SUB-CHAPTER M.2. OPERATING PRINCIPLES

1. NORMAL OPERATING PRINCIPLES

1.1. GENERAL REMARKS

Normal operation comprises:

- power operation and normal scheduled operating transients such as increases in load, reductions in load, load following, unit shutdown or startup,

- specific operations due to unplanned events, such as house load operations or loss of power sources for example.

Except for refuelling shutdowns, the unit can be shut down for long or short periods for operations involving maintenance or repair, fuel saving or power grid management. The shutdown mode, hot shutdown or RIS-RRA [SIS-RHR] shutdown, will depend on the nature of the intervention and on the shutdown duration. During prolonged operation at hot shutdown, the boron concentration in the primary circuit, which ensures the required shutdown margin, is adjusted according to the fuel burnup and duration of the shutdown.

A switchover to cold shutdown is made to carry out refuelling or to enable maintenance or repair operations which require the unit to be at cold shutdown.

The main operating principles are set out below in chronological order, from reactor shutdown at the end of the fuel cycle through to power operation at the beginning of the following fuel cycle. Operation with an extended cycle is also described.

1.2. REACTOR SHUTDOWN

The initial mode considered is the state of the reactor during power operation at the end of a fuel cycle. Unit shutdown begins by a reduction in the turbine load. The power level for disconnection from the grid and turbine shutdown will depend on the turbine generator unit chosen. The average temperature setting is switched from automatic mode to "flux level control" mode. As soon as the grid is disconnected, the load is automatically transferred to the turbine bypass system (GCT [MSB]). Flux level control is switched to manual mode and the turbine is tripped. Turbine tests are carried out if necessary during this phase.

The control rods are inserted manually to shut down the reactor. The primary coolant temperature is controlled by the turbine bypass system. The steam generators continue to be fed and their water level is controlled by the startup and shutdown systems (AAD [SSS]) and the feedwater flow control system (ARE [MFWS]). The primary system is borated to maintain the required shutdown margin. Hot shutdown tests and inspections are carried out.

Whilst cooling, the turbine is on its barring gear.

The primary system is then cooled to approximately 120°C by the GCT [MSB], using the four primary pumps to circulate primary fluid through the steam generator tubes. The maximum cooling rate is 50°C/hr. At the same time, the primary pressure is reduced by normal pressuriser spray to approximately 25 bar, whilst maintaining the required subcooled margin. An automatic sequence ensures simultaneous cooling and depressurisation of the primary system and boration is carried out in parallel. At 120°C and 25 bar, the RIS [SIS] trains 1 and 4 are connected and started up in RRA [RHR] mode to continue the RCP [RCS] cooling. The turbine bypass system may be isolated and the feedwater plant stopped and cooled in preparation for maintenance operations. Two primary pumps are shut down (RCP2101 and 2401).

The slabs of the reactor refuelling cavity are removed below 120°C.

When the primary temperature is less than 100°C, RIS [SIS] trains 2 and 3 can be connected and started up in RRA [RHR] mode in order to increase the primary system cooling capacity. The RCV [CVCS] letdown line is connected to the RIS/RRA [SIS/RHR] system.

At 90°C, the equipment hatch may be opened to enable tools and equipment to be taken into the containment.

The number of primary pumps in operation is adjusted for efficient cooling and to allow for oxygenation at 80°C, required after injection of hydrogen peroxide in the RCP [RCS]. The last primary pump (number 3 so as to keep normal pressuriser spray available for as long as possible) is shut down when the radiochemical criteria are met and the vessel head temperature is below 70°C. The primary system is maintained at 55°C.

Throughout the primary system cooling process, contraction is compensated by RCV [CVCS] charging pumps and REA [RBMWS] pumps, which draw boric acid and demineralised water from the storage tanks. Boration is continued until the required boron concentration during cold shutdown for fuel reloading is achieved.

After the last GMPP [RCP] has been stopped, the primary pressure is reduced to 5 bar by auxiliary spray and the primary pressure is maintained by nitrogen makeup during the final cooling stage. The pressuriser is maintained with a nitrogen gas bubble above the water.

1.3. DRAINING AND OPENING THE PRIMARY SYSTEM

One RIS [SIS] train in RRA [RHR] mode is stopped prior to primary system draining.

The primary system is drained to ¾ loop level by the RCV [CVCS] letdown line (via the RIS/RCV [SIS/CVCS] connection) and the excess volume of primary coolant is transferred to the TEP [CSTS] storage tanks for recycling. Adjusting the water level to ¾ loop level precludes core uncovery and ensures safe RIS [SIS] operation in RRA [RHR] mode.

Before opening the primary system, the RCP [RCS] is swept by injecting nitrogen via the primary pump casings and the vessel head vent, and venting is carried out by the vacuum pump linked to the pressuriser vent. The RCP [RCS] is then air-swept. The RCP [RCS] water level is maintained and controlled automatically at ¾ loop level before opening the RCP [RCS].

