audiovisual equipment. After that, detailed transcripts of all communication verbalized by human operators were created. Based on the communication transcripts, the characteristics of communications under off-normal conditions were identified by using a predefined speech act coding scheme. As a result, it was observed that the characteristics of communications were significantly varied with respect to the nature of off-normal conditions.



### **5.2.1 Previous work related to team communications**

Clear and effective communications are crucial for securing the safety of any human-involved systems. Accordingly, as summarized in Table 6, many researchers have put a great deal of effort into studying team communications with various purposes. For example, to identify the relationship between team performance and communication patterns under off-normal conditions [67] compared the scores of a team performance with predefined patterns of communications based on verbal protocols that were extracted from audiovisual records. Similarly, a comparison of team performance with communication patterns, classified by applying a predetermined speech act coding scheme to verbal protocols, has been conducted [40], [41]. In addition, several researchers tried to investigate the cognitive process of team members by scrutinizing verbal protocols extracted from a normal as well as an off-normal condition, such as identifying the characteristics of team decision making or identifying the mental model of team members [64], [73], [76]. It is to be noted that the research methods of team communications share at least two common elements – a verbal protocol analysis and a predefined coding scheme. In [2] one reads “There are many complex jobs in which the outcome of thinking does not emerge in observable action. For example, one can think out a plan of action, assess it, and decide it is inadequate for the purpose, or one can work out the implications of a situation, and memorize the decision for use later. If we want to train and support these types of work, then we need information about these mental processes. One apparently obvious way of getting this information is to ask people to ‘think aloud’ while they are doing the task. These verbal reports are called verbal protocols”.

Accordingly, the verbal protocol analysis would be regarded as “a meticulous investigation in order to extract useful information about detailed cognitive processes of human operators”. Although there is no explicit way of confirming that human operators express exactly what they think, many researchers have emphasized that analyzing verbal protocols is a good way to collect interesting as well as important insights observable while performing a task [11], [14], [78], [87]. For example, in [5] it is stated that: “Therefore, we turned to other domains and other problem solving skills from human subjects. Cognitive psychology has for some time been using a technique known as protocol analysis to arrive at such information”. In addition, [82] it is pointed out that, although resources, such as time or manpower, are required to generate verbal protocols, the verbal protocol analysis is generally preferred because it provides a rich source of data explaining the behavior of human operators. Actually, it is well known that the decision-ladder model that is one of the famous frameworks illustrating the cognitive processes of human operators in the course of decision making has been developed based on the results of the verbal protocol analysis [60], [59]. To conduct the verbal protocol analysis, it is indispensable to develop a well-defined coding scheme, by which the characteristics of verbal protocols are soundly identified. For this reason, many kinds of coding schemes have been suggested with respect to either the purpose of the verbal protocol analysis or the specificity of a domain. For example, [14] introduced a model-based coding scheme that is capable of distinguishing the following four types of statements

1. intention, representing goals and future states of the subject;
2. cognition, pertaining to attention to selected aspects of the current situation;
3. planning, pertaining to intermediate constructions to explore sequences of possibilities mentally;
4. evaluation, indicating explicit or implicit comparisons of alternatives.

In contrast, more sophisticated coding schemes have been suggested from the aviation and the nuclear domains as summarized in Tables 7 and 8, respectively [40], [49].

Reference	Domain	Purpose	Data source	Conditions	Analysis Method
[67]	Navy	Identifying the relationship between team performance and communication patt	Verbal protocols generated from audiovisual record	Off-normal conditions	Comparing the scores of a team performance with predefined patterns of communications
[83]	Aviation	Identifying the relationships between error types, learning stages, and communication patterns	Verbal protocols generated from audiovisual records	Normal and off-normal conditions	Comparing the scores of a team performance with communication patterns distinguished by a predefined speech-act coding scheme
[40],[41]	Aviation	Identifying the relationship between team performance and communication patterns	Verbal protocols generated from audiovisual records	Normal and off-normal conditions	Comparing the scores of a team performance with communication patterns distinguished by a predefined speech-act coding scheme
[73]	Psychology	Identifying mental model about a design team	Verbal protocols generated from audiovisual records	Normal conditions	Analyzing verbal protocols using a predefined coding scheme
[64]	NPP	Identifying the cognitive process among team members	Verbal protocols generated from audiovisual records. Analyzing verbal protocols using predefined types of cognitive processes	Off-normal conditions	Off-normal conditions
[76]	NPP	Identifying operators' mental model	Verbal protocols generated from audiovisual records	Off-normal conditions	Analyzing verbal protocols using predefined types of cognitive activities
[49]	NPP	Comparing communication patterns when human operators used computer- and paper-based procedure	Verbal protocols generated from audiovisual records	Off-normal conditions	Analyzing communication patterns based on a predefined speech-act coding scheme

Table 6: Previous works related to team communications

### 5.2.2 The off-normal operation strategy of nuclear power plants

To understand the importance of effective communication to cope with off-normal conditions, it is helpful to look at Fig. 18, which delineates the underlying strategy of off-normal operations in the reference nuclear power plants [8]. When an off-normal condition has occurred, human operators who are working in the MCR of an nuclear power plant have to follow predefined strategies according to the nature of the condition at hand – an abnormal condition and an emergency condition. First, the abnormal condition

Category	Definition
Command	A specific assignment of responsibility by one group member to another
Observation	Recognizing and/or noting a fact or occurrence relating to the task
Suggestion	Recommendation for a specific course of action
Statement of intent	Announcement of an intended action by speaker; includes statements referring to present and future actions but not to previous actions
Inquiry	Request for factual, task-related information; not a request for action
Agreement	A response in concurrence with a previous speech act; a positive evaluation of a prior speech act
Disagreement	A response not in concurrence with a previous speech act; a negative evaluation of a prior speech act
Acknowledgment	(a) Makes known that a prior speech act was heard (b) Does not supply additional information (c) Does not evaluate a previous speech act
Answer	Speech act supplying information beyond more agreement, disagreement, or acknowledgment
Response uncertainty	Statement indicating uncertainty or lack of information with which to respond to a speech act
Tension release	Laughter or humorous remark
Frustration/anger/derisive comment	Statement of displeasure with self, other persons, or some aspect of the task; or a ridiculing remark
Embarrassment	Any comment apologizing for an incorrect response
Repeat	Restatement of a previous speech act without prompting
Checklist	Prompts and replies to items on a checklist
Nontask-related	Any speech act referring to something other than the present task
Noncodable	Speech act which is unintelligible or unclassifiable with respect to the present coding scheme
Air Traffic Control (ATC)	Radio communication with ATC
Total communication	Sum of all the above

Table 7: Speech-act coding scheme used in the aviation domain

Category	Definition
Command-manipulation	A specific assignment of responsibility by one group member to another to manipulate an object
Command-others	An order to do anything other than manipulating an object
Call	A call for a specific person as a target for communication
Acknowledgment	A statement to indicate that a message was received
Inquiry-identification	A deliberate and well-defined request for information
Inquiry-confirmation	A statement for asking confirmation
Reply	A statement used to respond to an inquiry or other message that involves more information than a simple acknowledgment
Reply-confirmation	A short statement representing agreement or disagreement
Reply-report	A statement that reports the result of carrying out a command
Observation	A remark aimed at orienting other group members' attention to a specific aspect of operation
Statement of intent	An announcement of an intended action
Judgment	An expression that announces one's decision
Encouragement	A statement to build up team spirit
Nontask-related	A statement that does not refer to any aspect of the present task or operation
Uncodable	An ambiguous or unclear message

Table 8: Speech-act coding scheme used in the nuclear domain

covers the unstable status of the reference nuclear power plants due to one or more alarms. For example, if a single alarm has occurred, then human operators are able to select an appropriate alarm response procedure (ARP) by themselves, which is believed to be effective to remove the root cause of the generated alarm. Similarly, if human operators are faced with a set of alarms (i.e., multiple alarms), then they are able to select an appropriate abnormal operating procedure (AOP) to return to the normal con-

dition. When the emergency condition has occurred, however, human operators are not able to select an appropriate procedure based on their own decision any longer. Here, the emergency condition indicates a situation where in the reactor trip has occurred because either

1. human operators have failed to clear an abnormal condition resulting in one or more alarms,  
or
2. more serious problems that directly engendered the reactor trip have occurred.

When the reactor trip has occurred, human operators should start emergency tasks by conducting the standard post-trip action (SPTA) procedure to check the states of critical safety functions (CSFs). To sum up, CSFs define a set of crucial functions with their relative priority to prevent intolerable consequences resulting from emergency conditions. In other words, it is possible to secure the minimum level of safety, if all the CSFs of nuclear power plants are not jeopardized. Although there are several sets of CSFs, Table 9 summarizes some typical CSFs with the associated plant parameters, by which the status of each CSF can be monitored [12], [39], [86]. After the completion of the SPTA procedure, human operators have to conduct the diagnostic action (DA) that allows them to identify the nature of an emergency condition at hand (i.e., DA is a flowchart format procedure). In general, the emergency conditions of the reference nuclear power plants can be divided into two categories [8]. The first category includes Design Basis Accidents (DBAs) that can be ascertained by recognizing symptoms from various indicators and/or recent operating history. In the case of emergency conditions that belong to the second category, however, it is almost impossible to accurately identify them because either they have a complex nature or they have not been experienced. Canonical examples included in this category are multiple events (i.e., two or more emergency conditions have occurred simultaneously) or instrumentation failures that distort the correct symptom picture. Accordingly, to successfully cope with both categories of emergency conditions, two kinds of Emergency Operating Procedures (EOPs) are provided for human operators. The first one is an Optimal Recovery Procedure (ORP) that stipulates detailed tasks to be done by human operators that directly lead the state of the reference nuclear power plants to the safe shutdown condition. Meanwhile, for the emergency conditions that belong to the second category, a functional recovery procedure (FRP) is developed to provide the restoration tasks regarding the jeopardized CSFs. Therefore, based on the result of DA, human operators have to select either an ORP (when they clearly diagnose what event has occurred) or an FRP (when they fail to identify what event has occurred). In addition, human operators have to conduct an FRP if they recognize the jeopardy of any CSF by conducting a safety function status check (SFSC) procedure that should be carried out in parallel with the performance of an ORP.

CSF number of inserted control rods	Associated Parameter
Reactivity control	Neutron flux; status of trip breakers number of inserted control rods, etc.
Core heat removal	Core exit temperature; status of reactor coolant pumps (RCPs), etc.
Reactor Coolant System (RCS) heat removal	Water level of steam generators (SGs); steam pressure of SGs; feed water flow rate, etc.

Table 9: A part of typical CSFs considered in the reference nuclear power plants

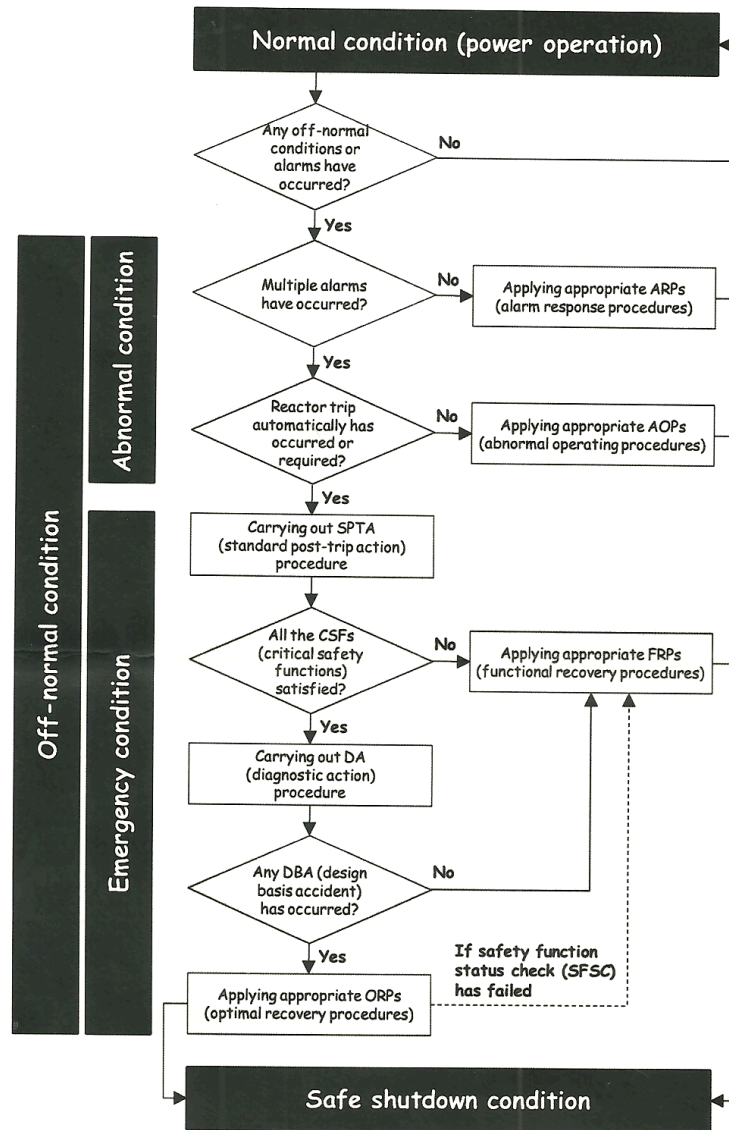


Figure 18: The off-normal conditions of nuclear power plants

### 5.2.3 The role of human operators working in the MCR of nuclear power plants

Human operators working in the MCR of the reference nuclear power plants have to conduct a series of predefined activities along with the nature of an off-normal condition. To this end, it is evident that

human operators need a huge amount of information, such as plant process parameters, the status of major components, and so forth. This strongly implies that human operators have to intensively communicate with each other to ask what they want to know as well as to answer the questions asked. In light of this concern, although there are several different types of team structures in nuclear power plants [51], Fig. 19 will be helpful in understanding the structure of a four person team that has the responsibility for operating the reference nuclear power plants.

In the reference nuclear power plants, each operating team working in the MCR consists of four human operators with their distinct duties

1. a senior reactor operator (SRO);
2. a reactor operator (RO);
3. a turbine operator (TO);
4. an electrical operator (EO).

In short, the SRO has the responsibility for all kinds of operations performed under off-normal conditions, and the RO and the TO have limited responsibility for operations related to the primary side (i.e., nuclear island) and the secondary side (i.e., turbine island), respectively. In addition, the EO simultaneously checks the status of electric power production as well as the supplement of an electrical power about all kinds of components and/or equipment installed in the reference nuclear power plants. To this end, each board operator (i.e., the RO, the TO, and the EO) has to manipulate many kinds of necessary components and equipment by using several control boards that are installed in the MCR with a lot of alarm tiles, indicators, trend recorders, control devices, and so forth. In addition, if necessary, board operators directly communicate with local operators (LOs) who are working near a moving component or equipment to give detailed instructions. It is to be noted that, as soon as the reactor trip has occurred (i.e., an emergency condition), another operator, called a safety supervisor (SS), has to join this four-person team. The role of the SS is to independently check the status of CSFs in parallel with emergency operations to be performed by four human operators. Because role of the SS under the emergency condition is more important than that of the EO, it is possible to regard the composition of the four-person team as the SRO, the RO, the TO, and the SS [57].

#### **5.2.4 Communications for off-normal operations**

It is evident that human operators working in the MCR of the reference nuclear power plants need to intensively communicate to follow a predefined strategy about an off-normal condition. Without loss of generality, Fig. 20 depicts four high-level tasks related to the reacting strategy of an off-normal condition. For example, when an abnormal condition has occurred, the first task is to detect one or more alarms indicating the occurrence of the abnormal condition. After that, human operators should

interpret the meaning of the generated alarms by gathering a set of symptoms, such as process parameters or the status of major components. If human operators have successfully identified the meaning of the generated alarms, then they will select an appropriate ARP or AOP that is supposed to effectively remove the cause of the abnormal condition with which they are faced. Similarly, although the high-level task related to clarifying the nature of a problem is institutionalized in the form of procedures (i.e., SPTA and DA procedure), human operators still have to complete four high level tasks when an emergency condition has occurred. Here, it is to be noted that communications play a crucial role in conducting the high-level tasks just mentioned.

Regarding this, [67] clearly summarized the role of communications in the course of a task performance as follows: “Communication during task execution is important for developing and maintaining team and situation knowledge in shared mental models. Furthermore, communication is especially important for developing strategic knowledge. With respect to team knowledge, communication supports team members to develop a common understanding of who is responsible for what task and what the information requirements are. With respect to situation knowledge, communication is important for maintaining an up-to-date understanding of the situation. Especially in novel situations, team members must communicate to respond to environmental cues, explain to each other why previous strategies do not work in the novel situation, jointly determine new strategies, and predict future states”.

The role of communications to deal with an off normal condition is more important than it seems, however, because human operators should conduct the previously described behaviors under a stressful, such as a high level of time pressure, as well as an unstable environment, i.e. a trivial mistake could result in a severe consequence [45], [48]. For example, it has been observed that human operators decreased their amount of communications with respect to the increase of a workload [79]. In addition, it has been reported that human operators adaptively changed their communication patterns when they had to accomplish the required tasks in a stressful environment [68].

This strongly implies that, as pointed out in [85], the change of communication patterns to cope with the increase of a workload due to a stressful environment could be a new source of a human error. Actually, the result of a recent study has revealed that one of the main causes of an unplanned reactor trip event is an inappropriate response to an off-normal condition, which is expected to be susceptible to communications [43]. In addition, communication is one of the important issues pertaining to emerging nuclear power plant technology [56], [89]. Accordingly, it is reasonable to assume that securing appropriate communication is one of the decisive factors for the successful completion of four high-level tasks to deal with off-normal conditions.

