1. PASSIVE SINGLE FAILURE ANALYSIS

The aim of the accident analysis in Chapter P is to demonstrate that the safety objectives have been fully achieved, despite the most adverse single failure. The assumed single failure may be the failure of an active component in the short and long-term or failure of a passive component in the long-term (beyond 24 hours):

- accident analyses in Chapters P.2.2 (PCC-2), P.2.3 (PCC-3) and P.2.4 (PCC-4) assume an single active failure. They demonstrate that a controlled state and a safe shutdown state are reached, with all safety criteria met, despite the most adverse active single failure;

- the above accident analyses do not consider the passive single failure. The present sub-chapter demonstrates that a safe shutdown state can be maintained in the long-term despite a passive single failure.

As stated in the sub-chapter dealing with safety objectives and principles (Chapter C.1.1), a passive single failure is defined as a failure that occurs in a component that does not need to change state in order to fulfil its function. This is only applicable to mechanical components. A passive failure is postulated to occur during the long-term phase, i.e. more than 24 hours after the assumed initiating event. A passive failure may be:

- a failure of the pressure boundary of a fluid system leading to a flow rate at the breach of 200 l/min until it is isolated. If such a breach is not detected and isolated it is assumed to develop until the flow rate corresponds to that of a complete pipe rupture;

- a mechanical breakdown that interferes with the normal flow in a fluid system.

After 24 hours, a safe shutdown state has been reached for all of the PCC-2 to PCC-4 events. The decay heat is completely removed by the F1 RIS/RRI/SEC [SIS/CCWS/ESWS] cooling train. If necessary (in the case of a loss of coolant accidents (APRP) [LOCA]) the primary coolant inventory is maintained by the RIS [SIS]. The consequences of a passive single failure on the following systems are addressed in 1.1 and 1.2 within this Sub-chapter, with reference to the protection measures which enable detection and control of a leakage resulting from a passive single failure in the:

- Essential Service Water System (SEC) [ESWS].
- Component Cooling Water System (RRI) [CCWS].
- Safety Chilled Water System (DEL) [SCWS].
- Safety Injection System (RIS) [SIS].

Note: a passive single failure is not considered to apply in the containment penetration zone if Containment Isolation is initiated (see Chapter C.1.1).
In addition, tolerance of the Emergency Feedwater System ASG [EFWS] to a passive single failure is addressed in 1.3 within this Sub-chapter, even though ASG [EFWS] operation is limited only to the short-term PCC phase (less than 24 hours). This study is performed because the ASG [EFWS] is the only F1 fluid system which is fitted with fluid inter-connections between all the emergency trains, (referred to as “passive headers”), which may be opened on demand during ASG [EFWS] operation following an accident. The purpose of this additional study is to demonstrate that a cliff edge effect does not exist if a passive single failure occurs whilst the passive headers are open.

The calculations of the radiological consequences in Chapter P.3 take into account the effect of passive failures.

1.1. SINGLE FAILURE ASSUMPTION IN SEC [ESWS], RRI [CCWS], AND DEL [SCWS]

In the event of a passive single failure, only one division of the safeguard building is affected. It is assumed that the passive single failure is isolated within 30 minutes of its detection (by action from the control room). This causes a minor discharge of cold water in the affected area. The resulting flood level is dealt with as an internal hazard due to a failure in the system itself (see Chapter C.4.8 “Internal flooding”).

As the consequences of passive single failures being limited to one division, their impact on the fulfilment of the safety functions is always enveloped by the consequences of the active single failure considered in demonstration of safe shutdown in the PCC studies in Chapters P.2.2, P.2.3 and P.2.4.

1.2. PASSIVE SINGLE FAILURE ASSUMPTION FOR THE SIS

In the event of a passive single failure only one division of the safeguard buildings is affected. Two different cases must be considered, corresponding to the different RIS [SIS] uses:

Non APRP [LOCA] events

For events other than the APRP [LOCA], the RIS [SIS] is used in RRA [RHR] mode, the ISBP [LHSI] pumps taking suction from the hot legs. The passive single failure will be detected by the sump level measurement in the affected division (additional information is given in the chapters on “Internal flooding” (see Chapter C.4.8) and “Safety injection system” (see Chapter F.3)). It is assumed that the leak (passive single failure) is isolated 30 minutes after it is detected, for example, by closing the isolation valve in the ISBP [LHSI] suction line inside the containment (by action from the control room).

