DETERMINISTIC SAFETY ASSESSMENT AND DESIGN BASIS ACCIDENT ANALYSIS

The Deterministic Safety Assessment (*DSA*) comprises a combination of Design Basis Accident Analysis (*DBAA*), Beyond Design Basis Accident Analysis (*BDBAA*) and Severe Accident Analysis (*SAA*) which provides a demonstration of the integrity of a plant, utility or facility through sufficient Defence in Depth (*DiD*). The purpose of DSA is to demonstrate the fault tolerance of the design, the effectiveness of the safety measures and to demonstrate that the risks associated with the design and operation are As Low As Reasonably Practicable (*ALARP*). DSA determines initiating faults and hazards that are reasonably foreseeable, justifies fault sequences that follow the faults and hazards, and assesses the design of the claimed safety systems against engineering safety principles.

Design Basis Accident Analysis

DBAA is focused on the key safeguards for those initiating faults that are most significant in terms of frequency and unmitigated potential consequences, consistent with DiD principles. BDBAA is for fault sequences that are beyond the design basis, which aims to demonstrate sufficient safety margins within the DBAA and ensure that a safeguard does not fail just beyond the design basis i.e. there is suitable withstand to cliff-edge effects. The SAA is a sub-set of BDBAA which considers significant but unlikely accidents and provides information on their progression, both within the utility or facility but also beyond the site boundary. This is used, for example, to inform emergency measures that may be taken to limit received radiation doses. SAA is particularly important in assessing the overall impact of the site in terms of the risks of major accidents that could lead to significant off-site consequence.

The Office for Nuclear Regulation (*ONR*) Safety Assessment Principles (*SAPs*) define the design basis as:

'The range of conditions and events that should be explicitly taken into account in the design of the facility, according to established criteria, such that the facility can withstand them without exceeding authorised limits by the planned operation of safety systems'.

There are two distinct approaches to DSA; the traditional (barrier) approach which is the fundamental basis of extant reactor plant safety justifications, and the function approach which is now deemed best practice.

The traditional approach considers the sources of radioactive material and conservatively justifies the physical barriers that prevent release of the material to workers or public. For a reactor plant, this includes the substantiation of the fuel cladding, coolant circuit and the containment. Although the traditional barrier approach remains the fundamental basis of many extant safety justifications, this approach is not considered current best practice and will not be considered in any further detail within this guidance.

The best practice (functional) methodology builds on this and includes the International Atomic Energy Agency (*IAEA*) approach to the control of safety functions. This approach emphasises the audit trail from a comprehensive Hazard Identification (HAZID), through to a Fault Schedule (*FS*), and then deterministic assessment, and Probabilistic Safety Assessment (*PSA*). It requires all elements of Systems, Structures and Components (*SSCs*) that form either the duty system or the DiD protective / mitigating safety measures to be fully defined.

DiD is demonstrated by making claims against various barriers which inhibit the fault sequence from progressing from an initiating event to its safety consequence. The concept is applied to all safety-related activities to ensure such activities are subject to independent layers of provision, such that if a failure was to occur, it would be detected and compensated/corrected for through appropriate measures.

DiD can be visually represented by the bow tie diagram in Figure 1.