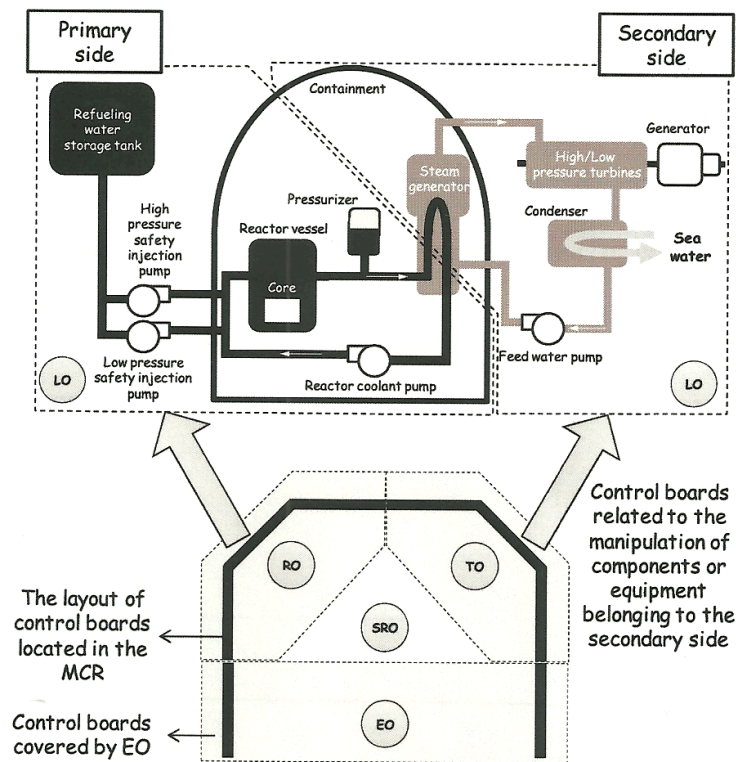


Figure 19: Simplified scheme of the roles of four human operators who are working in the MCR of the reference nuclear power plants

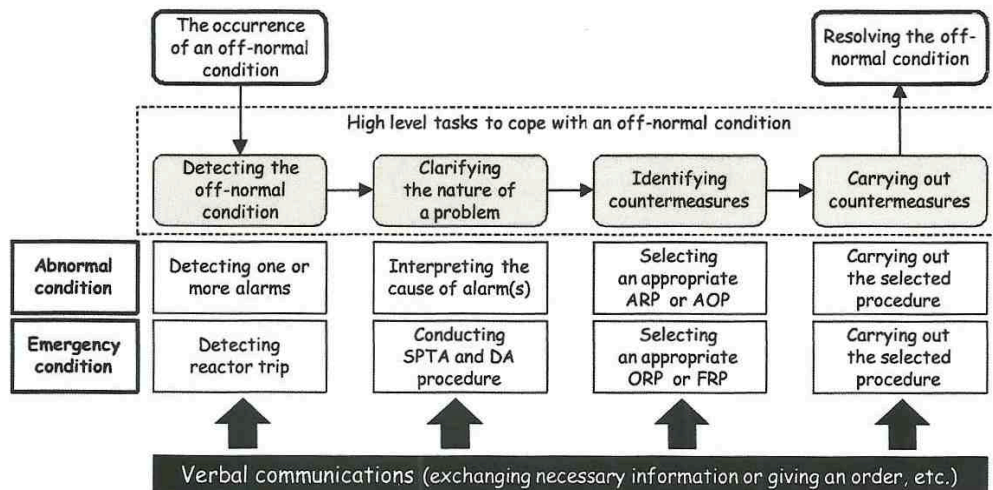


Figure 20: High-level tasks to cope with an off-normal condition



### **5.3 Description of the main systems of supervision, control and intervention of all the nuclear power plant and of the primary circuit in MCR e in RSR with description of critical situations in MCA, RSR and in TSC**

This section is devoted to the description of the main systems of supervision, control and intervention of all the nuclear power plant and of the primary circuit, and the description of the MCR and of the RSR, and of possible critical situations.

First, a brief summary of all the safety-related systems will be given. Then, the reactor trip systems, consisting of the class 1 E systems (safety sensors, RPS, RTB, safety grade HSIS) and the reactor trip variables and signals connected to low pressurizer pressure, high pressurizer pressure and high pressurizer water level, will be studied. Hence, we will investigate thoroughly the engineered safety feature systems, which consists of safety sensors, RPS, ESFAS, SLS, safety grade HSIS, which includes processors and VDUs common to above both RPS and ESFAS, conventional safety related switches. We will also treat the process variables monitored for the ESF like pressurizer pressure, pressurizer water level and the MCR isolation. The normal and safe shutdown from outside the MCR and normal and safe shutdown functions, will be studied. The post accident monitoring and the safety parameter displays system will be therefore analyzed. Moreover, the control systems not required for safety that can affect the performance of critical safety function describing the pressurizer pressure control, the pressurizer spray interlock and the pressurizer water level control, will be presented. Finally, we will present the diverse HSI Panel, the reactor trip, the turbine Trip and the main feedwater isolation.

#### **5.3.1 Identification of safety related systems and non safety-related systems**

Safety-related PSMS with safety-related portion of the HSIS consists of

1. RPS;
2. ESFAS and SLS;
3. Conventional switches (train level);
4. Safety VDUs – Part of safety-related HSIS for manual operation and monitoring of critical safety functions, including PAM.

A brief summary of all the safety-related systems is presented in this section, while more detailed descriptions will be given afterwards for reactor trip system, for engineered safety feature systems, for systems required for safe shutdown, for information systems important to safety, for control systems not required for safety, for diverse instrumentation and control systems.

Safety functions are those actions required to achieve the system responses assumed in the safety analyses, and those credited to achieve safe shutdown of the plant. Some safety functions are automatically initiated by the PSMS. These same safety functions may also be manually initiated and monitored

by operators using the HSIS. The HSIS is also used to manually initiate other safety functions that do not require time critical actuation and safety functions credited for safe shutdown. After manual initiation from the HSIS, all safety functions are executed by the PSMS. The HSIS also provides all plant information to operators, including critical parameters required for post accident conditions. The HSIS includes both safety and non-safety sections.

#### **5.3.1.1 Reactor Trip System**

The safety systems automatically trip the reactor and initiate Engineered Safety Features (ESF), if required, whenever predetermined limits are approached. The RPS maintains surveillance on nuclear and process variables, which are related to equipment mechanical limitations, such as pressure, and on variables that directly affect the heat transfer capability of the reactor, such as the reactor coolant flow and temperature. When a limit is approached, the RPS initiates the signal to open the Reactor Trip Breakers (RTBs). This action removes power from the Control Rod Drive Mechanism (CRDM) coils, permitting the rods to fall by gravity into the core. This rapid negative reactivity insertion will cause the reactor to shutdown.

#### **5.3.1.2 Engineered Safety Feature Systems**

The occurrence of a Postulated Accident (PA), such as a Loss-Of-Coolant Accident (LOCA) or a steam line break, requires a reactor trip plus actuation of one or more ESFs in order to prevent or mitigate damage to the core and Reactor Coolant System (RCS) and to ensure containment integrity.

#### **5.3.1.3 Reactor Protection System**

The RPS will determine if setpoints are being approached for selected plant parameters. If setpoints are approached, the RPS will process signals through logic functions, to respond properly to the various conditions.

#### **5.3.1.4 Engineered Safety Features Actuation System**

Once the required logic is generated, the RPS will send signals to the ESFAS, which combines signals from all four RPS trains in 2-out-of-4 voting logic. Once the ESFAS receives the appropriate voting logic combination, it sends signals to the SLS to actuate appropriate ESF components for protective action. The ESFAS also receives signals from conventional switches on the OC for train level manual actuation of ESF systems. In the event of loss of offsite power (LOOP) and/or PA, ESF loads are connected to the emergency power bus in a pre-determined sequence by the load sequencing function, provided by the ESFAS and SLS. There are two types of load sequencing: one for LOOP and the other for emergency core cooling system (ECCS) actuation concurrent with LOOP. The ESFAS also receives interlock signals from the RPS, such as the P-4 interlock, which indicates the reactor trip. Interlocks are developed redundantly within each RPS train.

The RPS will send interlock signals to the ESFAS, which combines signals from all four RPS trains in 2-out-of-4 voting logic.

#### **5.3.1.5 Safety Logic System**

The SLS receives ESF system level actuation demand signals and LOOP load-sequencing signals for the safety components from the ESFAS. The SLS also receives manual component level control signals from the OC (safety VDUs and operational VDUs). This system performs the component level control logic for safety actuators (e.g., Motor Operated Valves (MOVs), solenoid operated valves, switchgears).

The SLS receives manual component level control signals from the OC (safety VDUs and operational VDUs) to control plant components to achieve safe shutdown.

#### **5.3.1.6 Safety Grade HSI**

The safety VDU processors manage the displays on the safety VDUs located on the OC and the RSC. They receive process parameter information from the RPS, actuation status information from the RPS and ESFAS, and component status information from the SLS. The safety VDU processors also receive operator commands such as screen navigation and soft control from the safety VDUs. The safety VDUs are located on the OC and RSC and provide access to information and controls for safety systems. Command signals from safety VDUs and operational VDUs are transmitted to the RPS, ESFAS and SLS via the PSMS communication system (COM). COM is the interface system between the safety-related PSMS and non-safety related PCMS. It provides command priority logic between the safety VDUs and operational VDUs.

#### **5.3.1.7 Post Accident Monitoring**

The purpose of displaying PAM parameters is to assist MCR personnel in evaluating the safety status of the plant. In accordance with RG 1.97 PAM Type A, B, and C variables have redundant instrumentation and can be displayed on at least two redundant safety VDUs. Type A and B parameters are continuously displayed on the LDP and are continuously available on a safety VDU, or can be retrieved immediately.

#### **5.3.1.8 Bypassed and Inoperable Status Indication**

If any safety function is bypassed or inoperable at the train level, this is continuously indicated on the LDP. Other bypassed or inoperable conditions that do not result in inoperability of safety functions, at the train level, are displayed on operational VDUs but not on the LDP.

#### **5.3.1.9 Plant Alarms**

The alarm system provides all information necessary for detecting abnormal plant conditions. The alarm system enhances the operators ability to recognize fault conditions even when the number of faults, or their severity, are increasing. Information for all alarms is displayed on the alarm VDU, LDP, and the operational VDU. LDP alarms are located in the fixed area of the LDP.

#### **5.3.1.10 Safety Parameter Display System**

The Safety Parameter Display System (SPDS) provides a display of plant parameters from which the status of plant safety system operation may be assessed. The SPDS is displayed on operational VDUs

located in the MCR, TSC, and EOF. The primary function of the SPDS is to aid MCR operating personnel to make quick assessments of plant safety status. Duplication of the SPDS displays in the TSC and EOF improves the exchange of information between these facilities and the control room and assists plant management in the decision-making process. The SPDS operates during normal operations and during all classes of emergencies. The SPDS displayed information in the MCR, TSC, and EOF is identical. The functions and design of SPDS in the MCR are integrated into the overall Human-System Interface (HSI) design.

#### **5.3.1.11 Independence**

Each train of the PSMS is independent from each other and from non-safety systems, including the PCMS. The physical independence is designed based on the RG 1.75 which endorses IEEE Std 384-1992. Electrical independence is maintained through qualified isolation devices, including fiber optic data communications cables. Functional independence between controllers is maintained through communication processors that are separate from function processors, and through logic that (1) ensures prioritization of safety functions over non-safety functions and (2) does not rely on signals from outside its own train to perform the safety function within the train. Cabinets for each train of the PSMS are located in a separate plant equipment room fire area. These fire areas are separate from the fire areas where non-safety systems are located and separate from the fire areas of the MCR and the RSR. To ensure electrical independence, fiber optic cables or qualified isolators are used to interface all signals between plant equipment room fire areas. Electrical independence is also maintained between PSMS divisions and between the PSMS and non-safety systems within the MCR and the RSR. In addition to these plant equipment room fire areas, electrical independence and physical separation are also maintained between divisions for instrumentation inputs and plant component control outputs interfaced with PSMS cabinets.

#### **5.3.1.12 Human-System Interface**

The MCR is designed to perform centralized monitoring and control of the I&C systems that are necessary for use during normal operation, AOOs, and PAs. Furthermore, the HSIS are also designed to reduce the potential for human error and to allow easy operation. In addition to the MCR, the HSI also includes the RSC, TSC, EOF, and local control stations, such as auxiliary equipment control console.

### **5.3.2 Reactor Trip System**

#### **5.3.2.1 System Description**

The reactor trip (RT) system, which achieves the all RT functions, consists of the following Class 1E systems

1. Safety sensors;
2. RPS

Name	Quantity
Reactor Trip CCS Actuation	4
ECCS actuation	4
Containment Isolation Phase A	4
Containment Spray	8
MCR Isolation	4
Main Steam Line Isolation	2
Main feedwater Isolation	2
Emergency Feedwater Isolation	2 per loop
Emergency Feedwater Actuation	4
CVCS (Chemical and Volume Control System) Isolation	2
Turbine Trip	1
DAS Defeat (DAS Bypass)	1

Table 10: List of conventional switches on the operator console

Applicable criteria	Title	RPS	ESFAS	SLS	Safety HIS	Safety DCS	PCMS	DAS
	1.10 CFR 50 and 52							
a	50.55a(a)(1) Quality standards for systems important to safety	×	×	×	×	×		
b	50.55a(h)(2) Protection systems (IEEE Std 603–1991 or IEEE Std 270–1971)	×	×	×	×	×		
c	50.55a(h)(3) Safety systems (IEEE Std 603–1991)	×	×	×	×	×		
d	50.34(f)(2)(v) (I.D.3) Bypass and inoperable status indication	×	×	×	×	×	×	
e	50.34(f)(2)(xi) (II.D.3) Direct indication of relief and safety valve position			×		×	×	
f	50.34(f)(2)(xii) (II.E.1.2) Auxiliary feedwater system automatic initiation and flow indication	×	×	×	×	×		
g	50.34(f)(2)(xvii) (II.F.1) Accident monitoring instrumentation	×		×	×	×	×	
h	50.34(f)(2)(xviii) (II.F.2) Instrumentation for the detecting of inadequate core cooling	×			×	×		
i	50.34(f)(2)(xiv) (II.E.4.2) Containment isolation systems	×	×	×	×	×		
j	50.34(f)(2)(xix) (II.F.3) Instruments for monitoring plant conditions following core damages	×			×	×		
k	50.34(f)(2)(xx) (II.G.1) Power for pressurizer level indication and controls for pressurizer relief and block valves	×		×	×	×		
l	50.34(f)(2)(xxii) (II.K.2.9) Failure mode and effect analysis of integrated control system							

Table 11: Regulatory requirements applicability matrix per Nureg 0800 Standard Review plan (SRP) Sec. 7.1. Rev. 5

### 3. RTB

### 4. Safety grade HSIS.

Fig. 21 shows the RPS configuration, while Fig. 23 shows the overall reactor trip functional logic. The RPS automatically trips the reactor to ensure that specified acceptable fuel design limits are not exceeded. Fuel design limits are defined by several considerations, such as mechanical/hydraulic limitations on equipment, and heat transfer phenomena. The RPS maintains surveillance of process variables, which are direct measurements of equipment mechanical limitations, such as pressure and also on variables that are direct measurements of the heat transfer capability of the reactor (e.g., reactor coolant flow and reactor coolant temperature). Other parameters utilized in the RPS are calculated indirectly from a

combination of process variables, such as delta T (i.e., reactor coolant hot leg temperature [Thot] - reactor coolant cold leg temperature [Tcold]). Whenever a direct process measurement or calculated variable exceeds a setpoint, the reactor will be shutdown in order to protect against either gross damage to the fuel cladding or a loss of system integrity, which could lead to the release of radioactive fission products into the containment vessel (C/V).

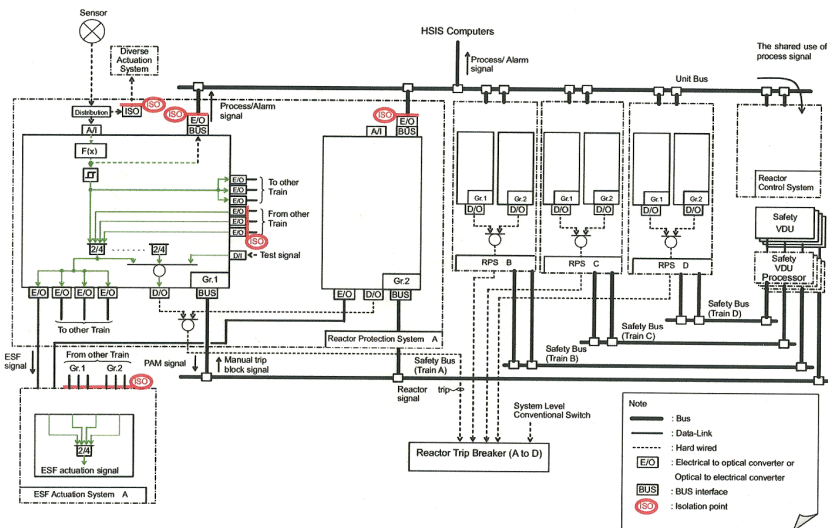


Figure 21: RPS configuration

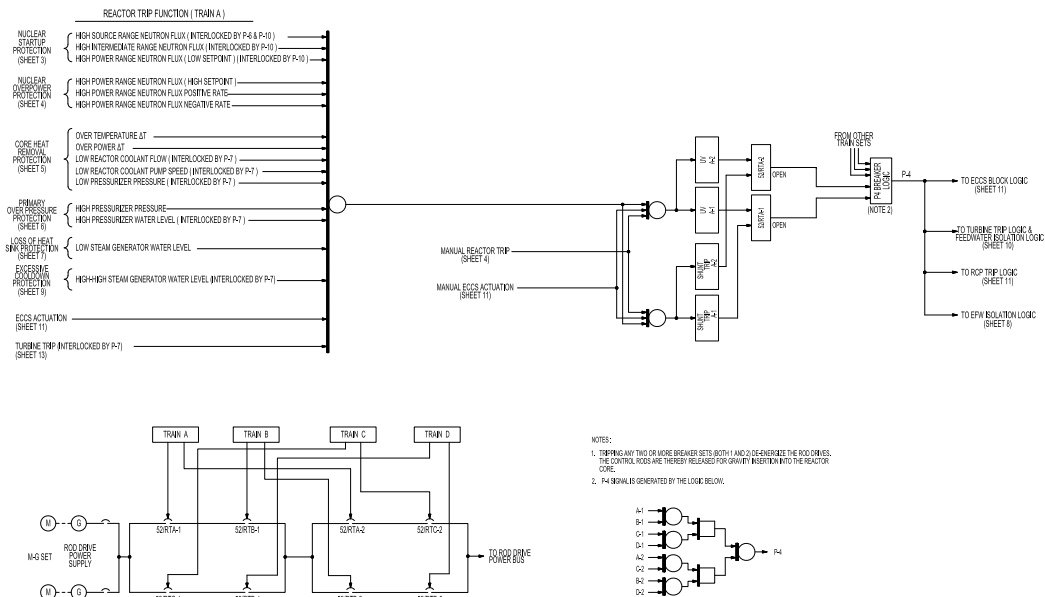


Figure 22: Functional logic diagram for reactor protection and control system

To initiate a reactor trip, the RPS interfaces with the following equipment

1. Sensors and manual inputs;
2. RTBs.

The RPS consists of four redundant and independent trains. Four redundant measurements using sensors from the four separate trains are made for each variable used for reactor trip. This applies to all measurements with the exception of source range and intermediate range nuclear instrumentation sensors and main turbine stop valve position, which only have two trains. Selected analog measurements are converted to digital form by analog-to-digital converters within the four trains of the RPS. When the monitored signal requires signal conditioning, it is applied prior to its conversion to digital form. Following necessary calculations and processing, the measurements are compared against the applicable setpoint for that variable. A partial trip signal for a given parameter is generated if one train's measurement exceeds its limit. Each train sends its own partial trip signal to each of the other three trains over isolated serial data links. The RPS will generate a RT signal if two or more trains of the same variable are in the partial trip state.

