SAFETY CASE DATASET MAP

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
Fault and Hazard Identification (HAZID) Reports	The purpose of the hazard and fault identification is to systematically consider all situations with the potential to cause harm in order to develop a comprehensive list of initiating faults / events with the potential to lead to unacceptable radiological consequences to workers, members of the public, or the environment. Such hazards / faults are then taken forward for evaluation in the fault assessment.	Hazard and Operability (HAZOP) Reports. Operating Experience. External Hazards Topic Reports. Internal Hazards Topic Reports.	Structured What IF Technique (SWIFT). HAZOP Studies. Failure Modes, Effects and Criticality Analysis (FMECA). Failure Modes and Effects Analysis (FMEA). Desktop Gap Analysis. Task Analysis. Review of Standards, RGP and Operating Experience.	The output is a comprehensive list of initiating faults / events associated with the plant, process or activity being considered. Typically this is presented in a **HAZID** / **HAZOP** Report. This is the first stage in the creation of the **Fault Schedule** and provides the basis for the subsequent fault assessment.	Fault Assessment (Unmitigated Radiological Dose). Fault Schedule. HAZOP / HAZAN Reports. Engineering Schedule. External Hazards Topic Reports. Internal Hazards Topic Reports.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Fault analysis: general FA.1-8). ONR, NS-TAST-GD-013, External Hazards, October 2018. IAEA, Format and Content of the Safety Analysis Report for Nuclear Power Plants (GS-G-4.1), IAEA: Vienna, 2004.
Fault Assessment (HAZAN) Reports	The fault assessment should identify and assess the risks to workers and to the public during fault conditions. For each initiating fault / event, the assessment should demonstrate that safety measures are suitably robust and sufficient in number to achieve a level of risk that is acceptable and ALARP.	Fault and Hazard Identification (HAZID). Operating Experience. External Hazards Topic Reports. Internal Hazards Topic Reports.	DBA. Beyond Design Basis Assessment (BDBA). Severe Accident Analysis (SAA). Probabilistic Safety Analysis (PSA). Human Reliability Analysis (HRA). Fault Tree Analysis. Event Tree Analysis.	The output is a refinement of the Fault Schedule, which should record the conclusions of the assessment of the unmitigated radiological consequences. The unmitigated consequences are used to confirm the significance of the safety functions to be fulfilled by individual safety measures and determine the further fault analysis that each initiating fault / event should be subject to.	Fault and Hazard Identification (HAZID). Fault Schedule. HAZID / HAZOP Reports. External Hazards Topic Reports. Internal Hazards Topic Reports. SSC Classification. Safety Function Categorisation. Schedule of Initiating Events and Safeguard Reliabilities. Engineering Schedule. Design Substantiation Reports (DSRs).	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Fault analysis: general FA.1-8). IAEA, Format and Content of the Safety Analysis Report for Nuclear Power Plants (GS-G-4.1), IAEA: Vienna, 2004.
Fault Schedule	The Fault Schedule provides: ♦ A list of all PIEs with their associated frequency. ♦ The safety functions and the associated safety systems and their safety classification for each fault sequence. ♦ For frequent faults, a second line of protection to satisfy the requirement of	Fault and Hazard Identification (HAZID). Fault Assessment (HAZAN Reports) Operating Experience. External Hazards Topic	Structured What IF Technique (SWIFT). HAZard and OPerability (HAZOP) Studies. Failure Modes, Effects and Criticality Analysis (FMECA).	The output is the creation of the Fault Schedule and provides the basis for the fault analysis.	Fault and Hazard Identification (HAZID). HAZID / HAZOP Reports. Fault Assessment (Unmitigated Radiological Dose). External Hazards Topic Reports.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Fault analysis: general FA.1-8).

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
	diversity protection. ♦ Reference to the fault analysis that demonstrates that the plant is adequately protected for the events listed. ♦ A logical link between the original HAZID reports, the Fault Schedule and the subsequent Fault Assessment.	Report. Internal Hazards Topic Report.	Failure Modes and Effects Analysis (FMEA). Desktop Gap Analysis. Task Analysis. Review of Standards, RGP and Operating Experience.		Internal Hazards Topic Reports. Engineering Schedule. DSRs.	
