**Westinghouse UK**
**AP1000® GENERIC DESIGN ASSESSMENT**
**Resolution Plan for GI-AP1000-PSA-01**
**Success Criteria for the Probabilistic Risk Assessment (PSA)**

| MAIN ASSESSMENT AREA | RELATED ASSESSMENT AREA(S) | RESOLUTION PLAN REVISION | GDA ISSUE REVISION |
|---|---|---|---|
| PSA | Fault Studies | 2 | 0 |

| | |
|---|---|
| **GDA ISSUE:** | The **AP1000®** PSA should be supported by design specific analysis of sufficient detail and scope and fully traceable.<br>During our assessment we have compiled evidence that the Success Criteria for the **AP1000** PSA does not meet our expectations. Deficiencies have been found in the following areas:<br>• Demonstration of overall success of sequences.<br>• Use of AP600 analysis without visible justification or sufficient evidence of applicability.<br>• Coverage of faults.<br>• Justification of time windows for operator actions.<br>• Traceability of the analysis. |
| **ACTION: GI-AP1000-PSA-01.A1** | Westinghouse should provide the procedure (Guidebook) established to guide the development of success criteria for the **AP1000** PSA.<br>The guidebook should provide clear information on:<br>• The methods to be used for the derivation of the success criteria.<br>• The code/s to be used for derivation of the success criteria including how the analysis should deal with the limitations of the code/s.<br>• Clear definition of the meaning of "success".<br>• How the operator time windows will be evaluated.<br>• How the success criteria analyses will be documented.<br>With agreement from the Regulator this action may be completed by alternative means. |
| **ACTION: GI-AP1000-PSA-01.A2** | Westinghouse should provide the **AP1000** Input deck/s (parameter file/s) for the code/s to be used.<br>With agreement from the Regulator this action may be completed by alternative means. |
| **ACTION: GI-AP1000-PSA-01.A3** | Westinghouse should provide a complete list of Initiating Events (IEs) correctly grouped, details of the success sequences & event tree headings to be evaluated including a demonstration that the analysis (both thermal-hydraulic and neutronics) is sufficient to support the |

| | |
|---|---|
| | success criteria for all the accident sequences in the **AP1000** PSA.<br>The review of the **AP1000** PSA conducted in GDA identified a number of Initiating Events missing from the PSA and a number of IEs incorrectly grouped. In addition, the Risk Gap Analysis undertaken by ONR's PSA team in the framework of GDA has concluded that the missing IEs could have an important contribution to the **AP1000** plant risk. In order to properly address the success criteria GDA Issue and to ensure completeness, Westinghouse should include in the success criteria evaluations the missing initiating events as appropriate and should also show that the IE grouping is correct for the purpose of success criteria evaluation.<br>With agreement from the Regulator this action may be completed by alternative means. |
| **ACTION: GI-AP1000-PSA-01.A4** | Westinghouse should provide the success criteria analyses and results for Loss of Coolant Accidents (LOCA).<br>• The sequence assumptions should be justified and clearly documented.<br>• Time-lines should be provided with clear link to relevant procedures, clues for operator actuation etc.<br>• A demonstration should be included that sufficient analysis has been performed to cover all the variety of LOCAs in the PSA (ie, LOCAs of different sizes and in different locations).<br>• The delineation of time windows for operator actuation has to be clearly documented.<br>• The minimum equipment requirement and performance for success should be clearly documented.<br>• Any conservatisms in the analysis should be described together with a justification that they are not important enough to bias the results of the analysis.<br>With agreement from the Regulator this action may be completed by alternative means. |
| **ACTION: GI-AP1000-PSA-01.A5** | Westinghouse should provide the success criteria analyses and results for Transients.<br>• The sequence assumptions should be justified and clearly documented.<br>• Time-lines should be provided with clear link to relevant procedures, clues for operator actuation etc.<br>• A demonstration should be included that sufficient analysis has been performed to cover all the |