The RPS sends system status and process data to the non safety-related part of the HSIS and PCMS, via the unit bus. The RPS also receives operator bypass and reset signals from the HSIS, which are not required for safety, via the unit bus. The interfaces between RPS trains and other systems are shown in Fig. 23 and described in Table 12.

7. INSTRUMENTATION AND CONTROLS

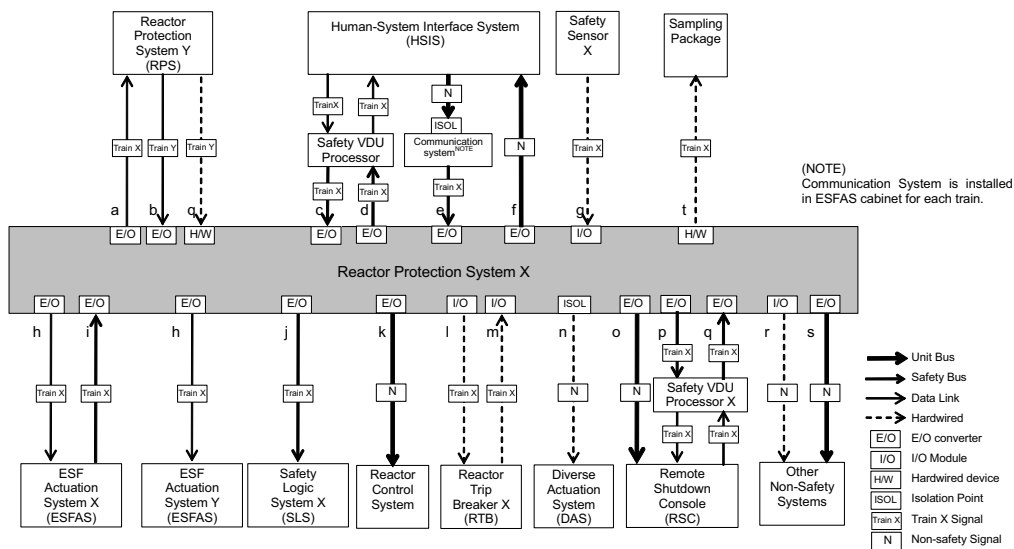


Figure 23: Interface between RPS and other systems

Figure 7.2-3 Interface between RPS and Other Systems (for Table 7.2-1)

5.3.2.2 Reactor Trip Logic

**Tier 2** **7.2-54** **Revision 3**  
 Each train of the RPS consists of two separate digital controllers to achieve defense-in-depth through functional diversity. Two different parameters are monitored by the separate sensors that interface to

Interface signals	Example of signals
(a) signal to other RPS trains	RT signals, bypass signals
(b) Signals from other RPS trains	RT signals, bypass signals
(c) Operation signals from safety VDU	Manual trip signals, operating and maintenance bypass
(d) Information signals to safety VDU	PAM signals, process status signals
(e) operation signals from operational VDU	Manual block, operating and maintenance bypass
(f) Information signals to non safety HSIS	Non safety indication, record and alarm signals
(g) Sensor signals	SG water level, NIS, RMS signals, turbine trip status signals
(h) ESF actuation signals to ESFAS	ESF actuation signals
(i) ESF actuation signals from ESFAS	ECCS actuation signals
(j) Interlock signals to SLS	Reactor coolant pressure signal, CCW surge tank water level for interlocks
(k) Process signals to reactor control systems	Pressurizer water level signal, pressurizer water level bypass signals, interlocks signals
(l) RT signals to SLS	RT Signals
(m) Status signals from RTB	RT status signals
(n) Process signals to DAS	Actuation signals, indication signals
(o) Non safety signals to RSC	Signals for non safety-related indication, record and operation for RSC
(p) Safety signals to RSC	Signals for safe shutdown to RSC
(q) Safety signals from RSC	Signals for safe shutdown from RSC
(r) Non safety signals to various purpose	Various uses as control, test and monitoring by hardwired or optical signals
(s) Hardwired signals from RPS (other train)	Source range neutron flux detector power off
(t) Control signals to the sampling package at local	Start/stop demand to the sampling pump

Table 12: Interface between RPS and other systems

two separate digital controllers within the RPS. Each of controllers process these inputs to generate reactor trip and/or ESF actuation signals. This twofold diversity is duplicated in each redundant RPS train. The processing of diverse parameters results in functional redundancy within each RPS train. Functional diversity provides two separate methods of detecting the same abnormal plant condition. Each functionally diverse digital controller within a train can initiate a reactor trip. The RT signal from each of the four RPS trains is sent to a corresponding RT actuation train. Each of the four RT actuation trains consists of two RTBs. The reactor is tripped when two or more RT actuation trains receive a RT signal. When a limit is approached, the RPS initiates signals to open the RTBs. This action removes power to the CRDM coils permitting the rods to fall by gravity into the core. This rapid negative reactivity insertion will cause the reactor to shutdown. The breakers are located in two fire-protected areas. Breakers with a “1” designation are located in one room. Breakers with a “2” designation are located in the second room. This configuration ensures a fire in one room does not prevent a reactor trip.

The cables of each train are isolated for fire. The isolation between train A and B and between train C and D is based on IEEE Std 384–1992 including minimum distance and barriers. Isolation between train A/B and train C/D is by separate fire areas. The logic functions within the RPS are limited to bistable calculations and voting for RT actuation. Each train performs 2-out-of-4 voting logic for like sensor coincidence to actuate trip signals to the four trains of the RTBs. Each train also includes a hardwired manual switch on the OC that directly actuates the RTBs. This switch bypasses the RPS digital controller.



The trip demand, whether generated manually or automatically, initiates the following actions: 1) it de-energizes the under-voltage trip attachments on the RTBs, and 2) it energizes the shunt trip devices on the RTBs. Either action causes the breakers to trip.

The RPS is a microprocessor-based digital system that achieves high reliability through segmentation of primary and back-up trip/actuation functions, use of four redundant trains, failed equipment bypass functions, and microprocessor self-diagnostics, including data communications. The system also includes features to allow for manual periodic testing of functions that are not automatically tested by the self-diagnostics, such as the actuation of RTBs. Manual periodic tests can be conducted with the plant on-line and without jeopardy of spurious trips due to single failure(s) during testing.

### 5.3.2.3 Reactor Trip Variables

The following variables and signals are monitored to generate a reactor trip signal. The complete list of RT initiating signals is provided in Table 13. Table 14 provides range, accuracy, response time, and setpoint for each RT variables. Response time described in this table is within the delay time assumed in the safety analyses. Setpoint described in this table is within the analytical limit assumed in the safety analysis.

Actuation signal	Number of sensors, switches, or signals	Division trip actuation logic	Permissives and bypass
High source range neutron flux	2 neutron detectors	1/2	P-6, p-10
High intermediate range neutron flux	2 neutron detectors	1/2	P-10
High power range neutron flux (low set-point)	4 neutron detectors	2/4	P-10
High power range neutron flux (high set-point)		2/4	None
High power range neutron flux positive rate		2/4	None
High power range neutron flux negative rate		2/4	None
Over temperature $\Delta T$		1 composite signal per RCS loop	2/4
Over power $\Delta T$	1 composite signal per RCS loop	2/4	None
Low reactor coolant flow	4 flow sensor per RCS loop	2/4 per RCS loop	P-7
Low RCP speed	1 speed sensor per RCP	2/4	P-7
Low pressurizer pressure	4 pressure sensors	2/4	P-7
High pressurizer pressure		2/4	None
High pressurizer water level	4 level sensor	2/4	P-7
Low SG water level	4 level sensor per SG	2/4 per SG	None
High SG water level		2/4 per SG	P-7
Manual reactor trip	1 switch per train	1/1	None
ECCS actuation	Valid signal	N/A	None
Turbine trip	Valid signal	N/A	P-7

Table 13: Reactor trip signals

Some of the following variables are used by multiple safety functions and non-safety control functions;

1. Neutron flux (source range, intermediate range and power range, neutron flux rate for power

- range);
2. Reactor coolant cold leg and hot leg temperature;
  3. Pressurizer pressure;
  4. Pressurizer water level;
  5. Reactor coolant flow;
  6. Reactor Coolant Pump (RCP) speed;
  7. Steam Generator (SG) water level;
  8. ECCS actuation signal;
  9. Manual RT actuation signal;
  10. Turbine trip signal.

#### **5.3.2.4 Reactor Trip Initiating Signals**

The following subsection describes the RT initiating signals that are grouped according to their protection function. Pre-trip alarms and non-safety interlocks are initiated below the RT setpoints to provide audible and visible indication of the approach to a trip condition.

#### **5.3.2.5 Low Pressurizer Pressure**

This trip protects the reactor against low pressure, which could lead to DNB. RT is initiated when two out of four pressurizer pressure channels exceed the low setpoint. This trip is automatically bypassed when reactor power is below P-7 permissive setpoint (turbine inlet pressure or power range neutron flux). The operating bypass is automatically removed when reactor power is above the P-7 permissive setpoint. Fig. 25 shows the logic for this trip function.

#### **5.3.2.6 High Pressurizer Pressure**

This trip protects the RCS against system over pressure. The trip signal is generated when two out of four pressurizer pressure channels exceed the trip setpoint. There are no operating bypasses associated with this trip. Fig. 25 shows the logic for this trip function.

#### **5.3.2.7 High Pressurizer Water Level**

This trip prevents water relief through the pressurizer relief valves for system over pressurization. The trip signal is generated when two out of four pressurizer water level channels exceed the trip setpoint. This trip is automatically bypassed when reactor power is below P-7 permissive. This operating bypass is automatically removed when reactor power is above the P-7 setpoint. Fig. 25 shows the logic for this trip function.

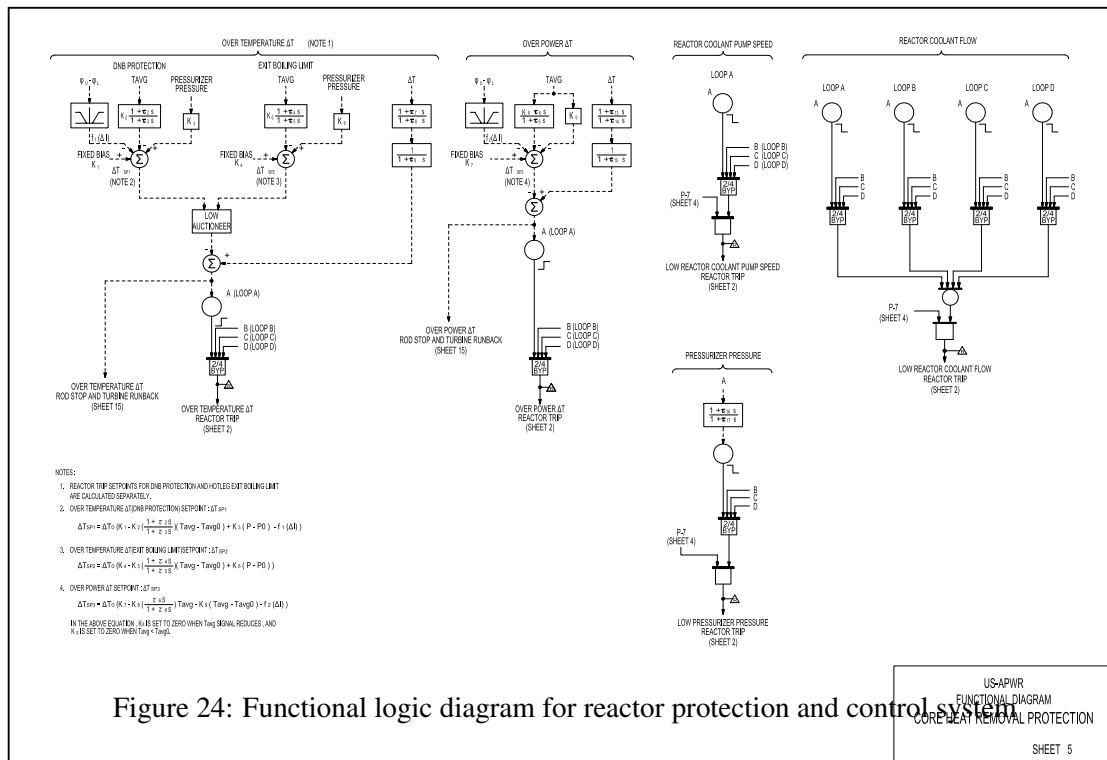


Figure 24: Functional logic diagram for reactor protection and control system

Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 5 of 21)

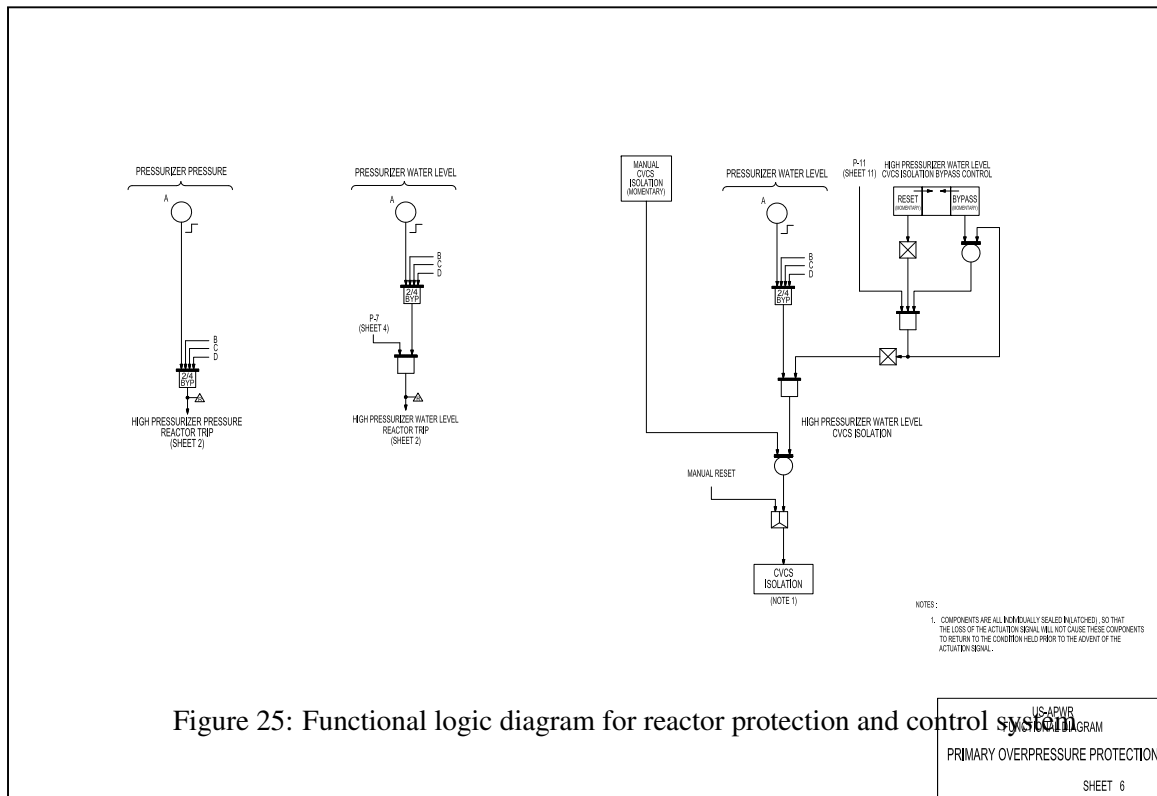


Figure 25: Functional logic diagram for reactor protection and control system

Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 6 of 21)

