SUB CHAPTER G.2. GENERAL ARCHITECTURE OF THE INSTRUMENTATION & CONTROL SYSTEMS

1. OVERALL INSTRUMENTATION & CONTROL ARCHITECTURE

1.1. OVERVIEW

The overall architecture of the Instrumentation & Control system (I&C) is given in figure G.2 FIG 1. The functional architecture is structured in different levels:

Level 0: process interface

Consisting of:

- instrumentation including the sensors, transducers, and data acquisition as far as it is implemented in digital transducers
- cubicles and actuators.

Level 1: automation system

Including: data acquisition, automation processes, monitoring and control implemented in specific NC systems (turbine, alternator, etc), in F2 and NC systems (PAS: Process Automation System and RCCL: Reactor Control, Surveillance and Limitation System) and in F1 systems (PS) [RPS]: Reactor Protection System and SAS: Safety Automation System).

Level 2: monitoring and control of the unit

Including: data processing relating to the Human-Machine Interface for the monitoring and control of processes implemented in the F2 system (MCP[PICS]: Process Information and Control System) and the F1B system (MCS[SICS]: Safety Information and Control System).

N.B.: The functions of priority management and actuation control (PACS: Priority and Actuator Control System) are assigned to the electrical cubicles.

The four PACS functions are the following:

- priority management of commands to an actuator (automatic and manual)) to an actuator, whatever their origin (PS [RPS], PAS, SAS, MCP [PICS], MCS [SICS], IHM [HMI], etc) and their function, and (in the case of simultaneous commands) selection of the command having the highest priority level (in the case of simultaneous commands).
- control of devices activating the movement of an actuator
- monitoring of actuators (management of actuator position and movement failures)
- essential protection of actuator components.
Figure G.2 FIG 2 shows an overview of the allocation of the PACS functions within the various I&C entities.

1.2. DESIGN BASIS

1.2.1. SAFETY REQUIREMENTS

I&C classification principles are given in Chapter C.2.

The process instrumentation is classified according to the specific functions to be carried out.

I&C functional requirements are defined in Chapter G.1.

The safety requirements related to I&C systems are given in Chapters G.3 and G.4.

In order to reduce the risk of common mode failure, the following requirements must be taken into account:

- Independence between the MCP [PICS] and the MCS [SICS]
- Diversity between the PAS and the PS [RPS].

1.2.2. Availability requirements

The availability objectives for typical I&C functions are defined in Chapter R.1 (I&C failure model).

Availability requirements concern I&C systems rather than I&C architecture. Refer to Chapters G.3 and G.4 for availability requirements.

1.2.3. Performance required

The global response times expected in a stable situation for I&C are:

- any process data displayed on the operator interface in less than 1.5 sec.
- operator action effective on the actuator in less than 1.5 sec.

1.3. DESCRIPTION OF INSTRUMENTATION & CONTROL SYSTEM ARCHITECTURE

1.3.1. Level 0

The sensors (analogue and binary), transducers and data acquisition devices are components of the following instrumentation:

- process instrumentation
- in-core instrumentation
The instrumentation includes measurement channels of various importance; the classification of a particular measurement channel depends on the highest level classification of the I&C function for which the measurement is used.

If a given measurement signal is processed in different level 1 systems, acquisition of the measurement occurs in the highest level I&C system: the signal is then generally transferred to other systems via the plant network.

Exceptions exist for measurement signals:
- which relate to high-performance I&C functions for which delay due to serial transmission is not acceptable: these signals are therefore exchanged wire-by-wire
  or
- which are required in the PS[RPS] and other automation systems (PAS, SAS, etc).

Then, the measurement signals are distributed hardwired to the other systems if necessary using decoupling modules. These decoupling modules are mounted within the system that has the highest classification.

The redundant sensors and transducers for a F1 I&C function and their cabling are physically separated and allocated to different divisions.

The cubicles are grouped in:
- class EE1 (seismic class 1) : for F1 I&C functions
- class EE2 (seismic class 1) : for F2E I&C functions
- class EE2 (seismic class 2 or NC) : for F2N I&C functions
- class NC (seismic class 2 or NC) : for NC I&C functions

The redundant actuators and cubicles for a F1 I&C function are arranged in separate divisions.

1.3.2. Level 1

Overview

The automation functions are implemented in the following level 1 systems:
- Process Automation System (PAS),
- Reactor Control, Surveillance and Limitation System (RCSL),
- Safety Automation System (SAS),
- Protection System (PS [RPS]).

Table G.2 TAB 1 gives an overview of the allocation of the I&C function categories to the I&C systems.

Process Automation System (PAS):

The main role of PAS is the monitoring and automation of the plant in all normal operating conditions. In addition, PAS performs some monitoring and control of sub-functions (F2N and NC classified) related to risk reduction.

PAS ensures the management of F2N and NC functions of the nuclear island (except for F2N functions assigned to RCSL) and of the conventional island (except for NC functions assigned to other specific systems such as the turbine or alternator I&C, for example).

PAS functions are monitored and controlled by the operators via the PICS. If the PICS becomes unavailable in PCC1 conditions (normal operation), some PAS functions required to maintain the plant in stable operating conditions can be monitored via MCS [SICS] (see 1.3.3 and 1.4 of Subchapter G.2).

The PAS is an F2/NC digital system.

Reactor Control, Surveillance and Limitation System (RCSL)

The RCSL is mainly dedicated to the processing of F2 and NC I&C classified functions related to core control and monitoring.

These include mainly:

- the core control functions
- the automatic LCO (limiting conditions of operation) functions, and limitation functions for core parameters and for the reactor coolant circuit requiring control rod actuation (part of these functions may be implemented in PAS if PAS equipment is more suitable).

The actuator control functions for the control rods are implemented in the RCSL; the control functions for the other actuators controlled by RCSL are implemented in other level 1 systems, and RCSL communicates with them via the plant network.

The RCSL is a F2 digital system.

Reactor Protection System (PS[RPS])

The PS[RPS] monitors the safety parameters in all operating conditions (PCC), and for all initiating events ensures:

- the automatic F1A protection and safeguard functions
- the automatic F1A control functions of the safeguard support systems
- the manual F1A I&C functions,

The PS[RPS] also provides information on safety parameters for the MCS[SICS] (F1B) and the MCP [PICS] (F2).

The parameters, the initiating signals and the PS[RPS] orders are displayed to the operator by the MCP[PICS] and MCP[SICS]. Safety Interlocks are implemented in the PS[RPS] to prevent manual actions and reset of automatic functions from the MCP[PICS] or MCS[SICS] if the process conditions do not allow it.

The PS[RPS] is an F1A digital system.

**Safety Automation System (SAS)**

The main functions ensured by SAS are:

- post-accident management functions (manual and automatic) necessary to bring the plant from the controlled state to the safe shutdown state after an initiating event (F1B).
- functions related to F1 support systems which do not change their status during an event (autonomous safety systems such as ventilation).
- F1B functions preventing significant radioactive release.
- F2 seismic-classified functions (F2E).

The part of the SAS performing the I&C functions related to the autonomous support systems is organised in autonomous sub-systems incorporating the necessary protection against external influences (for example, functional isolation, local controls, etc).

