UK EPR	Title: PCSR – Sub-chapter 14.2 – Analysis of the Passive Single Failure
	UKEPR-0002-142 Issue 04

Total number of pages: 53	Page No.: I / IV
Chapter Pilot: F. CERRU *Name/Initials* *Date 12-11-2012*	
Approved for EDF by: A. MARECHAL *Name/Initials* *Date 23-11-2012*	Approved for AREVA by: G. CRAIG *Name/Initials* *Date 23-11-2012*

REVISION HISTORY

Issue	Description	Date
00	First issue for INSA information.	11-12-2007
01	Integration of technical and co-applicant review comments	27-04-2008
02	PCSR June 2009 Update: - Clarification of text	27-06-2009
03	Consolidated Step 4 PCSR update: - Minor editorial changes - Correction of units (introductory text and section 3.7.3.1 2) - Addition of more detailed analysis to demonstrate that the UK EPR design is robust with respect to passive single failures (whole document)	28-03-2011
04	Consolidated PCSR update: - References listed under each numbered section or sub-section heading numbered [Ref-1], [Ref-2], [Ref-3], etc - Minor editorial changes - Update of references	23-11-2012

For information address:

AREVA NP SAS
Tour AREVA
92084 Paris La Défense Cedex
France

EDF
Division Ingénierie Nucléaire
Centre National d'Equipement Nucléaire
165-173, avenue Pierre Brossolette
BP900
92542 Montrouge
France

TABLE OF CONTENTS

1. INTRODUCTION

2. OVERALL METHODOLOGY PRESENTATION

2.1. DEFINITION OF THE PASSIVE SINGLE FAILURE CONCEPT APPLIED

2.2. MAIN FEATURES OF THE METHODOLOGY

2.3. LIST OF SYSTEMS TO ANALYSE

3. FRONTLINE SYSTEMS ANALYSIS

3.1. SAFETY INJECTION SYSTEM / RESIDUAL HEAT REMOVAL SYSTEM (RIS/RRA [SIS/RHRS])

3.2. MAIN STEAM RELIEF TRAIN (VDA [MSRT])

3.3. EXTRA BORATING SYSTEM (RBS [EBS])

3.4. REACTOR COOLANT SYSTEM (RCP [RCS])

3.5. MAIN STEAM SUPPLY SYSTEM (VVP [MSSS])

3.6. STEAM GENERATOR BLOWDOWN SYSTEM (APG [SGBS])

3.7. EMERGENCY FEED WATER SYSTEM (ASG [EFWS])

3.8. FUEL POOL COOLING SYSTEM (PTR [FPCS])

3.9. CLASSIFIED FIRE-FIGHTING WATER PRODUCTION / NUCLEAR ISLAND FIRE-FIGHTING WATER PROTECTION AND DISTRIBUTION (JAC/JPI [NIFPS])

3.10. FRONTLINE SYSTEMS SUMMARY

4. SUPPORT SYSTEMS

4.1. COMPONENT COOLING WATER SYSTEM (RRI [CCWS])

4.2. ESSENTIAL SERVICE WATER SYSTEM (SEC [ESWS])

4.3. ELECTRICAL BUILDING EMERGENCY CHILLED WATER SYSTEM (DEL [SCWS])

4.4. HEATING, VENTILATION AND AIR-CONDITIONING (HVAC)

4.5. SUPPORT SYSTEMS SUMMARY

5. CONCLUSION

SUB-CHAPTER 14.2 – ANALYSIS OF THE PASSIVE SINGLE FAILURE

1. INTRODUCTION

The UK EPR is designed in compliance with the single failure criterion as defined in PCSR Sub-chapter 14.0. This criterion includes either an active single failure in the first 24 hours after the occurrence of a Postulated Initiating Event (PIE) or a passive single failure at the PIE occurrence. This criterion is part of the assumptions made for the fault studies of PCSR Sub-chapters 14.3 to 14.5.

From a UK perspective, there is a need to review each design basis initiating event, meaning each PCC-2 to PCC-4 event, and to demonstrate that there are no passive single failures which could prevent the successful operation of the safety function that is provided to protect against the fault. Should any vulnerabilities to single failures be identified there will be a need for an ALARP assessment to be performed to see if the design should be changed to eliminate the single failure vulnerability.

Moreover, the failure to close of a VIV [MSIV] during SGTR or the failure to close of a safety relief valve are taken into account within the active single failures.

The aim of this sub-chapter is to present the analysis of the consequences of passive single failures at the time of the PIE for PCC-2 to PCC-4 events.

2. OVERALL METHODOLOGY PRESENTATION

The purpose of this section is to give the main features of the methodology adopted to analyse the passive single failure, including the main assumptions and the extent of the demonstration.

2.1. DEFINITION OF THE PASSIVE SINGLE FAILURE CONCEPT APPLIED

The passive single failure (PSF) analysis is a tool for the designer of the plant to demonstrate sufficient independence between the trains of a safety system. Such an analysis can highlight potential common cause failures that could prevent the safety systems from performing the safety functions they contribute to. In particular, it may point out some weaknesses in the design of headers or common pipe work between trains of a safety system.

As stated in section 1 of PCSR Sub-chapter 3.1, a PSF is defined as a failure that occurs in a component which does not need to change state to carry out its function. For the analysis of the PSF within the first 24 hours after the occurrence of a PIE, this is only applicable to mechanical components containing a fluid and to components that may lead to the loss of more than one train of a safety system.

The passive failure may be:

- A failure of the pressure boundary of a fluid system is assumed to develop until the flow corresponds to that of a full pipe rupture;
- Another mechanical failure impairing the normal process flow path of a fluid system.

The passive single failure is not applicable to M1 pressurised components for which a failure is excluded if:

- The components is part of the Reactor Coolant Pressure Boundary (CPP [RCPB]),
- The component is a non-breakable component (see Sub-chapter 3.4),
- The component is a high energy break preclusion pipe (i.e. the main steam system up to the first isolation device outside the containment).

2.2. MAIN FEATURES OF THE METHODOLOGY

Each safety system is designed to deliver the Plant Level Safety Functions (PLSF) [Ref-1], despite the most onerous single failures (SF) and preventive maintenance (PM). In most of the cases the combination of a SF and PM leads to the loss no more than two trains of a safety system. The general principle of the methodology is to assess the safety systems and verify that a passive single failure could not lead to the loss of more trains than is the number currently considered. This would lead to shortfalls in the current fault analysis that would have to be studied. From a practical point of view, the link between PLSF and safety systems is made in the fault schedule.

Subsequently, the study focuses on the safety system itself and attempts to identify potential headers, common pipe work or components that could lead to the loss of more than one train of the studied safety system.

Passive single failures not covered by active single failures are identified using the fluid system diagrams. Analysis of the impact of these failures is carried out and, for each system, conclusions are drawn from the system impact analysis regarding the delivery of the safety functions.

Three cases result from such an analysis:

Case 1: Short term passive single failures have no impact on the safety functions. The current fault analysis remains adequately conservative.

Case 2: A passive failure is identified which significantly affects the system performance. A study is performed to demonstrate that the safety function is achieved.

Case 3: A passive failure is identified which significantly affects the system performance and the safety function cannot be achieved. An ALARP assessment has to be performed.

2.3. LIST OF SYSTEMS TO ANALYSE

The following systems have been assessed in order to quantify whether the EPR design has shortfalls in its robustness to deal with passive single failures.

The list of the systems to be analysed is based on PCSR Sub-chapter 3.2. Based on this list, three categories of systems can be defined:

- Frontline systems
- Support systems
- Containment systems

2.3.1. Frontline systems

These systems are directly involved in the safety functions and are not limited to containment isolation.

- RIS/RRA [SIS/RHRS]
- VDA [MSRT]
- RBS [EBS]
- RCP [RCS]
- VVP [MSSS]
- APG [SGBS]
- ASG [EFWS]
- PTR [FPCS]
- JAC/JPI [NIFPS]

An analysis of each system is performed in section 3.

2.3.2. Support systems

These systems support frontline systems.

- HVAC
- DEL [SCWS]
- SEC [ESWS]
- RRI [CCWS]

An analysis of each system is performed in section 4.

2.3.3. Containment systems

These systems are limited to containment functions, they perform no other safety function required to reach the safe state.

- EBA [CSVS]
- REN [NSS]
- SAT
- EDE [AVS]
- RES
- SED
- RCV [CVCS]
- RPE [NVDS]
- SGN
- SIR
- SNL
- TEG [GWPS]
- DER

As active single failures imply a redundancy of the closing devices, no further analysis is required on these systems. The passive single failure does not impact the containment function.

3. FRONTLINE SYSTEMS ANALYSIS

3.1. SAFETY INJECTION SYSTEM / RESIDUAL HEAT REMOVAL SYSTEM (RIS/RRA [SIS/RHRS])

The RIS/RRA [SIS/RHRS] is involved in the performance of three fundamental safety functions [Ref-1]:

- Control of reactivity
- Residual heat removal
- Radioactive material containment

On each line connected to the RCP [RCS], radioactive material containment is performed by two isolation valves in series. This redundancy ensures that neither an active failure on a valve nor a passive failure on a line can impact the containment function.

As discussed in the System Design Manual [Ref-1], the failure of the RIS/RRA [SIS/RHRS] accumulator check valves to open is not considered within the active single failure criterion. Accumulator check valves were considered to be passive equipment as their opening or closure is only controlled by the pressure difference on the equipment.

Therefore, the loss of one MHSI and one LHSI on the same train is the most severe active single failure taken into account in the safety analyses.

For the RIS/RRA [SIS/RHRS], accumulator check valve failure to open leads to the loss of one complete RIS/RRA [SIS/RHRS] train, including accumulator injection, which is more onerous. A specific safety analysis has to be performed to quantify the impact of RIS i560VP failure to open on LOCA events.

As the four trains have no common line, this loss is the most severe failure that can be encountered, with any leak on the system leading in the worst case to the loss of one train (see Sub-chapter 14.2 – Table 1 and Sub-chapter 14.2 – Figure 1).

3.2. MAIN STEAM RELIEF TRAIN (VDA [MSRT])

The VDA [MSRT] system is involved in the performance of two fundamental safety functions [Ref-1]:

- Residual heat removal
- Radioactive material containment

The VDA [MSRT] system is made up of four completely separated trains, each one of them assigned to a steam generator. The isolation valve is directly connected to the main steam line, which complies with the break preclusion concept [Ref-2]. Therefore, no line break can occur upstream of the isolation valve.

The failure to open or to close of either the isolation valve or the regulating valve has been analysed within the active single failure criterion.

The most severe active single failure leads to the loss of one train, the isolation being still guaranteed by the two valves in series.

A leak on a VDA [MSRT] line does not impact the radioactive material containment as the isolating valve is still available to perform this function.

A leak on a VDA [MSRT] line does not prevent the system from fulfilling its residual heat removal function.

Therefore, passive single failures are bounded by active ones. No specific study is required for this system, see Sub-chapter 14.2 – Figure 2 and Sub-chapter 14.2 – Table 2.

3.3. EXTRA BORATING SYSTEM (RBS [EBS])

The extra borating system is involved in the performance of two fundamental safety functions [Ref-1]:

- Control of reactivity
- Radioactive material containment

On each line connected to the RCP [RCS], radioactive material containment is performed by two isolation valves in series. This redundancy ensures that neither an active failure on a valve nor a passive failure on a line can impact the containment function.

The RBS [EBS] is made up of two trains. An active single failure, such as the loss of a pump, leads to the loss of one train. In this case, one RBS [EBS] train remains available to achieve the safe state. Maintenance is not allowed on the RBS [EBS] during plant operation.

The junction between the two trains is not utilised in the safety analysis. It is closed during operation and can be opened manually if required.

In the worst case, a passive single failure leads to the loss of one train. Therefore, no specific study is required on this system; see Sub-chapter 14.2 – Figure 3 and Sub-chapter 14.2 – Table 3.

3.4. REACTOR COOLANT SYSTEM (RCP [RCS])

The RCP [RCS] is involved in the performance of three fundamental safety functions [Ref-1]:

- Control of reactivity
- Residual heat removal

- Radioactive material containment

There is no redundancy on the primary circuit; it complies with the break preclusion concept. Therefore, no passive failures are considered on the lines of this system. However, equipment on the RCP [RCS] must be studied within the single failure criterion analysis.

A failure to open or a failure to close of the normal spray valves has no impact on the safety studies.

As the severe accident valves are redundant, a failure to open or a failure to close of one of these valves has no impact on the safety studies.

Failure to open of a safety relief valve is already taken into account within the active single failure criterion, but failure to close must be analysed in an ALARP study.

The other equipment has been considered within the active single failure criterion. The passive single failure has no impact on the analyses, see Sub-chapter 14.2 – Figure 4 and Sub-chapter 14.2 – Table 4.

3.5. MAIN STEAM SUPPLY SYSTEM (VVP [MSSS])

The VVP [MSSS] is involved in the performance of three fundamental safety functions [Ref-1]:

- Control of reactivity
- Residual heat removal
- Radioactive material containment

The main steam line complies with the high energy break preclusion concept. The pressure relief valves are directly connected to the main steam line, so no line break can occur upstream of the valves.

The failure of the VIV [MSIV] to close during a SGTR is not considered in the safety studies. An ALARP analysis is to be done on this topic.

The failure to close of a main steam line following other types of accident, such as main steam line break, has been considered. Therefore, no additional analysis is required for these accidents.

Within the passive single failure criterion, a break on the reheat line has to be analysed. Although the diameter of this line is small compared to the main line, a specific study will be done to confirm the impact, see Sub-chapter 14.2 – Figure 5 and Sub-chapter 14.2 – Table 5.

3.6. STEAM GENERATOR BLOWDOWN SYSTEM (APG [SGBS])

The APG [SGBS] is involved in the performance of one fundamental safety function [Ref-1]:

- Radioactive material containment

Containment is guaranteed by isolation valve redundancy, a passive failure does not impact this function.

The transfer line between two steam generators may be required in the case of the long term mitigation of a SGTR, in order to decrease the affected SG (SGa) water inventory for SGa depressurisation and prevention of SGa overfilling.

A break on this transfer line would prevent the APG [SGBS] from decreasing the SGa water inventory. The impact of this passive single failure has to be analysed in a specific study, see Sub-chapter 14.2 – Figure 6.

Other parts of the system have no safety function; they are isolated by two isolating valves in series. So, apart from the transfer line, active or passive failures have no impact on the performance of safety function (see Sub-chapter 14.2 – Table 6 and Sub-chapter 14.2 – Figure 6).