The electrical connections of the rod control system mechanisms and core instrumentation are removed. The mechanical seals are removed, thereby opening the primary system. After the thermal insulation of the vessel head has been removed, the multistud tensioning machine (MSDG) is positioned to carry out vessel head opening operations.

1.4. CORE UNLOADING

Whilst the vessel head is being removed, the compartments of the reactor refuelling cavity are filled with borated water from the IRWST by an ISBP [LHSI] pump. When the cavity is full, the core instrumentation, including the lances of the system for measuring neutron flux using aeroballs, is removed and the rod control system mechanisms are disconnected. When the internals are withdrawn and placed in the reactor refuelling pool, fuel unloading operations can begin (approximately 70 hours or less, after the uncoupling) using the handling devices (loading machine, transfer tube, fuel handling crane). The primary coolant temperature is maintained below 50°C by the RIS [SIS] in RRA [RHR] mode. Fuel unloading takes approximately 40 hours. During this phase, an engineered safeguard train may be declared unavailable, to enable maintenance.

The decay heat of the unloaded fuel elements is added to that of the fuel elements already stored in the fuel building spent fuel pool. Thus, the second cooling train of the pool water purification and cooling system (PTR [FPPS/FPCS]) must be started up to maintain the pool temperature below 50°C (from the beginning of core unloading to the end of reloading).

Once the core is unloaded, two engineered safeguard trains may be declared unavailable to enable maintenance. Depending on the scheduled work, the sluice gate between the vessel compartment and the internals storage compartment is placed in position. The RCP [RCS] is drained into the IRWST to the level of the steam generator plena using the PTR [FPPS/FPCS] purification pumps. Maintenance work is carried out in this 'Fully Unloaded Reactor' state: inspection of steam generator tubes and steam generator plena work. In the fuel building, changing of rod cluster control assemblies and inspection of fuel elements are carried out if necessary.

1.5. CORE RELOADING

After closing the primary components (i.e. steam generator manways), the vessel refuelling cavity is filled with borated water from the IRWST using the ISBP [LHSI] pumps. The sluice gates are then removed, the transfer tube opened and the fuel is loaded into the vessel by means of the handling devices (fuel handling crane, transfer tube, refuelling machine). The primary temperature is maintained below 50°C by the RIS [SIS] in RRA [RHR] mode. Core loading and mapping operations last approximately 45 hours.

Once the loading is completed, the transfer tube is closed. The upper internals are put back in position, the rod cluster control assemblies reconnected, the aeroball lances inserted and the core instrumentation installed.

1.6. CLOSING AND FILLING THE PRIMARY COOLANT SYSTEM

The reactor building spent fuel pool compartments are drained down to the vessel flange, the water being transferred to the IRWST using the purification pumps, demineralisers and filters of the PTR [FPPS/FPCS].

The bottom of the vessel refuelling cavity and the vessel casing flange are cleaned. The reactor vessel is closed by the multistud tensioning machine (MSDG) which may be removed from the reactor building after use. The head penetration seals are re-assembled and the vessel head vent closed. When the primary system is able to be subjected to pressure, the RIS [SIS] in RRA [RHR] mode is protected by the pressuriser relief valves. The electrical connections of the rod control system mechanisms and core instrumentation are re-installed.

During these operations, the primary coolant temperature is controlled by the RIS [SIS] in RRA [RHR] mode.

The primary system is then drained down to ¾ loop level by the RCV [CVCS] letdown line (via the RIS/RCV [SIS/CVCS] connection) so that the gas-filled parts of the vessel, pressuriser and steam generator tubes are connected together. The RCP [RCS] level is automatically controlled by the RCV [CVCS] so as to prevent core uncovery and ensure safe RIS [SIS] operation in RRA [RHR] mode.

The vacuum pump is used to create a vacuum in the primary system. The resultant pressure is reduced to approximately 200 mbar to minimise the primary coolant oxygen content. The temperature is maintained below 40°C during this period to ensure a sufficient subcooled margin in the primary system.

The primary system is then filled by REA [RBMWS] makeup using the RCV [CVCS] pumps. The primary coolant is degassed at a high flow rate by means of the RCV [CVCS] and related systems. RCP [RCS] filling is stopped when the pressuriser level reaches 7m. The unit is started up with a steam bubble in the pressuriser.

With regards to the conventional island, operations on the turbine, the generator and the transmission power systems are completed. The turbine generator unit is on its barring gear. Two steam generators are needed and are filled to their no load level. The main atmospheric steam relief line (VDA [MSSS]) is available. The feedwater plant is filled, a vacuum created in the condenser and the heating and chemical treatment of the feedwater plant are begun.