Initiating Fault / Events Consequences	An initiating fault / event is defined by the ONRs Safety Assessment Principles (SAPs) as: "The starting point of a fault sequence. This may be an internal failure, or caused by an internal or external hazard or by human action, or a combination of these".	Fault and Hazard Identification (HAZID). Fault Assessment (HAZAN Reports). DSRs. External Hazards Topic Report. Internal Hazards Topic Report.	Structured What IF Technique (SWIFT). HAZard and OPerability (HAZOP) Studies. Failure Modes and Effects Analysis (FMEA). Logic Tree Analysis.	The output is a Schedule of Initiating Events and Safeguard Reliabilities. The Initiating Faults / Events are also recorded in the Fault Schedule, an example of which is given below.	Fault Assessment (Unmitigated Radiological Dose). Fault Schedule. Engineering Schedule. External Hazards Topic Reports. Internal Hazards Topic Reports.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Fault analysis: general FA.1-8).
Initiating Fault / Hazard Frequency	Determination of the frequencies for all initiating faults / events whose consequences require further assessment.	Fault and Hazard Identification (HAZID). Fault Assessment (HAZAN Reports). DSRs. External Hazards Topic Report. Internal Hazards Topic Report.	DBA. PSA. Human Reliability Analysis (HRA).	The output is a further development of the Fault Schedule, which should now record the estimated initiating event frequencies. The frequency estimates are also used in combination with the unmitigated consequences to determine the further fault analysis that each initiating fault / event should be subject to.	Fault Assessment (Unmitigated Radiological Dose). Fault Schedule. Engineering Schedule. DBA / PSA. External Hazards Topic Reports. Internal Hazards Topic Reports. Schedule of Initiating Events and Safeguard Reliabilities Report.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Fault analysis: general FA.1-8).
Design Basis Analysis (DBA)	The purpose of the DBA is to assess all the initiating faults / events identified as falling within the design basis. The DBA should provide evidence that the design (or design capability assessment) for the plant or facility is tolerant to faults and confirmation that the safety functional requirements for all safety measures are effective and have a suitable and sufficient safety margin.	Fault and Hazard Identification (HAZID). Fault Assessment (HAZAN Reports). External Hazards Topic Report. Internal Hazards Topic Report.	DBA.	The output is a further development of the Fault Schedule, which should now include the candidate safety measures to deliver the High Level and Fundamental Safety Functions for each of the initiating faults / events identified as falling within the design basis. Other output from the DBA will be used to develop emergency operating procedures and to provide input to the DBA and PSA.	Fault Assessment (Unmitigated Radiological Dose). Fault Schedule. Engineering Schedule. DBA / PSA. External Hazards Topic Reports. Internal Hazards Topic Reports.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Fault analysis: general FA.1, 4-9 & Target 4).

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
					Human Reliability Analysis (HRA). Schedule of Initiating Events and Safeguard Reliabilities Report.	
Beyond Design Basis Analysis (BDBA)	In addition to the assessment of the Design Basis faults, BDB faults must also be considered. These are faults and hazards with initiating events that have been excluded from the DBA on the basis of low frequency (i.e. $<10^{-5}$ per year for best estimate internal events and 10^{-4} per year for external hazards estimated on a conservative basis) but whose frequency is not sufficiently low ($>10^{-7}$ per year) for them to be discounted completely. The ONR SAPs define BDB as: *"Fault sequences initiated by internal and external hazards beyond the design basis should be analysed applying an appropriate combination of engineering, deterministic and probabilistic assessments".*	Fault and Hazard Identification (HAZID). Fault Assessment (HAZAN Reports). External Hazards Topic Report. Internal Hazards Topic Report.	Event Tree Analysis. Common Cause Failure (CCF) Analysis.	The BDBA should: ♦ Confirm that no cliff-edge effects exist i.e. there is no potential for a sudden and significant change in radiological consequences associated with events located just outside the design basis boundary (e.g. 9.0×10^{-6} per year). ♦ Identify the margins that exist BDB i.e. the point at which design basis safety measures can be expected to fail. ♦ Provide an input into the SAA. ♦ Provide inputs into the PSA to assess whether overall risk targets are met and confirm that no single fault type dominates the risk profile. ♦ Develop emergency operating procedures.	Fault Schedule. Engineering Schedule. Fault Assessment (Unmitigated Radiological Dose). DBA / PSA. External Hazards Topic Reports. Internal Hazards Topic Reports. Human Reliability Analysis (HRA). Schedule of Initiating Events and Safeguard Reliabilities Report.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: external and internal hazards EHA.18).