3.7. EMERGENCY FEED WATER SYSTEM (ASG [EFWS])

The ASG [EFWS] is involved in the performance of three fundamental safety functions [Ref-1]:

- Control of reactivity
- Residual heat removal
- Radioactive material containment

The ASG [EFWS] consists of four independent trains, interconnected by two "passive headers" as shown in Sub-chapter 14.2 - Figure 8***:***

- The tank passive header, located upstream of the ASG [EFWS] pumps, allows the use of the whole water inventory of the four ASG [EFWS] tanks in the case of ASG [EFWS] pump(s) unavailability.
- The pump passive header, located downstream of the ASG [EFWS] pumps, allows feed to be provided to any available SG from any available ASG [EFWS] pump, in case of ASG [EFWS] pump(s) unavailability or/and SGs unavailability.

These headers are isolated from the four ASG [EFWS] trains during plant normal operation, i.e. all relevant valves are closed. The exception is the valve of the tank-header located in a division under preventive maintenance, which is intentionally opened to make the tank available to any other ASG [EFWS] train. The header may be connected on demand. This connection is done manually and locally and is assumed to occur one hour after reactor trip (RT) in the PCC analyses.

The most limiting PCC event for ASG [EFWS] design and sizing is the Feedwater System Line Break (FWLB)*:*

- The water inventory present on the SG secondary side at the time of the reactor trip, is at a minimum when compared to other PCC accidents, as described in Appendix 14B. This maximises the demand on the ASG [EFWS] following the accident. In addition, the ASG [EFWS] flow delivered into the affected SG prior to its isolation can be lost without contributing to the RCP [RCS] heat removal.

- The affected SG is isolated after the accident, leaving only three SG available to cool the RCP [RCS] down to RIS/RRA [SIS/RHRS] connection conditions. Only two SG could be available if the active single failure affects one VDA [MSRT] or one ASG [EFWS] valve in any of these three SG.

- The ASG [EFWS] tank passive header must be opened during preventive maintenance of one ASG [EFWS] train to allow use of the water content of its ASG [EFWS] tank. In practice, the inventory of all four ASG [EFWS] tanks is required as discussed in "FWLB design case with active single failure”, section 3.7.1 of this sub-chapter.

- The ASG [EFWS] pump passive header must be open during preventive maintenance of one ASG [EFWS] train. This covers the situation of an active single failure otherwise preventing the ASG [EFWS] feed to one available SG due to failure of ASG [EFWS] pump or ASG [EFWS] valve. In practice, feed to at least two SG is required as discussed in "FWLB design case with active single failure", section 3.7.1 of this sub-chapter.

The following sub-sections present the "FWLB design case", i.e. the conservative FWLB transient assessed for sizing the ASG [EFWS], considering successively the active single failure and the passive single failure. The consequence of the passive single failure is then discussed.

The ASG [EFWS] tank is the only item of equipment whose design considers the passive single failure assumption. The design of the ASG [EFWS] pump is not sensitive to the assumed passive single failure, and its adequacy in meeting the safety objectives is demonstrated in the PCC accident analysis for the FWLB described in section 3 of Sub-chapter 14.5.

Additional information regarding leak detection is provided in the section related to "Flooding" in Sub-chapter 13.2.

3.7.1. FWLB design case with active single failure (ASF)

The Feedwater Line Break event with an active single failure (ASF) is considered in section 3 of Sub-chapter 14.5.

The chosen active single failure is a failure that impairs the ability of the F1 systems to cool the primary circuit to RIS/RRA [SIS/RHRS] connection conditions. The active single failure may be applied to one of the two RBS [EBS] trains, the VDA [MSRT], for sequences without LOOP, or to an emergency diesel generator for sequences with LOOP. The assumption made minimises the cooldown rate and maximises the ASG [EFWS] feed water consumption.

3.7.2. FWLB design case with passive single failure (PSF)

For this case, the active single failure (ASF) in the above "FWLB design case" is replaced by a passive single failure (PSF).

As a consequence, three VDA [MSRT] and two RBS [EBS] trains are available for the transfer to RIS/RRA [SIS/RHRS]. This enables the RCP [RCS] cooling to be performed at a rate of -50°C/h compared to a rate of -25°C/h for the ASF case.

The "FWLB design case with PSF" is shown in Sub-chapter 14.2 - Figure 7. The only difference from the previous definition given for the design case with ASF comes from the higher cooling rate. The SG cooldown ceases at RT + 5.2 hours instead of RT + 8.4 hours, as shown in the figure. As the SG are required for a shorter duration, the ASG [EFWS] tanks inventory requirement is correspondingly lower.

As is the case in the FWLB study in section 3 of Sub-chapter 14.5, 100 te of ASG [EFWS] water is assumed to be lost to the breach without contributing to the primary system heat removal in the period before manual isolation of the ASG [EFWS] line to the affected SG.

The conclusion of the FWLB design study assuming a Passive Single Failure is that 1,100 te of water are required in the ASG [EFWS] tanks. This value is obtained via an energy balance between the need for heat removal from the RCP [RCS], following the information shown in Sub-chapter 14.2 – Figure 7, and the capacity of the secondary side to remove heat in the case of a FWLB.

The total ASG [EFWS] tank water inventory is 1680 te, comprising 400 te in each tank of divisions 2 and 3, and 440 te in each tank of divisions 1 or 4, according to plant characteristics given in Sub-chapter 14.1.

In order to determine the quantity of ASG [EFWS] water that is available, different possible passive single failures are considered and analysed. Sub-chapter 14.2 - Figure 8 illustrates these.

3.7.3. Discussion of different passive single failures (PSF)

The different PSF are listed, and their consequences are discussed, below. The supporting illustration is provided by Sub-chapter 14.2 - Figure 8.

3.7.3.1. Passive single failures leading to a leak

3.7.3.1.1. Consideration of a PSF occurring before opening of the headers

Given that three ASG [EFWS] tanks are sufficient to reach the safe shutdown state (2 x 400 + 1 x 440 = 1240 te > 1100 te required as shown in section 3.2), a PSF anywhere on an ASG [EFWS] train is equivalent in terms of safety consequences to an ASF, for the following reasons:

- A leak in one train has no effect on the other trains as the passive headers are closed.
- The PSF is bounded by the ASF for the flow injected into the SG as at least two ASG [EFWS] pumps remain available.
- Even if the leak is not isolated, the associated loss of one tank is acceptable as three ASG [EFWS] tanks remain fully available and contain sufficient inventory.

As for the case of an ASF, the headers between the available ASG [EFWS] trains not affected by preventive maintenance and the PSF must be opened to feed at least two SGs, taking suction from the three remaining ASG [EFWS] tanks.

The division affected by the PSF is detected using sump level measurement. Note that the case where the passive headers are opened before such detection is effective, i.e. level < alarm threshold, is presented below.

3.7.3.1.2. Consideration of a PSF occurring after opening of the headers

- Actions performed by the operator related to the headers

  The headers will only be opened, when required, to the minimum extent necessary, e.g. between two trains only) and at the latest time possible. This maintains the most effective separation between the divisions,

  The following conservative assumptions are used to study the PSF consequences:

  - The tank passive header is opened before the ASG [EFWS] tanks assigned to the available ASG [EFWS] pumps are emptied. It is assumed that the four valves related to the four tanks are opened at the same time.

  - The pump passive header is opened to provide feed to at least two SG. In most cases, this constitutes realignment of the available ASG [EFWS] pump normally associated with the affected SG to the otherwise unfed SG associated with the division under preventive maintenance.

  If there is a leak in one division, detected by sump level measurement, the operator must:

  - Isolate the two passive headers to stop the loss of water inventory 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 of PSF

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

  - Leak in an ASG [EFWS] train, upstream of the tank passive header (close to the tank): - Location A in Sub-chapter 14.2 - Figure 8 "PSF"

    The ASG [EFWS] tank inventory is lost. After closing the two downstream valves on the tank-header and ASG [EFWS] train, the ASG [EFWS] pump is no longer available. Three ASG [EFWS] tanks and two ASG [EFWS] pumps remain available and provide feed to three SG via the pump passive header.

  - Leak in a tank passive header: - Location B in Sub-chapter 14.2 - Figure 8 "PSF"

    After isolation of the leak, by isolating the tank passive header by closing all the header valves the ASG [EFWS] tank assigned to the division under preventive maintenance is no longer available. Three ASG [EFWS] tanks and three ASG [EFWS] pumps remain available and provide feed to three SG via the pump passive header.

- Leak in an ASG [EFWS] train, between the connections with the passive headers: - Location C in Sub-chapter 14.2 - Figure 8 "PSF"

  After isolation of the leak, by closing the upstream and downstream ASG [EFWS] train valves, the ASG [EFWS] pump is no longer available. Four ASG [EFWS] tanks and two ASG [EFWS] pumps remain available and provide feed to three SG via the pump passive header.

- Leak in a pump passive header: - Location D in Sub-chapter 14.2 - Figure 8 "PSF"

  After isolation of the leak, by isolating the pump passive header by closing all the header valves, the ASG [EFWS] pump assigned to the affected SG is no longer available. It is also no longer possible to provide feed to the SG in the division under preventive maintenance. Four ASG [EFWS] tanks remain available via the tank passive header with two ASG [EFWS] pumps providing feed to two SG.

- Leak in an ASG [EFWS] train, downstream of the pump passive header: - Location E in Sub-chapter 14.2 - Figure 8 "PSF"

  After isolation of the leak, by closing the two upstream valves on the pump-header and ASG [EFWS] train, the ASG [EFWS] pump is no longer available. It is no longer possible to provide feed to the SG in the division under preventive maintenance. Four ASG [EFWS] tanks remain available via the tank passive header with two ASG [EFWS] pumps providing feed to two SG.

- Consequences of the leak

  Whatever the leak location in the ASG [EFWS], at least two ASG [EFWS] pumps and two SGs remain available to remove the heat. This includes the consequences of the equipment unavailability after isolation of the leak. This is the same minimum availability as that after an ASF. There is, therefore, sufficient water injection flow rate and steam release flow rate to perform the required heat removal function. This can be derived from the FWLB studies in Sub-chapter 14.5 and the following categorisation of the leaks.

  The leaks can be divided into two distinct categories, depending on their location in the ASG [EFWS], and their effect on the ASG [EFWS] water inventory available:

  - Leaks located upstream of the tank passive header, or in the tank passive header - locations A, B in Sub-chapter 14.2 - Figure 8 "PSF":

    - After isolation of the leak, three ASG [EFWS] tanks remain available (available water inventory = 1240 te),

    - 1100 te of ASG [EFWS] water are required to reach the RIS/RRA [SIS/RHRS] connecting conditions, on the basis of the very conservative "FWLB design case" analysis described in section 3.2,

    - Thus, the quantity of available ASG [EFWS] water inventory is sufficient to achieve RIS/RRA [SIS/RHRS] connection conditions.

- o Leaks located downstream of the tank passive header, including in the pump passive header - locations C, D, E in Sub-chapter 14.2 - Figure 8 "PSF":

  - After isolation of the leak, four ASG [EFWS] tanks remain available (available water inventory = 1680 te),

  - 1100 te of ASG [EFWS] water are required to reach the RIS/RRA [SIS/RHRS] connecting conditions, on the basis of the very conservative "FWLB design case" analysis described in section 3.2,

  - Consequently, the ASG [EFWS] heat removal function is not impaired as long as the total leakage does not exceed 580 te. Isolation of the leak will occur within the maximum typical delay time of RT + 1 hour. Considering a leak flow of 200 l/min, this would correspond to a loss of around 12 te.

3.7.3.2. Passive single failures leading to a flow restriction or blockage

Passive single failures impairing the normal process flow path in the fluid system, e.g. a flow restriction or blockage, are less onerous compared to the passive single failures leading to a leak. This is because less ASG [EFWS] water inventory is lost and hence unavailable for heat removal. At most, the inventory of one ASG [EFWS] tank is lost.

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

As described in the previous paragraphs and as shown in Sub-chapter 14.2 - Figure 8, it is possible for an ASG [EFWS] tank to be unavailable for primary system cooling after the leak arising from a postulated Passive Single Failure has been isolated.

Therefore, following isolation of the leak arising from the Passive Single Failure:

- three ASG [EFWS] tanks are available,

- at least two ASG [EFWS] pumps are available,

- at least two SGs are available.

Consequently, for the most limiting Passive Single Failure case, **1,240 te of ASG [EFWS] water is available**. This consists of 400 te in each of the tanks in divisions 2 and 3 and 440 te in the tank in divisions 1 or 4. The Passive Single Failure is applied so that the largest tank is lost to minimise the quantity of ASG [EFWS] water assumed to be available.

Consequently, the quantity of ASG [EFWS] water available (1,240 te) in the worst case scenario is greater than the quantity of ASG [EFWS] water required (1,100 te) on the basis of the conservative "FWLB design case" analysis described in section 3.2 of this sub-chapter.

3.7.4. Conclusion for ASG [EFWS]

Because of the existence and use of "passive headers", which provide fluid interconnections between the four ASG [EFWS] trains, the tolerance of the ASG [EFWS] to a passive single failure has been investigated.

If a passive single failure in one ASG [EFWS] train, or in one of the two ASG [EFWS] headers as assumed, at least three ASG [EFWS] tanks and two ASG [EFWS] pumps providing feed to two SGs remain available for RCP [RCS] heat removal This is sufficient to transfer the plant to the safe shutdown state, from which point heat removal is performed by the RIS/RRI/SEC [SIS/CCWS/ESWS] closed cooling chain. This assessment allows for a grace period to detect, locate and isolate the leak.

Consequently, it is concluded that a passive single failure in the ASG [EFWS] in the short term phase of a PCC accident does not lead to a cliff edge effect.

3.8. FUEL POOL COOLING SYSTEM (PTR [FPCS])

The PTR [FPCS] is involved in the performance of three fundamental safety functions [Ref-1]:

- Control of reactivity
- Residual heat removal
- Radioactive material containment

In PCSR Sub-chapter 14.0, it is stated that “due to the specific nature of the pool water cooling system, operating at low pressure, its in-service inspection programme etc, no passive failures are assumed for the PTR [FPCS] itself in the safety analysis for spent fuel pool PCC events”.

Even if a passive single failure is very unlikely on the PTR [FPCS], analysis of passive single failure is presented as a demonstration of defence in depth.

The system features considered for the analysis of the impact of the PSF criterion are detailed below:

- Start-up of a main PTR [FPCS] cooling train
- Isolation of the fuel building pool compartment drainage lines
- Isolation of the reactor building pool compartment drainage lines
- Instrumentation lance compartments draining to the IRWST
- Isolation of the main PTR [FPCS] train pump suction
- Isolation of the third PTR [FPCS] train pump suction
- Reactor building pool overflow lines opening

Claim

The PTR [FPCS] has been assessed for its ability to meet the passive single failure criterion. The system has been shown to withstand the passive single failure in some cases. However some safety functions are to be analysed further.

Arguments

The ability of the PTR [FPCS] to fulfil its safety function associated with start-up of a PTR [FPCS] main train is considered adequate when credit is claimed for the third PTR [FPCS] train.