The parameters, initiation and actuation signals, feedback signals of the SAS are displayed to the operator by the MCP[PICS] and MCS[SICS]. Safety Interlocks (E1B) are implemented in the SAS to prevent manual actions and the resetting of automatic functions from the MCP[PICS] or MCS[SICS] if the process conditions do not allow it.

The SAS is a F1B digital system.

### 1.3.3. Level 2

**Overview**

The data processing in level 2 is mainly used for the Human-Machine Interface (IHM[HMI]) for unit monitoring and control.

The functions are implemented in the following I&C systems:

- Process Information and Control System (MCP[PICS]).
- Safety Information and Control System (MCS[SICS]).
Table G.2 TAB 1 provides an overview of the allocation of categories of process I&C functions to I&C systems.

Figure G.2 FIG 3 provides an overview of the structure of the level 2 systems, the communication network and interfaces.

**Process Information and Control System MCP[PICS]**

MCP[PICS] is used by the operators to monitor and control the plant in all plant conditions (PCC and RRC).

The PICS has access to the information from all level 1 systems and presents the information to the operating personnel on the following IHM[HMI] equipment:

- monitoring and control workstations in the Main Control Room (MCR),
- supervisory workstations in the MCR,
- wall-mounted large screens (display only) for the plant state and plant parameters overview in the MCR,
- workstations for monitoring and control in the Remote Shutdown Station (RSS),
- display only workstations in the Technical Support Centre (TSC),
- printers and recorders.

The MCP[PICS] generates alarms in case of process or system anomalies and provides the operators with guidance for implementing appropriate measures.

Most of the actuators of the plant can be controlled by MCP[PICS] via level 1 systems.

Commands are executed by the operators from the screens and sent to the level 1 systems which act both on the E2/NC and on the E1 safety actuators.

In case of initiating events, the operators monitor the automatically initiated protection or risk reduction functions on the MCP[PICS] screens, and initiate, from the MCP[PICS] screens:

- reset of automatically initiated F1 I&C functions in the PS[RPS] and SAS,
- functions for post accident management in level 1 systems
- risk reducing functions in the PAS.

The MCP[PICS] sub-functions which ensure the control of the sub-functions are F2 classified; F1B sub-functions are safeguarded by the class F1B sub-functions implemented in the MCS [SICS].

Measures are provided in the MCP [PICS] and in the level 1 systems to prevent spurious commands due to internal MCP [PICS] failure or due to an internal hazards.

The MCP[PICS] is F2 classified and is implemented in a digital system with a computerised human-machine interface.
The equipment and architecture of the computerised human-machine interface workstations in the Main Control Room meet the requirements for F1B systems; the workstations for control and monitoring functions in the Main Control Room and the Remote Shutdown Station are seismically classified (seismic class 1). Other functions such as printing, archiving, etc, are implemented in seismic class 2 equipment (to ensure that no hazard is presented to equipment of seismic class 1).

The MCP[PICS] is independent of the MCS[SICS].

**Safety Information and Control System (MCS[SICS])**

The MCS[SICS] provides the safety-classified HMI functions that perform the F1 and F2E control and monitoring functions needed to bring the plant to a safe shutdown state in case of unavailability of MCP[PICS].

The MCS[SICS] allows:

- in case of unavailability of MCP[PICS] in PCC1 (due to internal failures in MCP[PICS]) to control and monitor the plant for a limited time in steady state power operation and, if MCP[PICS] cannot be recovered in 2 to 4 hours, to bring to and maintain the plant in the shutdown state (class F2/NC),

- in case of PCC 2-4 events coincident with unavailability of PICS to:
  - monitor the safety functions of the plant, especially the F1 automatic protection and post accident functions,
  - initiate the manual functions necessary to bring the plant from the controlled to the safe shutdown state (class F1B),
  - monitor and control the support systems of safety systems needed for post accident control,
  - initiate control functions for fire fighting in the nuclear island (class F2E).

Normally, MCS[SICS] is not used by the operators as long as PICS is available; exceptions are:

- periodic tests (F2),

- in accident conditions the monitoring of the main safety process parameters and the status of the safety systems.

As long as MCP[PICS] is available alarms are indicated on MCP[PICS] and MCS[SICS], but MCS[SICS] alarms are autoacknowledged.

As long as the MCS[SICS] controls are not needed they are not active, in order to reduce the risk of spurious actuation as a result of an internal hazard or internal failures within the MCS[SICS].

The MCS[SICS] controls become active by release controls in the safety control area. They are independent and separated from the command controls, so that a single fault or internal hazard can not generate both signals and initiate a spurious actuation.

In case of unavailability of MCP[PICS]:
- manual commands are sent from MCS[SICS] to the level 1 systems which block all commands coming from MCP[PICS] to prevent a spurious actuation being generated by MCP[PICS] malfunction or maintenance and,
- the alarm functions on MCS[SICS] (acoustic alarms, release, reset) that are not active as long as MCP[PICS] operates are activated.

The MCS[SICS] is classified F1B.

The MCS[SICS] is functionally independent of MCP[PICS] from an operational point of view and located in the MCR.

Main Control Room - MCR

The operating and safety functions of the plant are initiated and/or monitored from the Main Control Room MCR in all operating conditions (except if the MCR is unavailable).

The MCR is equipped with:

- workstations for monitoring and control of the plant,
- large MCP[PICS] screens allowing an overview of the status of the main parameters of the plant,
- an emergency operation area with conventional HMI MCS[SICS] equipment.
- equipment enabling F1A manual commands necessary to allow a controlled state to be reached.

Remote Shutdown Station (RSS)

If the MCR is unavailable due to an internal hazard, the operators monitor and control the plant from the Remote Shutdown Station.

For monitoring and control of the plant, the Remote Shutdown Station is equipped with:

- control facilities in order to block the commands coming from MCP[PICS] HMI equipment in the MCR; technical and administrative measures prevent spurious or non authorised activation of this function.
- backup workstations (same design as those installed in MCR, configured in control mode if the MCR is unavailable) from which the operators can bring the plant to safe shutdown state and control it.
- a backup computerised workstations in monitoring mode (display only).

All I&C equipment and support systems needed for operation from the Remote Shutdown Station, are separated from the Main Control Room area, and are located in different fire sectors.

Technical Support Centre TSC

The TSC is a room used by the crisis support team in case of an accident. This additional staff analyse the condition of the plant and support post-accident management.
The TSC is equipped with MCP[PICS] screens with access to all the information but without the command functions.

**Decentralised HMIs**

Some control and monitoring facilities can be installed locally, near to the equipment controlled and/or monitored (Control Room of the Waste Treatment Building BTE for example).

### 1.3.4. Communication between the Instrumentation and Control systems

**Communication within levels 1 and 2**

The data exchanges for the F2N and NC functions between the level 1 I&C systems (PS[RPS], SAS, PAS, RCSL) and between them and the MCP[PICS], are performed by the plant network, with some exceptions (for example due to response time constraints)

To the extent that it is possible, the internal exchanges within a system (including data exchange between divisions) are performed by the system itself without calling up external resources.

The plant network crosses the divisions and extends through:

- the nuclear island electrical buildings (SAB/BL)
- the waste treatment building (BTE)
- the diesel buildings
- the electrical building of the conventional island (BLNC).

The plant network is of class E1B and is designed to withstand a single failure as well as internal hazards within a division, for availability reasons.

Data exchange between MCS[SICS] and the PS[RPS], SAS and PAS systems is ensured essentially by hardwired links.