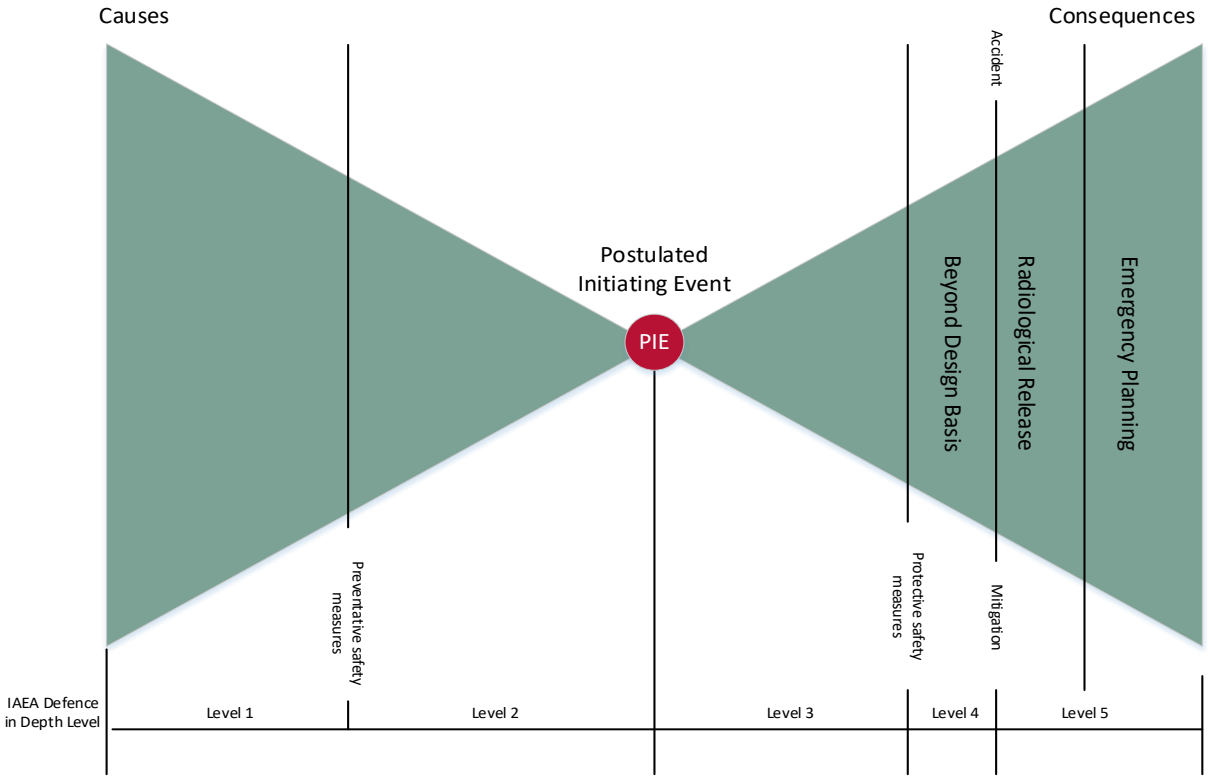

Figure 1: Defence in Depth Diagram.

The Postulated Initiating Event (*PIE*) is the point in the fault sequence at which normal operation and planned control of the safety function is lost. If nothing was done to rectify the situation the fault sequence would escalate, leading to radiation exposure of individuals. Preventative safety measures should be in place to stop initiating faults or hazards from affecting the duty system and leading to a PIE. The Preventative safety measures influence the magnitude and frequency of the PIE. Protective safety measures can stop the fault sequence from progressing further after the loss of the duty system, by providing an alternative means of maintaining the safety function. In the scenario that the duty, preventative and protective safety measures all fail, mitigating safety measures such as containment and / or personnel evacuation can be implemented to limit any radiological effects.

The major advantages of a DSA process that follows best practice are:

- An improved understanding of the key safety issues associated with the plant and the associated protection systems.

- Consistency in approach to safety cases in terms of provision of a fault schedule and in identification and substantiation of preventative/protective safeguards.

The principal objectives of a deterministic assessment are to:

- Guide the engineering requirements of the design and any subsequent modifications.
- Define the DiD engineering and associated procedural measures against loss of safety function, or against loss of physical barriers, and assess the adequacy in terms of single and dependent failures and whether risks are ALARP.
- Derive Safety Functional Requirements (*SFRs*) on SSCs, and verify that those requirements have been met at initial operation and through life.
- Determine the limits for safe operation so that the safety functions can be delivered reliably during all modes of operation, and under all reasonably foreseeable faults.

An example of how a DSA fits into the overall safety case structure is shown in Figure 2.