The ability of the PTR [FPCS] to fulfil its safety functions associated with isolation of the fuel building pool compartment drainage lines, isolation of the reactor building pool compartment drainage lines, isolation of the main PTR [FPCS] train pump suction and isolation of the third PTR [FPCS] train pump suction is not affected by a passive single failure.

The ability of the PTR [FPCS] to fulfil its safety function associated with the instrumentation lance compartments draining to the IRWST is not considered to be affected by a passive single failure.

The ability of the PTR [FPCS] to fulfil its safety function associated with the reactor building pool overflow lines opening is not considered to be affected by a passive single failure.

Evidence

The PTR [FPCS] plant level safety function is to maintain heat removal from fuel stored outside the reactor coolant system but within the site.

The single failure criterion applies to the PTR [FPCS] fuel pool cooling system for F1A or F1B class functions.

Due to the specific nature of the fuel pool water cooling system, operating at low pressure and its in-service inspection programme, no passive failures were assumed for the PTR [FPCS] itself in the PCSR safety analysis for spent fuel pool PCC events. However, the system features associated with the PTR [FPCS] have been reviewed to quantify the impact of a PSF on the ability of the system to fulfil its safety functions.

3.8.1. Start-up of a main PTR [FPCS] cooling train

The initial leak rate associated with a passive failure is conventionally assumed to be 200 l/min for the PTR [FPCS]. This assumed leak rate does not initially prevent the PTR [FPCS] system from cooling the spent fuel pool. The leak rate causes fuel pool draining at a rate of 12 m^3/h. This drainage rate can be compensated for by the Nuclear Island Demineralised Water Distribution System (SED) which supplies water at a rate of 30 m^3/h or by the Classified Fire Fighting Water Supply System (JAC/JPI [NIFPS]) at a rate of 150 m^3/h.

If the leak increases to the flow rate corresponding to a complete pipe break, the PTR [FPCS] main train must be stopped and isolated.

In this case, spent fuel pool water make-up can be provided by the Classified Fire Fighting Water Supply System (JAC/JPI [NIFPS]) at a make-up rate of 150 m^3/h and the fuel pool cooling may be recovered by the start-up of the third PTR [FPCS] train. In PCSR Sub-chapter 14.0 section 2.10.5 it is stated that the two principal PTR [FPCS] trains are F1B classified. The general rules for PCC studies specify that the safety analysis for PCC events must only be based on the use of F1 systems. However, due to the specific nature of the spent fuel pool, high thermal inertia and low pressure, some exceptions may be introduced to this rule in order to mitigate a limited number of specific PCC events. For these events, F2 systems that have beneficial effects may be claimed in the safety analysis. It is considered that, in the case of loss of a PTR [FPCS] main train, the safety benefit provided by the third PTR [FPCS] train is more relevant than the classification of the third train as F2. The use of the third PTR [FPCS] train would be in the event of a PSF on one main PTR [FPCS] train, coincident with a fault on the second main train.

For the case of the start-up of a main PTR [FPCS] cooling train, the safety criteria are met by means of the third PTR [FPCS] train.

3.8.2. Isolation of fuel building pool compartment drainage lines, isolation of reactor building pool compartment drainage lines, isolation of main PTR [FPCS] train pump suction, isolation of third PTR [FPCS] train pump suction

Intake sections of the cooling trains up to the second isolation valve, reactor building and fuel building drainage compartments up to the second isolation valve as well as the outlet from the cooling trains up to the first isolation valve are subject to the ‘break preclusion’ principle. Therefore, application of the passive single failure criterion does not change the safety case.

3.8.3. Instrumentation lances compartment draining to the IRWST

A leak on the instrumentation lances compartment drainage line may prevent some water from the instrumentation lance compartments from flowing directly to the IRWST (the volume of water concerned being 15 m^3 versus an instrumentation lance compartment volume of 200 m^3). Functional analysis shows that this leakage volume will not prevent the start-up of the MHSI or the ability of the MHSI to pump from the IRWST to the primary system. Therefore, application of a passive single failure is bounded by an active failure in this instance.

3.8.4. Reactor building pool overflow lines opening

This failure is addressed in the safety case by consideration of a PCC-4 event for a non-isolatable small break (< 50 mm equivalent diameter) on a line connected to the primary cooling loop (state E).

A leak on the reactor building pool overflow line may prevent water from the overflow line returning directly to the IRWST. Lost water will then be collected in the IRWST. The safety case assumes that the IRWST floor retentions of approximately 200 m^3 are filled by the water from the break. This delay in water from the overflow returning to the IRSWT is not expected to prevent the MHSI pump from operating properly.

This passive failure is considered to have little influence on the safety case and the safety criteria are still met.

3.8.5. Conclusion

A summary of the impact of a PSF on the system is provided in Sub- chapter 14.2 - Table 8.

3.9. CLASSIFIED FIRE-FIGHTING WATER PRODUCTION / NUCLEAR ISLAND FIRE-FIGHTING WATER PROTECTION AND DISTRIBUTION (JAC/JPI [NIFPS])

The JAC/JPI [NIFPS] is involved in the performance of one fundamental safety function [Ref-1] [Ref-2]:

- Residual heat removal

Claim

The JAC/JPI [NIFPS] system has been assessed for its ability to meet the passive single failure criterion. The system has been shown to withstand a passive single failure.

Arguments

The ability of the JAC/JPI [NIFPS] to fulfil its safety function associated with water distribution for spent fuel pool make-up is not affected by a passive single failure.

Evidence

The JAC/JPI [NIFPS] system is used for water make-up to the fuel pool following draining faults (PCC-3 and PCC-4) and is classified F1B for this role.

Two JAC tanks are incorporated into the EPR design, each with two pumps. If the PSF criterion is applied to the header downstream of one of the JAC tank (the suction header for one pump pair), leakage leads to the loss of two JAC pumps due to flooding. If one of the remaining two pumps is considered to be out of service for maintenance, one JAC pump is still available to contribute to the mitigation of the spent fuel pool PCC event (see Sub-chapter 14.2 – Figure 9).

In this case, however, the JAC system feature associated with fire-fighting is not available. With only one JAC pump available, benefit can be drawn from the F2 function associated with the make-up of the JAC system by the ASG [EFWS] system. If, with one JAC pump available, the ASG [EFWS] is used to make-up the JAC system, then the system features of spent fuel pool make-up and fire-fighting are maintained and the system therefore meets the single failure criterion.

Even in the case of a passive failure downstream of the tank JAC2120, it is considered to have sufficient water remaining to allow pumping by the ASG [EFWS] for fire-fighting (see Sub-chapter 14.2 – Figure 10).

If the PSF is applied to a JPI [NIFPS] line that supplies the spent fuel pool, the leak can be isolated and a second line remains available to supply make-up water to the spent fuel pool.

A summary of the impact of a PSF on the JAC/JPI [NIFPS] system is provided in Sub-chapter 14.2 - Table 9.

3.10. FRONTLINE SYSTEMS SUMMARY

Sub-chapter 14.2 - Table 10 lists the conclusion regarding the frontline systems analysed in this section.

4. SUPPORT SYSTEMS

4.1. COMPONENT COOLING WATER SYSTEM (RRI [CCWS])

The RRI [CCWS] is involved in the performance of two fundamental safety functions [Ref-1]:

- Residual heat removal
- Radioactive material containment

The system functions performed by the RRI [CCWS] that have been considered for this analysis are detailed below:

- Start-up of an RRI [CCWS] train
- Supply of cooling to a RIS [SIS] heat exchanger
- Supply of cooling to the RIS [SIS] pumps
- Supply of cooling to a PTR [FPCS] train
- Supply of cooling to the reactor coolant pump thermal barrier
- Supply of cooling to the DEL [SCWS] trains 2 and 3

Claim

The RRI [CCWS] has been assessed for its ability to meet the passive single failure criterion. The system has been shown to withstand the passive single failure criterion in some cases. However some safety functions are to be further reviewed to ensure that the consequences of a passive single failure are ALARP.

Arguments

The ability of the RRI [CCWS] to fulfil its safety function associated with starting a RRI [CCWS] train is not affected by a passive single failure.

The ability of the RRI [CCWS] to fulfil its safety function associated with supply of cooling to a RIS [SIS] heat exchanger and supply of cooling to the RIS [SIS] pumps is not affected by a passive single failure.

The ability of the RRI [CCWS] to fulfil its safety function associated with the supply of cooling to a PTR [FPCS] train is considered adequate when benefit is claimed for the third PTR [FPCS] train.

The ability of the RRI [CCWS] to fulfil its safety function associated with the supply of cooling to the reactor coolant pump thermal barrier has been identified as a shortfall and will be the subject of an ALARP assessment.

The ability of the RRI [CCWS] to fulfil its safety function associated with the supply of cooling to the DEL [SCWS] trains 2 and 3 is not affected by a passive single failure.

Evidence

The active single failure criterion applies to all equipment performing an F1 function, in order to ensure a sufficient level of redundancy.

The RRI [CCWS] is designed as four identical, geographically and electrically separated trains to perform the F1A classified RIS [SIS] safeguard function.

Cooling of the PTR [FPCS] (F1B) is achieved as follows:

- by RRI [CCWS] trains 1 or 2 for PTR [FPCS] train 1
- by RRI [CCWS] trains 3 or 4 for PTR [FPCS] train 2

Cooling of the DEL [SCWS] system (F1B) is achieved as follows:

- by RRI [CCWS] trains 1 or 2 for DEL [SCWS] train 2
- By RRI [CCWS] trains 3 or 4 for DEL [SCWS] train 3.

Cooling of the thermal barriers of reactor coolant pumps 1 and 2 (F1B) is provided by RRI [CCWS] trains 1 or 2 (see Sub-chapter 14.2 - Figure 11).

Cooling of the thermal barriers of reactor coolant pumps 3 and 4 (F1B) is provided by RRI [CCWS] trains 3 or 4 (see Sub-chapter 14.2 - Figure 12).

<u>Start-up of a RRI [CCWS] train</u>

A passive failure on the RRI [CCWS] train line does not result in a more onerous condition than that produced by an active single failure, e.g. the loss of one RRI [CCWS] pump.

<u>Supply of cooling to a RIS [SIS] heat exchanger and Supply of cooling to RIS [SIS] pumps</u>

A passive failure on the RRI [CCWS] cooling line of the RIS [SIS] heat exchanger or of the RIS [SIS] pump cooler does not lead to the loss of more than one RIS [SIS] train. This does not result in a more onerous condition than that produced by an active single failure.

<u>Supply of cooling to a PTR [FPCS] train</u>

A passive failure on the RRI [CCWS] cooling line of the PTR [FPCS] heat exchanger leads to the loss of a PTR [FPCS] main train. There are two main PTR [FPCS] trains. For a PCC event such as a breach in the PTR [FPCS] system, fuel pool cooling could be recovered by putting the F2 classified third PTR [FPCS] train into service. These circumstances are comparable to those detailed in section 3.8, which justifies the safety benefit of the third PTR [FPCS] train, despite its F2 classification.

<u>Supply of cooling to the reactor coolant pump thermal barrier</u>

Passive failure on a common line B of the RRI [CCWS] may lead to the loss of cooling of the thermal barriers of reactor coolant pumps 1 and 2 or 3 and 4. This failure is more onerous than that of the single active failure for this system and is not bounded by the ASF. This analysis has identified a shortfall that needs to be addressed.

Supply of cooling to the DEL [SCWS] trains 2 and 3

Passive failure on a common line B of the RRI [CCWS] may lead to the loss of cooling of the refrigeration unit of one DEL [SCWS] train. This is bounded by an active single failure in the DEL [SCWS] system.

A summary of the impact of a PSF on the RRI [CCWS] system is provided in Sub-chapter 14.2 - Table 11.

4.2. ESSENTIAL SERVICE WATER SYSTEM (SEC [ESWS])

The SEC [ESWS] is involved in the performance of two fundamental safety functions [Ref-1]:

- Residual heat removal
- Radioactive material containment

The system features performed by the SEC [ESWS] that have been considered are detailed below:

- Start-up of an SEC [ESWS] train

A passive failure is not considered to affect low speed rotation and low pressure washing of filter units (chain screens and rotating drum screens). Potential active failure of these components is already applied.

Claim

The SEC [ESWS] has been assessed for its ability to meet the passive single failure criterion. The system has been shown to withstand the passive single failure in some cases.

Arguments

The ability of the SEC [ESWS] to fulfil its safety function associated with the start-up of a SEC [ESWS] train is not affected by a passive single failure.

Evidence

The SEC [ESWS] is designed with four identical trains which are physically and electrically independent of one another so as to guarantee the RRI [CCWS] cooling function and the PTR [FPCS] cooling function (see Sub-chapter 14.2 – Figure 13).

A passive single failure on one SEC [ESWS] train may lead to the loss of that train.

Start-up of a SEC [ESWS] train

During preventive maintenance on a chain screen in the at-power state, a PSF on the header pump suction header, which is opened during this maintenance period, would result in the loss of one SEC [ESWS] train. Maintenance is only carried out on one chain screen at any one time when the unit is at power (see Sub-chapter 14.2 – Figure 14).

During preventive maintenance in the shut-down state, maintenance on the rotating drum-screens for SEC [ESWS] pumps 2 and 3 for the Flamanville site is currently planned to be carried out in parallel. The SEC [ESWS] pumps are supplied via the two chain screens and a common suction header. A PSF on the header pump suction header, which is opened during this maintenance period, would result in the loss of one SEC [ESWS] train. Note that the proposed outage programme for the UK would result in rotating drum-screen maintenance being carried out in series rather than in parallel.

The loss of one SEC [ESWS] train as a result of a passive single failure is the same consequence as that of an active single failure. A passive single failure is therefore bounded by an active single failure (see Sub-chapter 14.2 – Figure 15).

A summary of the impact of a PSF on the SEC [ESWS] system is provided in Sub-chapter 14.2 – Table 12.

4.3. ELECTRICAL BUILDING EMERGENCY CHILLED WATER SYSTEM (DEL [SCWS])

The DEL [SCWS] is involved in the performance of one fundamental safety function [Ref-1]:

- Residual heat removal

Claims

The DEL [SCWS] system has been assessed for its ability to meet the passive single failure criterion. The system has been shown to withstand the passive single failure.

Arguments

The ability of the DEL [SCWS] system to fulfil its safety function associated with chilled water production is not affected by a passive single failure.

The ability of the DEL [SCWS] system to fulfil its safety function associated with chilled water distribution for the DCL [CRACS], DVL [SBVSE], DWK [FBVS] and DWL [CSBVS] is not affected by a passive single failure.

The ability of the DEL [SCWS] system to fulfil its safety function associated with chilled water distribution for the RIS [SIS] is not affected by a passive single failure.

Evidence

The DEL [SCWS] system delivers chilled water to provide cooling for ventilation systems. These ventilation systems are used in the electrical buildings for cooling of electrical and instrumentation and control equipment.