1.7. HEATING THE PRIMARY COOLANT

After the vacuum-creating device has been shut off, primary pressure is raised by starting up the pressuriser heaters, without exceeding 30 bar, whilst the RIS/RRA [SIS/RHR] is connected. The maximum pressuriser temperature increase rate is 100°C/hr. The RCP [RCS] does not go into water solid mode. When the RCP [RCS] pressure reaches 20 bar, the RIS/RCV [SIS/CVCS] connection is isolated, the pressure being sufficient to enable normal RCP/RCV [RCS/CVCS] letdown. Primary pumps are started up at a minimum pressure of 25 bar. The first pump (GMPP [RCP] no.3 first for normal pressuriser spray) is started up before the primary coolant reaches 65°C. After the GMPPs [RCPs] have started up, RCP [RCS] pressure is placed in automatic control mode (heaters and normal spray). The power supplied by the four pumps and the fuel decay heat enables the primary coolant to be heated. The heating rate is limited to 50°C/hr (if the power supplied enables this). A single RIS [SIS] train in RRA [RHR] mode is enough to ensure temperature control during the primary heating process; the other trains are available if needed.

At the same time as this operation is being carried out on the primary circuit, the secondary circuit is made available. In particular, above 120°C, the four steam generators are filled to their no load setpoint level and can be supplied by the AAD [SSS]. The condenser is under vacuum and the GCT [MSB] is available. The feedwater plant is heated and chemically treated. Heating of the steam lines is begun.

When the RCP [RCS] temperature reaches 120°C, the last two RIS [SIS] trains (trains 1 and 4) still connected in RRA [RHR] mode are isolated. Temperature control is then ensured via the steam generators (GCT [MSB] and AAD [SSS]).

During the heatup process, the excess coolant volume due to primary expansion is drawn off through the RCV [CVCS] letdown line (automatic control of the pressuriser level) to the TEP [CSTS] storage tanks. At the same time, the pressure is progressively and automatically increased until it reaches hot shutdown conditions.

During the heatup, tests may be carried out at the required pressure and temperature values.

At hot shutdown the pressuriser level is set to its no load setpoint by the RCV [CVCS] letdown. The pressure is controlled using the pressuriser heaters and normal spray and the temperature is controlled by the steam generators. The steam generators are maintained at their no load water level by means of ARE [MFWS] valves, and their no load pressure level by GCT [MSB] control.

The feedwater plant is available and in service. The turbine generator unit is on its barring gear.

1.8. FROM HOT SHUTDOWN TO POWER OPERATION

At this stage, prior to criticality, all safety functions for power operation must be available. In hot shutdown, various tests are carried out, such as measurements of rod drop time. The primary coolant temperature is automatically controlled by the GCT [MSB]. Tests at zero power are carried out and the primary coolant is diluted by injection of demineralised water from the REA [RBWMS] using the RCV [CVCS] charging pumps. Power is then increased by controlling the flux level. The steam generators are supplied by the startup and shutdown pump (AAD [SSS]), then by the feedwater pumps (APA [MFWPS]) using the normal feedwater flow control system (ARE [MFWS]).

The turbine is commissioned, the generator is connected to the main grid and power is gradually increased. The normal steam generator control mode (priority to the turbine) replaces flux level control. At this power level, all RCP [RCS] controls are in automatic mode (see Chapter E.1) and power is gradually stepped up to 100 %.

1.9. POWER OPERATION – LOAD FOLLOWING

In basic operation, only long-term reactivity effects (fuel burnup, buildup of samarium) need to be compensated for by gradually diluting the primary coolant to a boron concentration of approximately 5 to 10 ppm at the end of the fuel cycle.

If required for reasons of grid production and consumption balance, the power plant may have to reduce power and then resume full power production a few hours later (see load following and power variation in Chapter C.6). As previously discussed, steam generator control is entirely automatic. Rod cluster control assemblies are inserted or extracted by temperature control and power distribution to compensate for rapid changes in reactivity. Slow variations (Xenon changes) are compensated for by modifying the boron concentration or moving the rod cluster control assemblies.

In addition to boration and dilution needs, the primary coolant is chemically treated in order to meet chemical and primary activity criteria. The corresponding fluid volumes may be recycled, concentrates in particular (boric acid). Part of the distillate (demineralised water) may be directed towards primary waste treatment so as to avoid tritium buildup in the primary system (see source term in Chapter L).

1.10. EXTENDED CYCLE OPERATION

In power operation, available reactivity is compensated for by primary boration. As burnup increases, the boron content is reduced. The end of the cycle is reached when the boron content reaches a value close to zero.

In order to extend power operation beyond the natural end of the cycle, the fall in reactivity due to fuel depletion may be compensated for by reducing the primary temperature.

When the control rods are almost entirely extracted and the turbine inlet valves wide open, the power level is determined by the core reactivity balance and turbine characteristics.

As there is no available built-in reactivity to ensure a constant average primary coolant temperature, the average primary coolant temperature, reactor power and steam pressure decrease steadily. The primary coolant mass is maintained constant during power operation. Thus, the drop in primary temperature brings about a re-adjustment of the main parameters (pressuriser level, reference temperature, protection signals etc.).

The extended cycle operation, based on repeated setpoint adjustments, consumes the remaining built-in reactivity.

Demonstration studies of a cycle extended by a maximum of 70 JEPP [EFPD] and an early shutdown of a typical value of 30 JEPP [EFPD] will be provided in the pre-operational safety report.