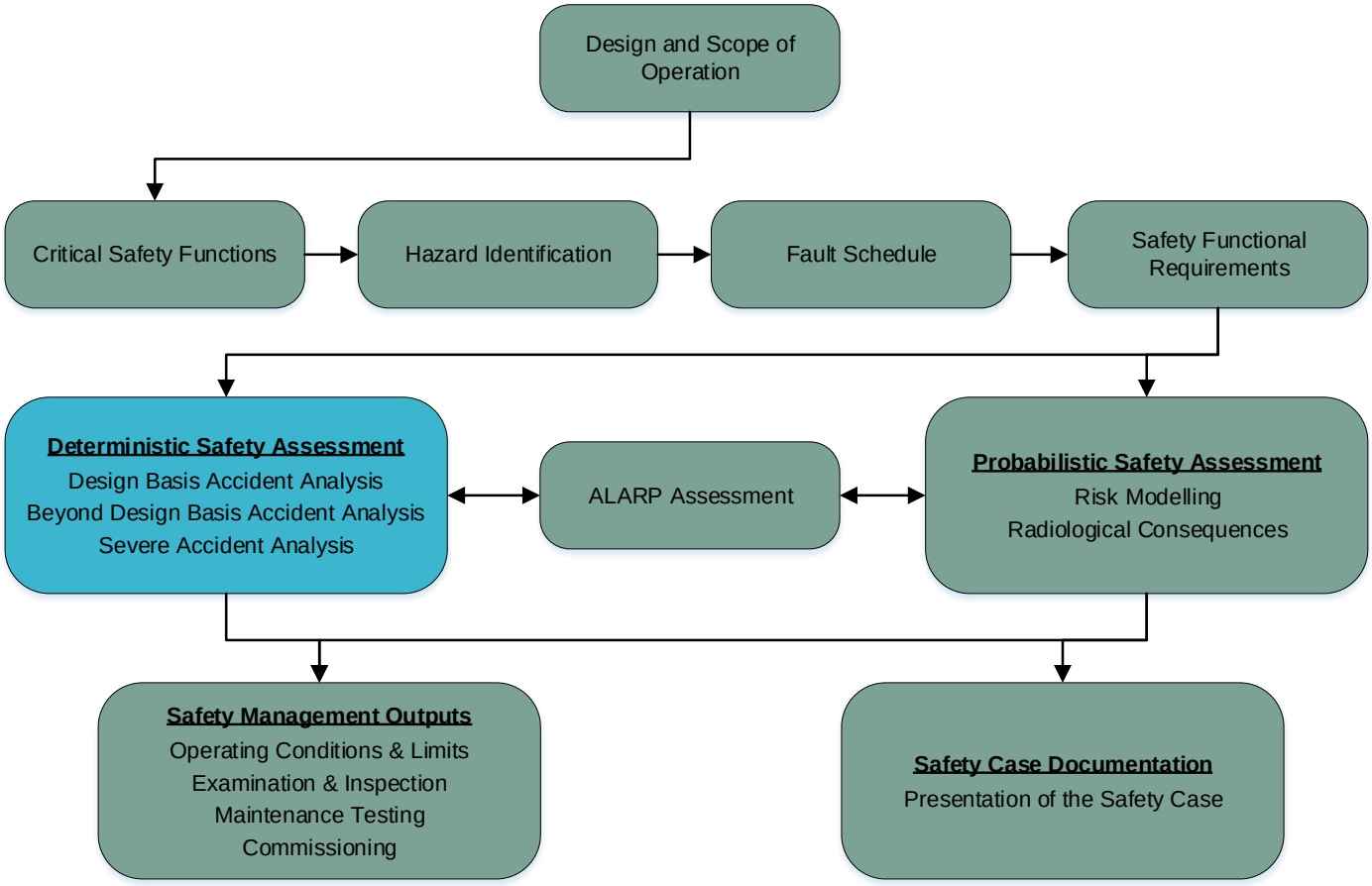

Figure 2: Role of DSA in the overall safety case structure.

An approach to the development of the DSA is provided in Table 1 for reference purposes only.

Step	Activity	Method	When
1	Identify need for Deterministic Safety Assessment (DSA)	Identify: • New Design • Existing DSA	All Stages
2	Scope of Operation	The DSA process begins with the definition of the scope of operations, which is translated into a bounding set of 'nodes' for assessment purposes.	Concept Design Stage
3	Critical Safety Functions (*CSFs*)	Early in the concept design stage CSFs decomposition shall be taken to a level at which PIEs can be identified which fulfils two purposes: • It provides preliminary SFRs, a loss of which can be the basis of the PIEs used in the Fault Schedule. • It provides logic that can be used as an input to the HAZID exercises to ensure that all aspects of the loss of control of function are identified and the DiD substantiation is questioned.	Concept Design Stage
4	Fault / Hazard Identification	Fault / Hazard Identification states that: • All possible causes that could result in harmful consequences need to be identified through appropriate HAZID techniques to ensure that they are satisfactorily addressed within the Safety Case. • The output of the HAZID process is the Hazard Listing which contains the totality of the HAZID information. • The causes should be screened out on the basis of low frequency and low consequence, to remove any further effort being applied to unimportant causes.	Concept Design Stage