**Communication between levels 0 and 1**

For F1 functions, the data exchanges between level 0 equipment and level 1 equipment are always performed by hardwired connections.

For F2/NC functions, the data exchanges between level 0 equipment and level 1 equipment are performed either via network or hardwired connections.

### 1.3.5. Technology

The platform used to implement the PS[RPS] and RCSL is the I&C digital system TELEPERM XS.

For the PAS and SAS, as well as the operator workstations in the Main Control Room, the Remote Shutdown Station and the Technical Support Centre, details will be provided once the digital system for the standard I&C has been chosen.

The MCS [SICS] uses conventional technology. However, the use of digital equipment is not precluded (recorders for example).
1.4. OPERATING MODES

1.4.1. Normal operation

Figure G.2 FIG 4 provides an overview of the I&C systems used for the monitoring and control of the plant in normal operation.

The PAS and RCSL carry out all the automated sub-functions in normal operation; the actuator commands go directly from the PAS to the cubicles and from the RCSL to the control rod drive mechanisms. The MCP[PICS] with its IHM [HMI] equipment allows the operators to monitor and control the state of the plant and the I&C functions necessary during normal operation.

For monitoring the state of the RPS and the SAS in normal operation, the PICS receives information from these systems over the plant network.

Unavailability of MCP[PICS]

If the MCP[PICS] is unavailable due to an internal failure, the operating team decides, based on the messages and alarms generated by the MCP [PICS] self-surveillance functions and the life sign function of the MCP [PICS] processing units (F1B monitoring function), to transfer operation of the unit from MCP[PICS] (i.e. the Main Operating area) to MCS[SICS] (i.e. the Back-up Operating area) (figure G.2 FIG 6). The MCS[SICS] is put into operation by implementing the functions described in Section 1.3.3 in Sub-chapter G.2.

It is intended that operation and monitoring of the plant in steady state power operation will be carried out by the MCS[SICS] for only a limited time period. If the MCP[PICS] is not returned to normal in 2 to 4 hours, the operators bring the plant to a safe shutdown state via MCS[SICS], PS [RPS], SAS and PAS and maintain it there.

1.4.2. Reference operating conditions

In accident condition (PCC2 to PCC4) two operating modes must be distinguished:

- operation with all I&C systems available
- operation with only F1 I&C systems available.

Accident mitigation with all I&C systems available

Figure G.2 FIG 5 gives an overview of I&C systems which are used to monitor and control the plant, when all I&C systems are available.

The initiating events are detected by PS[RPS]. The I&C protection functions necessary in the first 30 minutes are initiated automatically and implemented by PS[RPS].

If manual actions are necessary to reach a controlled state or safe shutdown state, the operators are alerted by alarms generated by the PS[RPS] or SAS displayed by the MCP[PICS].

With the help of alarm sheets and operating procedures, and based on the information delivered by all level 1 systems, the I&C functions in PAS, SAS and PS[RPS] are monitored and controlled on the MCP[PICS] screens to manage the post accident situation.

Operation with only F1 I&C systems available
The initiating events are detected by the PS[RPS]. The I&C protection functions necessary in the first 30 minutes are initiated automatically and implemented by the PS[RPS] (G.2 FIG 6).

If manual actions are necessary to reach a controlled state or safe shutdown state, the operators are alerted by alarms generated by the PS[RPS] or SAS and displayed by the MCS[SICS].

The manual post-accident functions are initiated through the MCS[SICS]: the corresponding actions are performed in the PS[RPS] or SAS.

1.4.3. Internal hazards

Unavailability of the Main Control Room

In case of an internal hazard in the Main Control Room, the plant remains in a PCC1 condition. The operators trip the unit and within 30 minutes evacuate to the Remote Shutdown Station. From there, they block all the commands coming from the Main Control Room IHM [HMI] equipment (G.2 FIG 7).

In normal operation, the remote shutdown screens are in standby mode so they can be rapidly brought into operation. The operators monitor and control the transition of the unit to a safe shutdown state using the remote shutdown screens. The operating mode of the level 1 systems is similar to normal operation (see 1.4.1 in this Sub-chapter).

Internal hazards in level 2 systems

The redundancy and separation implemented ensure that, even with a single failure, at least one division of the MCP[PICS] or MCS[SICS] remains available.

The operating mode which results is similar to that described in 1.4.2 in Sub-chapter G.2.

Internal hazards in level 1 systems

The most serious case of internal hazard impacting the level 1 systems in coincidence with a postulated single failure impacting the support systems results in the loss of two complete I&C divisions together with a PCC2 due to malfunctions of I&C equipment. Depending on the failure combination a complete loss of either MCP[PICS] or MCS[SICS] has to be supposed.

This situation is managed with either MCP [PICS] or MCS [SICS] (the one available in level 2) and the remaining E1 I&C equipment in two divisions of level 1 systems. Therefore a safe shutdown state can be reached.

1.4.4. External hazards

The maximum impact of external hazards on I&C equipment can be considered to be the case of loss of all equipment which is not qualified against earthquake: globally this corresponds to the PAS, the RCSL and part of the MCP [PICS].

This situation is the same as the loss of all operational I&C systems in accident conditions. The operating mode is described in 1.4.2. in this sub-chapter.
1.4.5. Risk reduction conditions

The need for risk reduction measures and the tripping of automatic RCC functions is signalled to the operators by the MCP [PICS].

In general, the manual RRC I&C functions are initiated through the MCP [PICS] and performed by the PAS or SAS.

Station Black-out (SBO)

The I&C operation mode considered below is the most onerous scenario consisting of a station black out (SBO) with one SBO-diesel generator lost.

Loss of Offsite Power (LOOP) is detected by the PS [RPS] which trips the reactor and starts the main diesel generators.

When all main diesels fail to start, the power supply of all I&C systems and equipment in all divisions is ensured by the batteries for 2 hours. In this phase, there is no ventilation in any divisions nor in the MCR and only a few actuators are supplied (the power supply of which is backed-up by batteries).

The start of one SBO-diesel (in division 1 or 4) is performed manually from the MCP [PICS] via RRC I&C functions processed by the PAS. The design of the I&C systems prevents control signals with a higher priority (e.g. the PS[RPS] load shedding signal of the main diesel) from blocking the actuators needed in this situation.

As soon as the power supply to the batteries, lighting and ventilation in the MCR and I&C cabinet rooms in one division (1 or 4) is provided by the SBO-diesel, the power supply to all I&C equipment located in the non ventilated divisions is shut off by local intervention, before overheating, to prevent spurious actuations or erroneous signals that could block necessary RRC I&C functions.

The operators monitor and control the plant from the MCR via the supplied MCP [PICS] division, by using the information delivered by the instrumentation of the remaining division processed in the remaining parts of PS[RPS], SAS or PAS. Actuators can be operated via the PAS to the extent that they are powered.

1.4.6. Severe accidents

(Preliminary design)

The management of severe accidents is performed by:

- dedicated automation cabinets in division 1 and 4

- dedicated instrumentation decoupled from the other I&C systems.

- information facilities necessary in severe accidents provided by the MCS [SICS]

- means of controlling the two Severe Accident relief valves, provided by the MCS [SICS].

Figure G2 FIG 11 gives the principle of the I&C architecture.
The I&C equipment necessary for the management of severe accidents is powered by an electrical source backed up by 12-hour batteries.