1.11. SPECIFIC OPERATIONS

In the circumstance of an event not caused by incident or accident operations and when normal guidelines are not suited to the operation of this event (such as house load operations or loss of power sources), specific guidelines shall be applied by the operators to replace or back up normal guidelines so as to manage the event..

2. PREVENTIVE MAINTENANCE PRINCIPLES

2.0. SAFETY REQUIREMENTS

2.0.1. Objectives and definitions

Preventive maintenance includes inspections, tests, maintenance, repairs and replacements aimed at reducing the frequency and occurrence of equipment failure. These operations imply planned inoperability for maintenance purposes, irrespective of the occurrence of failures during unit operation or shutdown.

Preventive maintenance shall be considered in an appropriate way in the safety analyses.

2.0.2. Regulatory framework

The "Technical Guidelines for design and construction of the next generation of pressurised water nuclear reactors" adopted during the plenary sessions of the GPR and German experts, in Chapter C.2.1 (single-failure criterion and preventive maintenance), address the issue preventive maintenance. In addition, the principles of preventive maintenance must be consistent with Chapters C.2.2 (Probabilistic Safety Analyses and diversity), C.3 (Human Factors), C.4 (Radiation protection for workers and the public) and D.2.1 (Safety Analysis Rules).

2.0.3. Deterministic safety requirements

The safety function ensured by equipment taken out of operation for preventive maintenance is considered as inoperable. However, if the nature of the preventive maintenance is such that the system may be made operational within a suitable timeframe enabling the safety function to be met if so demanded, the system may be considered as being operable.

With regards to safety analyses of PCC, RRC-A or RRC-B events as well as internal hazards, system inoperability inherent to preventive maintenance and the related safety analysis hypotheses to be applied are developed respectively in Chapters P.0, S.1.0, S.2.0 and C.4.0 of the Design and Safety Report

When the unit is in operation, preventive maintenance may not be carried out on more than one train at a time.

Except where a specific case is justified, periodic tests are designed to avoid tested safety functions being made unavailable.

2.0.4. Radiation protection requirements

The conditions for carrying out preventive maintenance shall take into account radiation protection measures set out in Chapter L

2.0.5. Deterministic human factor safety requirements

Preventive maintenance activities shall take human factors into consideration as set out in Chapter Q.

2.1. DEFINITION OF PREVENTIVE MAINTENANCE

2.1.1. Objectives of preventive maintenance

By definition, maintenance involves all technical, administrative and management actions during the service life cycle of an item of equipment, aimed at maintaining it in or re-establishing it to a state in which it can carry out the function it is required to perform. Preventive maintenance involves all actions carried out on an item of equipment with a view to reducing the probability of its operational failure.

The aim behind such a process is to ensure that, throughout the installation’s service life, the objectives of safety, availability and costs are achieved, while complying with the rules for the protection of the environment, staff safety, radiation protection and other regulations in force:

- the safety level defined in the design study phase is ensured by maintaining equipment reliability to the required level,
- installation availability is optimised by:
  - carrying out part of the preventive maintenance while the unit is in operation in line with safety analysis assumptions,
  - enhancing design and construction quality to minimise unplanned unit inoperability and meet the required duration when the unit is in shutdown status.
- maintenance costs are controlled by:
  - enhancing design quality by incorporating French and German operating feedback,
  - optimising the balance between preventive and corrective maintenance,
  - optimising the balance between systematic preventive maintenance and condition monitoring,
  - anticipating, by defining a provisional schedule for alternating the different types of unit shutdown, with or without maintenance, between two ten-yearly in-service inspections,
  - studying, at the design stage, exceptional maintenance (interval in excess of 10 years or hypothetical occurrence).

Requalification tests are carried out at the end of all maintenance operations. Requalification tests after preventive maintenance work on equipment make it possible to check that the equipment has the same performance as it had prior to the preventive maintenance work. Consequently, these tests are sufficient to determine whether the equipment is operable after the maintenance operations.

The tests and criteria to be checked are specific to the work carried out. Generally speaking, these tests comprise two complementary parts:

- intrinsic requalification: these tests are always required. They are limited to the purpose behind the intervention,
- functional requalification: this covers equipment in its environment, functional sub-assembly and the system which contains the equipment. It is carried out in a normal operating configuration or one representative thereof.

For preventive maintenance activities which are carried out while the unit is in operation, consistency between requalification means and contents and the maintenance activity must be sought. With this in view, the level of preventive maintenance carried out during operation will be adapted to the requalification possibilities afforded by the installation. Similarly, the requalification content will be adapted to the maintenance operations carried out.

2.1.2. Objectives related to preventive maintenance

In order to achieve EPR competitiveness objectives and preserve safety objectives, aspects related to availability, operating costs and radiation protection need to be taken into account at the installation design phase.