The DEL [SCWS] system is designed on a 4 x 100% basis to meet the active single failure criterion. This structure ensures that, if one DEL [SCWS] train becomes unavailable, three other 100% trains remain available. This design allows the DEL [SCWS] system to withstand the failure of a component. This design feature provides mitigation against the passive single failure.

There is a connection between DEL [SCWS] divisions 1 and 2 and DEL [SCWS] divisions 3 and 4 respectively. This maintains permanent cooling of the RBS [EBS] pump rooms in case of maintenance of the DEL [SCWS] system in division 1 and division 4 respectively.

However, to maintain the independence of the divisions, there are two redundant isolation valves installed in two different buildings on the corresponding interconnection lines (see Sub-chapter 14.2 – Figure 16).

Chilled water production and distribution for the DCL [CRACS], DVL [SBVSE], DWK [FBVS], DWL [CSBVS]

When the DEL [SCWS] chilled water production system is considered, a passive single failure could lead to the loss of a DEL [SCWS] train in a short time. If a leak rate, due to a passive failure of 200 l/min is assumed, the time taken to empty the DEL [SCWS] storage tank, which has a minimum volume of 230 litres, is less than 2 minutes. This PSF is bounded by the active single failure scenario.

In the case of maintenance activities on one DEL [SCWS] train, the cross-connection is used to provide chilled water supply from the paired DEL [SCWS] train. If a PSF is considered on the inter-connection between the two trains, one DEL [SCWS] train is unavailable due to maintenance and one DEL [SCWS] train is unavailable due to the PSF criterion. This outcome is bounded by the consideration of an active single failure on one DEL [SCWS] train coincident with maintenance on a second train. A passive single failure is bounded by the active single failure (see Sub-chapter 14.2 –Table 13).

4.4. HEATING, VENTILATION AND AIR-CONDITIONING (HVAC)

An active single failure is considered for HVAC systems that support classified frontline systems or provide a containment function:

- DCL [CRACS]: Main Control Room and Adjoining Rooms Air Conditioning System
- DVD: Diesel Generator Building Ventilation System
- DVL [SBVSE]: Safeguard Building Uncontrolled Area Ventilation System
- DVP: Water Pumping Station Ventilation System
- DWK [FBVS]: Fuel Building Ventilation System
- DWL [CSBVS]: Safeguard Building Controlled Area Ventilation System
- EBA [CSVS]: Containment Sweep Ventilation System
- EDE [AVS]: Annulus Ventilation System

Following IAEA Safety Standard NS-R-1 [Ref-1], it is not necessary to consider passive failure, if it is demonstrated that the failure is very unlikely and the function remains unaffected by the postulated initiating event.

Claim

Assessment of the impact on the HVAC systems DCL [CRACS], DVD, DVL [SBVSE], DVP, DWK [FBVS], DWL [CSBVS] and EBA [CSVS] has not been carried out as a single passive failure of these systems is considered unlikely to occur.

Arguments

The HVAC systems DCL [CRACS], DVD, DVL [SBVSE], DVP, DWK [FBVS], DWL [CSBVS] and EBA [CSVS] are complex. They involve long ducting systems with complex geometries, operating at low system pressures and temperatures.

Evidence

An active single failure is assessed for the HVAC systems that support classified frontline systems or that provide a containment function. Redundancy and alignment of system trains have been designed in order to cover an ASF.

In-service inspection of HVAC ventilation systems will be carried out in order to ensure that they are operating correctly.

Passive failure could be more onerous than active single failure only for common sections between HVAC of different trains. Information obtained from the INEEL database indicates a postulated leakage frequency of 1.0E-09 /h/m where h is time and m is length. If a time of 24 hours is considered with a duct length of 1000 m (considered as a bounding value for potential common length), the postulated probability of leakage is 2.4E-05. Doubling the length of ducting does not give rise to a change in the order of magnitude of the probability of leakage.

4.5. SUPPORT SYSTEMS SUMMARY

Sub-chapter 14.2 –Table 14 lists the conclusion regarding the support systems analysed in this section.

5. CONCLUSION

Even if not explicitly taken into account initially, UK EPR design, based on a 4-train design for the main safety systems, shows an overall good robustness against passive failure, with some particular exceptions.

These exceptions are the following (see also Sub-chapter 14.2 -Table 15):

<u>RIS/RRA [SIS/RHRS]: RIS i560VP failure to open</u>

This passive failure is taken into account in the Loss Of Coolant Accidents performed in section 6 of Sub-chapter 14.5. It is demonstrated that the acceptance criteria are still met when this passive failure is assumed.

<u>RCP [RCS]: Safety valves failure to close</u>

An ALARP analysis is required for this case [Ref-1]. It concludes that the current design is the solution which results in a risk to workers and members of the public as low as reasonably practicable.

<u>VVP [MSSS]: VIV [MSIV] failure to close during SGTR</u>

An ALARP analysis is required for this case [Ref-2]. It concludes that the current design is the solution which results in a risk to workers and members of the public as low as reasonably practicable.

APG [SGBS]: break on transfer line

The transfer line between two steam generators may be required in the case of the long term mitigation following a steam generator tube rupture (SGTR). It is only used to decrease the affected steam generator water inventory for depressurisation and prevention of overfilling. Nevertheless, the consequences of such a passive single failure have no direct impact on radiological releases outside containment. It would replace a far more onerous single failure regarding radiological releases following a SGTR. The worst case would then be a small leak inside the containment that the operator would be able to isolate. The safety analyses are hence unaffected by this passive single failure.

VVP [MSSS]: break on the VIV [MSIV] heating line°

The reheat line has a diameter of 100 mm. This is much smaller than the line from the main steam isolation valve, of 750 mm diameter. The failure to close of the main steam isolation valve is considered in the PCSR (except following a SGTR). The depressurisation due to the passive single failure on the VIV [MSIV] reheat line leads to lower consequences than the failure to close of the VIV [MSIV]. Therefore, the passive single failure is bounded by the active one. Following a SGTR, the single failure considered consists of the VDA [MSRT] being stuck open. The diameter of the VDA [MSRT] is 350 mm which is larger than the reheat line. Therefore, the passive single failure on the reheat line of the VIV [MSIV] is covered by the active single failure on the VDA [MSRT]. The safety analyses are hence unaffected by this passive single failure.

The overall analysis hence shows that the UK EPR design is robust with respect to passive single failures.[1]

[1] The robustness of the UK EPR cooling chain design against passive single failures is still to be demonstrated.

SUB-CHAPTER 14.2 - TABLE 1

RIS/RRA [SIS/RHRS] Failures Classification Summary

RIS/RRA [SIS/RHRS] Analysis	Classification*
RIS i560VP failure to open	Case 2**
Other parts of the system	Case 1

** Classification refers to cases listed in section 2.2*
*** This passive single failure is taken into account for Loss of Coolant Accidents in Sub-chapter 14.5 section 6*

SUB-CHAPTER 14.2 - TABLE 2

VDA [MSRT] Failures Classification Summary

VDA [MSRT] Analysis	Classification*
Global system	Case 1

** Classification refers to cases listed in section 2.2*

SUB-CHAPTER 14.2 - TABLE 3

RBS [EBS] Failures Classification Summary

RBS [EBS] Analysis	Classification*
Global system	Case 1

** Classification refers to cases listed in section 2.2*

SUB-CHAPTER 14.2 - TABLE 4

RCP [RCS] Failures Classification Summary

RCP [RCS] Analysis	Classification*
Safety valves failure to close	Case 3 – ALARP analysis [Ref-1]
Other parts of the system	Case 1

**Classification refers to cases listed in section 2.2*

SUB-CHAPTER 14.2 – TABLE 5

VVP [MSSS] Failures Classification Summary

VVP [MSSS] Analysis	Classification*
VIV [MSIV] failure to close during SGTR	Case 3– ALARP analysis [Ref-1]
Reheat line break	Case 2
Other parts of the system	Case 1

** Classification refers to cases listed in section 2.2*

SUB-CHAPTER 14.2 – TABLE 6

APG [SGBS] Failures Classification Summary

APG [SGBS] Analysis	Classification*
Transfer line break	Case 2
Other parts of the system	Case 1

** Classification refers to cases listed in section 2.2*

SUB-CHAPTER 14.2 – TABLE 7

ASG [EFWS] Failures Classification Summary

ASG [EFWS] analysis	Classification*
Global system	Case 2

** Classification refers to cases listed in section 2.2*

SUB-CHAPTER 14.2 – TABLE 8

PTR [FPCS] Failures Classification Summary

PTR [FPCS] analysis	Classification*
Start-up of a PTR [FPCS] main train	Case 2 Safety criteria met with PTR [FPCS] 3rd train
Fuel building and reactor building pool drain lines isolation, broken PTR [FPCS] (main and 3rd) train suction line isolation	Case 1
Instrumentation lances compartment draining to the IRWST	Case 1/2
Reactor building pool overflow lines opening	Case 1/2

** Classification refers to cases listed in section 2.2*

SUB-CHAPTER 14.2 – TABLE 9

JAC/JPI [NIFPS] Failures Classification Summary

JAC/JPI [NIFPS] analysis	Classification*
Water distribution for Spent Fuel Pool make-up	Case 1

** Classification refers to cases listed in section 2.2*

SUB-CHAPTER 14.2 – TABLE 10

Frontline Systems Failures Classification Summary

System	Failure	Classification
RIS/RRA [SIS/RHRS]	RIS i560 failure to close	Case 2
RBS [EBS]	Global system	Case 1
VDA [MSRT]	Global system	Case 1
RCP [RCS]	Safety valves failure to close	Case 3 – ALARP analysis [Ref-1]
VVP [MSSS]	VIV [MSIV] failure to close	Case 3 – ALARP analysis [Ref-2]
VVP [MSSS]	Break on the VIV [MSIV] heating line	Case 2
APG [SGBS]	Break on a transfer line	Case 2
ASG [EFWS]	Break on the header	Case 2 (already presented in the PCSR)
PTR [FPCS]	Break on the PTR [FPCS] main train	Case 2 Safety criteria met with PTR [FPCS] 3rd train
PTR [FPCS]	Break on the fuel building and reactor building pool drain lines, on the PTR [FPCS] (main and 3rd) train suction line	Case 1
PTR [FPCS]	Break on the instrumentation lances compartment draining to the IRWST	Case 1/2
PTR [FPCS]	Break on the reactor building pool overflow line	Case 1/2
JAC/JPI [NIFPS]	Global system	Case 1

SUB-CHAPTER 14.2 – TABLE 11

RRI [CCWS] Failures Classification Summary

RRI [CCWS] analysis	Classification*
RRI [CCWS] train start-up	Case 1
RIS [SIS] heat exchanger and RIS [SIS] pump cooling	Case 1
PTR [FPCS] heat exchanger cooling	Case 2 Safety criteria met with PTR [FPCS] 3rd train
Thermal barriers of the reactor coolant pumps cooling	Case 3
DEL [SCWS] cooling	Case 1

** Classification refers to cases listed in section 2.2*

SUB-CHAPTER 14.2 – TABLE 12

SEC [ESWS] Failures Classification Summary

SEC [ESWS] analysis	Classification
Start-up of a SEC [ESWS] train: RRI [CCWS] cooling	Case 1

** Classification refers to cases listed in section 2.2*

SUB-CHAPTER 14.2 – TABLE 13

DEL [SCWS] Failures Classification Summary

DEL [SCWS] analysis	Classification
Chilled water production and distribution for the DCL [CRACS], DVL [SBVSE], DWK [FBVS], DWL [CSBVS]	Case 1

** Classification refers to cases listed in section 2.2*

SUB-CHAPTER 14.2 – TABLE 14

Support Systems Failures Classification Summary

System	Failure	Classification
RRI [CCWS]	Break on the RRI [CCWS] train line	Case 1
RRI [CCWS]	Break on the RIS [SIS] heat exchanger and RIS [SIS] pump cooling line	Case 1
RRI [CCWS]	Break on the PTR [FPCS] heat exchanger cooling line	Case 2 Safety criteria met with PTR [FPCS] 3rd train
RRI [CCWS]	Break on the thermal barriers of the reactor coolant pumps cooling line	Case 3
RRI [CCWS]	Break on the DEL [SCWS] cooling line	Case 1
SEC [ESWS]	Break on a SEC [ESWS] train	Case 1
DEL [SCWS]	Break on the chilled water production and distribution (for the DCL [CRACS], DVL [SBVSE], DWK [FBVS], DWL [CSBVS]) line	Case 1
HVAC	Passive failure is considered to be unlikely	-

SUB-CHAPTER 14.2 – TABLE 15

Failures Having Required Further Analyses

System	Failure	Classification
RIS/RRA [SIS/RHRS]	RIS i560 failure to close	Case 2*
RCP [RCS]	Safety valves failure to close	Case 3 – ALARP analysis [Ref-1]
VVP [MSSS]	VIV [MSIV] failure to close	Case 3 – ALARP analysis [Ref-2]
VVP [MSSS]	Break on the VIV [MSIV] heating line	Case 2 **
APG [SGBS]	Break on a transfer line	Case 2 **
RRI [CCWS]	Break on the thermal barriers of the reactor coolant pumps cooling line	Case 3 ***