2. EQUIPMENT ARRANGEMENT

2.1. AMBIENT CONDITIONS

The I&C equipment is installed in different rooms (I&C equipment rooms in the SAB/BL, BLNC, BTE, buildings, I&C cabinets rooms, Main Control Room, Remote Shutdown Station, Technical Support Centre, etc).

The ambient conditions (temperature, humidity) in these rooms are defined in Chapter I.4.1.

The normal and emergency lighting as well as the lighting of evacuation routes is described in Chapter I.5.

The design principles ensuring effective protection of these rooms against electromagnetic interference IEM [EMI] and lightning are defined in Chapter H.4.2.

The IHM [HMI] rooms are provided with several lighting areas which can be manually controlled to provide sufficient light for the operators to perform their assigned tasks (Chapter Q.2.3).

2.2. INSTRUMENTATION & CONTROL SYSTEM POWER SUPPLY

The onsite emergency power supply, including the uninterruptible DC and AC power supply for I&C equipment, is described in Chapter H.

I&C cabinets’ power supply

The emergency power supply for the I&C cabinets is provided by AC/DC converters powered by four sets of battery-backed 400 V AC busbars. The converters are located in I&C cabinets rooms (divisions 1 to 4) and in the I&C rooms of the diesel buildings (divisions 1 to 4).

Generally a group of I&C cabinets will be supplied by two redundant AC/DC converters, powered by two redundant sets of busbars, one of which can be powered from the same division or the neighbouring division (i.e., 1+2 and 3+4). Either of the two converters is able to power all the I&C cabinets. The converters are located in power supply cabinets each of which contains several converters. These cabinets are located close to the I&C cabinets that they power.

The secondary voltage used to supply input/output signals is 24 or 48 V DC.

IHM [HMI] power supply

The uninterruptable AC power supply for IHM[HMI] is powered from the four 400 V AC busbars. These busbars are supplied from the four battery-backed-up 400 V AC busbars and in case of failure of the DC/AC converters via electronic switch-over to the four 400 V controlled voltage busbars.
The AC power supply is provided from all 4 divisions for HMI equipment located in MCR (operator workstations and wall-mounted large screens), divisions 1, 3 and 4 for workstations located in the remote shutdown stations, and Divisions 1 and 4 for the MCP[PICS] processing units located in I&C cabinet rooms.

2.3. EQUIPMENT ARRANGEMENT AND LAYOUT

Allocation of I&C systems to the buildings of the EPR

Due to the controlled ambient conditions, the I&C systems of the nuclear island are located mainly in buildings SAB/BL, within four rooms situated in separate divisions and in rooms at the level of the MCR. Part of the I&C system, for example the I&C instrumentation for fuel handling gear is installed in the BR and BK, in the BAN or the BTE. The I&C equipment is designed to remain operational even after an airplane crash. Thus, 2 out of the 4 divisions of the I&C systems of the IHM[HMI] that are F1 classified (including the MCR) are located in buildings protected by the aircraft shell...

Inside the buildings, the main hazards that could significantly damage one of the I&C divisions are fire, extreme temperatures or flooding. The combination of an internal hazard and a single failure, must not lead to the loss of F1 I&C functions in more than 2 divisions (in particular for the IHM[HMI] of the MCS[SICS]). This is achieved either by a physical separation of equipment into separate divisions, or by measures designed to prevent the propagation of hazards.

Thus, a spatial separation into 4 divisions is required for the 4 PS[RPS] redundancies, whereas for the SAS this separation depends on the controlled mechanical systems which are allocated to the 4 divisions. The MCS[SICS] supply boards are installed in the MCR. The MCP [PICS] supplies all the operating facilities necessary for operation of the unit from the MCR and, if the MCR is unavailable, from the Remote Shutdown Station. In order to ensure sufficient independence from the MCR, the MCP [PICS] processing units are located in the I&C equipment rooms of divisions 1 and 4. In the I&C equipment rooms, the I&C cabinets for the F1 I&C systems are grouped separately from the F2/NC I&C cabinets. All the systems for automation and IHM[HMI] (levels 0, 1 and 2) of the nuclear island that are controlled from the MCR via the MCP[PICS] and MCS[SICS] are located in the I&C equipment rooms of divisions 1 to 4.

The PAS is mainly located in the I&C equipment rooms of divisions 1 and 4, but certain parts are also installed in divisions 2 and 3, depending on the electrical and mechanical equipment controlled, in order to avoid electrical interconnections.

The SAS is distributed through the I&C equipment rooms of divisions 1 to 4 according to the allocation of the corresponding electrical and mechanical equipment.

The PS[RPS] is installed in the I&C equipment rooms of divisions 1 to 4.

The RCSL is installed in the I&C equipment rooms of divisions 1 and 4.

Reserve space is available in each I&C equipment room for possible modifications to power supply and air conditioning equipment. This will allow the preparation and implementation of future changes without affecting operation of the plant or its safety systems.

The MCP[PICS] processing units are installed in the I&C equipment rooms of divisions 1 and 4.
The I&C equipment directly linked to the IHM[HMI] equipment or which is used frequently by staff, is installed mainly at the MCR level, either in the MCR itself or in the IT rooms. This concerns mainly the MCP[PICS] peripherals, but also applies to access control equipment, fire monitoring, video and telephone systems. The peripherals for the monitoring systems, i.e. loose parts detection, turbine and generator vibration monitoring, perturbograph, flux map calculator, parts of the radioactivity detection, will be installed in the peripheral systems monitoring room.

The I&C equipment used for the conventional island (CI) or the BOP are installed in the I&C equipment rooms of the conventional island or in the rooms dedicated to the BOP, respectively.

The configuration and diagnosis tools of the I&C equipment are installed in the I&C maintenance room, situated in the SAB/BL at MCR level.

The I&C equipment and systems locally controlled are installed near the associated mechanical equipment (e.g., emergency generator sets and diesel building ventilation). The monitoring of their main functions and malfunctions is performed using the MCP[PICS].

The I&C equipment for the fuel handling systems (for example, the refuelling machine, swing bridge) is integrated into the mechanical systems or located nearby.

**Main Control Room MCR**

The Main Control Room MCR is located in a bunkered area, protected against radiation, external and internal missiles and earthquakes. All equipment installed in the MCR, whether or not it is required to operate in a seismic event, is designed not to interfere with the operators in performing their tasks, i.e. to maintain its stability (at least seismic class 2). Functional independence and physical separation are taken into account when equipment items of different safety classes are in close proximity within the MCR, in accordance with Chapter Q.

Ventilation and power supply on four trains, as well as lighting, are designed to maintain operational conditions in the MCR and the monitoring of the plant in all PCC and RRC conditions. The environmental conditions in the MCR are such as to allow the operators to work effectively and comfortably. The arrangement of the MCR level assures access by the operators into the MCR in all operating conditions of the unit. Evacuation of the MCR is possible by short routes to the lower level where the Remote Shutdown Station is located.

The MCR space is sufficient to allow the shift operating team to perform all necessary actions. The arrangement of the different operational areas facilitates coordination and communication between the members of the operating team.

The arrangement of the MCR level takes into account a limited need for access to the MCR by other staff members of the unit while preserving the necessary space for I&C staff exchange with the fire patrol and maintenance teams as well as with other staff in other rooms, such as the Head of Operations’ office, the I&C maintenance room, the records room and the peripheral systems monitoring room.