| | |
|---|---|
| | variety of (intact primary and secondary circuit) transients in the PSA including the transients currently missing from the PSA which were identified during ONR's GDA review.<br>• The delineation of time windows for operator actuation has to be clearly documented.<br>• The minimum equipment requirement and performance for success should be clearly documented.<br>• Any conservatisms in the analysis should be described together with a justification that they are not important enough to bias the results of the analysis.<br>With agreement from the Regulator this action may be completed by alternative means. |
| **ACTION: GI-AP1000-PSA-01.A6** | Westinghouse should provide the success criteria analyses and results for Steam Line Breaks.<br>• The sequence assumptions should be justified and clearly documented.<br>• Time-lines should be provided with clear link to relevant procedures, clues for operator actuation etc.<br>• A demonstration should be included that sufficient analysis (both thermal-hydraulic and neutronics) has been performed to cover all the variety of steam line breaks in the PSA (e.g. steam line breaks downstream of the MSIVs, upstream of the MSIVs both inside and outside containment, spurious opening of valves in the secondary circuit, double steam line breaks in the containment, feed water line breaks grouped together with steam line breaks in the PSA, feed water line breaks occurring as a consequence of steam line breaks, etc).<br>• The delineation of time windows for operator actuation has to be clearly documented.<br>• The minimum equipment requirement and performance for success should be clearly documented.<br>• Any conservatisms in the analysis should be described together with a justification that they are not important enough to bias the results of the analysis.<br>With agreement from the Regulator this action may be completed by alternative means. |
| **ACTION: GI-AP1000-PSA-01.A7** | Westinghouse should provide the success criteria analyses and results for Steam Generator Tube Ruptures (SGTR). |

| | |
|---|---|
| | • The sequence assumptions should be justified and clearly documented.<br>• Time-lines should be provided with clear link to relevant procedures, clues for operator actuation etc.<br>• A demonstration should be included that sufficient analysis (both thermal-hydraulic and neutronics) has been performed to cover all the variety of SGTRs in the PSA (including consequential SGTRs).<br>• The delineation of time windows for operator actuation has to be clearly documented.<br>• The minimum equipment requirement and performance for success should be clearly documented.<br>• Any conservatisms in the analysis should be described together with a justification that they are not important enough to bias the results of the analysis.<br>With agreement from the Regulator this action may be completed by alternative means. |
| **ACTION: GI-AP1000-PSA-01.A8** | Westinghouse should provide the success criteria analyses and results for Anticipated Transients Without SCRAM (ATWS).<br>• The sequence assumptions should be justified and clearly documented.<br>• Time-lines should be provided with clear link to relevant procedures, clues for operator actuation etc.<br>• A demonstration should be included that sufficient analysis (both thermal-hydraulic and neutronics) has been performed to cover all the variety of ATWS in the PSA.<br>• The delineation of time windows for operator actuation has to be clearly documented.<br>• The minimum equipment requirement and performance for success should be clearly documented.<br>• Any conservatisms in the analysis should be described together with a justification that they are not important enough to bias the results of the analysis.<br>With agreement from the Regulator this action may be completed by alternative means. |
| **ACTION: GI-AP1000-PSA-01.A9** | Westinghouse should develop a Gap Analysis to evaluate the implications of the new analysis on the **AP1000** Core Damage Frequency (CDF) and Large Release Frequency (LRF) (including development and quantification of new |

| | |
|---|---|
| | and modified event trees as necessary).<br>With agreement from the Regulator this action may be completed by alternative means. |
| **ACTION: GI-AP1000-PSA-01.A10** | Westinghouse should complete the documentation and provide a standalone document compiling all the PSA Success Criteria Analysis and Gap Analysis performed accompanied by the supporting references.<br>With agreement from the Regulator this action may be completed by alternative means. |
| **RELEVANT REFERENCE DOCUMENTATION RELATED TO GDA ISSUE** | |
| **Technical Queries** | |
| **Regulatory Observations** | |
| **Other Documentation** | |