Consequently, within the scope of the definition of the principles of preventive maintenance, account needs to be taken of:

- the objectives of the Probabilistic Safety Analyses (EPS [PSA]) for reducing the frequency of core meltdown (see Chapter R),
- dosimetry (less than 0.35 .mSv/year),
- optimised direct maintenance costs,
- the global aim of 91.1% availability for an 18-month cycle, for a unit service life of 60 years, incorporating the following sub-aims:
    - o unplanned inoperability of less than 2%,
    - o shutdown for reloading and partial inspection in 16 days,
    - o shutdown simply for reloading in 11 days,
    - o 10-yearly in-service inspection for complete overhaul in 40 days.

These sub-aims imply design requirements laid down in Section 2.3.1 in Sub-chapter M.2. Achieving the shutdown duration objectives is based on the following requirements:

- limiting maintenance activities during unit shutdowns, by carrying out preventive maintenance during operation (see Section 2.2.3 within Sub-chapter M.2 for implementation). Carrying out preventive maintenance on engineered safeguard systems during operation is possible because of the 4-train EPR design;
- being able to access the reactor building during operation in preparations for unit shutdown (polar crane, refuelling machine etc.) and following the end of the shutdown, as well as for certain preventive maintenance operations during the cycle;
- limiting the number of periodic tests during restart and reducing their impact on the restart critical path.

In addition, objectives concerning human factors, environmental protection, radiological cleanliness and industrial safety are also taken into consideration when maintenance tasks are defined.

2.2. CHOICE OF PREVENTIVE MAINTENANCE

2.2.1. Maintenance strategy

The EPR-adapted maintenance strategy requires safe operation to maintain public confidence, while achieving economic efficiency via optimum availability and control of maintenance costs.

Design and construction quality (manufacture and assembly) must be high enough to make it possible to limit any discrepancies between the final construction state and the safety requirements defined at the design stage. With this end in view, an approach will be implemented that is based on the "Compliancy" Project, developed throughout the French Nuclear Fleet, to correct any discrepancies thought to be critical and which, if unchecked, could lead to an additional In-service Surveillance programme having to be scheduled.

The maintenance strategy implemented for the EPR complies with that which is already in force in operational French nuclear power plants, but with the difference that it is incorporated at the design stage.

The Reliability Centred Maintenance (OMF) approach is one of the tools that make it possible to structure the technical and economic choices which constitute one of the foundations of the maintenance policy and which provides rigour, rationality, efficacy and traceability in maintenance choices. Reliability data used in OMF studies is obtained where possible from equipment manufacturers and approved by EDF, based on its own knowledge of equipment behaviour.

This maintenance strategy is not, however, entirely based on the OMF method. OMF is not applied in certain applications i.e. the following:

- families of identical equipment where maintenance by a sampling method can be justified,
- equipment subject to CPP / CSP regulations and to regulations concerning Pressurised Nuclear Containments (ESPNs),
- large primary or secondary components, or specific equipment for which the OMF method is not relevant,
- civil engineering structures.

Preventive maintenance programmes essentially concern equipment which is assessed as critical from an OMF point of view, with regards to safety, availability or maintenance. For equipment which is considered to be non-critical, preventive maintenance will be limited to minor operations such as upkeep and lubrication essential for smooth running. On such equipment, it is legitimate to wait for failure to occur before intervening. Naturally, maintenance must also take all regulatory requirements into account.

Technical and economic studies are carried out to optimise the choice between systematic preventive maintenance and condition monitoring.

In conclusion, the maintenance strategy contributes towards attaining the objective of unit availability and maintaining its safety level while at the same time controlling maintenance costs.

2.2.2. Inoperability for preventive maintenance

Because the EPR design provides four engineered safeguard trains, part of the preventive maintenance will be carried while the unit is in operation. This will make it possible to reduce the workload during shutdown and meet the objectives of shutdown duration discussed in Section 2.1.2. within Sub-chapter M.2

Preventive maintenance operations must be carried out in compliance with Technical Specifications (STE) so as to comply with safety study assumptions.

Inoperabilities due to preventive maintenance while the unit is in operation must not contribute in any significant way to the global frequency of core meltdown. Acceptability of inoperability duration arising from preventive maintenance is validated through EPS [PSA] studies.

An EPR Probabilistic Safety Analysis (EPS [PSA]), incorporating an annual 28-day inoperability period for preventive maintenance of an engineered safeguard train while the unit is in operation, has been carried out. The risk of core meltdown against this assumption meets the safety requirements. Results show that significantly longer durations would be compatible with the general probabilistic objective. Probabilistic safety analyses are set out in Chapter R.

The 28-day preventive maintenance period assumed in the EPS [PSA] may be reviewed within the scope of in-depth studies consistent with meeting the general safety objective.

EVU [CHRS] inoperability while the unit is in operation is also necessary to carry out preventive maintenance on the third PTR [FPPS/FPCS] train (reactor cavity and spent fuel pool cooling and treatment system). Preventive maintenance on it may be carried out during this period. A 14-day timeframe is supported by the EPS [PSA] studies.

<u>Unit operation</u>: preventive maintenance on a system is only allowed with the following nine provisos:

1) Equipment must be isolated while the unit is in operation.

