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	1	0

GDA ISSUE:	The **AP1000**$^{®}$ PSA should be supported by design specific analysis of sufficient detail and scope and fully traceable. 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: • Demonstration of overall success of sequences. • Use of AP600 analysis without visible justification or sufficient evidence of applicability. • Coverage of faults. • Justification of time windows for operator actions. • 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. The guidebook should provide clear information on: • The methods to be used for the derivation of the success criteria. • 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. • Clear definition of the meaning of “success”. • How the operator time windows will be evaluated. • How the success criteria analyses will be documented. 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. 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. 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. 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). • The sequence assumptions should be justified and clearly documented. • Time-lines should be provided with clear link to relevant procedures, clues for operator actuation etc. • 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). • The delineation of time windows for operator actuation has to be clearly documented. • The minimum equipment requirement and performance for success should be clearly documented. • 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. 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. • The sequence assumptions should be justified and clearly documented. • Time-lines should be provided with clear link to relevant procedures, clues for operator actuation etc. • 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. • The delineation of time windows for operator actuation has to be clearly documented. • The minimum equipment requirement and performance for success should be clearly documented. • 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. 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. • The sequence assumptions should be justified and clearly documented. • Time-lines should be provided with clear link to relevant procedures, clues for operator actuation etc. • 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). • The delineation of time windows for operator actuation has to be clearly documented. • The minimum equipment requirement and performance for success should be clearly documented. • 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. 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. • Time-lines should be provided with clear link to relevant procedures, clues for operator actuation etc. • 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). • The delineation of time windows for operator actuation has to be clearly documented. • The minimum equipment requirement and performance for success should be clearly documented. • 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. 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). • The sequence assumptions should be justified and clearly documented. • Time-lines should be provided with clear link to relevant procedures, clues for operator actuation etc. • 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. • The delineation of time windows for operator actuation has to be clearly documented. • The minimum equipment requirement and performance for success should be clearly documented. • 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. 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). 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. 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 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. Tasks 5 and 6 are not explicitly contained in the Guidebook, but are included here for completeness.

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.

Initiating event analysis is carried out in the following sequence of steps:

- Identification of Candidate Events
- Grouping of Candidate Initiating Events
- 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 Failure Modes and Effects Analysis (FMEA) is performed for of all the **AP1000** plant operating system at power and all front line PSA systems. Failure modes and effects analysis is a bottom-up approach to identifying initiating events. The approach consists of evaluating the impact of major component failures on frontline safety and support system failure modes, and ultimately the impact on normal plant operation. This approach is especially useful for identifying important common cause initiating events in support systems that simultaneously impact other plant systems. The FMEA should identify if systems have different routine system alignments. The FMEA should also identify if the initiator can impact both units at dual unit site (e.g., Loss Offsite Power or Loss of Service Water).

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 following analysis tools will be used to determine the SC:

- MAAP4 – valid for transients, quasi-steady state portions of the LLOCA, MLOCA, SLOCA, SGTR and SBO scenarios
- MAAP5 or LOFTRAN – valid for ATWS scenarios and SLB
- MAAP4, MAAP5 or GOTHIC – valid for containment integrity scenarios
- WCOBRA-TRAC –valid for the initial dynamic phase of large-break LOCA scenarios

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 have a 24-hour mission time, unless a safe, stable plant state cannot be reached in that time period. In these cases, 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) - 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.