| **Scope of work:** |
|---|
| The success criteria to support the **AP1000** PSA are based largely on runs made on the AP600 plant. The event trees are based upon accident progression of the AP600 plant using expert opinion and AP600 ERGs. The **AP1000** PSA needs to be based upon success criteria runs performed specifically for the **AP1000** plant and current operating procedures to assure proper representation of **AP1000** plant accident mitigation. This work needs to be properly documented along with the justification of the time windows for operation actions to provide traceability. All plant faults need to be properly represented in a systematic fashion to identify the PSA initiating events. |

| **Description of work:** |
|---|
| The Level 1 and Level 2 internal events PSA development for each of the initiating events will consist of tasks identified in the Accident and Success Criteria Guidebook. A high level description of each task is provided below. Task 5 is not explicitly contained in the Guidebook, but is included here for completeness. Shutdown faults will be reviewed as agreed upon and outside of the guidebook.<br><br>***Task 1: Define Event Tree (ET) Initiators -*** The plant model consists of scenarios that begin with initiating events (IE). For **AP1000** plants, the IEs are defined in accordance with the IE Guidebook. This task will contain descriptions of initiators and will provide a description of specific initiators that are grouped together as a more generic initiator. Each defined initiator or initiator group is the start of the event tree.<br><br>Initiating event analysis is carried out in the following sequence of steps:<br><br>– Identification of Candidate Events<br><br>– Grouping of Candidate Initiating Events<br><br>– Quantification of Initiating Event Frequency. |

In addition to reviewing operating experience a systematic evaluation of plant systems is performed to identify IEs resulting from equipment failures. To satisfy this requirement a systematic review is performed for all the **AP1000** plant systems to assess the possibility of an IE occurring due to a failure of the system. The systematic review will look at Mode 1, Full Power Normal Operation for all **AP1000** plant systems and consider key plant equipment for possible Initiating Event Failure Modes, including spurious actuations of equipment. Additionally, the Protection and Monitoring System Reactor Trip and Engineered Safety Feature functions will be reviewed to identify **AP1000** plant specific Initiating Events.

For Support Systems identified with a possible Initiating Event failure mode, the systems analysis will develop Support System Initiating Event Fault Trees which will model individual components of the system and account for all component failure combinations which will result in a loss of that support system.

Interfacing system Loss of Coolant Accidents (ISLOCAs) will be analysed in a specific notebook. ISLOCA analysis can be broken down into two tasks. The first task is the identification of potential ISLOCA pathways and the second task is to quantify the initiating event frequency for each non screened path from task one. The methodology outlined in this section is consistent with the guidance provided in WCAP-17154-P.

***Task 2: Develop ETs from IE Responses -*** Once initiators are defined, the ETs are developed from thermal hydraulic analyses of the plant response to the initiator or most restrictive initiator in an initiator group. The ETs will also include operator actions (both success and failure) directed from Emergency Operating Procedures (EOP) and/or other applicable procedures. Operator actions from the procedures are defined with an ET top. This ensures that the ET development is sequentially consistent with the features, procedures and operating philosophy of the plant.

The tops are combined to form an ET in a logical and time sequential order. ET diagrams are built using the Event Tree features of the CAFTA software system. The top branch of an event tree node is referred to as the success of the node and the bottom branch is referred to as the failure of the node.

Each ET top (and the systems, components, and/or operator actions included in that top) must meet one or more of the following functional SC conditions: RCS reactivity control, RCS pressure control, RCS inventory control, decay heat removal, or containment integrity. The tops must identify features that are necessary to satisfy success of that top. The collective tops for any ET path will identify the collective features that are necessary to reach a safe, stable state and result in no core damage. Each ET top may represent multiple system tops; but at a minimum, the ET top must contain at least one mitigating function (e.g. system top, operator action, etc.). The system tops must also consider dependencies which can impact the ability of the mitigating systems to operate and function effectively.