Step	Activity	Method	When
5	Extraction of Design Basis Causes	The Design Basis shall include all reasonably foreseeable initiating faults and hazards such as: • Causes within the Utility or Facility that are expected to occur more frequently than 10^{-5} per year. • Natural hazards occurring more frequently than 10^{-4} per year. • Man-made hazards occurring more frequently than 10^{-5} per year.	Concept Design Stage
6	Fault Schedule	The Fault Schedule considers: • Grouping of Causes into PIEs. • Fault Sequence Definition. • Plant and Facility Performance. • Fault Schedule Development.	Concept Design Stage
7	Safety Class Analysis (*SCA*)	SCA is a tool used for the determination and confirmation of the target number of protective safeguards for a Design Basis PIE. This is achieved by the provision of a set of guidelines defining the relationship of a PIE frequency and the unmitigated radiological consequences for each fault sequence to a target number of safeguards.	Scheme Design Stage
8	Definition of Safeguards	The Definition of Safeguards consists of: • Identification of Safeguards. • Definition of Safety Mechanisms Devices and Circuits (*SMDCs*) / Safety Systems. • Implementation of Redundancy through Single Failure Criterion (*SFC*). • Implementation of Diversity and Segregation through assessing common failures.	Concept and Scheme Design Stages

Step	Activity	Method	When
9	Determine Safety Functional Requirements (SFRs)	Determining SFRs will consider the: • Requirement for SFR. • Parent Safety Case review for design modifications. • Recording of CSFs (Level 1 SFRs). • Derivation of Level 2 SFRs. • Derivation of Level 3 SFRs. • Derivation of Level 4 SFRs. • Output to DSA and PSA.	Concept and Scheme Design Stages
10	Identify Operating Rules (*ORs*) and Operating Instructions (*OIs*)	Includes: • Identifying the need for an OR and OIs. • The generation of ORs. • The construction of OIs. • The justification of ORs and OIs.	Detailed Design Development Stage
11	Identify and Classify Structures, Systems and Components (SSCs)	Includes: • Categorising SFRs. • Classifying SSCs.	Detailed Design Development Stage

Step	Activity	Method	When
12	Beyond Design Basis Accident Analysis (BDBAA)	The BDBAA will: • Identify modes of failure under Beyond Design Basis (BDB) by identifying causes within the Utility or Facility that are expected to occur more frequently than 10-7 per year and less frequent than 10-5 per year as well as man-made hazards occurring more frequently than 10-7 per year and less frequent than 10-5 per year. • Perform margin assessment of hazards with the aim of demonstrating an absence of cliff-edges in SSCs. • Conduct analysis of the BDB faults in terms of an accident analysis including an assessment of radiological consequences. • Verify design and performance claims made within the PSA. • Support the ALARP assessment and design decision making process by identifying and assessing any safeguards that may improve the response to Beyond Design Basis Events (*BDBE*). • Provide input for off-site emergency planning.	Detailed Design Development Stage

Step	Activity	Method	When
13	Severe Accident Analysis (SAA)	The SAA will: • Evaluate the ability of the design to withstand severe accidents and to identify particular vulnerabilities. • Assess the need for additional features and associated SFRs that could be incorporated into the SSC design to provide DiD for severe accidents. • Identify accident management measures that could be carried out to mitigate accident effects. • Develop an accident management programme to be followed in severe accident conditions. • Provide input for emergency planning arrangements. • Support the PSA of the facilities design and operation.	Detailed Design Development Stage
14	Review against engineering safety principles	The DSA will demonstrate compliance against the Nuclear Safety Principles (*NSPs*), IAEA Safety Standards and the SAPs with reference to supporting design documentation where applicable. Where the engineering principles are not fully achieved this is to be demonstrated not to invalidate the safety argument on an ALARP basis.	Detailed Design Development Stage
15	Undertake comparison against acceptance criteria and sensitivity analysis	Undertake a: • Review against Acceptance Criteria. • Sensitivity Analysis	Detailed Design Development Stage

Step	Activity	Method	When
16	Consideration of ALARP	The ALARP argument should be underpinned by: • A full definition of each safeguard. • Assessment of the degree of diversity, redundancy and segregation within and between safeguards. • Application of the SFC to assess the redundancy of the protective safeguards associated with the PIE and the fundamental safety function. • Consideration of potential dependant failure mechanisms across the set of measures.	Detailed Design Development Stage
17	Produce Safety Justification and undertake due process	The high level deterministic argument should present a discussion on DiD and include an overview of the methodologies by which DiD measures have been identified, substantiated and the risks demonstrated to be ALARP.	Detailed Design Development Stage

Table 1: Deterministic Process Guide

Additional Information & Guidance

- IAEA Safety Standards, https://www.iaea.org/resources/safety-standards
- ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition Revision 1 (January 2020).