The failure causes a minor discharge of water inside the division, as, after 24 hours, the temperature of the primary coolant released into the safeguard building will be significantly less than 100°C.
Heat removal from the primary system is ensured by the remaining ISBP [LHSI] pump(s) which are already operating and which take suction from the hot leg(s) (in addition, it is possible to manually start-up the ISBP [LHSI] pump(s) on standby). If required, makeup of the primary system, is automatically performed by the ISMP [MHSI] pumps (in addition, it is possible to manually start up the ISBP [LHSI] pump(s) on standby), which take suction from the RIS [SIS] pool (PTR) [IRWST].

As the consequences of a passive single failure are limited to one division, its impact on the number of pumps available to fulfil the safety function is always enveloped by the consequences of the active single failure considered in demonstrating achievement of the safe shutdown state in the PCC studies in Chapters P.2.2, P.2.3 and P.2.4.

APRP [LOCA] events

In the event of an APRP [LOCA], the RIS [SIS] is used in safety injection mode, the ISBP [LHSI] pumps taking suction from the RIS [SIS] pool (PTR) [IRWST]. The passive single failure will be detected by the sump level measurement in the affected division (additional information is given in the chapters on “Internal flooding” (see Chapter C.4.8) and “Safety injection system” (see Chapter F.3)). It is assumed that the passive single failure is isolated within 30 minutes (by action from the control room) or an hour (locally performed action) of its detection. The isolation terminates the loss of RIS [SIS] pool (PTR) [IRWST] inventory. The failure causes a minor discharge of water in the relevant safeguard building, as, after 24 hours, the temperature of the primary fluid that is discharged into the safeguard building is lower than 100°C. The resulting increase in ambient temperature and the loss of RIS [SIS] pool (PTR) [IRWST] water inventory is acceptable. The effect on the net positive suction head (NPSH) of the other RIS [SIS] pumps is acceptable, and the RIS [SIS] pool shut-off valve in the affected division may be isolated if it is open.

Safety injection and removal of decay heat are thus performed by the remaining ISMP [MHSI] and ISBP [LHSI] train(s).

As the consequences of a passive single failure are limited to one division, its impact on the number of pumps available to fulfil the safety functions is enveloped by the consequences of the active single failure considered in the demonstration of achievement of the safe shutdown state in the PCC APRP [LOCA] analyses (see Chapters P.2.3e and P.2.4f).

**1.3. STUDY OF PASSIVE SINGLE FAILURE IN THE EFWS**

This section considers the tolerance of the ASG [EFWS] design to a passive single failure in the short-term phase of an accident, in order to demonstrate the absence of cliff edge effects.

The ASG [EFWS] consists in 4 independent trains that are inter-connected by 2 “passive headers” (see P.2.1 FIG 1):
the passive header located upstream the ASG [EFWS] allows all water in the 4 ASG [EFWS] tanks to be available to a single ASG [EFWS] pump;

the passive header located downstream of the ASG [EFWS] pumps allows all available GV [SGs] to be supplied from any available ASG [EFWS] pump, in case one or more of the other ASG [EFWS] pumps are unavailable and/or one or more of the other GV [SGs] are unavailable.

These headers are isolated during normal plant operation, i.e. all of the valves are closed, with the exception of the header valve upstream of the ASG [EFWS] pumps located in a division undergoing preventive maintenance, which is intentionally opened to make the tank available to other ASG [EFWS] trains, which may be connected on demand. This connection is performed manually at a local level (in PCC studies connection is assumed to take place 1 hour after the Automatic Reactor trip).

The most severe PCC event for the design and specification of the ASG [EFWS] is a Feedwater Line Break (RTE) [FLB], since:

- when the Automatic Reactor trip occurs, the water inventory in the steam generator (GV) [SG] secondary system is at a minimum value compared to that in other PCC accidents. This maximises the demand on the ASG [EFWS] following the accident. In addition, the ASG [EFWS] flow rate injected into the affected GV [SG] before it is isolated, is considered to be lost without contributing to the removal of primary system heat.

- the affected GV [SG] is isolated after the accident, which only leaves 3 GV [SGs] available to cool the primary system to RRA [RHR] connection conditions (and possibly only 2 GV [SGs] if the active single failure affects one Main Steam Relief Train (MSRT) or one ASG [EFWS] valve in any of the 3 available GV [SGs]).