The computerised operator workstations, the mimic display, the MCS[SICS], the communication facilities, and the centralised fire alarm system are installed in the Main Control Room.

**Related rooms**

The technical support centre TSC is located outside the MCR and has independent access.

The washrooms and a kitchen are also near the MCR.
Documentation is available in the offices, in the MCR and in the TSC.

Means of local control is installed if one of the following conditions is met:

- due to its safety function, the equipment must be controlled independently of the MCR and the Remote Shutdown Station.
- operations personnel require a direct link between staff and process, for example, visual or audible contact.
- the system operates independently and after commissioning does not need further manual action (at least does not need daily manual action) to perform its function.

**Remote Shutdown Station RSS**

Internal hazards leading to the unavailability of the MCR require the use of the Remote Shutdown Station (RSS) to bring the unit to safe shutdown and maintain it there. The design concept is that such internal hazards e.g. fire in the MCR, will not occur at the same time as other independent failures, accidents or hazards, with the sole exception of possible loss of the external power supply.

In order to achieve independence between the Remote Shutdown Station and the MCR, the RSS is installed in a different fire sector with a separate access. The corresponding processing units are situated in separate I&C equipment rooms in order to prevent the propagation of internal hazards. The links, for example ventilation ducts between the fire sectors, are designed not to propagate the fire.

Backup computerised workstations and communications equipment (phones) are installed in the Remote Shutdown Station.

**I&C interconnections between the various I&C rooms**

I&C interconnections between the various I&C rooms and the interior of an I&C room are isolated electrically according to the principle below:

- the E1 I&C equipment represents a low voltage island in each division; it is isolated electrically from the E1 equipment of other divisions and possible installation line surge, also from distribution boards, from I&C equipment in the other buildings and from I&C equipment in the same room but of a lower class (E2/NC).
- E2/NC I&C equipment represents a second low voltage island in the same I&C equipment room. The propagation of a line surge from another division or from another building is avoided by electrical isolation.

This isolation is achieved by:

- the use of opto-isolators, isolation modules or fibre-optic cabling in the case of cabled connections
- the use of fibre optics in the case of bus connections.

120-minute fire resistant barriers conforming to ETC-F will be installed between the I&C equipment rooms of the various fire sectors and between the service shafts and the cable runs of the various divisions.
I&C cabinets

The arrangement of the I&C equipment rooms and of the SAB rooms allows sufficient space for all the I&C cabinets to be installed in the nuclear island.

Inside these rooms, the I&C cabinets for the same I&C system are located side by side to form a suite of cabinets. Requirements are met for independence of the various lines of defence and for access control to the different classes of equipment.

In the installation of the various electronic components in the cabinets, the following EMI requirements are taken into account:

- enclosed and shielded casing comprising the cabinet itself (notably the doors)
- sufficient separation between the I&C cables and the low voltage power supply cables
- cable shield bonded directly at the cable entry into the cabinet on an instrument earth bar.
- additional shielding devices for the particular electromagnetic interference sources.

All the cabinets, control desks and panels are linked by their chassis reinforcement to the steel structure of the building in conformance with requirements in Chapter H.4.2.

The E1 I&C equipment cabinets are seismically-qualified in terms of the associated soil spectrum. The E2/NC I&C equipment cabinets will not affect the E1 cabinets in a seismic event (no missile effect). The I&C equipment is designed to meet the design requirements according to its seismic class.

I&C cabling

The I&C cabling uses several independent network connections in addition to conventional cabling, notably to interconnect the various I&C systems. They can be described as follows:

1) level 2 – MCP[PICS] Level 2 network connection to operator workstation screens.

2) main communication network (unit network) - network connections between the four SAB/LAB divisions, the diesel building, the conventional island, the BAN and the BTE.

3) network connections between one SAB/BL division and another division (for example, point to point connections of E1 I&C equipment including between the operating system boards and the conventional MCS[SICS] panel).

4) network connections within a SAB/BL division

5) possible connection of level 0 on specific networks (maintenance network for example) for operating functions outside real time for using "intelligent" technologies for sensors and actuators.

All the cables between the cabinets inside I&C equipment rooms pass through the cable deck under the rooms. The cables between the I&C rooms of different divisions or from the I&C room to the process, are drawn into the trunking for the various divisions. The I&C interconnections between divisions use fibre optic networking with no metal parts. If copper cables are used, isolation devices must ensure that an internal hazard related to a single failure cannot lead to the loss of F1 I&C in more than two divisions.
The I&C control and measurement cables as well as the network cables (fibre-optic or axial) are separated from the low- and medium-voltage cables, according to the recommendations of Chapter H.4.1. Separate routing in the trunking or metal service shafts on the independent cable routes, is required only for the detection of neutron flux and radiation.

F1 signals assigned to the various divisions, do not use the same cabling, the same sub-distribution network or the same penetrations and are protected against the propagation of an internal hazard. They do not use the same junction boxes or the same cables as F2/NC signals or they are distinctly separated from the latter at least in the main channels.

The cabling to the MCR is mainly the junction cabling to the MCS[IICS] conventional panel which is linked via the electronic rooms via the trunking / cable trays dedicated to each division. The cabling of the MCP[PICS] processing unit (situated in divisions 1 and 4) to the MCR and the Remote Shutdown Station is separately laid to each division via independent cable trunking in order to address possible internal hazards.

Shielded earthed conventional I&C cables are used between level 1 and level 0. The concept of earthing which is based on an earth loop around each building and a mesh network connected to the I&C equipment between the buildings includes protection against lightning conforming to Chapter H.4.2.

Fibre optic cables are used for transmission in the applications where insensitivity to electrical or electromagnetic interference, galvanic isolation between systems or divisions, or bus length up to 2,000m, are required. Due to the use of several networks, the applications can be connected by gateways, routers and switches.

Separation means are used for the fibre optic interconnecting local networks across a division with high data concentration (for example the unit network or the level 2 network). The local networks are tolerant to a single failure (redundant local network or bus ring) in order to reach a high level of reliability for data transmission and will be set up in different cable channelling in order to address possible internal hazards.

3. QUALIFICATION PRINCIPLES FOR THE VARIOUS INSTRUMENTATION & CONTROL EQUIPMENT AND SYSTEMS

3.1. INTRODUCTION

Definition of Assessment

Judgment based on evidence of the suitability of I&C items for the performance of a specific function or type of function.

Definition of Evaluation

Attribution of a qualitative or quantitative value to the characteristics of a system.

Definition of Qualification
The I&C qualification is the process by which an I&C item is shown to be capable of responding continuously to design requirements for safety performance, in the environmental conditions existing at the moment that it is needed.

An I&C item is defined as a single I&C component or a I&C system.

I&C qualification covers both I&C hardware and software. The term I&C Item encompasses both:

- The I&C components that can be configured in a I&C system conforming to the I&C system specifications
- The I&C systems supporting the I&C functions such as specified in the I&C functional specifications.

According to the above definition:

- qualification concerns only the I&C items involved in the support of F1A, F1B and F2 classified functions. The qualification requires staggered depth of evaluation of the I&C item according to the classification of the I&C system or equipment.
- qualification must be maintained during the entire lifetime of the I&C item.