Postulated Initiating Events (PIE) / Design Basis Faults	Subset of initiating events. Events that if left unchecked could lead to radiological consequences. These often group together into a number of identified initiating events that may lead to the same consequence.	Fault and Hazard Identification (HAZID). Fault Assessment (HAZAN Reports). DSRs. External Hazards Topic Report. Internal Hazards Topic Report.	Fault Grouping Methodology.	The output is a set of bounding design basis fault scenarios.	Fault Schedule. Engineering Schedule. Fault Assessment (Unmitigated Radiological Dose). External Hazards Topic Reports. Internal Hazards Topic Reports.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Fault analysis: general FA.1-8).
Design Basis External Hazards	List of external hazards that could challenge the nuclear safety of the plant.	Site Characterisation Data. Fault and Hazard Identification (HAZID). External Hazards Topic Report. Operational Experience.	DBA including specialist assessment e.g. Extreme Value Analysis of weather data. Seismic characterisation of the site strata. Review of Operational Experience.	The output is a complete set of external hazards relevant to the site against which the design must be shown to be resilient.	Site Layout. Engineering Schedule. External Hazards Topic Reports. Internal Hazards Topic Reports.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Fault analysis: general FA.1, 4-9 & Target 4). ONR, NS-TAST-GD-013, External Hazards, October 2018.

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
Design Basis Internal Hazards	List of Internal hazards that could occur on the site as a result of the operations undertaken there and therefore over which the licensee is able to exert some control. Internal hazards typically include thing like vehicle impacts, internal flooding, fire and explosion etc.	Site Layout. Fault and Hazard Identification. Operational Experience. Internal Hazards Topic Report.	DBA.	The output is a complete set of internal hazards to be considered in the design and safety case.	Site Layout. Qualification Requirements. Engineering Schedule. External Hazards Topic Reports. Internal Hazards Topic Reports.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Fault analysis: general FA.1, 4-9 & Target 4). ONR, NS-TAST-GD-014, Internal Hazards, November 2019.
Human Factors / Human Reliability Analysis	Consideration of human factors can influence safety at all stages of the plant lifecycle, from design to decommissioning, and therefore where human performance claims are made in the safety case these must be appropriately supported by the relevant features of the system design, which will allow them to be substantiated within the safety case. In other words, the human actions identified within the various safety analyses underpinning the safety case must be shown to be achievable to the performance required or assumed.	Fault and Hazard Identification (HAZID). Fault Assessment (HAZAN Reports). Operational Experience. DBA. Internal Hazards Topic Report.	Technique for Error Rate Prediction (THERP).	The Human Factors / **Human Reliability Analysis** should: ♦ Identify and analyse all human actions and administrative controls that are necessary for safety. ♦ The analysis should be conducted as part of DBA, PSA and SAA aspects of the safety case. ♦ Proportionate analysis should be undertaken to support the claims and arguments made in regard to these actions and administrative controls. ♦ The human reliability analysis should include: pre-fault human actions during maintenance, calibration or testing activities where error could result in the non-availability of equipment or systems important to safety [i.e. Type A HFEs]; actions that contribute to initiating events [i.e. Type B HFEs]; post-fault human actions [i.e. Type C HFEs]; and long-term recovery actions in severe accidents.	Fault Schedule. Engineering Schedule. Fault Assessment (Unmitigated Radiological Dose). DBA / PSA. External Hazards Topic Reports. Internal Hazards Topic Reports. Schedule of Initiating Events and Safeguard Reliabilities Report.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: human factors EHF.1-12). ONR, NS-TAST-GD-058, Human Factors Integration, March 2017. ONR, NS-TAST-GD-059, Human Machine Interface, November 2019. ONR, NS-TAST-GD-063, Human Reliability Analysis, October 2018. ONR, NS-TAST-GD-064, Allocation of Function Between Human and Engineered Systems, December 2017.