- the passive header located upstream of the pumps must be open during preventive maintenance of an ASG [EFWS] train in order to enable water in the ASG [EFWS] tank to which it is connected to be used. In practice, 4 ASG [EFWS] tanks are necessary (see “RTE [FLB] design with active single failure” below).

- the passive header located downstream of the pumps must be open during preventive maintenance of an ASG [EFWS] train with an active single failure which obstructs the ASG [EFWS] supply to an available SG (EFWS pump or valve failure). In fact, at least 2 GV [SGs] must be supplied.

The following discussion is based on the bounding RTE [FLB] transients considered in the ASG [EFWS] design, which involve an active single failure (see Chapter P.2.4c) and a passive single failure.

EFWS tank is the only equipment item whose design is affected by the passive single failure assumption. Design of the ASG [EFWS] pumps is not sensitive to the assumed passive single failure and its adequacy in terms of the safety objectives is confirmed by PCC studies of the RTE [FLB] accident (see Chapter P.2.4c).
With regard to leak detection, additional information can be found in the chapter on internal flooding (see Chapter C.4.8).

**1.3.1. FLB DESIGN CASE INVOLVING SINGLE ACTIVE FAILURE**

Feedwater Line Break with an active single failure is considered in Chapter P.2.4c.

The chosen active single failure is a failure that impairs the ability of the F1 systems to cool the primary circuit to RRA [RHR] connection conditions. The active single failure may be applied to one of the two RBS [EBS] trains, the VDA (sequences without MDTE [LOOP]) or to a main diesel generator (sequences with MDTE [LOOP]), to minimise the cooldown rate and maximise ASG [EFWS] feed water consumption.

**1.3.2. RTE [FLB] DESIGN CASE INVOLVING PASSIVE SINGLE FAILURE**

For this case the active single failure in the RTE [FLB] design case is replaced by a passive single failure.

As there is no active single failure, 3 VDA and 2 RBS [EBS] trains are available for the transfer to RIS/RRA [SIS/RHRS] cooling. The availability of an additional RBS [EBS] train means that the primary system inventory is increased relative to the “RTE [FLB] with Active Single Failure” case. As the period of GV [SG] cooling is reduced by slightly more than 3 hours, less ASG [EFWS] water is required in the tanks.

As is the case in the RTE [FLB] study in Chapter P.2.4c, 100te of ASG [EFWS] water is considered to be lost to the breach without contributing to the removal of primary system heat (in the period before manual isolation of the ASG [EFWS] line in the affected GV [SG]).

The conclusion of the RTE [FLB] design study assuming Passive Single Failure is that:

1,100te of water is required in the ASG [EFWS] tanks.

In order to determine the amount of ASG [EFWS] water that is available, different possible passive single failures are considered and analysed. Figure P.2.1 FIG 1 provides an explanatory illustration.
1.3.3. Discussion of different passive single failures (PSF)

1.3.3.1. Passive single failures causing a leak

1.3.3.1.1. Passive Single Failure before headers are opened

Given that 3 ASG [EFWS] tanks are sufficient to reach the safe shutdown state (2x400 + 1x440 = 1,240 tonnes > 1,100 tonnes necessary), a Passive Single Failure anywhere on an ASG [EFWS] train is equivalent, in terms of safety consequences, to an Active Single Failure. The reasons are as follows:

- a break in one train does not affect the other trains (as the passive headers are closed),
- in terms of the flow injected into the GV [SG], the consequences of a Passive Single Failure are enveloped by those of an Active Single Failure (at least 2 ASG [EFWS] pumps remain available),
- in terms of the water inventory, the loss of a single tank is acceptable even when the leak is not isolated (3 ASG [EFWS] tanks remain fully available).

With regard to an Active Single Failure, the headers between the available ASG [EFWS] trains (those which are not affected by the preventive maintenance and an Active Single Failure) must be opened in order to supply at least 2 GV [SGs] by using the 3 remaining ASG [EFWS] tanks.

The division affected by the Passive Single Failure is detected via a rising sump level. The case where the passive headers are opened before the occurrence of a sump level detection alarm (level < threshold) is presented below.

1.3.3.1.2. Passive Single Failure when headers are opened

- Actions performed by the operator on headers

In order to maintain the maximum segregation between the divisions, the headers are opened only to the minimum extent necessary (for example, between 2 trains only) and at the latest possible time.