RT Function	Variables to be monitored	Range of variables	Instrument accuracy	Response time	Setpoint
Over power $\Delta T$	(a) $\Delta T$	0 to 150%	Total 5,2% RTP	Total 6.0 s	110.65% RTP
	(b) reactor coolant cold leg temperature	510 to 630°F			
	(c) reactor coolant hot leg temperature	530 to 650°F			
	(d) neutron flux (difference between top and bottom power range neutron flux detectors)	-60 to + 60%			
Low reactor coolant flow	Reactor coolant flow	0 to 120% of rated flow	3% of rated flow	1.8 s	90% of rated flow
Low RCP speed	RCP speed	0 to 120% of rated pump speed	0.5% of rated pump speed	0.6 s	95.5% of rated flow
Low pressurizer pressure	Pressurizer pressure	1700 to 2500 psig	2.5% of span	1.8 s	
High pressurizer pressure	Pressurizer pressure	1700 to 2500 psig	2.5% of span	1.8 s	
High pressurizer water level	Pressurized water level	0 to 100% of span	3% of span	1.8 s	
Low SG water level	SG water level	0 to 100% of span (narrow range taps)	3% of span	1.8 s	
High high SG water level	SG water level	0 to 100% of span (narrow range taps)	3% of span	1.8 s	70% of span
manual reactor trip actuation	Switch position	N/A	N/A	N/A	N/A
ECCS actuation	Pressurizer pressure	1700 to 2500 psig	2.5% of span	3.3 s	1765 psig
	Main steam line pressure	0 to 1400 psig	3% of span	3.3 s	525 psig
	Containment pressure	-7 to 80 psig	2.8% of span	3.3 s	6.8 psig

Table 14: Reactor trip variables, ranges, accuracies, response time and setpoint (nominal)

### 5.3.3 Engineered Safety Feature Systems

#### 5.3.3.1 System Description

The ESF system consists of

1. Safety sensors;
2. RPS;
3. ESFAS;
4. SLS;
5. Safety grade HSIS which includes processors and VDUs common to above both RPS and ESFAS;

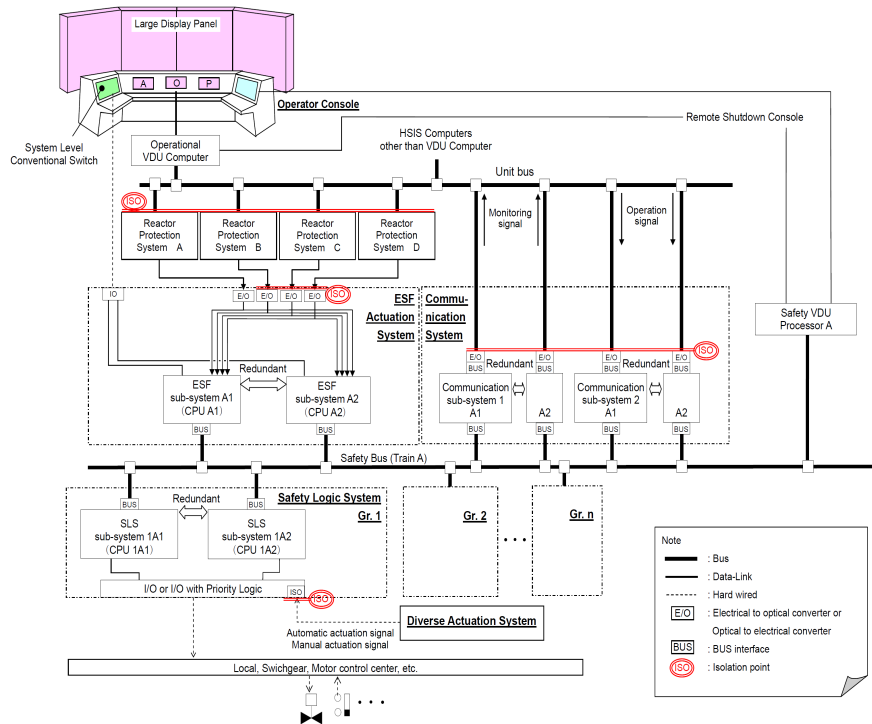


Figure 7.3-1 Configuration of Engineered Safety Features Actuation System and Safety Logic System  
 Figure 26: Configuration of engineered safety features actuation system and safety logic system

Tier 2

7.3-36

Revision 3

6. Conventional safety-related switches (for system related actuation).

Fig. 26 shows the overall ESF system configuration.

ESF systems provide I&C functions to sense accident conditions and initiate the operation of necessary ESF system components to mitigate accident conditions in a timely manner. The occurrence of a PA, such as a LOCA or a steam line break, requires a RT plus actuation of one or more ESF systems in order to mitigate the consequences. The RPS receives signals from various sensors and transmitters. The RPS then determines if the set-points are being exceeded and, if they are, the RPS combines the signals into logic matrices indicative of primary or secondary system boundary ruptures.

Once the required logic combination is completed, the RPS sends ESF actuation signals to each train of the ESFAS. Each train of the ESFAS combines the signals from all RPS trains using 2-out-of-4 voting logic to actuate its respective train of the SLS.

Control from the ESF system includes; the ECCS, containment systems, containment spray system (CSS), emergency feedwater system (EFWS), annulus emergency exhaust system, and MCR HVAC system. These systems, its subsystems and/or components are actuated by the ESFAS signal as necessary to mitigate specific accident/event condition(s). Examples of systems activated by the ESFAS include; ECCS, main steam line isolation, containment spray (CS), containment isolation, emergency feedwater (EFW), MCR isolation, emergency generator start up, ESWS, and RT (at the train level). Individual ESF systems can be manually actuated from the MCR.

The following items make up the ESF system:

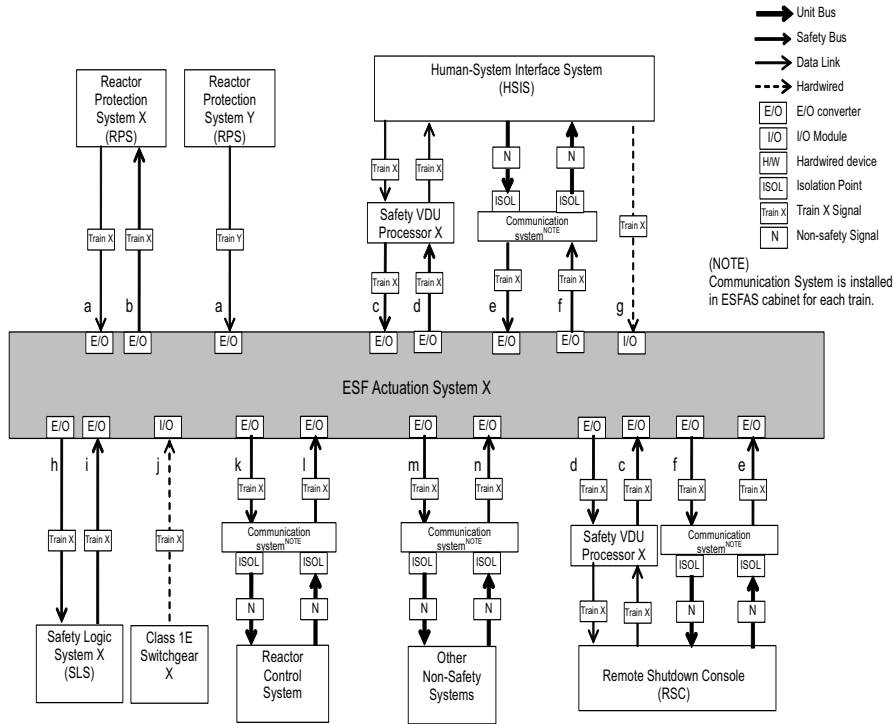
1. Process variable sensors;
2. RPS for processing process input signals and voting to determine the need for system level ESF actuation;
3. ESFAS for voting logic, which combines signals from all RPS trains and generates train level actuation signals to the SLS. The ESFAS also sequences the actuation of plant components to avoid overloading plant electrical systems during LOOP conditions;
4. SLS to distribute train level actuation signals from the ESFAS to the control logic for designated plant components;
5. Systems and components associated with ESF system;
6. Safety VDU processors and safety VDUs to provide manual component level control of plant components after initial automatic actuation by the ESFAS. Safety VDUs also provide reset for ESFAS actuation;
7. Conventional switches for manual initiation at train level.

The ESFAS and SLS send system status and process data to the HSIS and PCMS, which is not required for safety, via the unit bus. The ESFAS and SLS also receive manual component control and reset signals from the HSIS, which are not required for safety, via the unit bus. The interfaces for each ESFAS division are shown in Figs. 27, 28.

#### **5.3.3.2 ESF System Level Logic**

There are four trains for the ESF system in the US-APWR. The system level ESF actuation signals from all four RPS trains are transmitted over isolated data links to an ESFAS controller in each train of the ESF system. Each ESFAS controller consists of a duplex architecture using dual CPUs to enhance reliability. The RPS provides bistable calculations and voting logic to the ESFAS for ESF actuation. 2-out-of-4 coincidence voting logic is performed within each train through the redundant subsystems within each ESFAS controller. Each ESFAS subsystem generates a train level ESF actuation signal when the required 2-out-of-4 coincidence is met from the four RPS actuation signals. System level ESF manual actuation signals are hardwired from conventional switches located on the OC. These signals are also processed by the logic in each redundant subsystem of each ESFAS train to generate the same train level ESF actuation signal.

Train level manual actuation signals are generated for each ESFAS signal from separate switches for each ESFAS train. To avoid spurious actuation from a single contact or signal path failure, each switch contains two contacts that are interfaced to two separate digital inputs. Each ESFAS subsystem processes these signals through redundant train level manual actuation 2-out-of-2 logic.



7. INSTRUMENTATION AND CONTROLS  
 Figure 7.3-2 Interface between ESFAS and other systems (for Table 7.3-1)

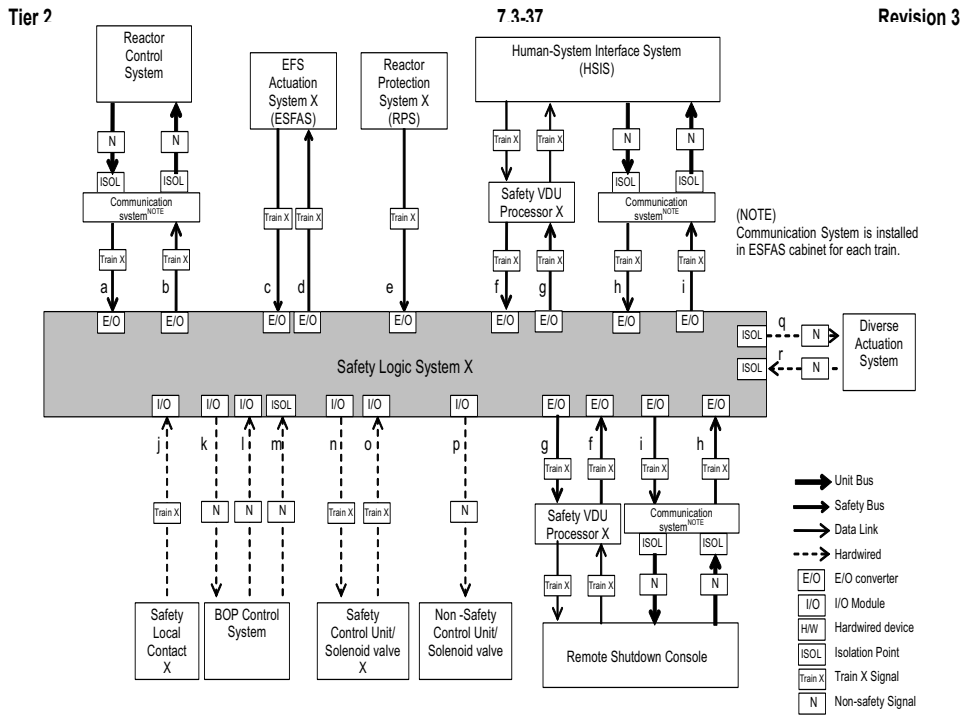


Figure 28: Interface between SLS and other systems

Figure 7.3-3 Interface between SLS and Other Systems (for Table 7.3-2)

Whether automatically or manually initiated, train level ESF actuation signals are transmitted from both subsystems of the ESFAS controller to the corresponding train of the SLS. The number of ESFAS trains that generate train level ESF actuation signals corresponds to the number of mechanical ESF trains being actuated.

The ESFAS also provides automatic load sequencing for the Class 1E GTG to accommodate the site LOOP accident. Each ESFAS train monitors three under voltage inputs, using 2-out-of-3 logic, to detect a loss of power condition for its respective train, and generates a LOOP signal. Upon detecting a loss of power, the ESFAS starts the Class 1E GTG for its train and disconnects the loads for its train from the electrical bus. Once the Class 1E GTG is capable of accepting loads, the ESFAS sequences the loads for its train back onto the electrical bus in an order appropriate for the current train level ESF actuation signal(s). The ESFAS sequencing logic accommodates ESF actuation signals occurring prior to or during a loading sequence. The ESFAS load sequencing function is independent for each train. The ESFAS also provides automatic load sequencing when an ESFAS is actuated during normal power conditions (i.e., no LOOP). Safety plant components are manually loaded on the non-safety alternate ac power source from the SLS during station blackout (which includes a loss of the Class 1E GTG Power Source).

#### **5.3.3.3 Process Variables Monitored for ESF**

A number of process variables, equipment status and plant parameters that are monitored to establish the degraded plant condition(s) and are used for generating ESF actuation signals to initiate various required ESF systems. Tables 15, 16 provides a list of process variables and signals. Tables 17, 18 provides range, accuracy, response time, and setpoint for each ESF actuation variables. Response time described in this table is within the delay time assumed in the safety analyses. Setpoint described in this table is within the analytical limit assumed in the safety analysis.

Some of the following variables are shared instrument used by multiple safety functions and non-safety control functions

- Pressurizer pressure;
- Pressurizer water level;
- Main steam line pressure;
- SG water level;
- Containment pressure;
- Containment high range area radiation;
- MCR outside air intake radiation;
- MFW pumps trip signal;
- RT signal (P-4 interlock);
- LOOP signal;
- Reactor coolant cold leg and hot leg temperatures (Tavg signal).



Actuacion signal	Number of sensors, switches, or signals	Actuation logic	Permissives and bypass
1 emergency core cooling system – logic diagram			
Low pressurizer pressure	4 pressure sensors (shared with RT)	2/4	Operating bypass permitted while P-11 is active, automatically unbypassed by inactive P-11
Low main steam line pressure	4 pressure sensors per steam line	2/4 per steam line	Operating bypass permitted while P-11 is active, automatically unbypassed by inactive P-11
High containment pressure	4 pressure sensors	2/4	None
Manual actuation	1 switch per train	1/1	Can be manually reset to block re-initiation of ECCS signal while P-4 is active. This block is automatically removed when P-4 becomes inactive
2 containment spray – logic diagram			
High 3 containment pressure	4 pressure sensors (shared with ECCS)	2/4	None
Manual actuation	2 switch per train	2/2	None
3 main control room isolation logic diagram			
MCR outside air intake radiation	2 gas radiation detectors	1/2	None
	2 Iodine radiation detectors	1/2	None
	2 particulate radiation detectors	1/2	None
ECCS actuation	Valid ECCS signal	1/1	None
Manual actuation	1 switch per train	1/1	None
4 containment purge isolation logic diagram			
Containment high range area radiation	4 radiation detectors	2/4	None
ECCS actuation	Valid ECCS signal	1/1	None
Manual containment isolation	1 switch per train	1/1	None
Manual CS actuation	2 switch per train	2/2	None
5 containment isolation Phase A logic diagram			
ECCS actuation	Valid ECCS signal	1/1	None
Manual actuation	1 switch per train	1/1	None

Table 15: Engineered safety features actuation signals

#### 5.3.3.4 ESF Initiating Signals, Logic, Actuation Devices and Manual Controls

The following subsections provide a functional description of ESF actuation signals, actuated systems/components and initiating logic for actuating each ESF function. Except as noted in specific sections below, all actuation signals are latched at the train level, whether automatically or manually initiated, and require manual reset. Latching ensures the protective action goes to completion and ensures that components remain in their safety position after the process returns to its pre-trip condition. Manual reset can only be initiated after the process returns to its pre-trip condition. Except as noted in specific sections below, the description is for one train and is applicable to all four trains. All manual actuations, bypasses, overrides, and resets are initiated separately for each train.