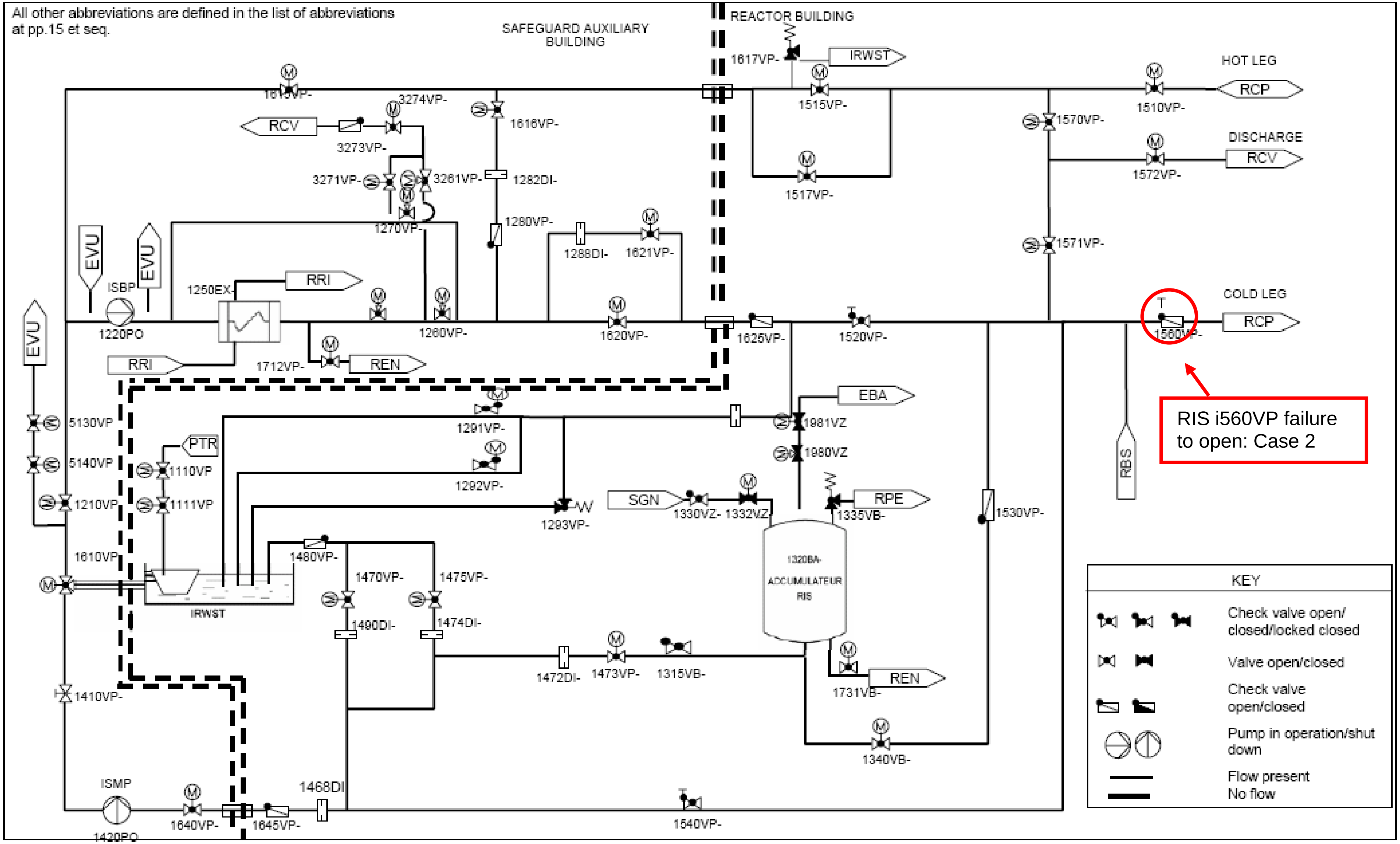
**This passive single failure is taken into account for Loss of Coolant Accidents in Sub-chapter 14.5 section 6*

*** These two cases are analysed in section 5. The arguments presented demonstrate that the safety analyses are essentially unaffected even though the passive single failure analysis leads to a case 2 classification.*