2) Maintenance activities leading to F1- or F2-classified equipment inoperability, are taken into account in PCC-2 to -4 studies involving these systems. The design rules for PCC-2 to -4 operating conditions require the combination of inoperabilities resulting from the maintenance activities, a single failure and the loss of external power supply at the most unfavourable moment.

3) Maintenance activities during operation do not override the radioactive containment requirements stipulated in Chapter F.0

4) Inoperabilities due to preventive maintenance while the unit is in operation must not contribute in any significant way to the global frequency of core meltdown. Acceptability of inoperability durations as a result of preventive maintenance is validated via EPS [PSA] studies.

5) Provisions must be made at the design stage to reduce the risks of human errors during maintenance work. Realistic human error scenarios will be defined and covered by safety analysis.

6) The rules of combination of scheduled inoperabilities must be stipulated in the Technical Specifications. Scheduled combination scenarios will de identified and approved:

   a) via a deterministic analysis (see proviso 2), checking in particular those activities which should constitute a consistent set of exclusions between safety functions and support functions,

   b) if necessary via a probabilistic analysis to evaluate the impact on the global frequency of meltdown..

7) Equipment must be accessible and its environment conducive to preventive maintenance during operation (space, logistics etc.), including a full inspection or standard equipment exchange. The maintenance activity must not lead to a hazard risk that is liable to bring about:

- an event initiating an accident transient,

- damage to equipment in the locality of the maintenance work being carried out.

8) Provisions for re-establishing power supply when maintenance work is carried out during operation must not jeopardise electrical protection selectivity.

9) Any equipment on which maintenance has been carried out or whose operability is potentially affected by the work shall be requalified with a view to confirming its operability.

With regards to the E[1] status of the reactor, preventive maintenance is only scheduled on one electrical train at a time.

With regards to the F[2] status of the reactor, preventive maintenance is scheduled on two electrical trains simultaneously. However, given the engineered safeguard train design, and the auxiliaries supplied by these safeguard trains, it is not possible to lockout electrical trains 1 and 2 or electrical trains 3 and 4 simultaneously so that the two main PTR [FPPS/FPCS] trains remain available. The EPS [PSA] described in Chapter R incorporates these inoperability assumptions with regard to electrical trains during these shutdown phases. During the shutdown phases, the engineered safeguard systems may be inoperable for reasons of preventive maintenance provided that the number of trains required by the Technical Specifications is met in the various E states of the unit.

For F2-classified and non-classified systems, preventive maintenance is generally authorised at any time. However, restrictions may be necessary as a result of constraints related to unit availability and Technical Specifications requirements.

2.2.3. Implementing system preventive maintenance

This paragraph deals with the main characteristics of preventive maintenance for plant systems. For further information, refer to the chapters of the safety report for each plant system.

Following an initial examination of the different systems and equipment, the following main conclusions have been drawn up (non-exhaustive list):

- For fuel building systems:

  - PTR [FPPS/FPCS] (reactor cavity and spent fuel pool cooling and treatment system): preventive maintenance of the PTR system [FPPS/FPCS] is scheduled while the unit is in operation when the decay heat level of the spent fuel in the pool is low, towards the end of cycle. In practice, a higher decay heat might also be considered provided there is a lower temperature heat sink. Maintenance work may only be carried out on one train at a time (a main train or the third train).

  - DWK (fuel building ventilation): with regards to fuel building ventilation, preventive maintenance is scheduled while the unit is in operation, outside fuel handling periods, when it is required.

- For systems located outside the reactor building, when it is allowed by safety design requirements, preventive maintenance may be carried out while the unit is in operation. Maintenance is carried out on one engineered train at a time.

[1] E status: cold shutdown for reloading
[2] F status: cold shutdown core fully unloaded

- RIS [SIS] – Safety injection system and residual heat removal: the four-train RIS/MP [SIS/MH] and RIS/BP [SIS/LH] design enables preventive maintenance while the unit is in operation, mainly on pumps and heat exchangers,

- ASG [EFWS] – Auxiliary feedwater system: the ASG [EFWS] four-train design enables preventive maintenance while the unit is in operation, limited mainly to pumps.

- In the event of an accident, the GV (steam generator [SG]) of the train being maintained may be supplied by any other train, which makes it possible to meet the single failure criterion even in the case of isolation of a ruptured GV [SG]. Similarly, a passive header on the suction of each ASG [EFWS] pump makes it possible to use the capacity of all the emergency feedwater tanks.

- RRI [CCWS] – Component cooling water system: since maintenance of an RIS [SIS] train is possible while the unit is in operation, making an RRI [CCWS] train inoperable for preventive maintenance reasons is also allowed. It is carried out in parallel to that of the RIS [SIS] of the same train.

  The systems which have to be permanently cooled by the RRI [CCWS] are supplied by common sections which remain supplied by the available RRI [CCWS] train.