#### 5.3.3.5 Emergency Core Cooling System

ESF actuation signal for ECCS function is generated when any of the following initiating signals are

Actuacion signal	Number of sensors, switches, or signals	Actuation logic	Permissives and bypass
10 emergency feedwater isolation – logic diagram			
High SG water level	4 level sensors per SG (shared with RT)	2/4 per SG	Permitted while P-4 is active automatically blocked while steam line pressure is low. Operating bypass permitted while P-11 is active, automatically un-bypassed by inactive P-11
Low main steam line pressure	4 pressure sensors per steam line (shared with ECCS)	2/4 per steam	Automatically blocked while EFW isolation signal from other SG is initiated
Manual actuation	2 switches per SG	1/2 per SG	None
11 CVCS isolation logic diagram			
High pressurizer water level	4 level sensors (shared with RT)	2/4	Operating bypass permitted while P-11 is active, automatically un-bypassed by inactive P-11
Manual actuation	1 switch per train	1/1	None

Table 16: Engineered safety features actuation signals

ESF function	Variables to be monitored	Range of variables	Instrument accuracy	Response time	Setpoint
Emergency core cooling system actuation					
(a) Low pressurizer pressure	Pressurizer pressure	1700 to 2500 psig	2.5 of span	3.0 s	1765 psig
(b) Low main steam line pressure	Main steam line pressure	0 to 1400 psig	3% of span	3.0 s	525 psig
(c) high containment pressure	Containment pressure	-7 to 80 psig	2.8 of span	3.0 s	6.8 psig
Containment spray					
High 3 containment pressure	Containment pressure	-7 to 80 psig	2.8 of span	3.0 s	34.0 psig
Main control room isolation					
High MRC outside air intake radiation	MCR gas radiation	$10^{-7}$ to $10^{-2}$ $\mu\text{Ci/cc}$	6% of span	60 s	$20^{-6}$ $\mu\text{Ci/cc}$
	MCR iodine radiation	$10^{-11}$ to $10^{-5}$ $\mu\text{Ci/cc}$	6% of span	60 s	$8 \times 10^{-10}$ $\mu\text{Ci/cc}$
	MCR particulate radiation	$10^{-12}$ to $10^{-7}$ $\mu\text{Ci/cc}$	6% of span	60 s	$8 \times 10^{-10}$ $\mu\text{Ci/cc}$
Containment purge isolation					
High containment high range area radiation	Containment area radiation	1 to $10^7$ R/h	6% of span	15 s	100R/h
Main feedwater isolation					
(a) high – high SG water level	SG water level	0 to 100% of span (narrow range taps)	3% of span	3.0 s	70% of span
(b) low Tavg coincident with RT (P-4)	Reactor coolant	530 to 630°F	2.0°F	8.0 s	564°F
Main steam line isolation					
(a) low main steam line pressure	Main steam line pressure	0 to 1400 psig	3% of span	3.0 s	525 psig
(b) high main steam line pressure negative rate	Main steam line pressure	0 to 1400 psig	3% of span	3.0 s	100 psig
(c) high – high containment pressure	Containment pressure	-7 to 80 psig	2.8% of span	3.0 s	22.7 psig

Table 17: Engineered safety features actuation variables, ranges, accuracies, response times, and set-points (nominal)

ESF function	Variables to be monitored	Range of variables	Instrument accuracy	Response time	Setpoint
Emergency feedwater actuation					
Low SG water level	SG water level	0 to 100% of span (narrow range taps)	3% of span	3.0 s	13% of span
Loop signal	Loop signal	0 to 8.25 kV	1.5% of span	3.0 s	4727 V with ≤ 0.8 s time delay
Emergency feedwater isolation					
(a) high	SG water level SG water level	0 to 100% of span (narrow range taps)	3% of span	3.0 s	50% of span
(b) low main steam line pressure	Main steam line pressure	0 to 1400 psig	3% of span	3.0 s	525 psig
CVCS isolation					
High pressurizer water level	Pressurizer water level	0 to 100%	3% of span	3.0 s	92% of span

Table 18: Engineered safety features actuation variables, ranges, accuracies, response times, and setpoints (nominal)

present. The logic for this actuation is shown on Figs. 29, 30

1. Manual actuation;
2. Low pressurizer pressure initiating signal is generated on a condition when 2-out-of-4 signals for low pressurizer pressure are present and pressurizer pressure ECCS actuation bypass is not activated. Logic for this actuation circuit is shown on Fig. 30;
3. Low main steam line pressure initiating signal is generated when 2-out-of-4 signals for low pressure in any one of the four loops A, B, C, or D are present and main steam line pressure ECCS actuation bypass is not active. Logic for this actuation circuit is shown on Fig. 29. The low pressurizer pressure ECCS actuation bypass and low main steam line pressure ECCS actuation bypass can be activated manually only when pressurizer pressure interlock P-11 is present (i.e., when the pressurizer pressure signal is lower than the P-11 setpoint). These manually initiated operating bypasses are automatically removed when the pressurizer pressure signal is higher than the P-11 setpoint.
4. High containment pressure initiating signal is generated when 2-out-of-4 signals for high containment pressure are present. There is no operating bypass associated with this ECCS actuation signal. Logic for this actuation circuit is shown on Fig. 30.

An activated ECCS signal is latched separately for each train and cannot be manually overridden for 160 seconds. After ECCS is manually overridden the override is automatically removed when the P-4 RT interlock clears (i.e., RTB re-closed). An ECCS actuation signal cannot be manually reset for 160 seconds after actuation and until the initiating signals have cleared. An ECCS actuation signal aligns the required ESF systems valves (e.g., containment isolation valves, EFW valves) and starts the ESF system pumps and fans, required to mitigate the specific accident and/or AOO conditions.

An ECCS actuation signal results in the following actions

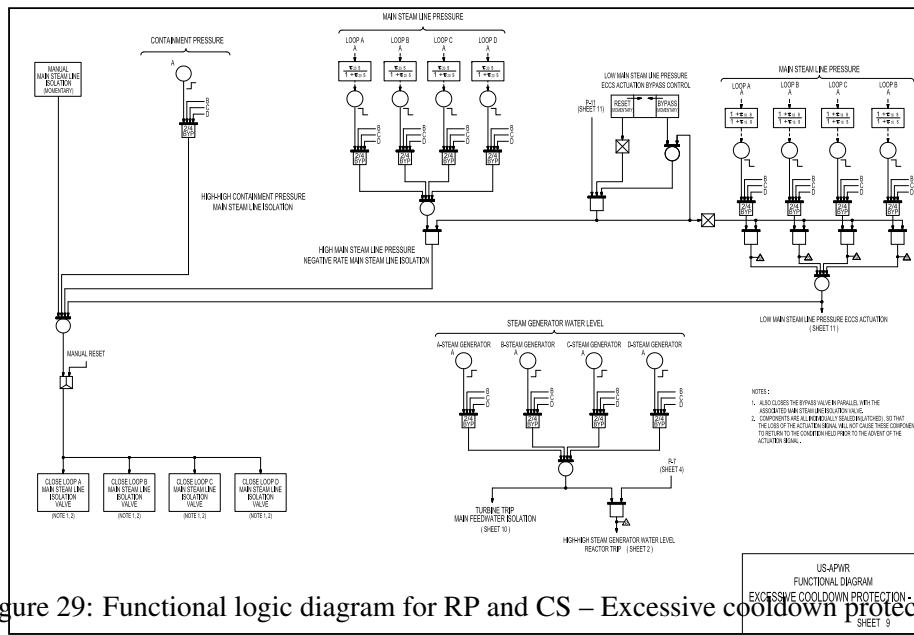


Figure 29: Functional logic diagram for RP and CS – Excessive cooldown protection

Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 9 of 21)

- Tier 2
1. Trip RCPs: There are two Class 1E RCP breakers for each RCP. One breaker is located in the Class 1E electrical room and the other is located in the electrical room in the turbine building. All Class 1E RCP breakers are tripped in 15 seconds after both the ECCS actuation signal and the P-4 RT interlock signal are present. The P-4 interlock is generated when breaker open status signals are received from any combination of RTBs that would result in a RT. The logic for this actuation is included on Fig. 30.
  2. Start emergency generator: Actuation of ECCS signal starts the emergency power source.
  3. Safety injection pumps.
  4. RT is initiated by the ECCS actuation signal.
  5. Main feedwater isolation.
  6. Emergency feedwater actuation.
  7. Containment isolation phase A.
  8. Containment purge isolation.
  9. Hydrogen igniter actuation: This is a non-safety function. Isolation is provided within the PSMS for this function.
  10. MCR isolation.
  11. ESWS actuation.

The ECCS actuation signal also initiates automatic load sequencing.

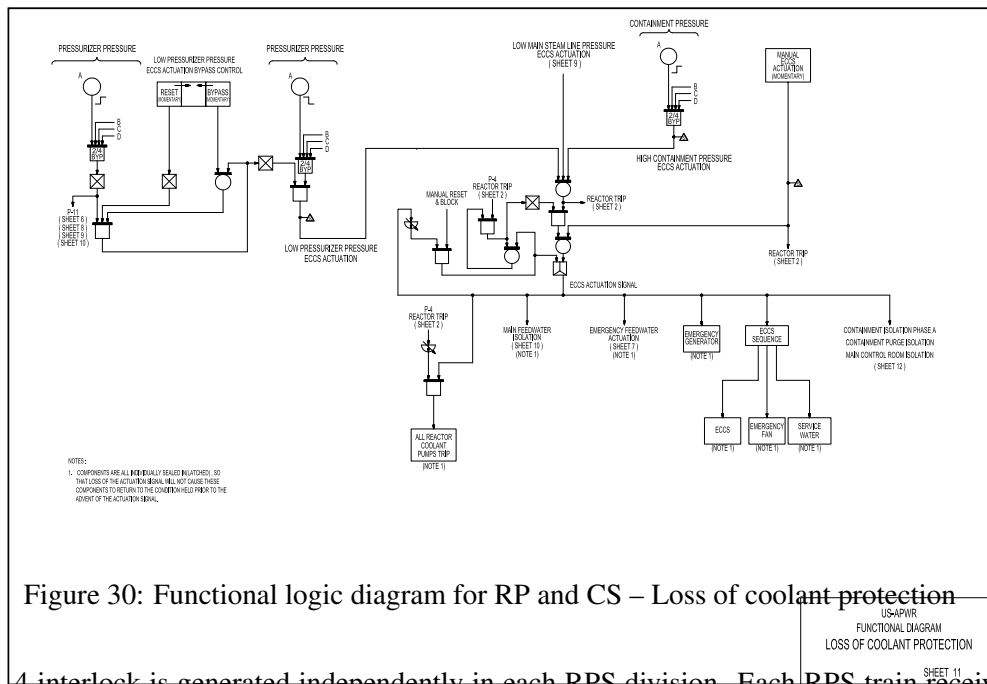


Figure 30: Functional logic diagram for RP and CS – Loss of coolant protection

The P-4 interlock is generated independently in each RPS division. Each RPS train receives status signals from the RTBs in its own train. RTB status signals are interfaced between RPS trains through the same fiber optic data links used for all RPS partial trip signals. P-4 interlocks from each RPS train are interfaced to each ESFAS train through 2-out-of-4 logic.

**5.3.3.6 MCR Isolation**

ESF actuation signal for this function is generated when any of the following initiating signals are present. The logic for this actuation circuit is shown on Fig. 31.

1. Manual actuation
2. ECCS actuation signal
3. High MCR outside air intake radiation: There are six MCR outside air intake radiation monitors interfaced separately to RPS trains A and D (two gas monitors, two iodine monitors, and two particulate monitors). RPS trains A and D provide separate bistable setpoint comparison functions for each monitor. These bistable output signals are distributed from RPS trains A and D to each of the four ESFAS trains. Within each of the four ESFAS trains the MCR Isolation signal is actuated on a signal from either the A or D train detectors using 1-out-of-2 logic for each type of monitor. The MCR Isolation actuation signal is distributed to the Main Control Room HVAC System (MCRVS) which consist of two 100% trains (A and D) of subsystems Main Control Room Emergency Filtration System (MCREFS) and four 50% trains of subsystems Main Control Room Air Temperature Control System (MCRATCS).

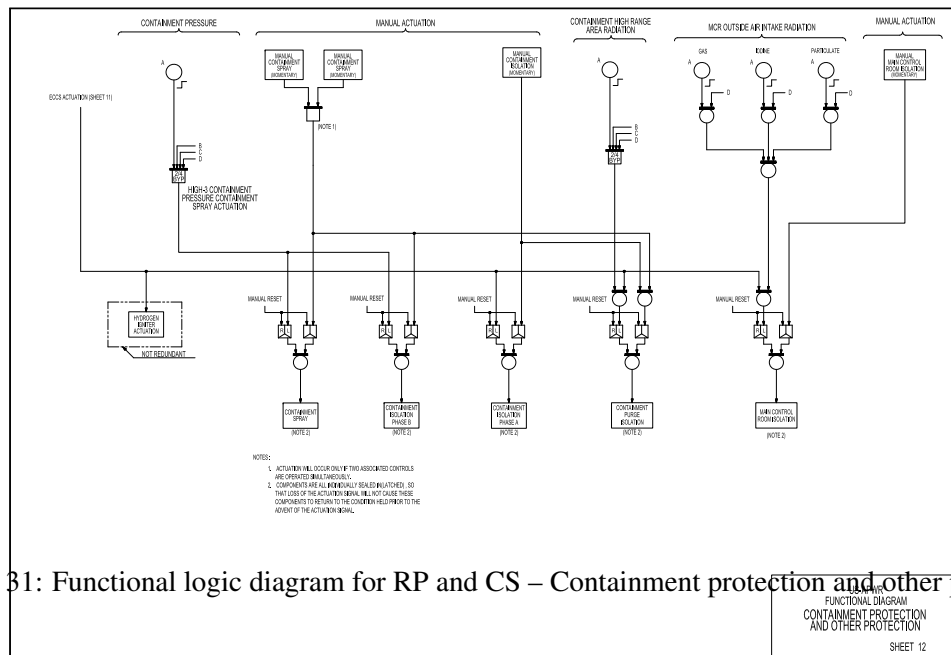


Figure 31: Functional logic diagram for RP and CS – Containment protection and other protection

### 5.3.4 Systems Required for Safe Shutdown

Tier 2

7.2-44

Revision 3

#### 5.3.4.7 System Description for Normal and Safe Shutdown

Plant operators can achieve normal shutdown (using both safety-related and non safety-related systems) from the MCR or RSR. Safe shutdown is achieved using only safety-related I&C systems.

The systems necessary for both normal and safe shutdown perform two basic functions. First, they provide the necessary reactivity control to maintain the core in a sub-critical condition. Second, the systems provide residual heat removal (RHR) capability to maintain adequate core cooling. Boration capability is also provided to compensate for xenon decay and to maintain the required core shutdown margin.

Manual controls through the safety VDUs or operational VDUs on the OC in the MCR, or at the RSC in the RSR, allow operators to transition to and maintain hot standby, transition to cold shutdown, and maintain cold shutdown. If the MCR is uninhabitable, controls and monitoring of shutdown functions can be performed from the RSR, which is located outside the MCR fire area in the reactor building.

#### 5.3.4.8 Normal and Safe Shutdown Plant Systems

There are no plant systems specifically dedicated to achieve normal and safe shutdown systems. However, there are number of plant systems that are available to establish and maintain normal and safe shutdown conditions. The PSMS is designed to mitigate accident conditions and automatically achieve stable hot standby conditions for the plant. The following functions support the cold shutdown objectives

1. Perform reactivity control to maintain the core in a sub-critical condition
2. Maintain RCS inventory

3. Provide boration capability to compensate for xenon decay and maintain the required core shutdown margin
4. Provide pressure control
5. Provide RHR capability to maintain adequate core cooling. The following systems can be used to support these objectives.
6. RHR system – for decay heat removal and maintaining reactor coolant temperature within acceptable limits.
7. CVCS – for reactivity control and RCS inventory control.
8. Reactor pressure control – Initial reduction in reactor coolant pressure is achieved via passive systems.

#### **5.3.4.9 Normal and Safe Shutdown from Outside the MCR**

GDC 19 requires, equipment at appropriate locations outside the control room shall be provided with

- a design capability for prompt hot standby of the reactor, including necessary I&C systems to maintain the unit in a safe condition during hot standby, and
- a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

In the event the MCR is uninhabitable for any reasons including fire, the control and monitoring of normal and safe shutdown functions can be performed from the RSR, which is located outside the MCR fire area in the reactor building. This capability meets the requirements of GDC 19.

The requirements for designing the RSR are

- LOOP is possible following the evacuation from MCR, and
- during normal operation, operators may have to evacuate the MCR immediately, without any action to plant, whenever they decide that evacuation from the MCR is necessary.

The RSR is designed in accordance with the following principles based on the above requirements.

1. The RSR is designed to shutdown the reactor, maintain the reactor in hot standby condition, and transition the reactor safely to cold shutdown. There are no unique required control actions outside the RSR to achieve or maintain hot standby or cold shutdown. Periodic RCS effluent sampling is a local operation for shutdown from the RSR, as it is for shutdown from the MCR.
2. The I&C equipment in the RSR is electrically isolated from any credible faults that may originate in the MCR. In addition, I&C equipment in the RSR is not affected by any spurious signals that may originate in the MCR. Prior to activation of HIS at the RSR, it is assumed that there are no prior failures that adversely affect the operability of I&C equipment in the RSR.

3. The safety-related I&C equipment in the RSR meets all Class 1E requirements including seismic category I qualification and conformance to the single failure criterion.
4. When control is transferred from the MCR to the RSR, there is no disturbance to the state of plant components or to continuous control processes (i.e., phase seamless transition).
5. The operator has the same functional control and monitoring capability at the RSR as in the MCR. The RSC provides equivalent functions of the operational VDUs and the safety VDUs in the MCR. The equipment arrangement of the RSC is displayed in Fig. 32. The transfer of control to the RSR has no effect on any non-safety or safety-related control functions, including automatic load sequencing to accommodate LOOP. The operator has complete capability to control all manual and automatic modes.
6. Adequate emergency lighting is provided on the pathways from the MCR to the RSR and to accommodate local effluent sampling.
7. Communication is provided between the RSR and local effluent sampling areas and emergency response facilities.
8. During normal plant operation, the RSR is locked to prevent inadvertent access. Access to the RSC, and the MCR/RSC transfer systems including the transfer switches, is under strict administrative control through secured areas with key access. Any access to these areas is indicated and alarmed in the MCR. All HIS at the RSR is electrically isolated from the safety and non-safety control systems. Controls at the RSR are disabled when controls are active in the MCR. Therefore, a fire or any other failure in the RSR, during normal operation, will have no effect on MCR controls.
9. The RSR is located in the reactor building. The transfer switch panels are in two separate locations, one is in the RSR, and another one is located outside of the MCR on the escape route to the RSR.

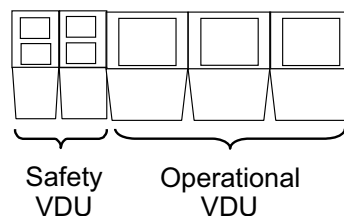


Figure 32: Equipment arrangement of remote shutdown console



The cable routes for each transfer switch panels are separated into another fire area shown in Fig. 33. All safety functions are controlled by the PSMS. All PSMS controllers are located in Class 1E I&C rooms, which are electrically and physically isolated from both the MCR and RSR. Therefore, all functions of the PSMS, including safe shutdown functions, are independent from the MCR, and can be controlled from VDUs in the RSR. Therefore, if any PSMS function is required, including ESF, it can be manually actuated from the RSR. If any ESF function actuates inadvertently, it can be controlled or terminated from the RSR.