However, as the header opening procedure is yet to be precisely defined, the consequences of a Passive Single Failure are studied using the following conservative assumptions:

- the passive header located upstream of the pumps is assumed to be opened before the ASG [EFWS] tanks allocated to the available ASG [EFWS] pumps are drained. It is assumed that the 4 valves in the 4 tanks are opened at the same time.
- the passive header located downstream of the pumps is assumed to be opened in order to supply at least 2 GV [SGs]. In most cases, the operation consists of realigning the available ASG [EFWS] pumps that are allocated to the affected GV [SG] towards the GV [SG] that is not supplied, depending on the division undergoing preventive maintenance.
If there is a leak in one division, which is detected by a sump level measurement, the operator must:

- isolate the 2 passive headers to stop water loss from more than one tank,
- locate and isolate the leak,
- realign the passive headers to maximise the availability of water inventory and pumps.

Possible locations for Passive Single Failure

It is assumed that the Passive Single Failure may occur anywhere on an ASG [EFWS] train or a passive header:

- leak in an ASG [EFWS] train, close to the tank, upstream of the passive header located upstream of the pumps, (location A in figure P.2.1 FIG 1 - Passive Single Failure):
  - After the 2 downstream valves are closed (on the header upstream of the pumps and on the ASG [EFWS] train), ASG [EFWS] no. 3 pump is no longer available and the ASG [EFWS] no. 3 tank inventory is lost. The components that remain available are the 3 ASG [EFWS] tanks and the 2 ASG [EFWS] pumps that supply 3 GV [SGs] via the header downstream the pumps.

- Leak in the passive header located upstream the pumps (location B in figure P.2.1 FIG 1 - Passive Single Failure):
  - After the leak has been isolated, by isolating the header upstream of the pumps (all header valves closed), the ASG [EFWS] tank allocated to the division in preventive maintenance is no longer available. The components that remain available are 4 ASG [EFWS] tanks and the 2 ASG [EFWS] pumps supplying 3 GV [SGs] via the header downstream the pumps.

- leak in an ASG [EFWS] train, between the connections to the passive headers (location C in figure P.2.1 FIG 1 - Passive Single Failure):
  - After the leak has been isolated, by closing the upstream and downstream valves in the ASG [EFWS] train, ASG [EFWS] no. 3 pump is no longer available. The components that remain available are 4 ASG [EFWS] tanks and the 2 ASG [EFWS] pumps supplying 3 GV [SGs] via the header downstream of the pumps.

- leak in the passive header downstream of the pumps (location B in figure P.2.1 FIG 1 -Passive Single Failure):
after the leak has been isolated, by isolating the header downstream of
the pumps (all header valves closed), the ASG [EFWS] pump allocated to
the affected GV [SG] is no longer available and it is no longer possible to
supply the GV [SG] in the division in preventive maintenance. The
components that remain available are 4 ASG [EFWS] tanks feeding the
header upstream of the pumps and the 2 ASG [EFWS] pumps supplying
2 GV [SGs].

- leak in an ASG [EFWS] train downstream of the passive header located
downstream of the pumps (location E in figure P.2.1 FIG 1 -Passive Single
Failure):

  after the leak has been isolated, by closing the 2 valves located upstream
(on the header downstream of the pumps and on the ASG [EFWS] train
respectively), ASG [EFWS] no. 3 pump is no longer available and supply
to GV no. 3 is no longer possible. The components that remain available
are 4 ASG [EFWS] tanks feeding the header upstream the pumps and 2
ASG [EFWS] pumps, which supply 2 GV [SGs].

- Consequences of the leak

Whatever the leak location in the ASG [EFWS], at least 2 ASG [EFWS] pumps
and 2 GV [SGs] remain available to remove the RCS heat, taking into account the
unavailability of the equipment after the leak has been isolated (same minimum
availability as after an Active Single Failure). This is sufficient to ensure the
necessary heat removal function in terms of the water injection rate and the steam
release rate.

The leaks may be separated into 2 distinct categories, depending on their location
in the ASG [EFWS] and their effect on the quantity of ASG [EFWS] water
available:

- leaks located upstream of the header upstream of the pumps, or on the header
  upstream the pumps (locations A, B in figure P.2.1 FIG 1 -Passive Single
  Failure):

  in this case, after the leak has been isolated, 3 ASG [EFWS] tanks remain
available (giving an available water inventory of 2x400+440=1,240te),

  however, only 1,100te of ASG [EFWS] water are required to reach
RIS/RRA [SIS/RHRS] connection conditions, based on the highly
conservative RTE [FLB] design case analysis,

  thus, the volume of available ASG [EFWS] is sufficient to achieve
RIS/RRA [SIS/RHRS] connection conditions.