The life cycle:

- starts with the specification and the selection of I&C items
- continues with the operation, maintenance and possibly modification and retrofit of the I&C item
- ends when the safety function that the I&C item supports is no longer required.

Qualification requires:

- as input data, the assessment and evaluation of the suitability of the selected I&C item. This is based on a comparison of the characteristics of the I&C item with the technical specifications for the I&C item.
- the evaluation and assessment of the compliance of the I&C item with the specifications of the I&C item.
- a final assessment to ensure that the elementary systems are able to meet the requirements specifications for the safety functions.

3.2. QUALIFICATION AND LIFE CYCLE

A feasibility study of the qualification of the I&C item defines the main concepts and steps of the qualification process and demonstrates that:

- the qualification is feasible in the context of the requirements of the equipment class of the I&C item.
- the requirements are verifiable by a process limited to a cost-effectiveness report by a person or machine.
- all new developments will meet the safety requirements from the beginning.
- the qualification can be maintained as long as the safety function in which the I&C item participates is necessary.

A qualification plan defines the main steps of the qualification of the I&C item based on the feasibility of its qualification.

Following the I&C item life cycle stage:
- a compliance assessment ensures that the I&C item meets the specification of the I&C item. It completes the design stage and allows the implementation of the I&C item into the plant.
- a final assessment ensures that after it is installed and implemented, the I&C item will support the safety function as required.
- during operations and retrofit, the I&C item will be maintained in a qualified state in order to continue operation (G.2 FIG 8).

3.2.1. Qualification of an I&C item during the specification, design and implementation steps

The specification of an I&C item is evaluated and assessed to ensure that it meets its technical specifications.

The evaluation and assessment demonstrate that the I&C item meets its technical specifications.

At the specification and selection stage of an I&C item, the designer selects either a pre-existing I&C item or develops a new I&C item suitable for ensuring the safety functions.

The I&C item can be a single I&C component or a family of equipment, the I&C components can be configured to perform various types of I&C function (typical application functions).

Input data for suitability and assessment

Before acceptance of the specification of the I&C item, the suitability study evaluates and assesses the compliance of the I&C item’s specification to the technical specifications.

If pre-existing items are selected, the evaluation documentation of the conformity of the pre-existing items must be taken into account to facilitate the qualification process.

Assessment and evaluation of conformity

On the basis of the suitability assessment, a qualification plan is elaborated and executed in order to evaluate and assess the compliance of the I&C item properties with respect to the I&C item specification.

The qualification plans should be agreed between assessor and designer in order to limit analysis and tests to the extent defined by the relevant acceptance criteria.

The qualification plan defines the safety relevant subjects of the qualification for the I&C systems and components, for which the compliance shall be evaluated and assessed.
These are:

- the specified properties of components and configurations of the I&C item (e.g.: functionality, performance, reliability, fault tolerance...),

- the influence factors (environmental conditions like temperature, electromagnetic fields) under which compliance shall be demonstrated,

- the properties of the I&C system software (computer based items),

- the specified plant specific properties of the functions (e.g. the application functions of the plant, specific service functions...).

The qualification plan:

- identifies the pre existing qualification documentation,

- identifies the I&C item specifications and documentation that are the basis for qualification.

The qualification plan establishes:

- the principles for evaluating the properties of components and configurations of the I&C item (type tests, analysis...),

- the approach for evaluating the properties of the I&C system software,

- the approach for evaluating the properties of the plant specific functions (application software).

The qualification plan:

- specifies the acceptance criteria for the tests and test sequences,

- specifies the acceptance criteria for analysis,

- indicates if acceptance shall be based on quantitative figures or qualitative judgment,

- specifies the documentation to be produced for each property to be qualified.

The compliance assessment is based on the evaluation of the results.

The qualification plan includes the qualification of the I&C equipment (see 3.5 within Sub-chapter G.2) and the specific I&C qualification (see 3.6 within Sub-chapter G.2).

3.2.2. Final assessment

Installation checks and commissioning tests demonstrate that the I&C item co-operates within the I&C and with the equipment under control as required by the safety functions.

The final assessment gives assurance that all the I&C items are capable of continuously meeting the design basis performance requirements needed for the safety function while being subject to the environmental conditions existing at the time that the safety function is needed.
3.2.3. Maintaining the qualification

The qualification must be maintained over the operating lifetime of the I&C system in the following cases:

- modification of the physical configuration of the I&C system
- replacement of equipment or software of the I&C system
- modification or extension to the application software
- modification of any tools that are used for the qualification evaluations
- modification of interfaces

3.3. QUALIFICATION PROCESS

The EPR I&C consists of I&C systems using pre-existing configurable equipment families as far as possible.

The qualification process of such I&C systems evaluates and assesses:

- the general (non plant specific) properties of the I&C system,

  the majority of general properties of the I&C system are covered by the pre-existing evaluations and assessments of the equipment family (see 3.2.1 within Sub-chapter G.2), and

- the plant specific properties of the I&C system.

If an equipment product line is used, with already assessed properties for equal or more severe service, only the plant-specific evaluations and assessments are necessary.

The qualification process is summarized on G.2 FIG 9.

3.3.1. Non Plant Specific Evaluation and Assessment

Non plant specific evaluations and assessments address the use of I&C components and the basic configuration(s) of the equipment family.

The basic configurations are I&C systems built up with I&C components of an equipment family that operate all together in defined architectures. These architectures are representative of allowed configuration that can be realized with the equipment family.

The evaluation and assessment of:

- the properties of the components and the basic configurations of the equipment family,
- the properties of the system software of the equipment family (i.e., evaluation of the confidence that the system will perform as specified),
- the properties of the tools of the equipment family.
Give assurance that the components of the equipment family:

- perform their functions as specified in the component specifications,
- operate together in all the allowed configurations as specified in the equipment family specification.

3.3.2. Plant-Specific Qualification

The plant specific evaluation and assessment give assurance that the properties of the equipment family make it possible to build up the I&C systems according to their specifications, i.e. the pre-existing assessments of the general properties of the equipment family give assurance that:

- the intended configurations of the I&C systems are allowed configurations for the equipment family,
- the components of the equipment family operate all together in the intended configurations as specified.

3.3.3. Documentation of the Equipment Family

The documentation specifies the properties of all I&C components and the allowed configurations of the equipment family.

The documentation should provide a means for determining:

- the safety integrity and performance that can be achieved for the plant application functions in the anticipated configuration(s),
- the functional and performance behaviour in case of defined conditions (normal and abnormal),
- the influence of the functions and components not submitted to qualification.

The I&C components and allowed configurations that already passed qualification program should be explicitly identified by the equipment family documentation.

3.4. QUALIFICATION PRINCIPLES

Qualification of an I&C item may be accomplished by:

- tests,
- analysis,
- operating experience.

These may be used individually or in any combination depending upon the particular properties of the I&C item.
3.4.1. TESTS

Tests are separated into type tests and plant specific tests.

The type tests are performed independently from the intended use of the I&C item in the plant.

The plant specific tests are performed to give assurance that the I&C items meet the plant specific requirements.

Type Tests

Type tests are performed on a sample of I&C items of the same design.

Type tests of I&C equipment using simulated environmental conditions constitute the preferred method for demonstrating that the sample complies with the properties of the I&C item even if submitted to the influence factors under which the I&C items are able to perform their task.

Normally type tests are performed in the context of non-plant specific qualification.