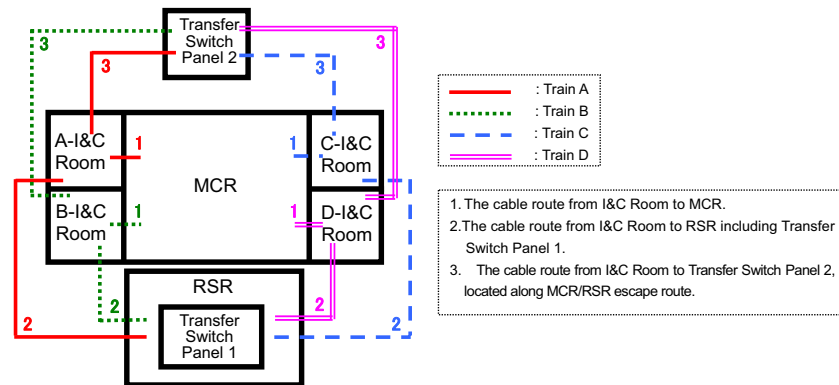


Figure 33: The cable route of the remote shutdown room

#### 5.3.4.10 Normal and Safe Shutdown Functions

HSI is provided in the MCR and RSR for control of normal and safe shutdown plant components and for monitoring functions as shown in Tables 19, 20, respectively. Shutdown functions consist of normal shutdown operation, and safe shutdown operation (i.e., safe shutdown using only safety-related plant equipment). These shutdown functions are described as follows. The COL Applicant is to provide a description of component controls and indications required for safe shutdown related to the ultimate heat sink (UHS).

Figure 7.4-2 The Cable Route of the Remote Shutdown Room

### 5.3.5 Information Systems Important to Safety

#### 5.3.5.1 System Description

This section describes the I&C systems PSMS and PCMS that provide information to plant operators for

- assessing plant conditions and safety system performance, and making decisions related to plant responses to abnormal events;
- preplanned manual operator actions related to accident mitigation.

Systems	Components	Normal shutdown	Safe shutdown	Train number for safe shutdown		Remarks
				Required number	Actual number	
RT systems	RTB	No	Yes	2	4	
RCS	RCP	Yes	No	–	–	Available with off-site power
	Safety depressurization valve	No	Yes	1	2	Note 1
	Safety depressurization valve block valve	No	Yes	1	2	Note 1
	Pressurizer heater backup group	No	Yes	2	4	
	Pressurizer spray valve	Yes	No	–	–	
	Reactor vessel vent valve	No	Yes	1	2	These valves could be used only if the venting becomes necessary
CVCS	Charging pump	Yes	No	–	–	Automatic start in loop
	Charging flow control valve	Yes	No	–	–	
	Letdown line 1 <sup>st</sup> (2 <sup>nd</sup> ) stop valve	Yes	No	–	–	
	Letdown line inside C/V isolation valve	Yes	No	–	–	
	CHP inlet line VCT side 1 <sup>st</sup> , 2 <sup>nd</sup> isolation valve	Yes	No	–	–	
	CHP inlet bat side isolation valve	Yes	No	–	–	
	CHP inlet line RWSAT side isolation valve	No	Yes	–	–	These valves are automatically opened on low volume control tank water level

Note 1. The configuration of the Safety Depressurization Valves and Safety Depressurization Valve - Block Valves meets the single failure criteria (for both electrical and mechanical failures), to ensure the capability for depressurization when required and to prevent spurious depressurization. There are two depressurization lines, each with one Safety Depressurization Valve (normally closed) and one Safety Depressurization Valve – Block Valve (normally open), each assigned to different trains. Four trains are used, such that the four valves in the two depressurization lines do not share any common train assignments. Should a Safety Depressurization valve fail to open when required, depressurization can be achieved through the other line. Should a Safety Depressurization valve spurious open, the series block valve can be closed.

Table 19: Component controls for shutdown

Systems	Instruments	Number of required channels	Normal shutdown	Safe shutdown	Remarks
RCS	Pressurizer water level	2	Yes	Yes	
	Pressurizer pressure	2	Yes	Yes	
	Reactor coolant hot leg temperature (wide range)	1 per loop	Yes	Yes	
	Reactor coolant cold leg temperature (wide range)	1 per loop	Yes	Yes	
	Reactor coolant pressure	1 per loop	Yes	Yes	
CVCS	Boric acid tank water level	1 per tank	Yes	No	
	RCP seal water return line flow	1 per RCP	Yes	No	
	RCP seal water outlet temperature	1 per RCP	Yes	No	
	Charging Flow	1	Yes	No	Used to maintain RCS inventory during safe shutdown
SIS	Safety injection pump discharge flow	1 per line	No	Yes	
	Safety injection pump minimum flow	1 per line	No	Yes	
	Safety injection pump discharge pressure	1 per line	No	Yes	
	Safety injection pump suction pressure	1 per line	No	Yes	
	Accumulator pressure	1 per tank	No	Yes	For ACC isolation during safe shutdown
RHRS	CS/RHR Hx outlet temperature	1 per line	Yes	Yes	
	CS/RHR pump discharge flow	1 per line	Yes	Yes	
	CS/RHR pump minimum flow	1 per line	Yes	Yes	
	CS/RHR pump discharge pressure	1 per line	Yes	Yes	
	CS/RHR Pump suction pressure	1 per line	Yes	Yes	
EFWS	EFW pit water level	2 per PIT	No	Yes	
	EFW flow	1 per line	No	Yes	
	EFW pump discharge pressure	1 per line	No	Yes	
CFS	SG water level (wide range)	1 per SG	Yes	Yes	
MSS	Main steam line pressure	2 per line	Yes	Yes	

Table 20: Summary of PAM variables types and source documents

The information systems important to safety also provide the necessary information from which appropriate actions can be taken to mitigate the consequences of AOOs.

This section describes the following information systems important to safety

1. Post accident monitoring (PAM);
2. Bypassed and inoperable status indication (BISI);
3. Plant annunciators (alarms);
4. Safety parameter displays system (SPDS).

Information important to safety, which supports emergency response operations, is available via the emergency response data system (ERDS). The information important to safety is available for display at the following facilities:

1. MCR;
2. RSR;
3. TSC;
4. EOF.

Controls for credited manual operator actions are available in the MCR.

#### **5.3.5.2 Post–Accident Monitoring**

The purpose of displaying PAM parameters is to assist MCR personnel in evaluating the safety status of the plant. PAM parameters are direct measurements or derived variables representative of the safety status of the plant. The primary function of the PAM parameters is to aid the operator in the rapid detection of abnormal operating conditions. As an operator aid, the PAM variables represent a minimum set of plant parameters from which the plant safety status can be assessed.

Safety–related PAM parameters are displayed on the safety VDUs, operational VDUs, and on the LDP. Non safety–related PAM parameters are displayed on operational VDUs. The parameters selected comply with the guidelines of RG 1.97. Display of at least two trains of each safety–related parameter is available.

The safety VDUs for each train are isolated from each other and from non–safety systems. IEEE Std 497–2002 provides selecting and categorizing principles for PAM variables. Table 21 provides a summary of the selection criteria and source documents for each PAM variable type. Table 22 provides the US–APWR design attributes for each variable type. Table 23 provides a list of PAM variables, their ranges, monitored functions or systems, quality and variable type.

The COL Applicant is to provide a description of site–specific PAM variables, which are type D variables for monitoring the performance of the UHS and type E variables for monitoring the meteorological parameters.

Variable type	Selection criteria for the variable type	Source documents
A	Planned manually controlled actions for accomplishment of safety-related functions for which there is no automatic control	<ul style="list-style-type: none"> <li>– Plant accident analysis licensing basis</li> <li>– Emergency procedure guidelines (EPGs) or EOPs</li> <li>– Plant abnormal operating procedures (AOPs)</li> </ul>
B	Assess the process of accomplishing or maintaining plant critical safety functions	<ul style="list-style-type: none"> <li>– Functional restoration EPGs or</li> <li>– Plant critical safety functions related EOPs</li> <li>– Plant critical safety function status trees</li> </ul>
C	<ul style="list-style-type: none"> <li>– Indicate potential for a breach of fission product barriers</li> <li>– Indicate an actual breach of fission product barriers</li> </ul>	<ul style="list-style-type: none"> <li>– Plant accident analysis licensing basis</li> <li>– Design basis documentation for the fission product barriers</li> <li>– EPGs or EOPs</li> </ul>
D	<ul style="list-style-type: none"> <li>– Indicate performance of safety systems</li> <li>– Indicate the performance of required auxiliary support features</li> <li>– Indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition</li> <li>– Verify safety system status</li> </ul>	<ul style="list-style-type: none"> <li>– Plant accident analysis licensing-basis</li> <li>– Event specific EPGs or EOPs</li> <li>– Functional restoration EPGs or EOPs</li> <li>– Plant AOPs</li> </ul>
E	<ul style="list-style-type: none"> <li>– Monitor the magnitude of releases of radioactive materials through identified pathways</li> <li>– Monitor the environmental conditions used to determine the impact of releases of radioactive materials through identified pathways (e.g., wind speed, wind direction, and air temperature)</li> <li>– Monitor radiation levels and radioactivity in the plant environments</li> <li>– Monitor radiation and radioactivity levels in the control room and selected plant areas where access may be required for plant recovery</li> </ul>	<ul style="list-style-type: none"> <li>– Procedures for determining radiological releases through plant identified pathways</li> <li>– Procedures for determining plant environs radiological concentration</li> <li>– Procedures for determining plant habitability</li> </ul>

Table 21: Summary of PAM variable type and source documents

Requirements	Type				
	A	B	C	D	E
1 single failure	Yes	Yes	Yes	–	–
2 seismic qualification	Yes	Yes	Yes	Yes	–
3 environmental qualification	Yes	Yes	Yes	Yes	
4 power supply	Yes	Yes	Yes	If required	If required
5 QA	Yes	Yes	Yes	–	–
6 independence and separation	Yes	Yes	Yes	–	–
7 information ambiguity	Yes	Yes	Yes	–	–
8 instability	Yes	Yes	Yes	Yes	Yes
9 continuous display	Yes	Yes	–	–	–
10 recording	Yes	Yes	Yes	–	Yes

Table 22: PAM main design criteria for each variable type

### 5.3.5.3 Safety Parameter Display System

The SPDS provides a display of key plant parameters from which the plant’s critical safety function status may be assessed. The primary function of the SPDS is to help operators and emergency response personnel make quick assessments of plant safety status. The SPDS is operated during normal operations as well as during all classes of emergencies.

The functions and design of SPDS are included as a part of the overall HSI design. Following is list of SPDS parameters for each critical safety function.

Variable	Range	Monitored function or systems	Quantity	Type
Reactor coolant hot leg temperature (wide range)	32 to 752°F	Core cooling	1 per loop	A, B, D
Reactor coolant cold leg temperature (wide range)	32 to 752°F	Core cooling	1 per loop	A, B, D
Reactor coolant pressure	0 to 3000 psig	Core cooling maintaining RCS integrity	2	A, B, C, D
Degrees of subcooling	360°F subcooling to 360°F superheat	Core cooling	2	A, B, D
Pressurizer water level	0 to 100% of span	Primary coolant system	4	A, B, D
SG water level (wide range)	0 to 100% of span	Secondary system (SG)	1 per SG	B, D
SG water level (narrow range)	0 to 100% of span	Secondary system (SG)	4 per SG	A, B, D
Main steam line pressure	0 to 1400 psig	Secondary system (SG)	1 per SG	A, B, D
EFW flow	0 to 250% of design	Emergency feedwater system	1 per line	A, B, D
Wide range neutron flux	10 <sup>-6</sup> to 100% full power	Reactivity control	2	B, D
Core exit temperature	200 to 2300°F	Core cooling fuel cladding	2 train (8 thermocouples for each train)	B, C
Containment pressure	-7 to 80 psig	Maintaining RCS integrity Maintaining containment integrity	4	B, C, D
RV water level	Bottom of hot leg to top vessel	Core cooling	2	B, D
Containment isolation valve position (excluding check valves)	Open/closed	Maintaining containment integrity	1 per valve	B, D
Reactor coolant soluble boron concentration	0 to 4000 ppm	Reactivity control	-(sampling)	B
CS/RHR pump discharge flow	0 to 130% of design flow	RHR or decay heat removal system	1 per line	D
CS/RHR pump minimum flow	0 to 110% of design flow	RHR or decay heat removal system	1 per line	D
Accumulator pressure	0 to 1000 psig	Safety injection system	1 per tank	D
Accumulator water level	0 to 100% of span	Safety injection system	1 per tank	D
Safety injection pump discharge flow	0 to 110% of design flow	Safety injection system	1 per tank	D

Table 23: PAM variables

1. Reactivity Control

- a. Neutron flux;
- b. Status of RTBs;
- c. Control rod position.

2. RCS Inventory

- a. Pressurizer water level;
- b. Reactor coolant hot leg temperature (wide range);
- c. Reactor coolant cold leg temperature (wide range);
- d. Reactor coolant pressure.

3. Core Cooling

- a. Reactor coolant hot leg temperature (wide range);
- b. Reactor coolant cold leg temperature (wide range);
- c. Degrees of subcooling;
- d. Core exit temperature;
- e. Reactor coolant pressure.

4. Secondary Heat Sink

- a. SG water level (narrow range);
- b. SG water level (wide range);
- c. EFW flow;
- d. MFW flow.

#### 5. RCS Integrity

- a. Reactor coolant pressure;
- b. Reactor coolant hot leg temperature (wide range);
- c. Reactor coolant cold leg temperature (wide range);
- d. Degrees of subcooling;
- e. Core exit temperature.

#### 6. Containment Integrity

- a. Containment pressure;
- b. Containment temperature;
- c. CS/RHR pump discharge flow;
- d. Status of Containment isolation valves.

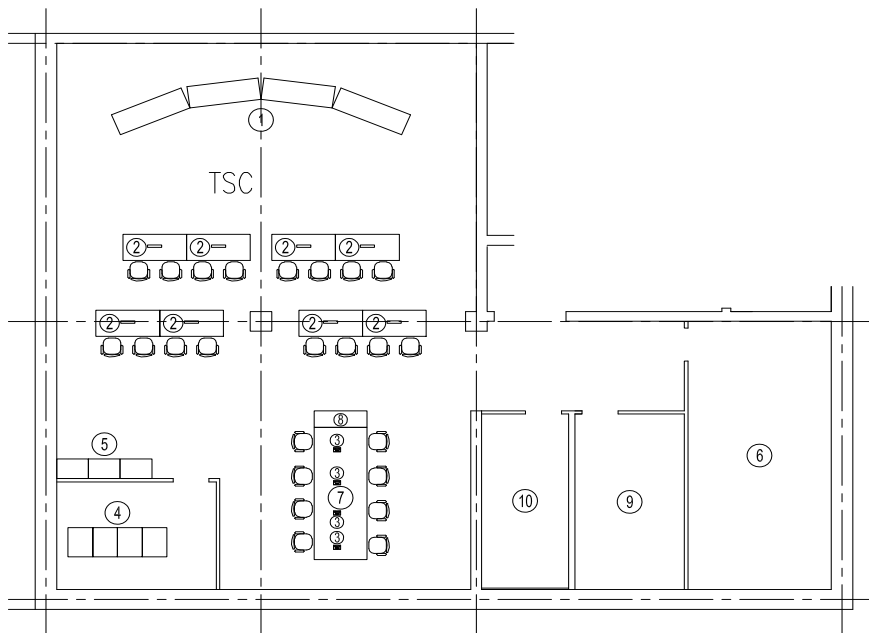
The SPDS is provided by the PCMS on operational VDUs, alarm VDUs, and the LDP. The LDP provides a continuous display of the status of each critical safety function. The status displayed for each critical safety function corresponds to the critical safety function status algorithm defined in the emergency operating procedures (EOPs). The computer that processes SPDS functions and all related HSI components are redundant, to ensure operation is not adversely affected by credible malfunctions. SPDS signals originate in plant instrumentation or within the controllers of the PCMS and PSMS. These signals are interfaced to the PCMS via the redundant unit bus.

The data interface to the PSMS is physically and functionally isolated so as not to affect the safety system in the event of SPDS component failure. The SPDS is developed through an augmented quality program, which includes software V&V.

#### **5.3.5.4 Technical Support Center**

The onsite TSC provides the following functions:

1. Provides plant management and technical support to plant operations personnel during emergency conditions;
2. Relieves the reactor operators of peripheral duties and communications not directly related to reactor system manipulations;



	Contents
1	Large Display Panel
2	Plant Monitoring VDUs
3	Communication equipments (phone, facsimiles, etc.)
4	Display Processor Data Transmitter
5	Cabinet for plant records and historical data, etc.
6	NRC consultation rooms
7	Sufficient table and chairs for staffs
8	Printers/hardcopies
9	Kitchen
10	Rest room

Figure 34: Layout of TSC

3. Prevents congestion in the MCR;
4. Performs EOF functions for alert emergency class, for site area emergency class, and for general emergency class until the EOF is functional Adequate working space for the personnel assigned to the TSC at the maximum level of occupancy is approximately 75 sq ft/person. The TSC working space is sized for a minimum of 25 persons, including 20 persons designated by the licensee and five NRC personnel. The TSC arrangement drawing is shown in Fig. 34. The size and layout of TSC gives necessary space to maintain and repair TSC equipment, and is sufficient for storage of plant records and historical data.

The TSC is the primary onsite communications center for the plant during an emergency. The TSC facility consists of PCMS operational VDUs (information only, no control) and the LDP, which receives plant information from the unit bus. The TSC also provides personal computers with interfaces to exter-

nal information systems via the station bus. PCMS equipment is redundant including its power supply. In addition, the TSC provides telephones and facsimiles machines, which utilize multiple methods of telecommunication. The TSC is located in the access building. Its location is close to the MCR, which is located in the reactor building. The walking time from the TSC to the MCR does not exceed two minutes. The TSC ventilation system includes high-efficiency particulate air (HEPA) and charcoal absorbers.

### **5.3.6 Control Systems Not Required for Safety**

The function of the US-APWR control systems not required for safety is to establish and maintain the plant operating conditions within prescribed limits. These control systems improve plant safety by minimizing the frequency of protection responses required and relief the operator from routine tasks.

The control functions not required for safety are implemented by the PCMS. The PCMS regulates conditions in the plant automatically in response to changing plant conditions and changes in plant load demand. These operating conditions include the following:

1. Step load changes of plus or minus 10% while operating in the range of 15 to 100% of full power;
2. Ramp load changes of plus or minus 5% per minute while operating in the range of 15 to 100% of full power (subject to core power distribution limits);
3. Full load rejection from 100% power.