**** To be performed.*

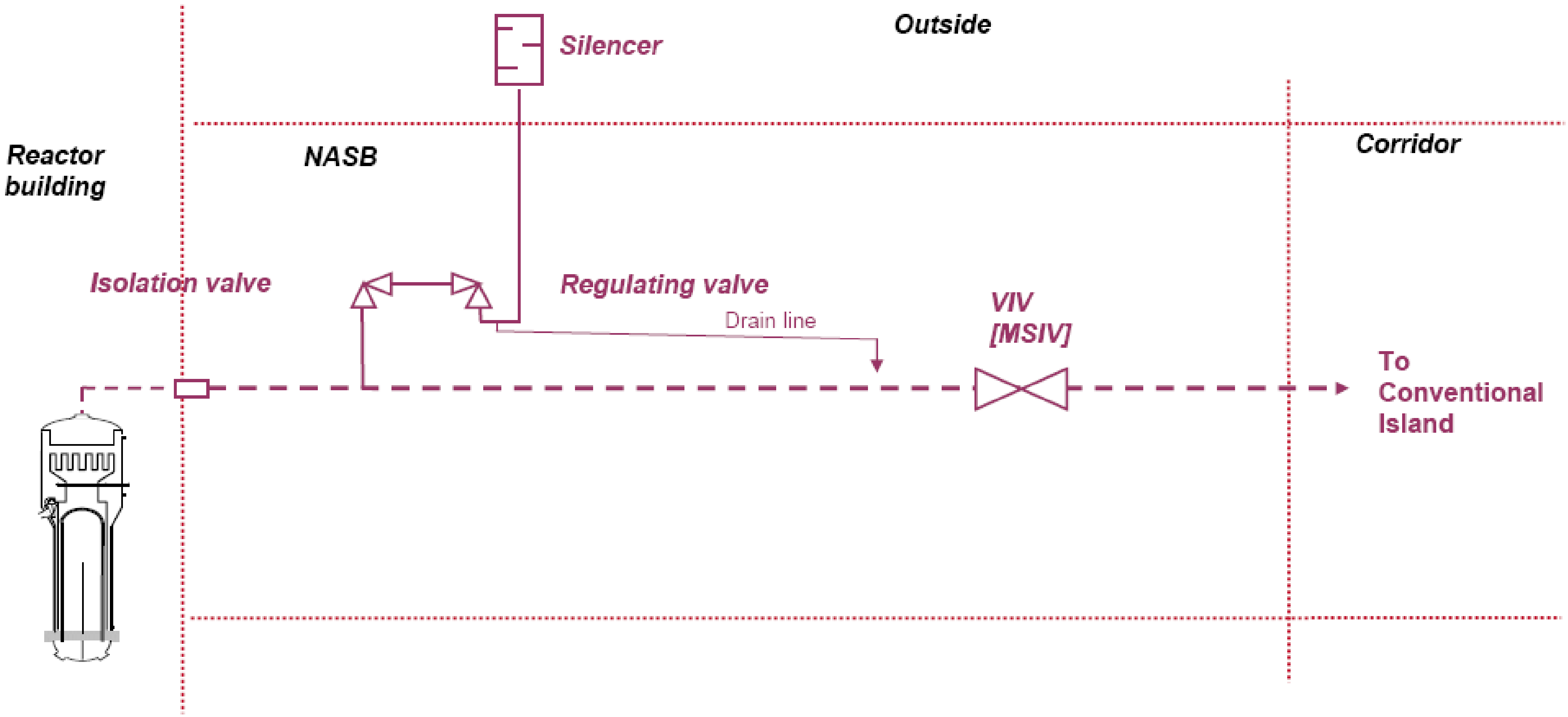
SUB-CHAPTER 14.2 - FIGURE 1

RIS/RRA [SIS/RHRS] Detailed Scheme



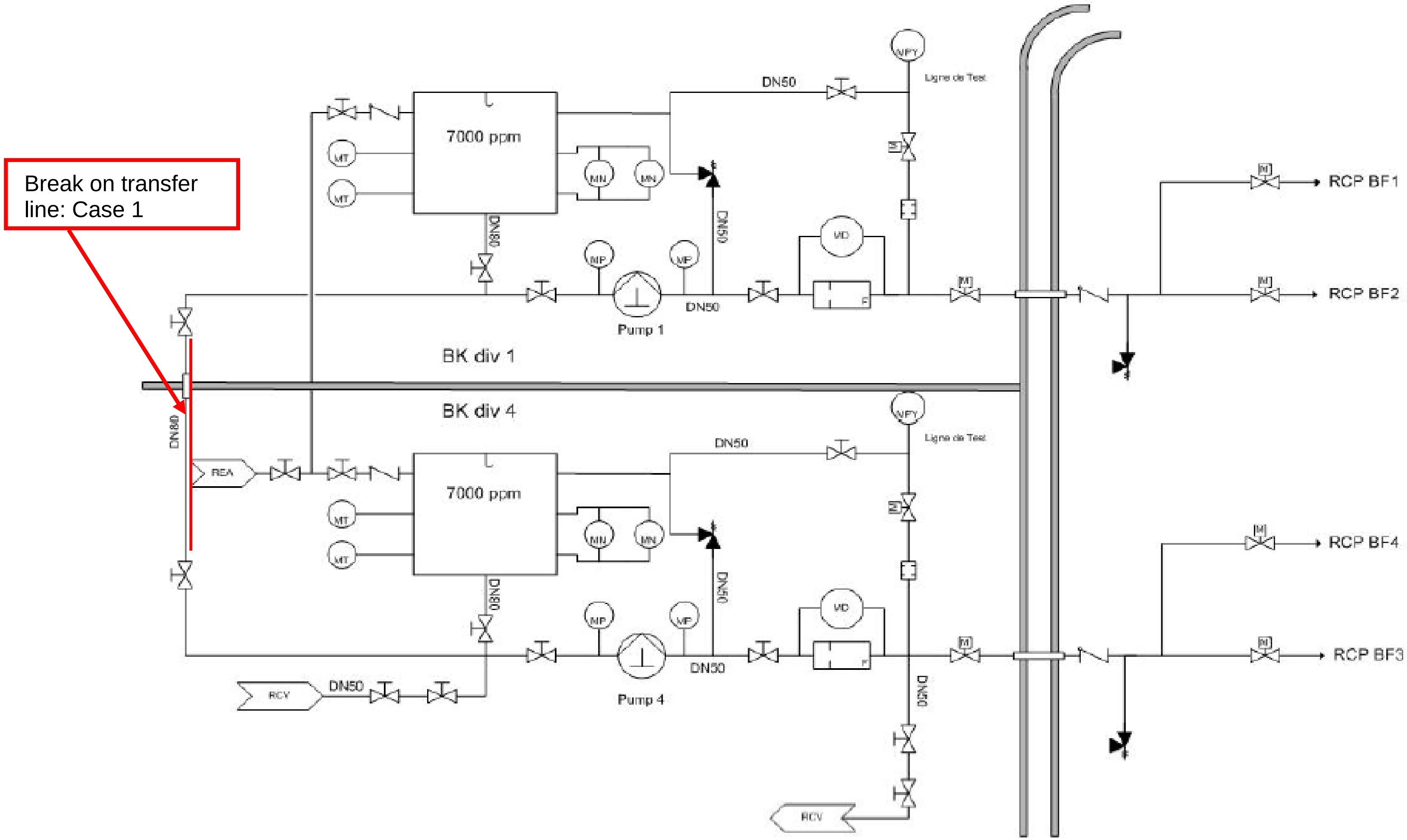
SUB-CHAPTER 14.2 - FIGURE 2

VDA [MSRT] Detailed scheme



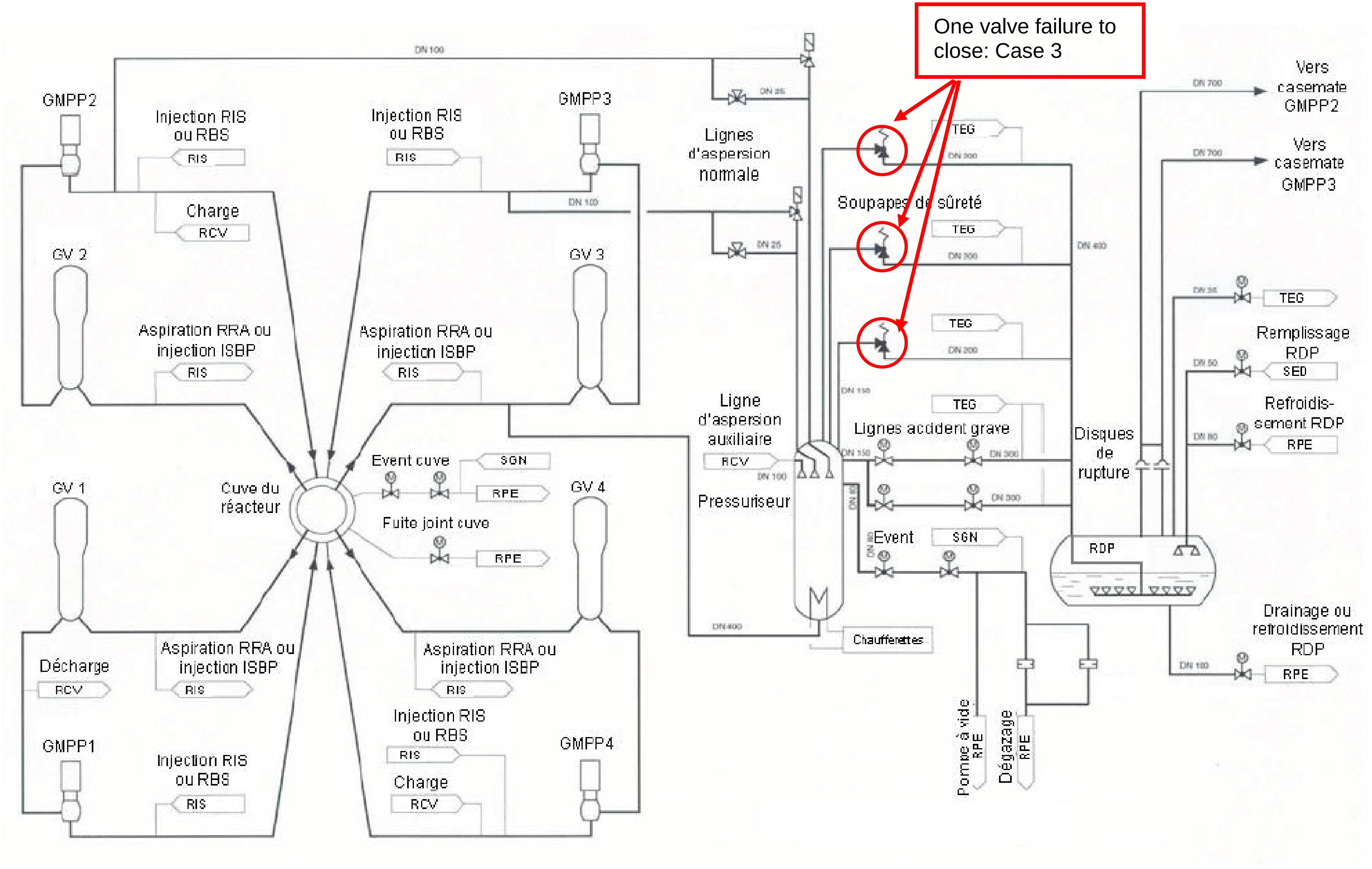
SUB-CHAPTER 14.2 – FIGURE 3

RBS [EBS] Detailed scheme



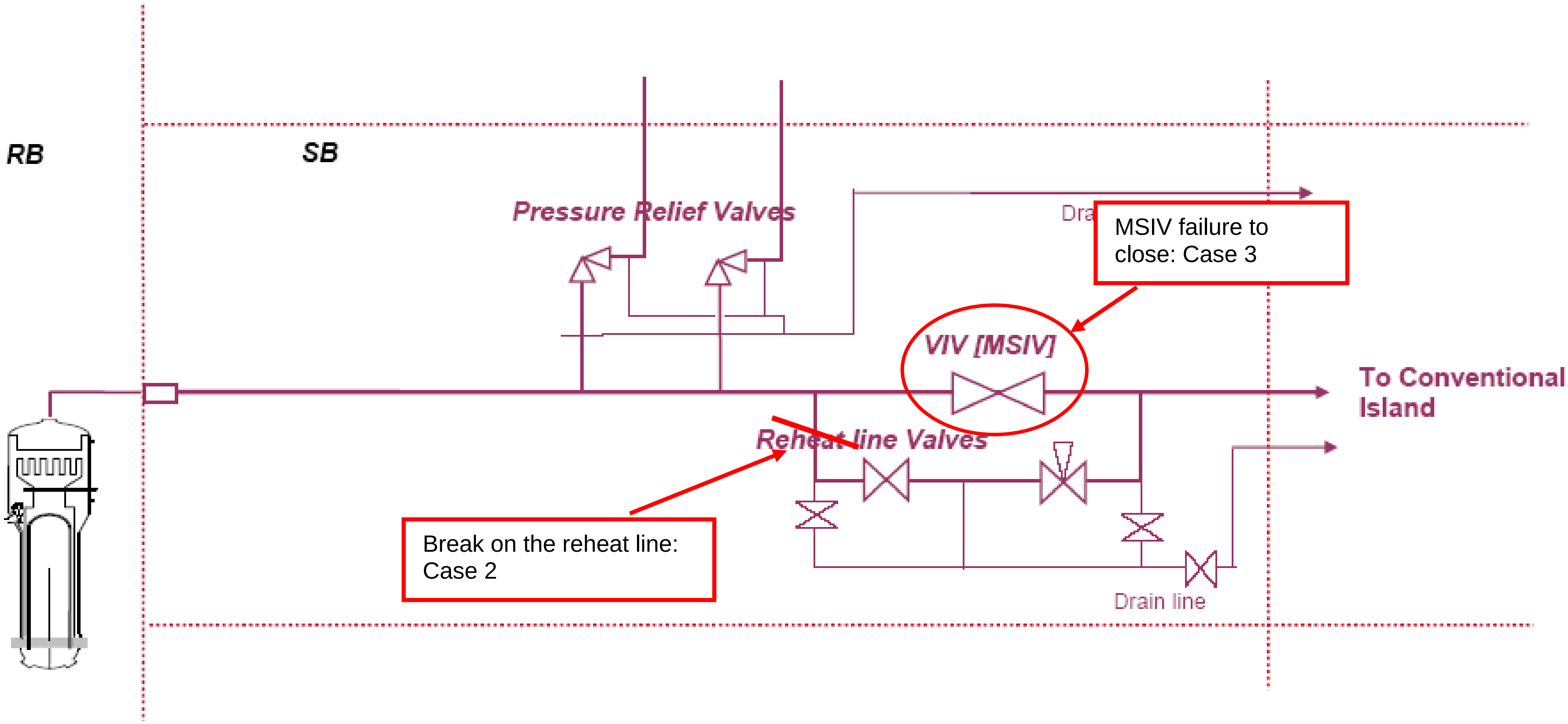
SUB-CHAPTER 14.2 – FIGURE 4

RCP [RCS] Detailed scheme



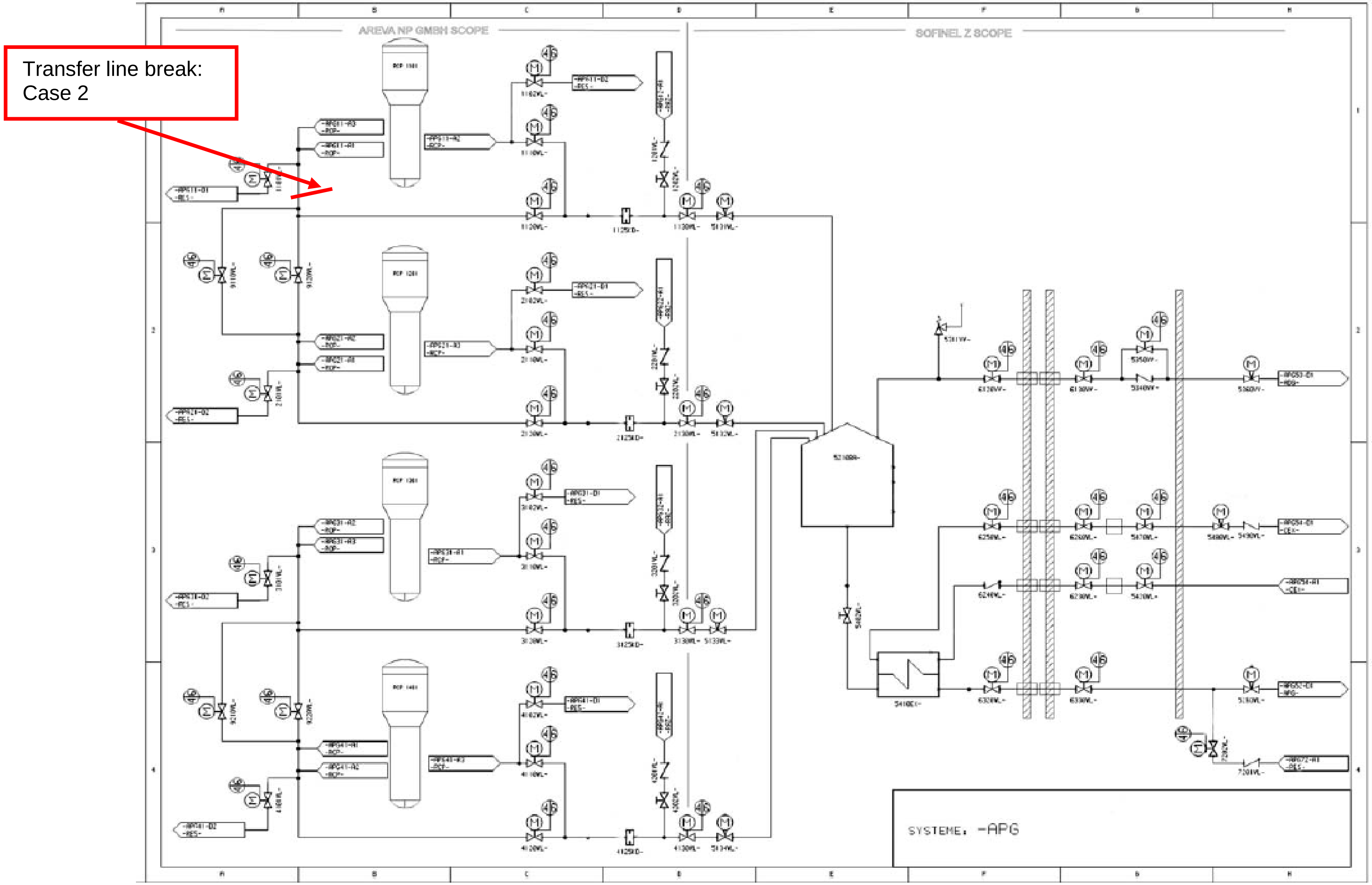
SUB-CHAPTER 14.2 – FIGURE 5

VVP [MSSS] Detailed scheme



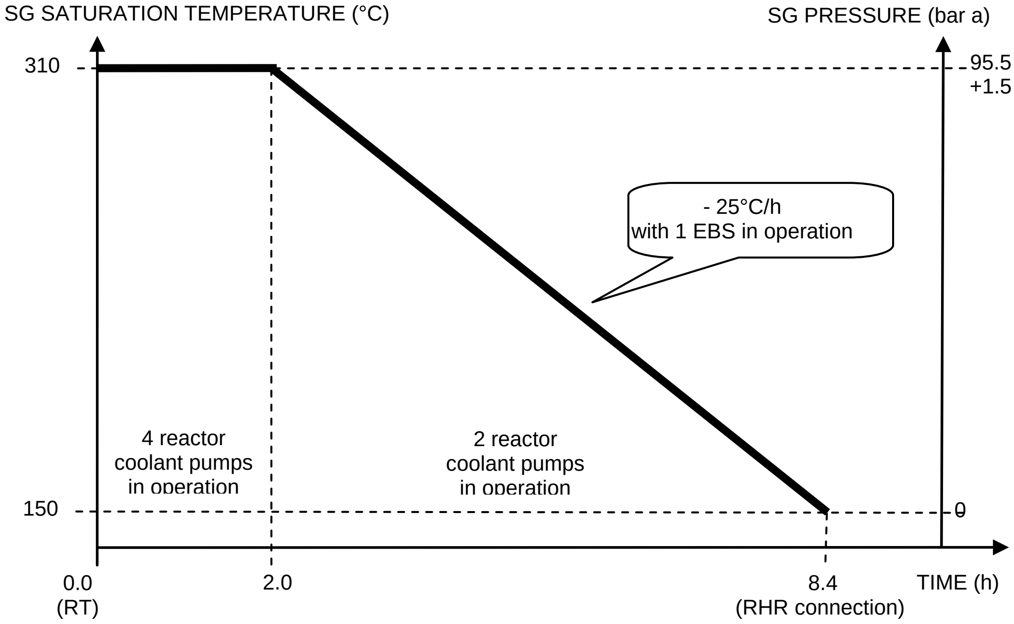
SUB-CHAPTER 14.2 – FIGURE 6

APG [SGBS] Detailed scheme



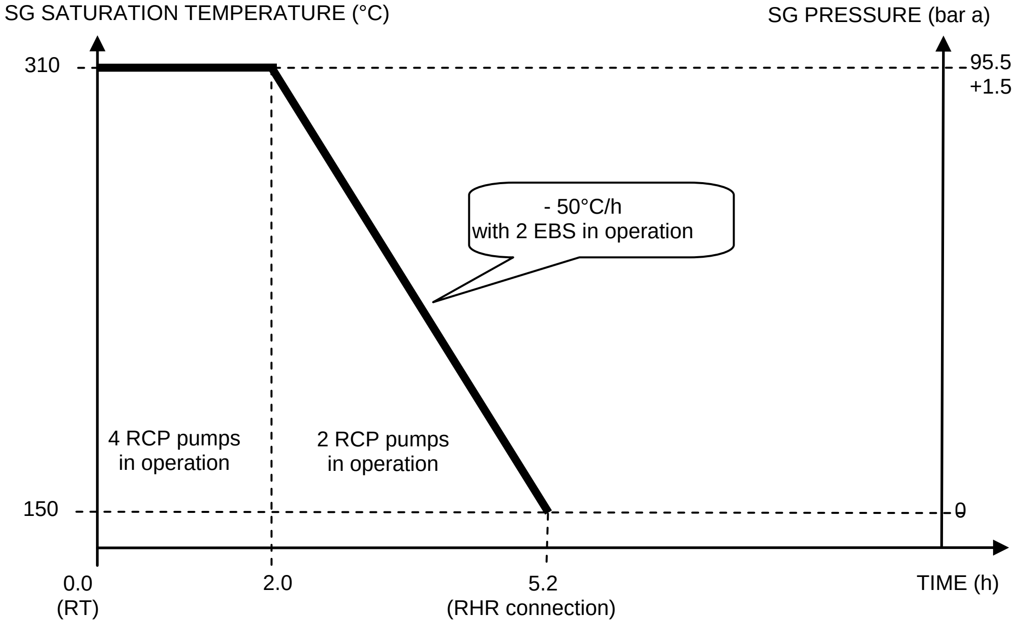
SUB-CHAPTER 14.2 - FIGURE 7

ASG [EFWS]: Design Transient "TRANSFER TO RIS/RRA [SIS/RHRS] CONNECTING CONDITIONS"



REQUIRED EFWS WATER INVENTORY: 1350 te
AVAILABLE EFWS WATER CONTENT: 1680 te (4 tanks: 2x400 + 2x440)

ACTIVE SINGLE FAILURE

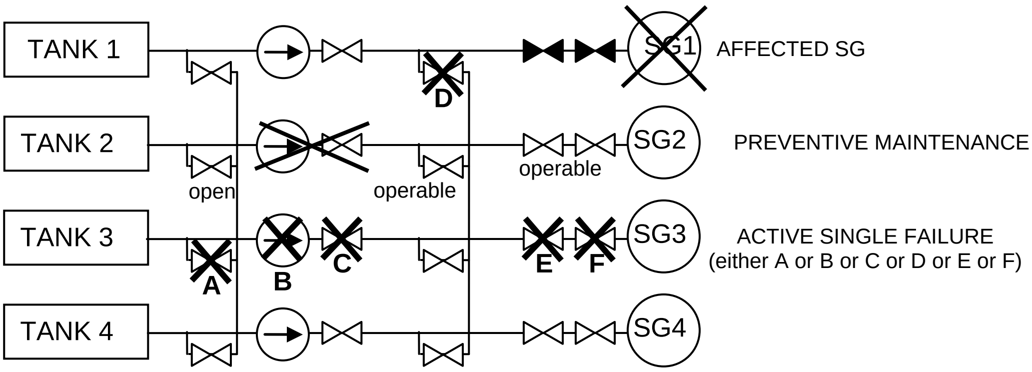


REQUIRED EFWS WATER INVENTORY: 1100 te
AVAILABLE EFWS WATER CONTENT: 1240 te (3 tanks: 2x400 + 1x440)

PASSIVE SINGLE FAILURE

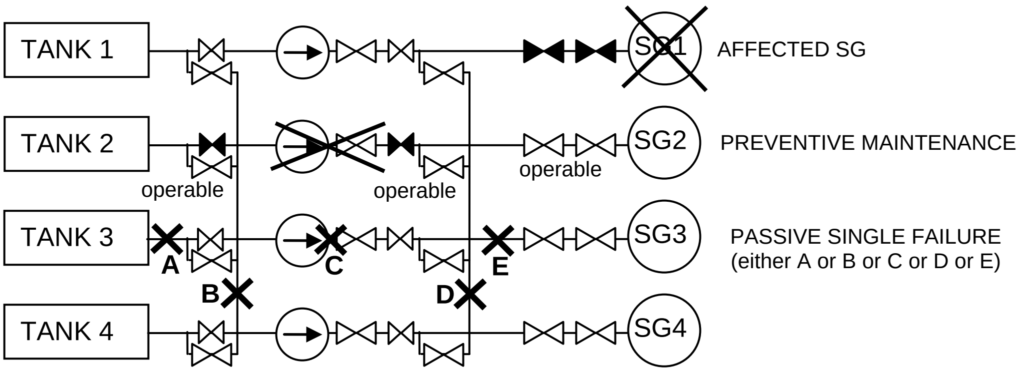
SUB-CHAPTER 14.2 - FIGURE 8

ASG [EFWS]: Comparison between Active and Passive Single Failures



	A	B	C	D	E	F	MIN	
Number of tanks available:	4	4	4	4	4	4	4	via tank passive header
Number of pumps available:	3	2	2	2	3	3	2	via pump passive header
Number of SG available:	3	3	3	3	2	2	2	