***Task 3: Determination of Success Criteria (SC) -*** The SC is determined for the ET top node paths; it is defined as the minimum requirements per top event that fulfill the basic function (e.g. reactivity control, inventory control, etc.) which prevents core damage. The minimum requirements could be any one or combination of the following: systems

(ADS, CVS, RNS, etc.), structures (containment, etc.), components (MOVs, AOVs, HXs, etc.), and/or human actions (completed operator actions within the specified time window).

The MAAP code will be used as the primary code to support success criteria. Westinghouse will provide a copy of the **AP1000** plant MAAP parameter file. Other codes like LOFTRAN and CENTs may also be used to support success criteria. Documentation of the results will be provided for these codes.

A detailed section will be included in the SC notebook which includes the T/H analysis and background information to support the SC including the operator action timing. Accident sequences will use a minimum mission time of 24-hours, unless a safe, stable plant state cannot be reached in that time period. For sequences where a stable condition would not be achieved in the 24-hours, the mission time will be extended until a safe, stable plant state can be reached.

Other points to consider in the development of the **AP1000** SC:

- The success criteria for operator actions must only consider the time from the cue for the operator action according to the procedures until the latest time that the operator action can still be successful as predicted by thermal hydraulic analyses.
- Success criteria for operator actions may be dependent on the available equipment.
- Success criteria may consider the most limiting success for preceding top events.

***Task 4: Determination of Plant Damage States (PDS) and Quantification*** - The PDSs are core damage paths as defined by the ET logic with a specific plant condition that occurs during the core damage accident scenario (e.g. availability of electric power, RCS pressure, secondary side SG inventory, containment isolation, etc.). The PDSs will be translated into the Level 2 model for both the containment event trees and Level 2 fault tree model. The AS notebook will outline the conditions for each PDS and the PDS assigned to each core damage path. If the ET logic path does not result in core damage, a PDS is not assigned.

Since significant work has been done to the Internal Events PSA for European and US customers please note that the Level 1 and Level 2 quantification will also include updates to the following supporting analyses:

- Data Analysis
- Human Reliability Analysis
- Level 2 Success Criteria and Accident Sequence
- Systems Analysis

A qualitative assessment of unincorporated Class 1 and 2 design changes will be provided for their qualitative impact to the Internal Events PSA. This deliverable will

provide a comparison of the Internal Events PSA to the UK GDA design reference point. On a case by case basis, design changes may be requested to be reviewed on a quantitative basis. A systematic approach will be used to define which design changes will be quantitatively assessed.

***Task 5: Documentation of PSA Success Criteria Analysis and Gap Analysis –*** An **AP1000** plant Calculation Note will be provided for the IE analysis, AS analysis, SC analysis, Level 1 Quantification analysis, and Level 2 Quantification analysis. A high level Gap Analysis between the previously provided PCSR and the updated PSA will be provided. This report will also provide a road map to the compliance of all the PSA Success Criteria Analysis to the documentation.

A mapping of the ONR Action Items for this Issue to the above planned success criteria tasks is included below:

- GI-**AP1000**-PSA-01.A1 - Corresponds to the updated Accident Sequence and Success Criteria Guidebook.
- GI-**AP1000**-PSA-01.A2 - Corresponds to Tasks 3 & 4.
- GI-**AP1000**-PSA-01.A3 – Corresponds to Tasks 1, 2 & 3.
- GI-**AP1000**-PSA-01.A4 – Corresponds to Tasks 2, 3 and 4 for Loss of Coolant Accidents (LOCA)
- GI-**AP1000**-PSA-01.A5 – Corresponds to Tasks 2, 3 and 4 for Transients
- GI-**AP1000**-PSA-01.A6 – Corresponds to Tasks 2, 3 and 4 for Steam Line Breaks
- GI-**AP1000**-PSA-01.A7 – Corresponds to Tasks 2, 3 and 4 for Steam Generator Tube Ruptures (SGTR)
- GI-**AP1000**-PSA-01.A8 – Corresponds to Tasks 2, 3 and 4 for Anticipated Transients Without SCRAM (ATWS)
- GI-**AP1000**-PSA-01.A9 – Corresponds to Task 5
- GI-**AP1000**-PSA-01.A10 - Broad action, with elements of Tasks 1-4