- SEC [ESWS] – Essential service water system: when preventive maintenance is carried out on the SEC [ESWS], the RRI [CCWS] of the same train is inoperable. Its four-train design makes it possible to carry out preventive maintenance on one train. Preventive maintenance is carried out at the same time as on the corresponding train of the RRI [CCWS] . Maintenance of the two chain screens supplying trains 1 and 4 is carried out while the unit is in operation. The SEC [ESWS] of the train in question may remain supplied if necessary by general purpose means.

- SRU – Ultimate heat sink: SRU preventive maintenance is carried out train by train, while the unit is in operation. It may render the EVU [CHRS] and, for train 1, the third PTR [FPCS] train, inoperable. A probabilistic approach will be used to justify the preventive maintenance timeframe.

- EVU [CHRS] – Containment heat removal: EVU [CHRS] preventive maintenance is possible whilst the unit is in operation and is carried out in parallel with that of the SRU (ultimate heat sink).

- LHP/Q/R/S – Emergency power supply diesels: maintenance of these diesel generator sets is carried out during power plant operation. The four-train design makes it possible for one set to be inoperable whilst meeting the deterministic safety requirements. Consistent with engineered safeguard systems, the preventive maintenance timeframe for diesel generating sets will be validated by probabilistic analyses.

- Electrical panels: maintenance and in particular regulatory inspections of the panels when live, are possible while the unit is in operation. Maintenance with isolation of a certain number of panels is also possible. The definitive list can be drawn up after in-depth studies. Control and protection panels are not isolated while the unit is in operation, nor are essential functions such as isolation of the primary system, containment isolation, steam generator isolation and steam dump. Power supply is ensured by dedicated interconnections to a neighbouring division during maintenance, for example in the case of maintenance of a main diesel generator set. The power supply to the containment isolation valves is also ensured via an interconnection.

- LJP/S – Emergency diesel generator sets: preventive maintenance of these generator sets is possible while the unit is in operation if the timeframe is validated by EPS [PSA] studies.

- DVL – Electrical building main ventilation system (un-restricted radiological zones): each of the four electrical and Instrumentation and Control trains is ventilated by a classified DVL train. In addition, an operational, non-classified DVL train, common to two electrical trains, ensures ventilation during the preventive maintenance phases on a classified train. Both are cooled by the electrical building chilled water system (DEL). Safety analysis justifies the acceptability of loss of DVL in support of two trains. Preventive maintenance on safety-classified DVL systems in un-restricted radiological zones may be carried out while the unit is in operation.

- DEL - Electrical building chilled water system: since preventive maintenance is authorised while the unit is in operation on the DVL systems, maintenance is also possible on the DEL which cools it. The design of the other cooling systems cooled by the DEL, such as the DCL, allows a DEL train to be made inoperable.

  Preventive maintenance of a DEL train will be carried out at the same time as for the DVL. It can, preferentially, be carried out when external temperatures are low so as to limit the consequences in the event of failure.

- DCL - Ventilation of the main control room: the DCL design makes it possible to carry out preventive maintenance on an air conditioning train whilst the unit is in operation. With regards to train batteries, maintenance will be carried out at the same time as the DEL in question.

- Containment isolation in specific conditions:

  Generally speaking, preventive maintenance whilst the unit is in operation is not possible on the isolation devices themselves because of their process or safeguard function.

  In certain conditions, preventive maintenance on an isolation valve may be considered while the unit is in operation if the other valve can be locked closed during the maintenance operation and if the function or part of the function to which it contributes is not required while the unit is in operation either for safety or normal operation of the unit.

To comply with safety and operating requirements, preventive maintenance of numerous systems and equipment can only be carried out during shutdown. Such is the case for:

- the primary coolant system and its connected lines, and in particular valves located below the cold and hot legs,
- secondary GV [SG] sections and connected steam isolation or steam dumping equipment,
- preventive maintenance work with isolation on the busbars and electrical panel gear, in particular Instrumentation and Control which is unable to be isolated whilst the unit is in operation,
- systems ensuring a negative pressure in the containment annulus,
- maintenance of equipment that is borderline with guidelines necessary for maintenance while the unit is in operation can only be carried out in shutdown status,
- parts of systems which cannot be requalified while the unit is in operation,
- in E status, when the reactor cavity is full, maintenance and inspection work on an electrical train is possible, if the other three trains are available,
- in F status, when the reactor is fully unloaded, a second train may be isolated for maintenance and inspection work. However, trains 1 and 2 or trains 3 and 4 must not be isolated simultaneously. Interconnection design between trains and auxiliaries supplied by these engineered safeguard trains is such that this requirement must be met in order to maintain permanent availability of the three PTR [FPCS] trains.

  These assumptions are taken into account in the probabilistic safety analyses.
- at the design stage, carrying out GV [SG] tube inspections on the primary system using nozzle dams is only permitted with the core unloaded. During these inspection operations, provision has been made to ensure dual isolation from the spent fuel pool using transfer tube isolation valves or the various gates and doors.

  Installing GV [SG] nozzle dams with the core loaded is not authorised at this stage of the design.

  However, over the lifetime of 60 years, for operational reasons, installing GV [SG] nozzle dams with the core loaded is not ruled out. An additional demonstration concerning the risk of draining the cavities would be required as a prior condition to installing nozzle dams.