ACTIVE SINGLE FAILURE

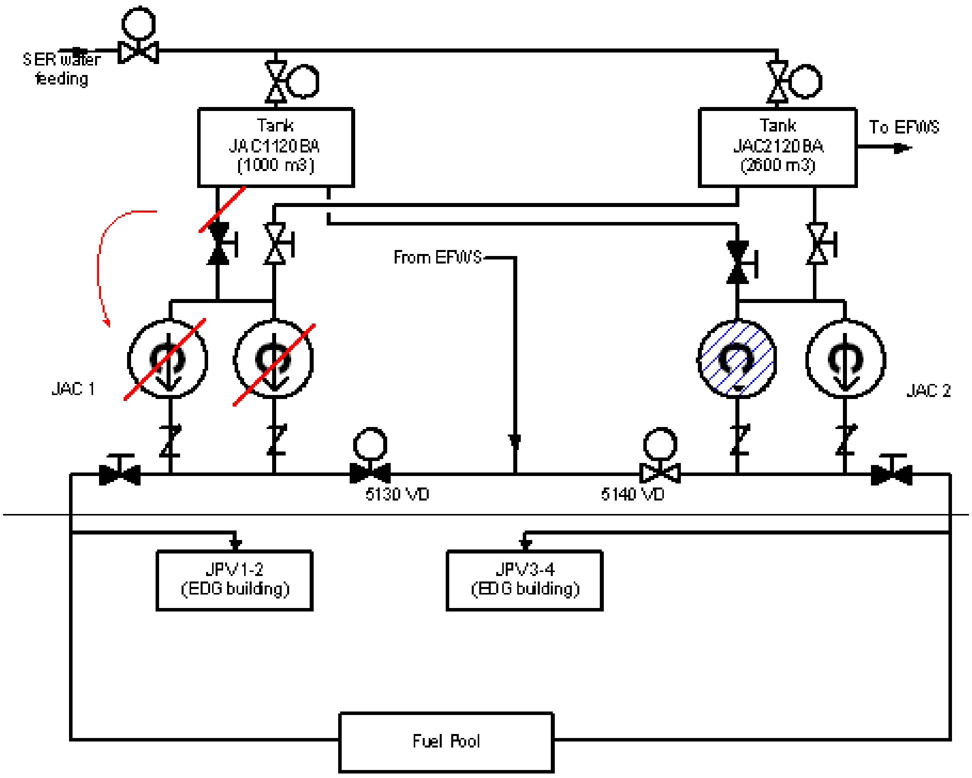


After leak (PSF) isolation,	A	B	C	D	E	MIN	
Number of tanks available:	3	3	4	4	4	3	B: tank-header fully isolated
Number of pumps available:	2	3	2	2	2	2	D: pump-header fully isolated
Number of SG available:	3	3	3	2	2	2	

PASSIVE SINGLE FAILURE

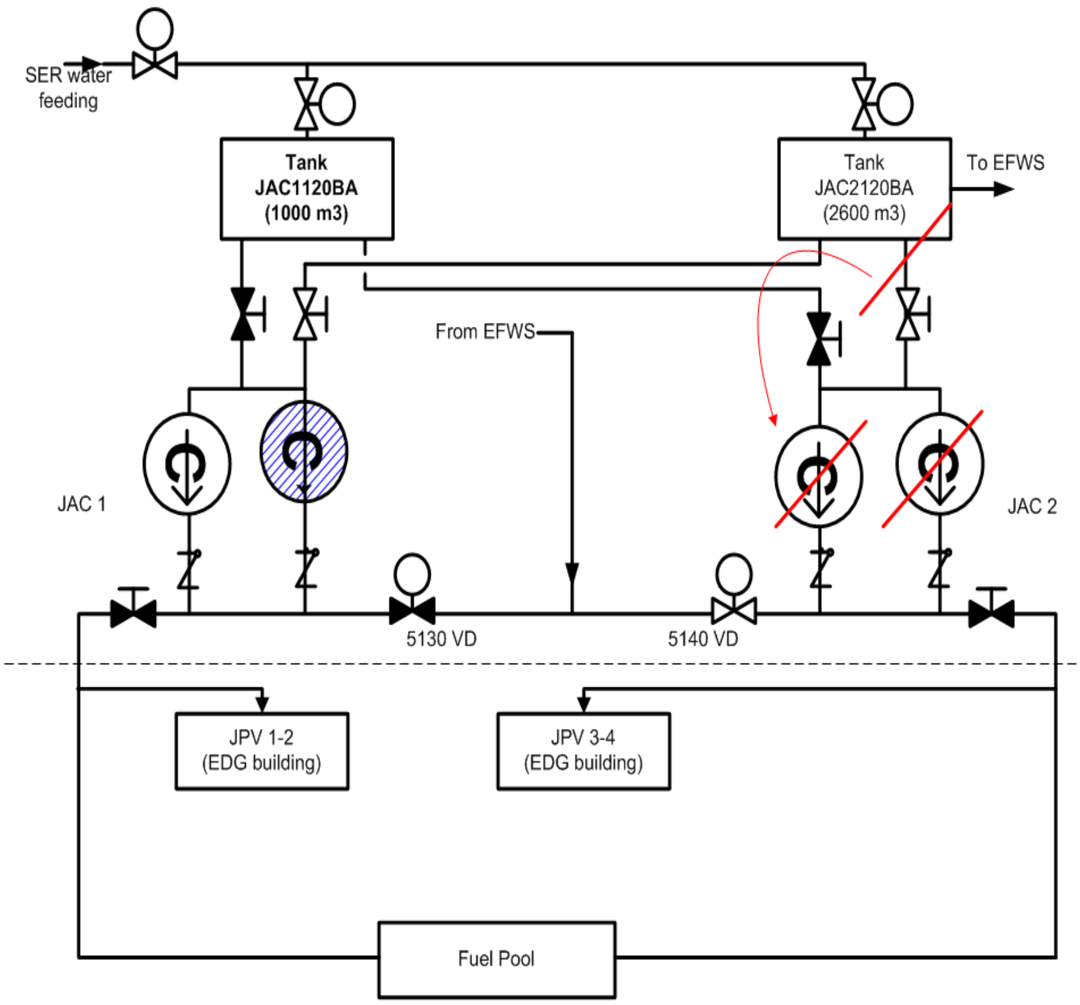
SUB-CHAPTER 14.2 – FIGURE 9

JAC/JPI [NIFPS] Scheme (1/2)



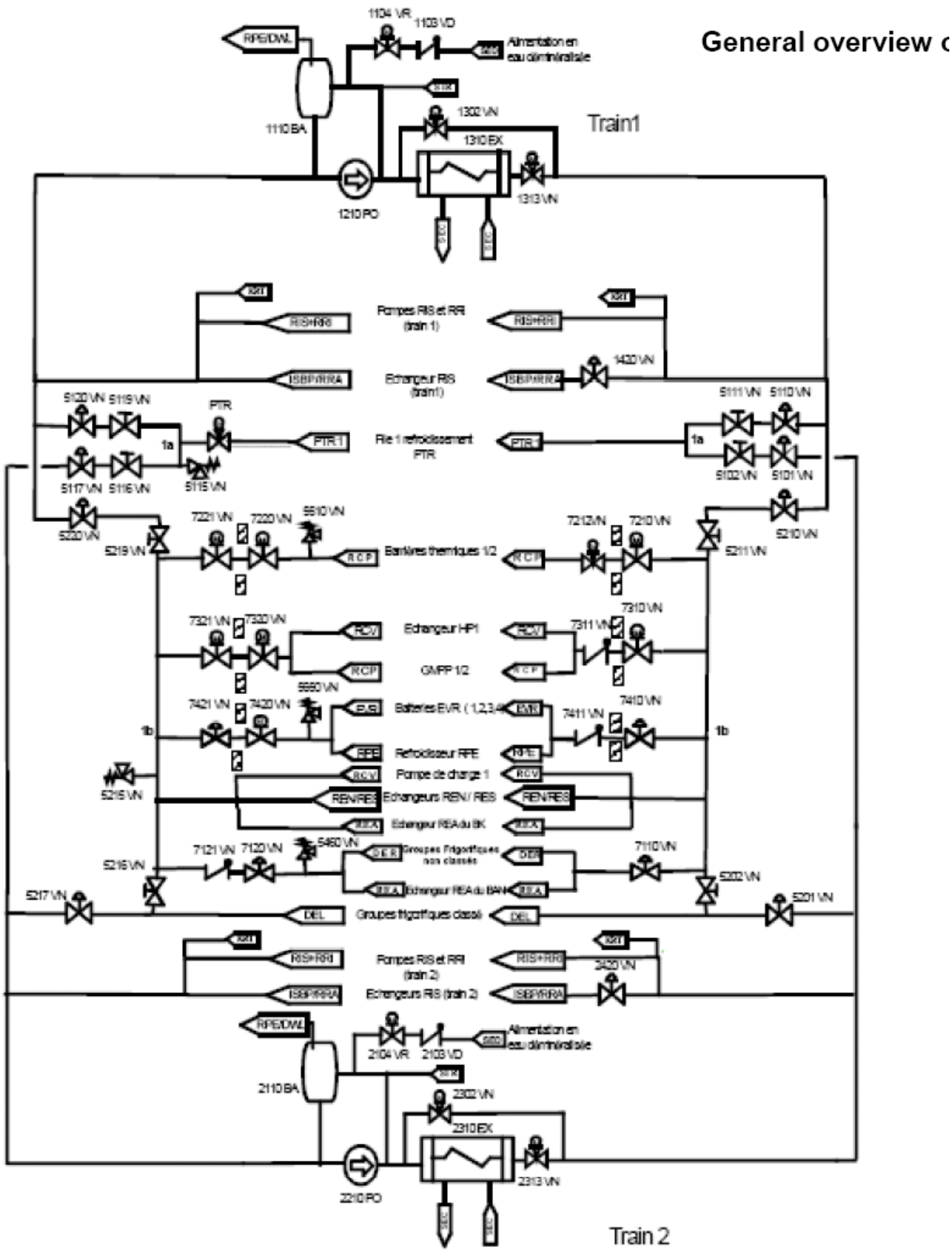
SUB-CHAPTER 14.2 – FIGURE 10

JAC/JPI [NIFPS] Scheme (2/2)