**Schedule/ programme milestones:**

This effort will result in 10 deliverables:

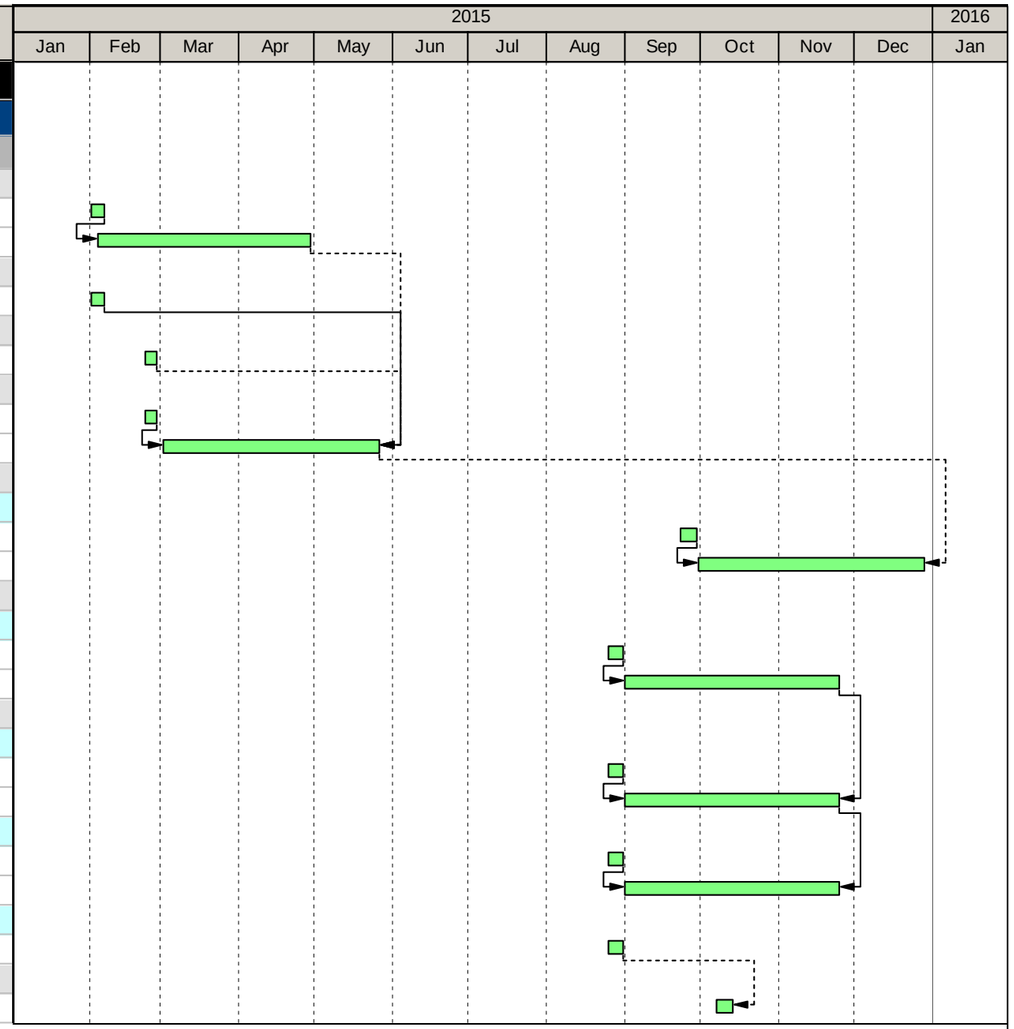
1. **AP1000** Plant PRA Accident Sequence and Success Criteria Guidebook
2. **AP1000** Plant At-Power Internal Events PRA, Initiating Event Analysis Notebook
3. **AP1000** Plant At-Power Internal Events PRA, Interfacing System Loss of Coolant Accident Initiating Event Analysis Notebook