These capabilities are accomplished without a reactor trip. Full load rejection is an event in which the main generator is cut off from the transmission system by a tripping of the main transformer breaker or the switchgear breaker without causing a turbine trip. In a load rejection scenario, the turbine governor valves are immediately fully closed, and the turbine bypass valves are opened fully, dumping the excess steam in the condenser. Reactor power is decreased by the automatic insertion of the control rods.

#### **5.3.6.5 Pressurizer Pressure Control**

The pressurizer pressure control function maintains the pressurizer pressure at its nominal operating value during normal operation and transients, see Fig. 35. During normal plant operation, the primary system pressure is monitored and controlled to prevent pressure from increasing to a limit where actuation of the PSMS is required to prevent design limits from being encroached. Additionally, the primary system pressure is prevented from decreasing to a value that may encroach on thermal design limits. The pressurizer pressure control function is designed to provide a stable and accurate control of pressure to its predetermined setpoint. Small or slowly varying changes in pressure are regulated by modulation of the proportional heaters. Reset (integral) action is included to maintain pressure at its setpoint. A fast pressure increase is controlled by reducing the proportional heater output and actuating pressurizer spray. Spray continues until pressure decreases to a point where the proportional heaters alone can regulate pressure.



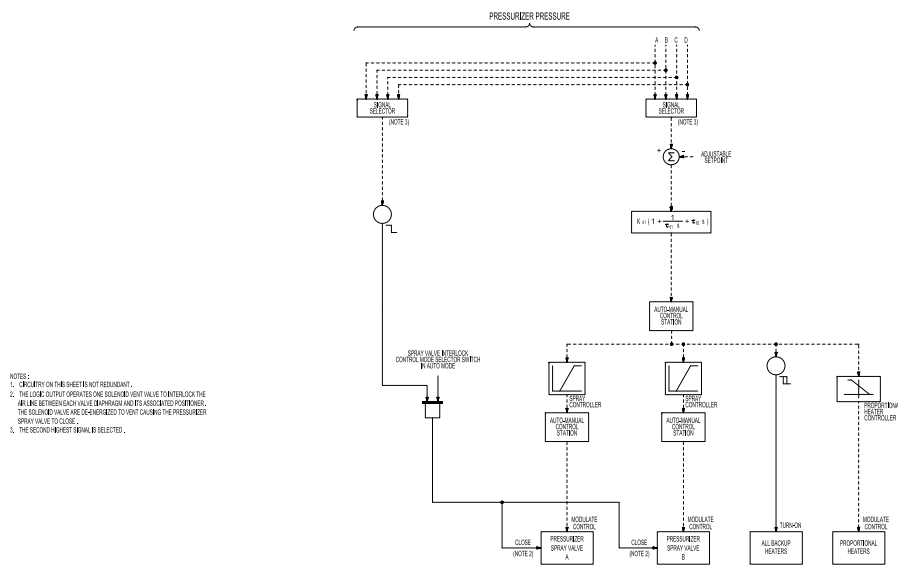


Figure 35: Functional logic diagram for RP and CS – Pressurizer pressure control

For normal transients including a full-load rejection, the pressurizer pressure control function acts promptly to prevent reaching the high pressurizer pressure RT setpoint. A decrease in pressure, greater than that which can be handled only by controlling the proportional heaters, will result in the actuation of the backup heaters. These backup heaters are switched-off automatically when the proportional heaters alone are able to restore the falling pressure. During normal steady-state plant operation, proportional heater output is regulated to compensate for pressurizer heat loss. During normal transient operation, the pressure is regulated to provide adequate margin to ESF systems actuation or reactor trip.

The automatic pressure control function can be manually selected by the operator when nominal pressure is established during plant startup. Automatic pressure control function can be maintained from zero to 100% power.

Pressurizer pressure input signals for pressurizer pressure control are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains are processed through the SSA within the PCMS before being used for pressurizer pressure control function.

Pressurizer pressure control function output signals are provided from the reactor control system in the PCMS to switchgear for the backup heaters, power controllers for the proportional heaters, and electro-pneumatic positioners for the pressurizer spray valves. The PCMS provides the following HSI signals for pressurizer pressure control function:

1. Pressurizer pressure control auto/manual – Allows transfer between the automatic control mode by pressurizer pressure input signals or function level manual control mode. In manual mode pressurizer heaters are controlled directly by the operator, but control signal to pressurizer spray valves may be in auto or manual mode.

2. Pressurizer spray valve A auto–manual – Allows transfer between the automatic control mode by pressurizer pressure control or component level manual control mode for each pressurizer spray valve. In the manual mode the operator can fix the spray valve position.
3. Pressurizer spray valve B auto–manual – Same as for pressurizer spray valve A.

#### **5.3.6.6 Pressurizer Spray Interlock**

An interlock is provided to prevent excessive depressurization of the RCS that could result from excessive spray, from a control system malfunction or operator violation of operating procedures, refer to Fig. 35.

To generate this interlock the PCMS receives pressurizer pressure signals from the RPS and processes these signals through SSA, as discussed above. The interlock blocks automatic or manual pressurizer spray valve opening. It interlock is provided from the Reactor control system in the PCMS to permissive solenoids on the Pressurizer Spray Valves.

The pressurizer spray Interlock is generated from a separate controller group from the pressurizer pressure control function discussed above, which generates pressurizer spray valve opening demands. This improves the potential for preventing inadvertent pressurizer spray valve opening that may be generated due to failures in the PCMS pressurizer pressure control function group.

The pressurizer spray interlock may be manually bypassed to allow plant depressurization for cold shutdown. Plant operators are alerted by alarms and indications to conditions of control system malfunctions and/or abnormal operating conditions.

#### **5.3.6.7 Pressurizer Water Level Control**

The pressurizer water level control function maintains pressurizer water level at its programmed value, refer to Fig. 36. The programmed value is determined as a function of reactor coolant  $T_{avg}$  to minimize charging and letdown control operations. This arrangement minimizes potential challenges to the protection systems actuation during normal operational transients.

The Pressurizer provides a reservoir for the RCS inventory changes that occur due to changes in reactor coolant density. As the reactor coolant temperature is increased from hot zero–load to full–load values, the RCS fluid expands. The pressurizer water level control adjusts letdown and charging flow to allow the pressurizer to absorb this change. The pressurizer water level control function provides a stable and accurate method of pressurizer water level control at the prescribed setpoint value, which is programmed by  $T_{avg}$ . Automatic level control may be manually selected from the point in the startup cycle where the hot zero–load level is established. Automatic pressurizer water level control can be maintained from zero through 100% power.

Pressurizer water level input signals for the pressurizer water level control are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains are processed through the SSA within the PCMS before being used for the pressurizer water level control function.  $T_{avg}$  input

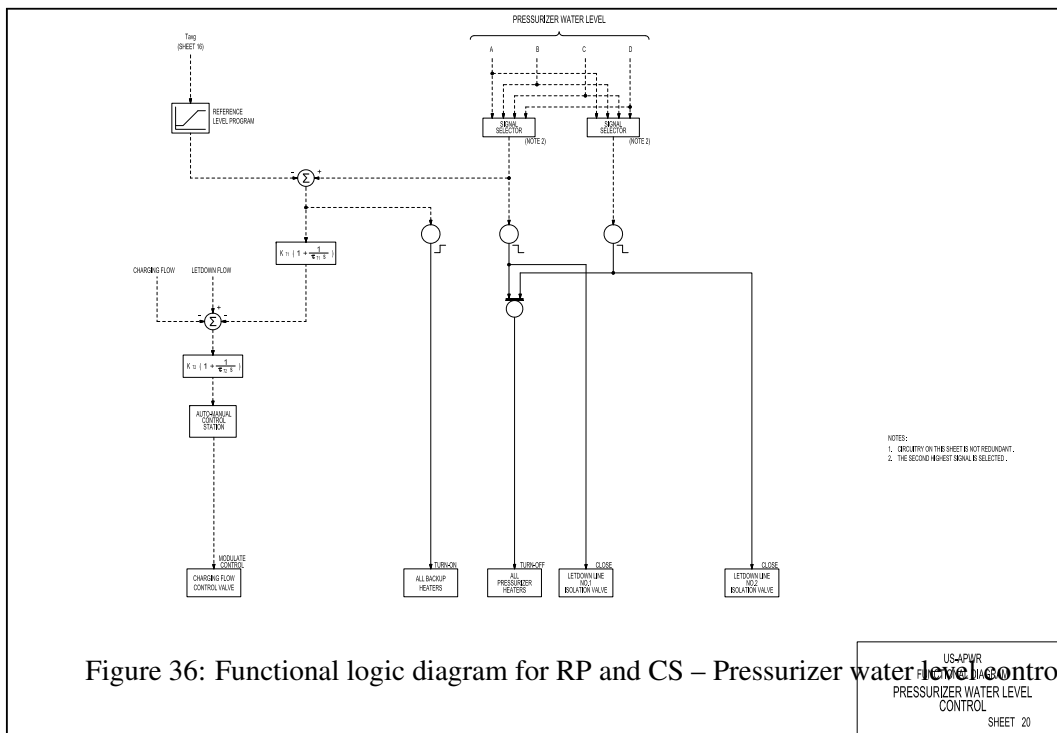


Figure 36: Functional logic diagram for RP and CS – Pressurizer water level control

signals for pressurizer water level control are interfaced from the RPS to the PCMS via the unit bus.

Signals from each of the four RPS trains, corresponding to each RPS loop, are processed through the SSA within the PCMS before being used for Pressurizer water level control.

The pressurizer water level control function output signals are provided from the reactor control system in the PCMS to electro–pneumatic positioners for the charging flow control valve.

The PCMS provides the following HSI signals for the pressurizer water level control function:

1. Charging flow control valve auto/manual – Allows transfer of the charging flow control valve between the automatic control mode by pressurizer water level control or manual control mode. In the manual mode the operator can fix the charging flow control valve position.

### 5.3.6.8 Low Pressurizer Water Level Interlock

An interlock is provided to prevent excessive low pressurizer water level conditions that could result from excessive letdown or inadequate charging initiated by either a control system malfunction or operator violation of operating procedures, refer to Fig. 36. To generate this interlock the PCMS receives pressurizer water level signals from the RPS and processes these signals through SSA, as discussed above.

This interlock automatically closes letdown line isolation valves #1 and #2. The interlock also de-energizes the backup heaters to prevent damage during low pressurizer water level conditions where they may become uncovered. This interlock is provided from the reactor control system in the PCMS to backup heater switchgear and the control solenoid on letdown line isolation valve #1 and #2.

One of the low pressurizer water level interlocks is generated from a separate controller group from

the pressurizer water level controls which generates charging flow demands. This improves the potential for preventing excessive low pressurizer water level conditions that may be generated due to failures in the PCMS pressurizer water level control group. Plant operators are alerted by alarms and indications to conditions of control system malfunctions and/or abnormal operating conditions.

### **5.3.7 Diverse Instrumentation and Control Systems**

The DAS is the non-safety diverse instrumentation and control system for US-APWR. The DAS provides monitoring, control and actuation of safety and non-safety systems required to cope with abnormal plant conditions concurrent with a CCF that disables all functions of the PSMS and PCMS. The DAS includes an automatic actuation function, HSI functions located at the diverse HSI panel (DHP), and interfaces with the PSMS and PCMS.

The DAS design consists of conventional equipment that is totally diverse and independent from the MELTAC platform of the PSMS and PCMS, so that a beyond design basis CCF in these digital systems will not impair the DAS functions. In addition, the DAS includes internal redundancy to prevent spurious actuation of automatic and manual functions due to a single component failure. The DAS is also designed to prevent spurious actuations due to postulated earthquakes and postulated fires. The DAS interfaces with the safety process inputs and outputs of the SLS are isolated within these safety systems. In addition, hardwired Class 1E logic within the SLS (not affected by a CCF) ensures that control commands originating in the DAS or SLS, which correspond to the desired safety function, always have priority. Therefore, there is no adverse interaction of the DAS with safety functions and no erroneous signals resulting from CCF in the SLS that can prevent the safety function.

Within the DAS, manual actuation is provided for systems to maintain all critical safety functions. For conditions where there is insufficient time for manual operator action, the DAS provides automatic actuation of required plant safety functions needed for accident mitigation. Key parameter indications, diverse audible and visual alarms, and provisions for manual controls are located in a dedicated independent DHP located in the MCR. Conventional hardwired logic hardware and relays for automatic actuation are installed in two diverse automatic actuation cabinets (DAACs), each located in a separate room. Each DAAC is powered by a separate non-Class 1E UPS. During plant on-line operation, the system can be tested manually without causing component actuation that would disturb plant operations.

#### **5.3.7.1 Diverse HSI Panel**

The DHP, which is located in the MCR, consists of conventional hardwired switches, conventional indicators for key parameters of all critical safety functions, and audible and visual alarms. The DHP installed equipment is used for manual control and actuations credited in the defense in depth and diversity coping analysis. Actuation status of each safety system actuated from the DHP can be confirmed by monitoring the safety function process parameters displayed on the DHP. The DHP is powered by a non-Class 1E UPS and located in the MCR. Therefore, the DHP is qualified as Seismic Category II.

### **5.3.7.2 Reactor Trip, Turbine Trip and Main Feedwater Isolation**

Reactor trip, turbine trip and MFW isolation are automatically actuated on the following signals:

1. Low pressurizer pressure: 2-out-of-4 voting logic of the four pressurizer pressure low signals;
2. High pressurizer pressure: 2-out-of-4 voting logic of the four pressurizer pressure high signals;
3. Low SG water level: 2-out-of-4 voting logic of the one SG water level low signals from each SG.

The four pressurizer pressure signals are interfaced from each of the four PSMS trains. This configuration allows the DAS to meet the target reliability of the PRA with one channel continuously bypassed or inoperable.

To support the single failure criterion for all PSMS functions, there are four SG water level signals (one per each train A, B, C, and D) on each SG. However, for the DAS, which does not need to meet the single failure criterion, only one water level signal is required from each SG.

The reactor trip is actuated by tripping the non-safety CRDM motor-generator set. This actuation leads to de-energizing the power for the CRDM by a means that is diverse from the RTB to release the control rods for gravity insertion into the reactor core. Diversity from the PSMS is maintained from sensor-inputs to final actuators.

The Turbine Trip is actuated by opening the solenoid valves for turbine trip. Diversity from the RT function in the PSMS is maintained from sensor-input up to the power interface module.

The MFW isolation is actuated by closing the MFW regulation valve. Diversity from the feedwater isolation function in the PSMS is maintained from sensor input up to the power interface module.

These DAS actuation functions are automatically blocked when all the following conditions are established

1. Status signals are received indicating that the minimum combination of the RTBs have actuated for the RT function. This is referred to as the P-4 interlock. The P-4 interlock is processed independently in each DAAC. Signals from all RTBs are interfaced from the PSMS, prior to any software processing, to each DAAC, as shown in Fig. 37.
2. The turbine emergency trip oil pressure trip signal is generated when oil pressure channels exceed the trip setpoint.

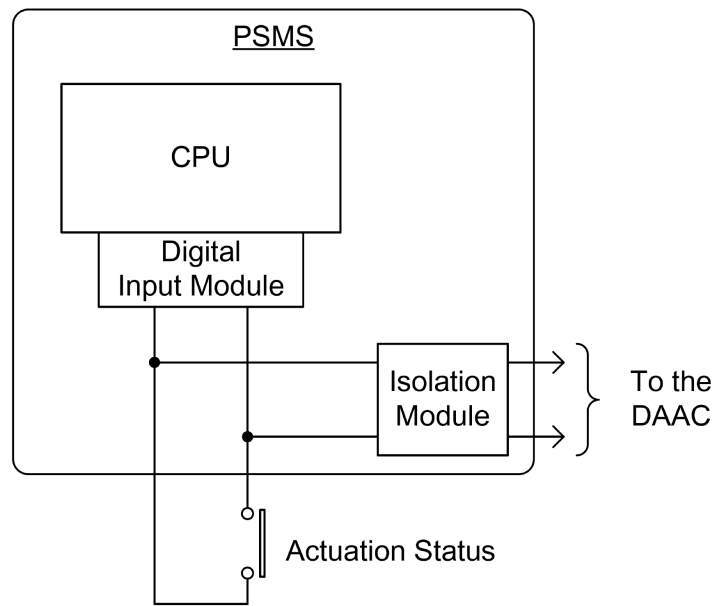


Figure 37: Interface of signals with the PSMS

## ***Acknowledgements***

The authors wish to thank Riccardo Colagè and Rocco Iarlori for their contribution, given during the preparation of their M.Sc. and Bachelor theses.

## References

- [1] V. Ahlstrom, A. Koros, and M. Heiney, Team processes in airway facilities operations control center, *Technical Note*, DOT/FAA/CT-TN00/14, U.S. Department of Transportation, Federal Aviation Administration, 2000.
- [2] L. Bainbridge, and P. Sanderson, Verbal protocol analysis, in J. R. Wilson and E. N. Corlett (Eds.), *Evaluation of human work: A practical ergonomics methodology*, 2<sup>nd</sup> ed., pp. 169–201, London, UK, Taylor & Francis, Ltd., 1990.
- [3] L. Berglund, *Systemframtagning av högautomatiserade styroch reglersystem med hänsyn till driftsäkerhet och livstidskostnad*, EKZ7, Stockholm, Statens Vattenfallsverk, 1982.
- [4] C. E. Billings, and E. S. Cheaney, The information transfer problem: Summary and comments, in C. E. Billings and E. S. Cheaney (Eds.), *Information transfer problems in the aviation system*, NASA Technical Paper 1875, 1981.
- [5] H. S. Blackman, and W. R. Nelson, Techniques for incorporating operator expertise into intelligent decision aids and training, *Reliability Engineering and System Safety*, Vol. 22, pp. 371–385, 1988.
- [6] C. Burns, and K. J. Vicente, A participant–observer study of ergonomics in engineering design: How constraints drive design process, *Applied Ergonomics*, Vol. 31, pp. 73–82, 2000.
- [7] S. K. Card, T. P. Moran, and A. Newell, *The psychology of human–computer interaction*, Hillsdale, NJ, Lawrence Erlbaum Associates Inc., 1983.
- [8] Combustion Engineering Owner’s Group (CEOG), *Combustion engineering emergency response guidance*, CEN–152, Rev. 4, 1996.
- [9] S. L. N. Chen–Wing, and E. C. Davey, Designing to avoid human error consequences, *Proceedings of the Workshop on Human Error, Safety, and System Development*, Paper Session 5, 1998.
- [10] X. Chen, Z. Zhou, Z. G. Gao, W. Wu, T. Nakagawa, and S. Matsuo, Assessment of human–machine interface design for a Chinese nuclear power plant, *Reliability Engineering and System Safety*, Vol. 87, pp. 37–44, 2005.
- [11] A. D. Cohen, Verbal report on learning strategies, *TESOL Quarterly*, Vol. 28, No. 4, pp. 678–682, 1994.
- [12] W. R. Corcoran, V. M. Callaghan, G. C. Bischoff, R. T. Pearce, and J. H. Barrow, Transient management using the safety function approach, in P. L. Lassahn, D. Majumdar, and G. F. Brockett (Eds.), *Anticipated and abnormal plant transients in light water reactors*, Vol. 2, pp. 1059–1072, New York, Plenum Press, 1984.