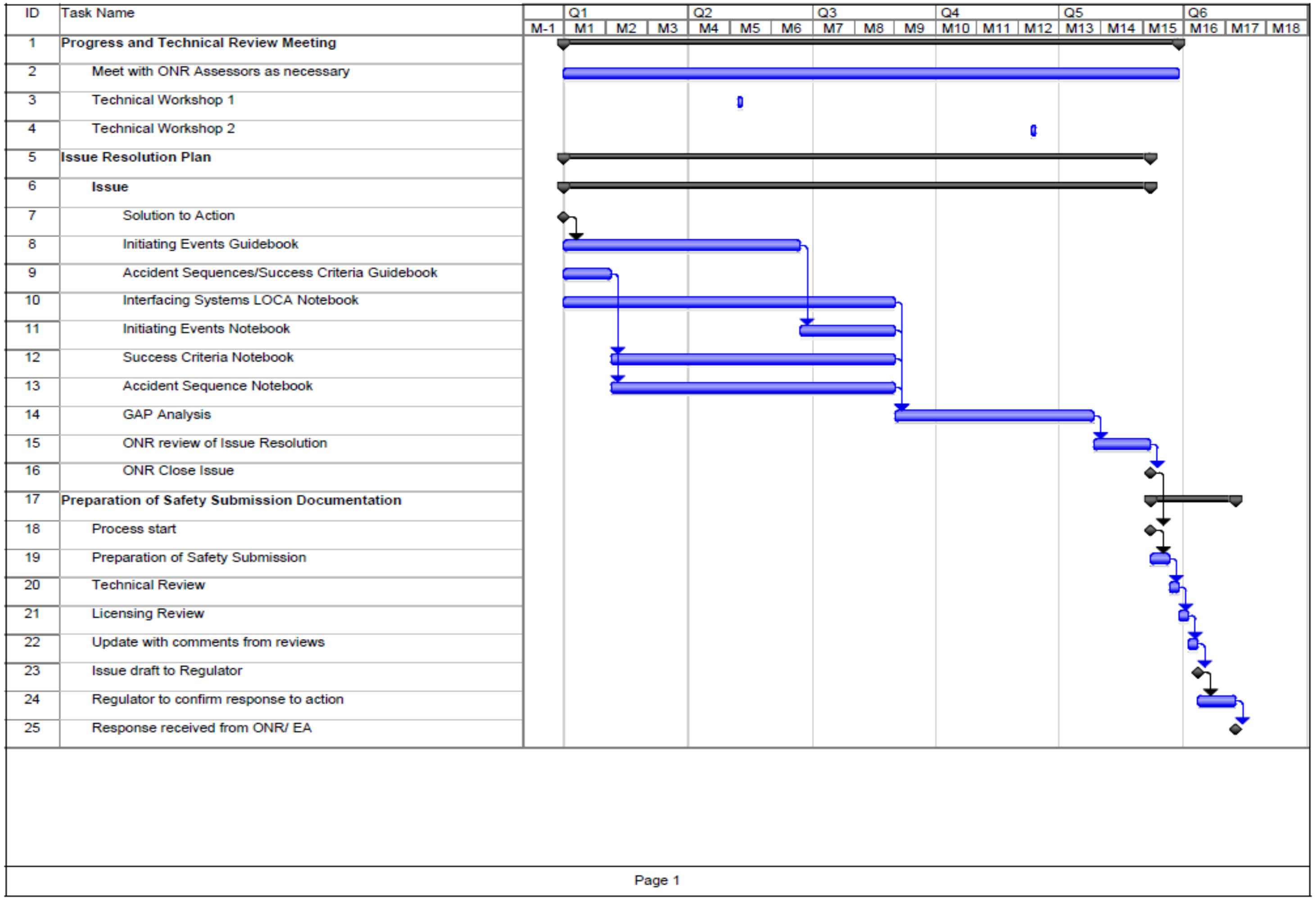
Task 5: Documentation of PSA Success Criteria Analysis and Gap Analysis – This effort will be documented in an **AP1000** plant Calculation Note compiling all the PSA Success Criteria Analysis performed accompanied by the supporting references.

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 - This action item is already complete.
- 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:

Because all Resolution Plan start dates are subject to future contract placements, dates are presently undefined; therefore schedule dates have been anonymised for consistency. Actual dates will be inserted when contracts are placed.



ID	Task Name
1	**Progress and Technical Review Meeting**
2	Meet with ONR Assessors as necessary
3	Technical Workshop 1
4	Technical Workshop 2
5	**Issue Resolution Plan**
6	**Issue**
7	Solution to Action
8	Initiating Events Guidebook
9	Accident Sequences/Success Criteria Guidebook
10	Interfacing Systems LOCA Notebook
11	Initiating Events Notebook
12	Success Criteria Notebook
13	Accident Sequence Notebook
14	GAP Analysis
15	ONR review of Issue Resolution
16	ONR Close Issue
17	**Preparation of Safety Submission Documentation**
18	Process start
19	Preparation of Safety Submission
20	Technical Review
21	Licensing Review
22	Update with comments from reviews
23	Issue draft to Regulator
24	Regulator to confirm response to action
25	Response received from ONR/ EA

Methodology:

The following analysis tools will be used to determine the SC;

- MAAP4 – valid for transients, quasi-steady state portions of the LLOCA, MLOCA, SLOCA and SBO scenarios
- MAAP5 or LOFTRAN- valid for ATWS scenarios
- MAAP4, MAAP5, or GOTHIC – valid for containment integrity scenarios
- WCOBRA-TRAC – valid for the initial dynamic phase of large break LOCA scenarios

The event trees as well as the GAP 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 Rev 17 of the DCD and meet the requirements (Capability Category II or higher) of the ASME PRA Standard.

Impact assessment:

None are anticipated at this time. However, a placeholder has been placed in the attached schedule in the event the Resolution Plan effort results in updates to the PCSR.