- Leaks located downstream the of header which is upstream of the pumps,
  including leaks on the header downstream of the pumps (locations C, D, E in
figure P.2.1 FIG 1 -Passive Single Failure):
after the leak has been isolated, 4 ASG [EFWS] tanks remain available (giving an available water inventory of 1,680 tonnes),

- only 1,100 tonnes of ASG [EFWS] water are required to reach RIS/RRA [SIS/RHRS] connection conditions based on the highly conservative RTE [FLB] design case,

- thus, the volume of available ASG [EFWS] is sufficient to achieve RIS/RRA [SIS/RHRS] connection conditions.

1.3.3.2. Passive single failures causing a flow restriction or a blockage

Passive single failures that obstruct the normal flow in the fluid system, for example, a flow restriction or blockage, are less penalizing than passive single failures which cause a leak as less ASG [EFWS] feed water is lost for heat removal. This case is therefore enveloped by the case of loss of an ASG [EFWS] storage tank.

1.3.3.3. Quantity of ASG [EFWS] water available in the case of a Passive Single Failure

As described in the previous paragraphs and as shown in figure P.2.1 FIG 1, it is possible for an ASG [EFWS] tank to be unavailable for primary system cooling after the postulated Passive Single Failure has been isolated.

Therefore, following isolation of the Passive Single Failure:

- 3 ASG [EFWS] tanks are available,
- at least 2 ASG [EFWS] pumps are available,
- at least 2 GV [SGs] are available.

Consequently, for the most penalizing Passive Single Failure case, the quantity of ASG [EFWS] water available is as follows:

1,240 tonnes of water is available in the ASG [EFWS] tanks, with 400 tonnes in each of the tanks in divisions 2 and 3 and 440 tonnes in the tank in divisions 1 or 4. In order to minimise the quantity of ASG [EFWS] water available, the Passive Single Failure is applied so that the largest tank is lost.

Consequently, the quantity of ASG [EFWS] water available (1,240te) in the worst case scenario is greater than the required quantity of ASG [EFWS] water (1,100te).
1.3.4. CONCLUSION

A passive single failure is assumed on the ASG [EFWS] system in the long-term phase of a PCC accident (after 24 hours), even though the ASG [EFWS] is only used in the short-term accident phase passive single failures do not have to be considered for this F1 system. Due to the existence of the “passive headers” which enable fluid inter-connections between the 4 ASG [EFWS] trains and applying the technical specifications, the tolerance of the ASG [EFWS] to passive single failure can be demonstrated.

When we assume that there is a passive single failure on an ASG [EFWS] train or on one of the 2 ASG [EFWS] headers, at least 3 ASG [EFWS] tanks and 2 ASG [EFWS] pumps supplying 2 GV [SGs] remain available to remove heat from the primary system. This is sufficient to return the plant to the safe shutdown state, from which point heat removal is performed by the RIS/RRI/SEC [SIS/CCWS/ESWS] cooling system. The assessment allows for the detection, location and leak isolation time.

It is thus concluded that an assumed passive single failure in the ASG [EFWS] in the short-term phase of a PCC accident does not lead to a fault escalation (cliff edge effect).
**FIG 1: ASG [EFWS]: COMPARISON BETWEEN AN ACTIVE AND A PASSIVE SINGLE FAILURE**

### ACTIVE SINGLE FAILURE

- **Number of available tanks:**
  - Active: 4 4 4 4 4 4
  - Passive: 3 3 4 4

- **Number of available pumps:**
  - Active: 3 2 2 2 3 3
  - Passive: 2 3 2 2

- **Number of available GV [SG]:**
  - Active: 3 3 3 3 2 2
  - Passive: 3 3 3 2 2

### PASSIVE SINGLE FAILURE

- **After leak isolation**
  - (Passive single failure),
  - Number of available tanks: 3 3 4 4 4 3
  - Number of available pumps: 2 3 2 2 2 2
  - Number of available GV [SG]: 3 3 3 2 2

---

**UK-EPR**

**FUNDAMENTAL SAFETY OVERVIEW**

**VOLUME 2: DESIGN AND SAFETY**

**CHAPTER P: REFERENCE OPERATING CONDITION STUDIES (PCC)**

**SUB-CHAPTER : P.2**

**SECTION : P.2.1**

**FIGURE : 1**

**PAGE : 11 / 11**