Plant Specific Tests

Specific tests are carried out in addition to the type tests in order to cover the specific use in the plant of the I&C item. Specific tests can be carried out mostly in the supplier’s factory and completed by operational tests on site.

3.4.2. Analysis

Analysis is used in most steps of the qualification process. In the following, some examples describe the use of analysis.

Analysis of the I&C item specifications is the basis for the definition of the qualification plan.

In particular analysis is the basic method for evaluating hardware and software development (e.g. this analysis evaluates hardware and software design, component tests, verification/validation and documentation).

Analysis (e.g. failure effect analysis, critical load analysis, ...) is appropriate for the evaluation of properties that cannot be evaluated by tests.

Analysis of the results of type tests and evaluation according to the acceptance criteria leads to the compliance assessment of the type-tested properties.

3.4.3. Operating Experience

A conventional (as opposed to computer based) I&C item that has operated successfully may be qualified for equal or less severe service (i.e., less severe operating conditions for the I&C item with a similar functional task) on the basis of operating experience.

Operating experience may also support the evaluation of the quality of pre existing items including software.

Operating experience will be evaluated on the basis of both:

- the cumulated operating time of the pre existing I&C item,
- the history of failure reports and modifications of the pre-existing I&C item.

Operating experience requires accurate collection of the above-mentioned history characteristics including similarity of use. A traceable documentation requires an early involvement of suppliers and users.

### 3.5. EQUIPMENT QUALIFICATION

Equipment qualification is preferably performed by tests.

Type tests have to demonstrate the compliance of the components and intended configurations with their specifications, if they are submitted to the environmental conditions that they must withstand.

Some properties of the components can be evaluated and assessed only if they operate together with other components. Therefore test configurations of components are used to evaluate and assess the component properties.

For programmable equipment, specific test software must be loaded into the test configurations so as to make it possible to demonstrate that the items perform correctly their functions during the test (e.g., for EMI and seismic tests).

In most cases pre-existing evaluations and assessments of components and test configurations of the selected equipment family exist.

These pre-existing evaluations are analyzed for the purpose of verifying whether the test configurations cover the specified properties of all the allowed configurations of the equipment family: (mounting, installation, load and temperature distribution inside the cabinets, application functions running during EMI and seismic tests, etc...).

Additional plant specific tests may be necessary depending on the results of this analysis.

### 3.6. SPECIFIC QUALIFICATION FOR I&C SYSTEMS

This section deals with evaluations and assessments that are additional to 3.5 in this subchapter.

It focuses on computer based I&C systems built up with equipment families. These are the most complete and most usual cases.

Qualification of conventional I&C systems may be derived from this section.

The qualification plan distinguishes between different system, software and tools properties (G.2 FIG 10).

The qualification plan takes advantage as much as possible from pre-existing evaluations that can be assessed in a non-plant specific qualification step.

**Non plant specific evaluations address:**

1. Properties of components and anticipated configurations,
2. The properties of the system software,
It covers e.g.:
- Operational Software.
- Application software libraries.
- System testing software.
- Operating features (service functions, self test, modes of operation ...).

3. The properties of the tools,
They are used for e.g.:
- Configuration.
- Implementation.

However additional evaluations have to be assessed in order to give assurance that the I&C system complies with I&C system specifications.

**Plant specific evaluations address:**

4. The properties of the application software.
5. The properties of the integrated and configured hardware and system software.
6. The properties of the complete I&C system.

The following properties are considered when establishing a qualification plan and are evaluated and assessed in terms of compliance with I&C system specification.

### 3.6.1. Properties of Components and intended Configurations

If the qualification plan requires evaluation and assessment of I&C system properties, the pre existing evaluations of the properties of the equipment family are analysed to check whether the components and the allowed configurations cover the specified properties of I&C system.

The degree of evaluation and assessment depends on the equipment class of the I&C system:

- functional properties are related to the different types of application functions that the I&C system is able to execute.
  In order to give assurance that the I&C system is able to execute the specified application functions, the functional properties are evaluated and assessed.
- performance properties are related to the speed and accuracy with which the I&C system executes the application functions.
  These properties may be evaluated together with the functionality properties, because independent evaluation is impossible in many cases.
- safety and integrity properties are related to the reliability of the I&C system. This depends on:
the reliability of the I&C system hardware that can be calculated on the basis of reliability data of the components and the I&C system architecture,

- the safety integrity of software that can be evaluated by qualitative analysis of the development process in order to assess a sufficient degree of confidence in the software.

3.6.2. Properties of System Software

The evaluation of confidence in the system software is particularly important for the assessment of the safety integrity achievable for the specified application functions.

The system software must be consistent in terms of safety integrity estimated on the basis of the feasibility of the system equipment.

The analysis of confidence in the system software is strongly linked to the development process.

Development proceeds in stages for E1A, E1B and E2 equipment. The requirements concern, for example:

- the architecture design of the equipment and software
- the development process
- the verification and validation process
- the appropriate use of commercial components supplied by third parties (processors made by Intel, Motorola,…).
- additional validation tests

The evaluation of confidence is based on an analysis of the development documentation.

The analysis verifies:

- the content of the documentation
- that the development process follows well defined stages
- that the results of each stage are verified by analysis or testing
- that the software is validated after integration into the equipment

The I&C IT systems constructed from families of equipment represent the most contained case and the most current case. Thus, this evaluation is carried out by analysing the documentation of the family of equipment. Pre-existing evaluations are used to assess confidence in the system software.

Gradation of requirements

The evaluation and assessment of the confidence in system software components depends on the equipment class.
Gradation criteria for the individual equipment classes follow the different requirements of the system requirements specifications as expressed in rules and standards.

Within the system software, there are functions of different importance for the execution of the application functions. A graduated scale of confidence is assessed within each class of equipment. The criteria can be set out as follows:

- the highest confidence level is demanded for the functions whose results directly affect the application functions (for example, application software libraries, exception processing in the case of errors,...).

- a reduced confidence level is demanded for:
  a) functions designed to have their results verified offline.
  b) operating functions whose results do not affect the application functions.
  c) operating functions whose results have only an indirect influence on the operation of the unit (that is, production of messages or diagnostic signals on the state of equipment, recording data, modifying parameters, periodic testing).

- confidence assessment is not required for functions which are not used, in the sense that they do not question the confidence in the system software.

3.6.3. I&C System Tools Evaluation and Assessment

The evaluation and the assessment of tools depend on:

- the task supported by the tool (e.g. transformation of source code into executable code, verification and validation of the application software, service, hardware configuration),

- the consequences of errors potentially introduced by the tools,

- what verifications may detect or mitigate errors introduced by a tool.

The tools that influence the safety integrity of the safety functions (notably the corresponding executable code) are identified by the qualification plan.

An evaluation and an assessment of these tools is necessary if all of the conditions below are true:

- the tool output can directly inject, or induce, an error into the executable code,

- the tool output is not systematically verified,

- alternative development process and methods do not exist to mitigate the consequences of errors induced by tools,

- the tool does not benefit of a large amount of operating experience for similar use.

3.6.4. Application Software Evaluation and Assessment

The evaluation of confidence of the application software analyses:
- the application software, developed in well defined steps,
- the verification and validation process, which is part of the development cycle of the application software.

In most cases the application software is specified and developed by means of functional diagrams. The executable code is generated automatically from these diagrams. The whole development process is supported by I&C system tools.