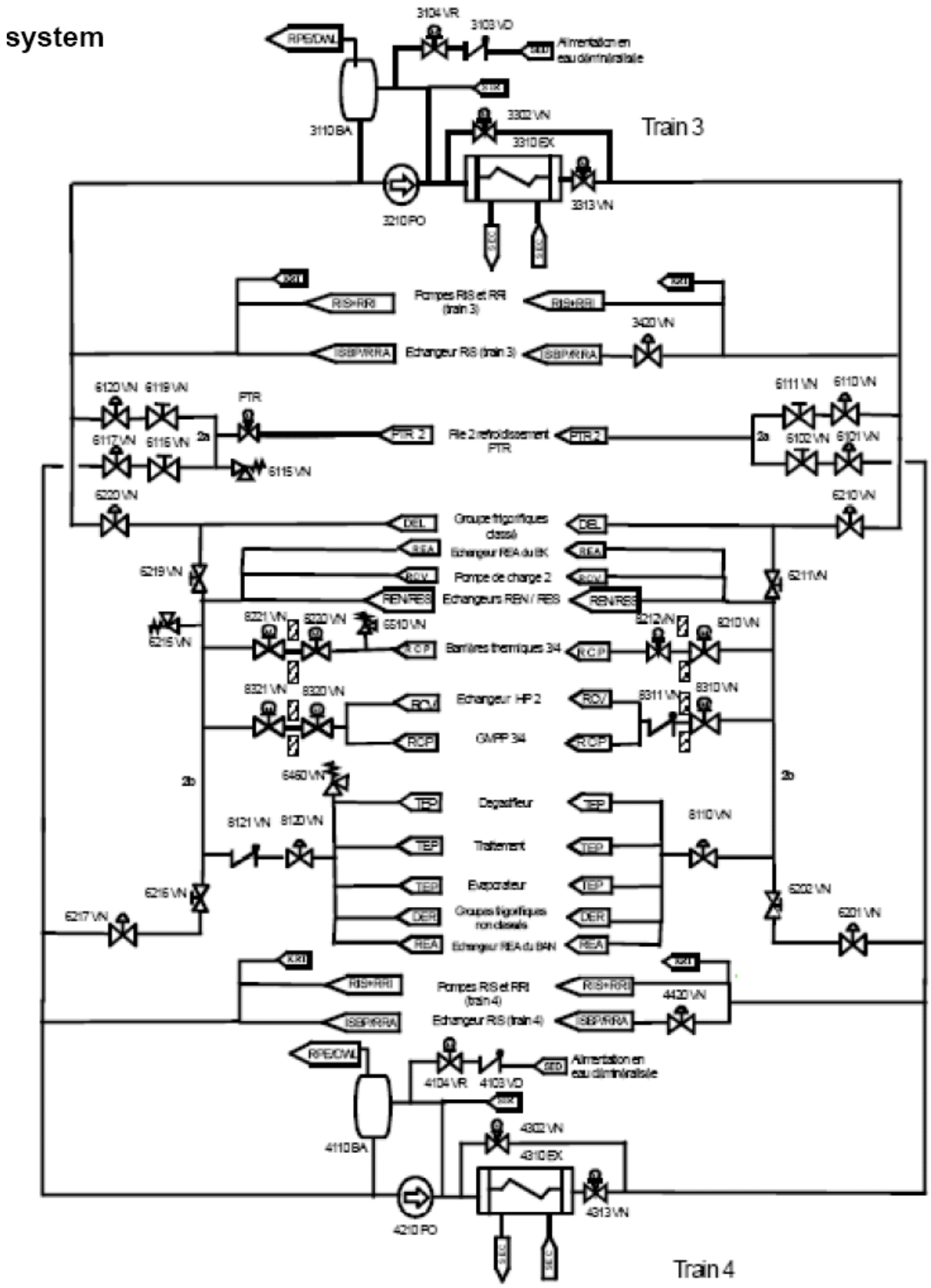
SUB-CHAPTER 14.2 – FIGURE 11

RRI [CCWS] Detailed Scheme – Trains 1 & 2



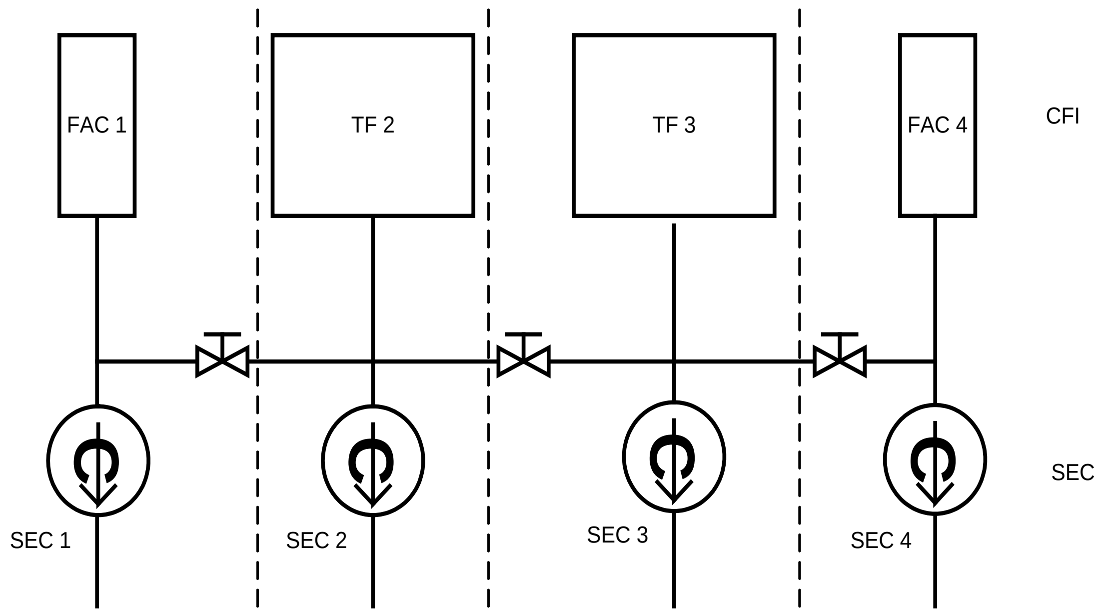
SUB-CHAPTER 14.2 – FIGURE 12

RRI [CCWS] Detailed Scheme – Trains 3 & 4



SUB-CHAPTER 14.2 – FIGURE 13

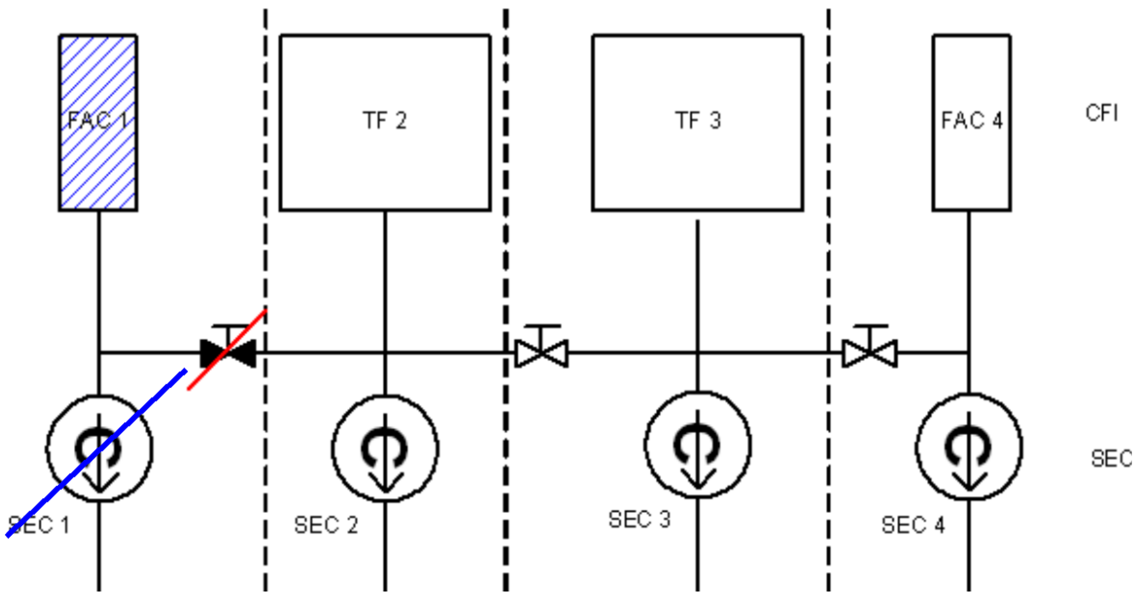
SEC [ESWS] Scheme (1/3)



FAC: Filtre à chain: Chain Screen
TF Tambour filtrant: Rotating Drum Screen

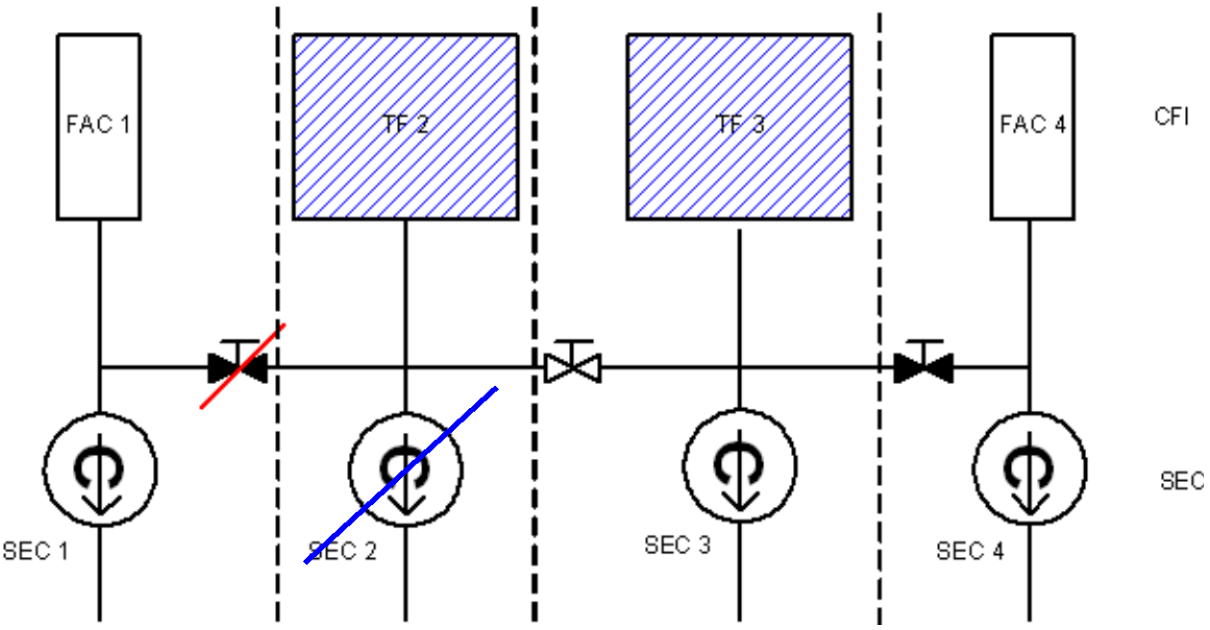
SUB-CHAPTER 14.2 – FIGURE 14

SEC [ESWS] Scheme (2/3)



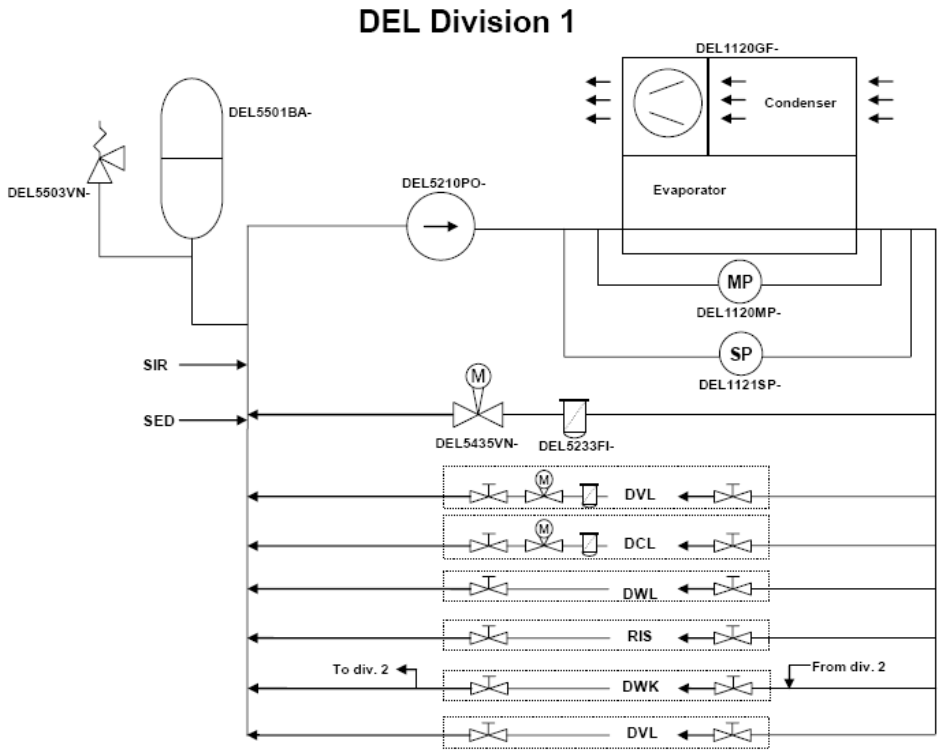
SUB-CHAPTER 14.2 – FIGURE 15

SEC [ESWS] Scheme (3/3)



SUB-CHAPTER 14.2 – FIGURE 16

DEL [SCWS] Detailed Scheme



SUB-CHAPTER 14.2 – REFERENCES

External references are identified within this sub-chapter by the text [Ref-1], [Ref-2], etc at the appropriate point within the sub-chapter. These references are listed here under the heading of the section or sub-section in which they are quoted.

2. OVERALL METHODOLOGY PRESENTATION

2.2. MAIN FEATURES OF THE METHODOLOGY

[Ref-1] Classification of structure systems and components. NEPS-F DC 557 Revision D. AREVA. October 2012. (E)

3. FRONTLINE SYSTEMS ANALYSIS

3.1. SAFETY INJECTION SYSTEM / RESIDUAL HEAT REMOVAL SYSTEM (RIS/RRA [SIS/RHRS)

[Ref-1] System Design Manual – Safety injection system and Residual Heat Removal System – Part 2: System Operation. NESS-F DC 539 Revision A. AREVA. May 2009. (E)

3.2. MAIN STEAM RELIEF TRAIN (VDA [MSRT])

[Ref-1] System Design Manual – Main Steam Relief Train – Part 2: System Operation. NESS-F DC 580 Revision A. AREVA. November 2009. (E)

[Ref-2] System Design Manual – Steam Generator Blowdown System APG P2 - System Operation. SFL-EZS-030046 Revision G. Sofinel. December 2008. (E)

3.3. EXTRA BORATING SYSTEM (RBS [EBS])

[Ref-1] System Design Manual – Extra Boration System – Part 2: System Operation. NESS-F DC 535 Revision A. AREVA. April 2009. (E)

3.4. REACTOR COOLANT SYSTEM (RCP [RCS])

[Ref-1] System Design Manual – Reactor Coolant System – Part 2: System Operation. NESS-F DC 538 Revision A. AREVA. May 2009. (E)

3.5. MAIN STEAM SUPPLY SYSTEM (VVP [MSSS])

[Ref-1] System Design Manual – Main Steam Supply System – Part 2: System Operation. NESS-F DC 578 Revision A. AREVA. November 2009. (E)

3.6. STEAM GENERATOR BLOWDOWN SYSTEM (APG [SGBS])

[Ref-1] System Design Manual – Steam Generator Blowdown System APG P2 - System Operation. SFL-EZS-030046 Revision G. Sofinel. December 2008. (E)

3.7. EMERGENCY FEED WATER SYSTEM ASG [EFWS]

[Ref-1] System Design Manual – Emergency Feedwater System – Part 2: System Operation. SFL-EFMF 2006.829 Revision E1. Sofinel. September 2009. (E)

3.8. FUEL POOL COOLING SYSTEM (PTR [FPCS])

[Ref-1] System Design Manual – Fuel Pool Cooling System – Part 2: System Operation. SFL-EFMF 2006.712 Revision G1. Sofinel. August 2009. (E)

3.9. CLASSIFIED FIRE-FIGHTING WATER PRODUCTION / NUCLEAR ISLAND FIRE-FIGHTING WATER PROTECTION AND DISTRIBUTION (JAC/JPI [NIFPS])

[Ref-1] System Design Manual - Classified fire-fighting water production system – Part 2: System Operation. ETDOIG080015 Revision A1. EDF. August 2009. (E)

[Ref-2] System Design Manual - Fire Fighting Water System of the Nuclear Island (JPI) – Part 2: System Operation. EZH/2007/en/0006 Revision D. EDF. July 2008. (E)

4. SUPPORT SYSTEMS

4.1. COMPONENT COOLING WATER SYSTEM (RRI [CCWS])

[Ref-1] System Design Manual – Component Cooling Water System – Part 2: System Operation. SFL-EFMF 2006.446 Revision F1. Sofinel. August 2009. (E)

4.2. ESSENTIAL SERVICE WATER SYSTEM (SEC [ESWS])

[Ref-1] System Design Manual – Essential Service Water System – Part 2: System Operation. ETDOFC/080069 Revision A1. EDF. September 2009. (E)

4.3. ELECTRICAL BUILDING EMERGENCY CHILLED WATER SYSTEM (DEL [SCWS])

[Ref-1] System Design Manual – Safety Chilled Water System – Part 2: System Operation. SFL-EZL-030004 Revision H. EDF. November 2008. (E)

4.4. HEATING, VENTILATION AND AIR-CONDITIONING (HVAC)

[Ref-1] Safety of Nuclear Power Plants: Design (Requirements for Design). ISSN 1020-525X IAEA Safety Standards Series N° NS-R-1. IAEA. 2000. (E)

5. CONCLUSION

[Ref-1] ALARP demonstration for the design of the pressurizer safety valves regarding the passive single failure. PEPR-F DC 28 Revision A. AREVA. November 2010. (E)

[Ref-2] UK EPR – Main steam isolation valves ALARP assessment regarding functional diversity and single failure criterion. PESS-F DC 27 Revision A. AREVA. November 2010. (E)

SUB-CHAPTER 14.2 – TABLE 4

[Ref-1] ALARP demonstration for the design of the pressurizer safety valves regarding the passive single failure. PEPR-F DC 28 Revision A. AREVA. November 2010. (E)

SUB-CHAPTER 14.2 – TABLE 5

[Ref-1] UK EPR – Main steam isolation valves ALARP assessment regarding functional diversity and single failure criterion. PESS-F DC 27 Revision A. AREVA. November 2010. (E)

SUB-CHAPTER 14.2 – TABLE 10

[Ref-1] ALARP demonstration for the design of the pressurizer safety valves regarding the passive single failure. PEPR-F DC 28 Revision A. AREVA. November 2010. (E)

[Ref-2] UK EPR – Main steam isolation valves ALARP assessment regarding functional diversity and single failure criterion. PESS-F DC 27 Revision A. AREVA. November 2010. (E)

SUB-CHAPTER 14.2 – TABLE 15

[Ref-1] ALARP demonstration for the design of the pressurizer safety valves regarding the passive single failure. PEPR-F DC 28 Revision A. AREVA. November 2010. (E)

[Ref-2] UK EPR – Main steam isolation valves ALARP assessment regarding functional diversity and single failure criterion. PESS-F DC 27 Revision A. AREVA. November 2010. (E)