This list will be gradually added to as in-depth studies are carried out, in line with the conclusions from accident studies.

2.3. TAKING PREVENTIVE MAINTENANCE INTO ACCOUNT AT THE DESIGN STAGE

2.3.1. Design requirements

Design requirements have already been taken into account at the EPR design stage so as to meet availability objectives while complying with safety objectives. In particular, these include:

- design of the nuclear island with four divisions and engineered safeguard trains giving total segregation of the four mechanical and electrical divisions, except for certain possible electrical interconnections. This facilitates preventive maintenance on electrical panels when the unit is shut down, and also enables maintenance work to be carried out on engineered safeguard trains when the unit is in operation,

- providing an equipment handling and storage area adjacent to the equipment hatch, which forms an extension of the reactor building containment during shutdown,

- provision of two PTR [FPCS] trains which ensure cooling of the spent fuel pool. A third additional train may back up this cooling system. Power supply to the three PTR [FPCS] trains is possible via dedicated electrical connections when the panels are isolated during shutdown,

- during shutdown and startup operations, two-phase conditions are maintained in the pressuriser. This is possible because the design allows a sufficient temperature difference to be developed along the pressuriser surge line,

- as a result of its high-speed acquisition rate, the internal core instrumentation (aeroball-type measurement system) does not require long periods of core stabilisation during startup before being able to carry out flux mapping,

- the GV [SG] inlet and outlet plena design facilitates installation of nozzle dams using robots and fitting of a second section with a loose parts trap,

- carrying out of maintenance at the secondary system level while the unit is in operation is made possible through by providing redundancy in the pumping station, in particular with regard to the APA [MFWPS] (motor-driven main feedwater pumps) and CEX (condenser extraction systems) ,

- by design, the EPR containment is permanently accessible. The conditions for carrying out work in the reactor building are made acceptable in terms of temperature, humidity and noise. Access and work zones are classified green from a radiological point of view. For unit shutdowns, after previously purging the containment atmosphere, provision has been made to carry out work in the reactor building in the seven days prior to and the three days following shutdown. During a normal cycle, work inside the building reactor may also be carried out as part of preventive maintenance.

2.3.2. Maintenance programme

Maintenance optimisation (FMD approach: see Section 2.1 within Sub-chapter M.2 – maintenance strategies) planned at the design phase, provides a positive contribution for all objectives: to installation safety and unit availability, by matching maintenance activities to the importance to risk of actual systems and equipment; to the environment by limiting waste after a consistent and optimised maintenance programme; and to radiation protection and human factors through equipment maintainability inbuilt at the design stage.

Where systems with the highest contribution to risk are concerned, EPR preventive maintenance programmes will de drawn up at the design analysis stage. In addition, a check will be made to see that they comply with safety, availability, dosimetry and cost objectives defined at the initial project stage. The maintenance programmes must also be in line with periodic testing programmes defined for safety functions.

The aim of the FMD approach is to optimise preventive maintenance programmes on equipment that has been declared safety critical. These maintenance programmes must meet the safety objectives defined at the design stage. With regards to these safety objectives, optimisation consists of enhancing availability whilst meeting maintenance-related constraints.

At the in-depth design study stage, adjustments can be made, mainly with regards to the choice of equipment technology (by making standard exchanges possible for sensitive equipment), on systems (by enhancing maintainability with a view to limiting the time needed for work to be carried out), instrumentation (by enabling monitoring of equipment so as to limit large-scale preventive maintenance operations), and by allowing condition monitoring to be implemented.

Developing maintenance programmes means that ensure:

1) compatibility of the duration of work carried out with scheduled maintenance timeframes:

   o within the framework of unit shutdowns: shutdown simply for loading in 11 days, partial inspection in 16 days, ten-yearly in-service inspection in 40 days,

   o within the framework of the duration of inoperability for preventive maintenance whilst the unit is in operation validated by a probabilistic approach of engineered safeguard systems (see Section 2.2.2 within Sub-chapter M.2).

2) feasibility with regards to:

   o accessibility of work zones, in particular, accessibility of the reactor building service zone during reactor operation,

   o intervention dosimetry and any required decontamination,

   o isolations: while the unit is in operation, the equipment on which maintenance work is scheduled to be carried out must be isolable from the adjacent system via suitable isolation devices that can be controlled from the control room or by local manual action (if such isolating devices are accessible while the unit is in operation),

   o isolation and draining durations,

- o requalification after work has been carried out: work carried out while the unit is in operation must be requalifiable in the unit state in question,

- o system startup (filling, venting, chemical and thermal treatment),

In particular, for each system, design phase studies are aimed at differentiating between equipment for which maintenance may be carried out while the unit is in operation and equipment for which it must be carried out during unit shutdown. Taking the above considerations into account at the design phase will make it possible to optimise maintenance programmes whilst ensuring that they are in line with the requirements for availability, safety, radiation protection linked to the installation, considerations related to human factors, environmental protection, radiological cleanness and personnel safety.