- [13] E. Davey, *Criteria for operator review of workplace changes*, Canadian Nuclear Society Conference, Toronto, Ontario, CA, 2000.
- [14] K. A. Ericsson, and H. A. Simon, *Protocol analysis: Verbal reports as data*, Cambridge, MA, MIT Press, 1993.
- [15] R. P. E. Gordon, The contribution of human factors to accidents in the offshore oil industry, *Reliability Engineering and System Safety*, Vol. 61, pp. 95–108, 1998.
- [16] M. Grozdanovic, Methodology for research of human factors in control and managing centers of automated systems, *The Scientific Journal Facta Universitatis: Working and Living Environmental Protection*, Vol. 1, No. 5, pp. 9–22, 2000.
- [17] Hankook Daily News, Take-off without cabin crews (reported by Song, D. Y.), Article in Hankook Daily News, Seoul, Korea, 9 August (in Korean), 2006.
- [18] J. Hugo, and H. Engela, Function allocation for industrial human–system interfaces, *Proceedings of the 4<sup>th</sup> International Cyberspace Conference on Ergonomics*, Idaho National Laboratory, 2005, The SPAR–H human reliability analysis method. NUREG/CR-6883, U. S. Nuclear Regulatory Commission, Washington, DC, 2006.
- [19] International Atomic Energy Agency (IAEA), *Basic safety principles for nuclear power plants*, IAEA Safety Series No. 75–INSAG–3, Vienna, Austria, IAEA, 1988.
- [20] International Atomic Energy Agency (IAEA), *Human reliability analysis in probabilistic safety assessment for nuclear power plants: A safety practice*, IAEA Safety Series No. 50–P–10, Vienna, Austria, IAEA, 1996.
- [21] International Atomic Energy Agency (IAEA), *Implementing digital instrumentation and control systems in the modernization of nuclear power plants*, IAEA Nuclear Energy Series No. NP–T–1.4, Vienna, Austria, IAEA, 2009.
- [22] Institute of Nuclear Power Operations (INPO), *Point Lepreau 1, 4/26/1999: Containment isolation system button-up during degassing of the degasser condenser*, 908–990426–1, Retrieved August 14, 2008, from <http://www.INPO.org>, 1999.
- [23] Institute of Nuclear Power Operations (INPO), *Gentilly 2, 11/26/2000: Recirculated service water diesel motor pump 7131-P36 damaged*, 851–001126–1, Retrieved August 14, 2008, from <http://www.INPO.org>, 2000.
- [24] Institute of Nuclear Power Operations (INPO), *Cooper 1, 2/12/2002: Unintended increase in reactor power due to misoperation of reactor recirculation pump speed control*, 298–020212–1, Retrieved August 14, 2008, from <http://www.INPO.org>, 2002.

- [25] Institute of Nuclear Power Operations (INPO), *Gentilly 2, 2/12/2002: Local radiological alert due to a moderator leak in upgrading plants*, 851-020212-1, Retrieved August 14, 2008, from <http://www.INPO.org>, 2002.
- [26] Institute of Nuclear Power Operations (INPO), *Cernavoda 1, 6/12/2003: Inadvertent draining of inservice fire water tank 7140-TK1 results in start and damage of the diesel engine driven pump*, 121-030612-1, Retrieved August 14, 2008, from <http://www.INPO.org>, 2003.
- [27] Institute of Nuclear Power Operations (INPO), *Duane Arnold 1, 12/30/2003: High temperature in fuel pool because of procedure use problem*, 331-000111-1, Retrieved August 14, 2008, from <http://www.INPO.org>, 2003.
- [28] Institute of Nuclear Power Operations (INPO), *Millstone 2, 3/15/2004: Automatic reactor scram after a steam generator feed pump trip*, 336-040315-1, Retrieved August 14, 2008, from <http://www.INPO.org>, 2004.
- [29] Institute of Nuclear Power Operations (INPO), *Nine Mile Point 1, 5/4/2004: Two control rods scrammed during rod scram timing test*, 220-040504-1, Retrieved August 14, 2008, from <http://www.INPO.org>, 2004.
- [30] Institute of Nuclear Power Operations (INPO), *Point Lepreau 1, 6/6/2004: Primary heat transport (PHT) thermal transient*, 908-040606-1, Retrieved August 14, 2008, from <http://www.INPO.org>, 2004.
- [31] Institute of Nuclear Power Operations (INPO), *Darlington 2, 2/8/2005: Unit 2 turbine leading (normal) mode inadvertently entered*, 932-041101-1, Retrieved August 14, 2008, from <http://www.INPO.org>, 2005.
- [32] Institute of Nuclear Power Operations (INPO), *Susquehanna 2, 5/27/2005: B circulating water pump shutdown instead of B condensate pump*, 388-050527-1, Retrieved August 14, 2008, from <http://www.INPO.org>, 2005.
- [33] Institute of Nuclear Power Operations (INPO), *Gentilly 2, 7/12/2005: 3481-TK2 tank draining and 3481-P1 and P2 pump cavitations*, 851-050530-1, Retrieved August 14, 2008, from <http://www.INPO.org>, 2005.
- [34] Institute of Nuclear Power Operations (INPO), *Perry 1, 7/9/2006: Reactor operation in unanalyzed region*, 440-060709-1, Retrieved August 14, 2008, from <http://www.INPO.org>, 2006.
- [35] Institute of Nuclear Power Operations (INPO), *Monticello, 3/14/2007: Half scram due to cold water transient during valve operation at Monticello Nuclear Generating Plant*, 263-070314-1, Retrieved August 14, 2008, from <http://www.INPO.org>, 2007.

- [36] Institute of Nuclear Power Operations (INPO), *Trillo 1, 11/28/2007: During routine tests, start-up of emergency diesel generator GY60 activated by reactor protection system*, 715-071128-1, Retrieved August 14, 2008, from <http://www.INPO.org>, 2007.
- [37] T. Ivergård, and B. Hunt, *Models in process control*, in T. Ivergård & B. Hunt (Eds.), *Handbook of control room design and ergonomics: A perspective for the future*, 2nd Ed., pp. 11-42, Boca Raton, FL, CRC Press, 2008.
- [38] S. Jones, and S. Hickey, Improving driver/signaler safety critical communications – Report on conduct of surveys, *AEA Technology Rail*, 10/T014/AEAR/49/TRT, No. 1.1, 2004.
- [39] A. C. Kadak, and J. D. Candon, A functional approach to transient management, in P. L. Lassahn, D. Majumdar, and G. F. Brockett (Eds.), *Anticipated and abnormal plant transients in light water reactors*, Vol. 2, pp. 1127-1140, New York, Plenum Press, 1984.
- [40] B. G. Kanki, and H. C. Foushee, Communication as group process mediator of aircrew performance, *Aviation, Space, and Environmental Medicine*, May, 402-410, 1989.
- [41] B. G. Kanki, S. Lozito, and H. C. Foushee, Communication indices of crew coordination, *Aviation, Space and Environmental Medicine*, January, pp. 56-60, 1989.
- [42] J. G. Kemeny, B. Babbitt, P. E. Haggerty, C. Lewis, P. A. Marks, C. B. Marrett, et al., *The need for change: The legacy of TMI – Report of the president's commission on the accident at Three Mile Island*, New York, Pergamon Press, 1979.
- [43] J. Kim, and J. Park, Task types and error types involved in the human-related unplanned reactor trip events, *Nuclear Engineering and Technology*, Vol. 40, No. 7, pp. 615-624, 2008.
- [44] S. Kim, J. Park, and Y. J. Kim, Some Insights about the Characteristics of Communications Observed from the Off-Normal Conditions of Nuclear Power Plants, Special Issue: Human Factors in Control Rooms of Nuclear Power Plants, Vol. 21, No. 4, pp. 361-378, 2011.
- [45] T. Kontogiannis, Stress and operator decision making in coping with emergencies, *International Journal of Human-Computer Interaction*, Vol. 45, pp. 75-104, 1996.
- [46] H. Liao and J.-L. Chang, Human Performance in Control Rooms of Nuclear Power Plants: A Survey Study, in *Human Factors and Ergonomics in Manufacturing & Service Industries*, Special Issue: Human Factors in Control Rooms of Nuclear Power Plants, Vol. 21, No. 4, pp. 412-428, 2011.
- [47] D. Meister, *Human factors: Theory and practice*, New York, Wiley, 1971.

- [48] D. Meister, Cognitive behavior of nuclear reactor operators, *International Journal of Industrial Ergonomics*, Vol. 16, pp. 109–122, 1995.
- [49] D. Min, Y. H. Chung, and W. C. Yoon, Comparative analysis of communication at main control rooms of nuclear power plants, *Proceedings of IFAC/IFIP/IFORS/IEA Symposium*, Atlanta, GA, 2004.
- [50] Mitsubishi Heavy Industries Ltd, *Design Control Document for the US–APWR*, Chap. 7, Instrumentation and Controls, MUAP–DC007, Rev. 3, Tokyo, Japan, 2011.
- [51] N. Moray, Advanced displays, cultural stereotypes and organizational characteristics of a control room, in J. Misumi, M. Wilpert, and R. Miller (Eds.), *Nuclear safety: A human factors perspective*, New York, Taylor & Francis, 1999.
- [52] P. Murphy, The role of communications in accidents and incidents during rail possessions, *Engineering psychology and cognitive ergonomics*, Vol. 5, Aerospace and transportation systems, Aldershot, UK, Ashgate, 2001.
- [53] N. Naito, J. Itoh, K. Monta, and M. Makino, An intelligent human–machine system based on an ecological interface design, *Nuclear Engineering and Design*, Vol. 154, pp. 97–108, 1995.
- [54] D. A. Norman, Categorization of action slips, *Psychological Review*, Vol. 88, pp. 1–15, 1981.
- [55] National Research Council, *Digital instrumentation and control systems in nuclear power plants: Safety and reliability issues*, Washington, DC, National Academies Press, 1997.
- [56] J. M. O’Hara, J. C. Higgins, and W. S. Brown, Identification and evaluation of human factors issues associated with emerging nuclear plant technology, *Nuclear Engineering and Technology*, Vol. 41, No. 3, pp. 225–236, 2009.
- [57] J. Park, and W. Jung, The requisite characteristics for diagnosis procedures based on the empirical findings of the operators’ behavior under emergency situations, *Reliability Engineering and System Safety*, Vol. 81, pp. 197–213, 2003.
- [58] P. Quinot, and G. Desfontaines, The Main Components of the European Pressurized Water Reactor, *Nuclear Engineering and Design*, No. 187, pp. 121–133, 1999.
- [59] J. Rasmussen, and A. Jensen, Mental procedures in real–life tasks: A case study of electronic trouble shooting, *Ergonomics*, Vol. 17, No. 3, pp. 293–307, 1974.
- [60] J. Rasmussen, The human as a system component, In H. T. Smith and T. R. G. Green (Eds.), *Human interaction with computers*, pp. 67–96, London, Academic Press, 1980.

- [61] J. Rasmussen, Skills, rules, and knowledge: Signals, signs, and symbols, and other distinctions in human performance models, *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. 13, pp. 257–266, 1983.
- [62] J. T. Reason, and K. Mycielska, *Absent-minded?: The psychology of mental lapses and everyday errors*, Englewood Cliffs, NJ, Prentice Hall, 1982.
- [63] J. T. Reason, *Human error*, Cambridge, Cambridge University Press, 1990.
- [64] S. J. Reinartz, and G. Reinartz, Verbal communication in collective control of simulated nuclear power plant incidents, *Reliability Engineering and System Safety*, Vol. 36, pp. 245–251, 1992.
- [65] M. S. Sanders, and E. J. McCormick, *Human factors in engineering and design*, New York, McGraw–Hill, 1993.
- [66] D. H. B. Scaldasferri, R. Del Pozzo, P. V. Gomes, J. Mola, T. R. Mansur, Strain Measurement on a Compact Nuclear Reactor Pressurizer, *Proceedings of the 18<sup>th</sup> International Conference on Structural Mechanics in Reactor Technology – SMiRT 18*, Beijing, China, 2005.
- [67] J. M. Schraagen, and P. C. Rasker, Communication in command and control teams, *Proceedings of the 6<sup>th</sup> International Command and Control Research and Technology symposium*, U.S. Naval Academy, June 19–21, Annapolis, Maryland. Available at: [www.dodccrp.org/events/6th ICCRTS/Tracks/Papers/Track2/102\\_tr2.pdf](http://www.dodccrp.org/events/6th ICCRTS/Tracks/Papers/Track2/102_tr2.pdf), 2001.
- [68] D. Serfaty, E. Entin, and C. Volpe, Adaptation to stress in team decision making and coordination, *Proceedings of the Human Factors Society 37<sup>th</sup> Annual Meeting*, Santa Monica, California, pp. 1228–1232, 1993.
- [69] J. B. Sexton, and R. L. Helmrich, Analyzing cockpit communication: The links between languages, performance, error and workload, *Human Performance in Extreme Environments*, Vol. 5, No. 1, pp. 63–68, 2000.
- [70] T. B. Sheridan, and R. Parasuraman, Human automation interaction, *Reviews of Human Factors and Ergonomics*, Vol. 1, pp. 89–129, 2005.
- [71] A. Sorge, G. Hartmann, M. Warner, and I. Nicholas, *Microelectronics and manpower in manufacturing*, Berlin, International Institute of Management, 1982.
- [72] SPAR, Standardized Plant Analysis Risk–Human Reliability Analysis, SPAR–H, Idaho National Laboratory, 2005.
- [73] J. Stempfle, and P. Badke-Schaub, Thinking in design teams—an analysis of team communication, *Design Studies*, 23, 473–496, 2002.

- [74] O. Strater, Investigation of communication errors in nuclear power plants, in R. Dietrich (Ed.), *Communication in high risk environments*, Hamburg: Helmut Buske Verlag. GmbH, Sharkey, Catherine, 2005.
- [75] A. D. Swain, H. E. Guttman, *Handbook of human reliability analysis with emphasis on nuclear power plant applications*, NUREG/CR-1278, US Nuclear Regulatory Commission, Washington, DC, 1983.
- [76] K. Takano, K. Sasou, and S. Yoshimura, Structure of operators' mental models in coping with anomalies occurring in nuclear power plants, *International Journal of Human-Computer Studies*, Vol. 47, pp. 767-789, 1997.
- [77] T. Toriizuka, Application of performance shaping factor (PSF) for work improvement in industrial plant maintenance tasks, *International Journal of Industrial Ergonomics*, Vol. 28, pp. 225-236, 2001.
- [78] H. Ujita, Human characteristics of plant operation and man-machine interface, *Reliability Engineering and System Safety*, Vol. 38, pp. 119-124, 1992.
- [79] J. M. Urban, J. L. Weaver, C. A. Bowers, and L. Rhodenizer, Effects of workload and structure on team processes and performance: Implications for complex team decision making, *Human Factors*, Vol. 38, No. 2, pp. 300-310, 1996.
- [80] U.S. Nuclear Regulatory Commission (NRC), *Human-system interface design review guidelines*, NUREG-0700, Revision 2, Washington, DC, NRC, 2007.
- [81] U.S. Nuclear Regulatory Commission (NRC), *ATHEANA user's guide*, NUREG-1880, Washington, DC, NRC, 2007.
- [82] I. Vessey, The effect of information presentation on decision making: A cost-benefit analysis, *Information and Management*, Vol. 27, pp. 103-119, 1994.
- [83] M. Visciola, A. Armando, and S. Bagnara, Communication patterns and errors in flight simulation, *Reliability Engineering and System Safety*, 36, 253-259, 1992.
- [84] C. D. Wickens, S. E. Gordon, and Y. Liu, *An introduction to human factors to engineering*, New York, Addison-Wesley, 1998.
- [85] D. R. Wieringa, D. K. Farkas, Procedure writing across domains: Nuclear power plant procedures and computer documentation, *Proceedings of the 9<sup>th</sup> Annual International Conference on Systems Documentation*, pp. 49-58, 1991.

- [86] C. D. Wilkinson, Elements of effective control room response to emergencies, in P. L. Lassahn, D. Majumdar, and G. F. Brockett (Eds.), *Anticipated and abnormal plant transients in light water reactors*, Vol. 2, pp. 1049–1057, New York, Plenum Press, 1984.
- [87] T. D. Wilson, The proper protocol: Validity and completeness of verbal reports, *Psychological Science*, Vol. 5, No. 5, pp. 249–251, 1994.
- [88] R. M. Wilson, W. B. Runciman, R. W. Gibberd, and J. D. Hamilton, The quality in Australian health care study, *Medical Journal of Australia*, Vol. 163, pp. 458–471, 1995.
- [89] H. Yoshikawa, Distributed HMI system for managing all span of plant control and maintenance, *Nuclear Engineering and Technology*, Vol. 41, No. 3, pp. 237–246, 2009.