4. **AP1000** Plant At-Power Internal Events PRA, Accident Sequence Analysis Notebook
5. **AP1000** Plant At-Power Internal Events PRA, Success Criteria Analysis Notebook
6. **AP1000** Plant At-Power Internal Events PRA, Quantification Notebook
7. **AP1000** Plant At-Power Internal Events PRA, Level 2 Quantification Results Notebook
8. GDA PSA Road Map and Gap Analysis Report
9. MAAP Parameter File Calculation Note
10. Qualitative Assessment of Class 1 and 2 Design Changes

Deliverables associated with shutdown faults will be agreed upon at a later date.

Please see the following page for the schedule.

| # | Activity Name |
|---|---|
| 1 | **UK Generic Design Assessment (GDA) Resolution Plans (51)** |
| 2 | **PROBALISTIC SAFETY ANALYSIS (PSA)** |
| 3 | **PS.01 Success Criteria for PSA-Resolution Plan** |
| 4 | **PS.01 Success Criteria/Accident Sequence Guidebook** |
| 5 | SC and AS Guidebook Revision-Submit to ONR |
| 6 | SC and AS Guidebook Revision-ONR Review of Submittal |
| 7 | **PS.01 MAAP Parameter File** |
| 8 | MAAP Parameter File-Submit to ONR |
| 9 | **PS.01 ISLOCA Analysis** |
| 10 | ISLOCA IE Analysis Notebook-Submit to ONR |
| 11 | **PS.01 Initiating Event Notebook** |
| 12 | IE Notebook Revision-Submit to ONR |
| 13 | IE Notebook Revision-ONR Review of Submittal |
| 14 | **PS.01 Accident Sequence Notebook** |
| 15 | **PS.01 Overall Accident Sequence Notebook - ONR Delivery** |
| 16 | Accident Sequence Notebook-Submit to ONR |
| 17 | Accident Sequence Notebook-ONR Review of Submittal |
| 18 | **PS.01 Success Criteria Notebook** |
| 19 | **PS.01 Overall Success Criteria Notebook - ONR Delivery** |
| 20 | Success Criteria Notebook-Submit to ONR |
| 21 | Success Criteria Notebook-ONR Review of Submittal |
| 22 | **PS.01 Quantification** |
| 23 | **PS.01 Level 1 Quantification and Notebook** |
| 24 | Level 1 Quantification Notebook-Submit to ONR |
| 25 | Level 1 Quantification Notebook-ONR Review of Submittal |
| 26 | **PS.01 Level 2 Quantification and Notebook** |
| 27 | Level 2 Quantification Notebook-Submit to ONR |
| 28 | Level 2 Quantification Notebook-ONR Review of Submittal |
| 29 | **PS.01 Qualitative Assessment of Class 1 & 2 Design Changes** |
| 30 | Qualitative Assessment of Class 1 & 2 Design Changes-Submit to ONR |
| 31 | **PS.01 Gap Assessment** |
| 32 | Gap Assessment-Submit to ONR |



| **Methodology:** |
| --- |
| The MAAP code will be the primary code to support success criteria analysis.<br><br>The event trees as well as the Level 1 and Level 2 quantification analysis will be performed using the CAFTA software. |

| **Justification of adequacy:** |
| --- |
| The Accident Sequence and the Success Criteria documentation shall be reflective of the **AP1000** plant designed as of an appropriate revision of the DCD and to follow the requirements of the ASME PSA Standard to the extent achievable by a pre-operational plant in which final design information may not be available. |

| **Impact assessment:** |
| --- |
| The Pre-Construction Safety Report will be updated as appropriate. |