Starting from the functional diagram, the specification of the application software is performed based on reusable and qualified application software libraries. The resulting application software contained in a database constitutes the starting point for the automatic generation of the code that will be processed by the computer based I&C system.

This way of specifying the application software facilitates the evaluation of the confidence. In effect the application software specifications can be verified by process engineers. This way of application software generation is recommended for all the classes of I&C systems.

3.6.5. Evaluation and Assessment of the Plant Specific Configurations

Many of the I&C system properties depend also on plant specific configurations, operation and maintenance procedures.

The compliance of the plant specific configurations with the general design requirements of RCC-E are evaluated and assessed. (Chapter B.6).

3.6.6. Integration and validation of the application software in the I&C system.

Before installation of the I&C system in the plant, the application software is validated after integration of the executable code in the I&C system.

Evaluation and assessment gives assurance that the validation is carried out and documented according to the validation plan of the I&C system (RCC-E).
### G.2 TAB 1: ALLOCATION OF CATEGORIES OF FUNCTION TO SYSTEMS

<table>
<thead>
<tr>
<th>Categories of I&amp;C functions</th>
<th>Function class</th>
<th>Level 1 systems</th>
<th>Level 2 systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal operation, non safety related</td>
<td>NC</td>
<td>PAS</td>
<td>MCP[PICS]</td>
</tr>
<tr>
<td>Normal operation safety related, not seismic qualified</td>
<td>F2N</td>
<td>PAS or RCSL</td>
<td>MCP[PICS]</td>
</tr>
<tr>
<td>LCO surveillance</td>
<td>F2N</td>
<td>RCSL or PAS *</td>
<td>MCP[PICS]</td>
</tr>
<tr>
<td>Limitation</td>
<td>F2N</td>
<td>RCSL or PAS *</td>
<td>MCP[PICS]</td>
</tr>
<tr>
<td>Safety related and seismic classified functions</td>
<td>F2E</td>
<td>SAS</td>
<td>MCP[PICS] and MCS[SICS]</td>
</tr>
<tr>
<td>Reactor Protection</td>
<td>F1A</td>
<td>PS[RPS]</td>
<td>MCP[PICS] and MCS[SICS]</td>
</tr>
<tr>
<td>Post-accident functions</td>
<td>F1B</td>
<td>SAS (optionnally PS[RPS]), SAS</td>
<td>MCP[PICS] and MCS[SICS]</td>
</tr>
<tr>
<td>Autonomous safety systems</td>
<td>F1B</td>
<td>SAS</td>
<td>MCP[PICS]** or local control stations</td>
</tr>
<tr>
<td>Prevention of significant radioactive release</td>
<td>F1B</td>
<td>SAS</td>
<td>MCP[PICS] and MCS[SICS] or local control stations</td>
</tr>
<tr>
<td>Resulting PCC 3 or PCC 4 in case of malfunction.</td>
<td>F1B</td>
<td>SAS</td>
<td>MCP[PICS] and MCS[SICS]</td>
</tr>
<tr>
<td>Mitigation of Common Cause Failure (CCF) impacting RPS</td>
<td>F2</td>
<td>PAS</td>
<td>MCP[PICS]</td>
</tr>
<tr>
<td>Mitigation of CCF impacting mechanical safety systems</td>
<td>F2</td>
<td>PAS, RCSL, SAS or PS[RPS]</td>
<td>MCP[PICS]</td>
</tr>
</tbody>
</table>

* the initialisation sub function can also be implemented in PS[RPS]

** only surveillance of main parameters
G.2 FIG 1: OVERALL I&C ARCHITECTURE

Level 0
- Process interface
  - Operational systems
    - Control rods
  - Safety systems
- Specifics I&C (turbine...)
- Instrumentation
- Actuators

Level 1
- System automation
  - Control
  - Trip

Level 2
- Supervision and control
  - Control rods
  - Trip
  - Instrumentation
  - Actuators
G.2 FIG 3: STRUCTURE OF LEVEL 2

- TSC
- RSS
- MCR
- Decentralised HMI
- Operation area: worksation, worksation, worksation
- Supervision area: worksation
- Emergency operation area: SICS
- MCP treatment units
- PAS
- RCSL
- PS
- SAS

Hardwired link
Network link
G.2 FIG 4: NORMAL OPERATION

- Remote Shutdown Station
- Process control area
- Safety control area
- PICS
- SICS
- PAS
- RCSL
- PS
- SAS

Level 0: Process interface
Level 1: System automation
Level 2: Supervision and control

Operational systems
Core control rods
Safety systems
G.2 FIG 5: OPERATION DURING ACCIDENT MITIGATION WITH THE OPERATIONAL I&C SYSTEMS
G.2 FIG 6: OPERATION WITH F1 SAFETY I&C SYSTEMS ONLY

- Remote Shutdown Station
- Process control area
- Safety control area
- PICS
- SICS
- PAS
- RCSL
- Level 2: Supervision and control
- Level 1: System automation
- Level 0: Process interface

Operational systems
Core control rods
Safety systems
G.2 FIG 7: OPERATION FROM THE REMOTE SHUTDOWN STATION

- Remote Shutdown Station
- Process control area
- Safety control area
- PICS
- SICS
- PAS
- RCSL
- PS
- SAS

Level 2: Supervision and control
Level 1: System automation
Level 0: Process interface
G.2 FIG 8 : QUALIFICATION AND LIFE CYCLE OF THE I&C ITEM

Suitable for

- Continuation of operation of the system
- First operation of the safety functions
- Implementation of the I&C item in the plant
- Inputs during Life Cycle

Maintaining of the Qualification

Final Assessment

Compliance Assessment

Suitability Analysis from Specification Design Implementation

Installation & Commissioning

Operation Retrofit

Life Cycle
G.2 FIG 9 : QUALIFICATION AND LIFE CYCLE OF THE I&C ITEM

**EVALUATION:**

- **Non plant-specific**
  
  - Pre-existing evaluation of equipment family properties
    (conventional or computer based equipment)
  
  - Pre-existing evaluation of software confidence of the equipment family
    (only for computer based equipment):
      - evaluation on the basis of the development and validation documents
      - evaluation on the basis of the operating experience

**ASSESSMENT:**

- **Plant-specific**
  
  - Suitability Assessment

- Development and qualification of the plant specific hardware and software (if any)

- Compliance Assessment
G.2 FIG 10 : QUALIFICATION AND LIFE CYCLE OF THE I&C ITEM

Compliance Evaluation and assessment

Assessment of pre-existing evaluations

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>II</td>
<td>III</td>
</tr>
<tr>
<td>- Operational Software</td>
<td>- Application Software Libraries</td>
<td>- System Testing / Operating feature - Service function</td>
</tr>
<tr>
<td>- System Testing / Operating feature - Service function</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assessment of additional evaluations

<table>
<thead>
<tr>
<th>Properties of the Application Software</th>
<th>Properties of the Integrated and Configuration Hardware and System Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>IV</td>
<td>V</td>
</tr>
<tr>
<td>Developed with tools of the equipment family</td>
<td></td>
</tr>
</tbody>
</table>

Properties of the Complete System Integration and Validation of the Application Software in the I&C

Final Assessment
G.2 FIG 11 : SEVERE ACCIDENT I&C PRINCIPLES