Severe Accident Analysis (SAA)	The combination of the DBA, BDBA and PSA should ensure that all credible fault scenarios are identified and suitable and sufficient safety measures are incorporated into the design to prevent / mitigate the consequences and ensure that the residual risk is ALARP, the ONR also requires a SAA be undertaken. The ONR define a severe accident as: *"An accident with off-site consequences with the potential to exceed 100 mSv, or lead to a substantial unintended relocation of radioactive material within the facility that*	Fault and Hazard Identification (HAZID). Fault Assessment (HAZAN Reports). External Hazards Topic Report. Internal Hazards Topic Report.	SAA Computer Codes (e.g. MAAP - The Modular Accident Analysis Program).	The **SAA** should: ♦ To verify the severe accident design or to support design changes. ♦ Inform the development of training for severe accident response. ♦ Develop and validate severe accident management arrangements. ♦ Inform the design of severe accident management systems.	Fault Schedule. Engineering Schedule. Fault Assessment (Unmitigated Radiological Dose). DBA / PSA. External Hazards Topic Reports. Internal Hazards Topic Reports. Human Reliability Analysis (HRA).	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: chemical engineering EPE.4, Fault analysis: severe accident analysis FA.15-16 & 25). ONR, NS-TAST-GD-007, Severe Accident Analysis, September 2017.

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
	places a demand on the integrity of the remaining physical barriers".				Schedule of Initiating Events and Safeguard Reliabilities Report.	
Probabilistic Safety Assessment (PSA)	The purpose of this stage is to identify the requirements of the PSA (there are 3 levels of PSA) in order to inform the risk to the public and workers is acceptable and ALARP.	Fault and Hazard Identification (HAZID). Fault Assessment (HAZAN Reports). External Hazards Topic Report. Internal Hazards Topic Report.	PSA Level 1, 2 and 3.	The output is an adequate representation of the plant and any human involvement. This requires: ♦ Representation of faults and hazards leading up to the PIE should be modelled where appropriate. ♦ Pre-initiator human failure events leading directly to or contributing to a PIE are clear and adequate. ♦ The general approach used for the inclusion of post-initiator human failure events into the system models is clear and adequate. ♦ There is clear representation of the protection system as defined in the design basis analysis together with any further mitigation measures claimed to reduce the risk to ALARP. ♦ The link between the headings in the event tree and the relevant thermal hydraulic analysis performed to support the event sequence is transparent. ♦ The level of detail in the fault tree is sufficient to ensure: i) The logic is correct. ii) All dependencies are captured. iii) All common cause failures are adequately represented as an integral part of the PSA model. iv) The redundancy claims are clearly evident. v) The methods for deriving common cause failure rates in redundant systems should be identified clearly and common cause failure rates are to the identified in the logic model. ♦ The descriptive text for all event tree headings should be clear and consistent and preferably expressed as a function success.	Fault Schedule. Engineering Schedule. Fault Assessment (Unmitigated Radiological Dose). DBA. External Hazards Topic Reports. Internal Hazards Topic Reports. Human Reliability Analysis (HRA). Schedule of Initiating Events and Safeguard Reliabilities Report.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Fault analysis: PSA FA.10-14 & Target 5). ONR, NS-TAST-GD-030, Probabilistic Safety Analysis, June 2019.

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
Design / Engineering Substantiation	The provision of evidence to demonstrate that the individual SSCs contributing to an engineering safeguard or SMDC satisfies the performance criteria stipulated by the SFR now, and for the planned operational life of the facility, with acceptable demonstration of no 'cliff-edge' effects.	International and national industry codes, standards and best practice. Engineering Schedule. Equipment Technical Reports.	Design Substantiation. Functional Testing and Inspection.	The output is a Design Substantiation Report that clearly demonstrates how the SSC satisfies the claim placed on it with a strong degree of confidence.	Fault Schedule. SSC Classification. Safety Function Categorisation. Schedule of Initiating Events and Safeguard Reliabilities. Engineering Schedule. Fault Assessment (Unmitigated Radiological Dose). External Hazards Topic Reports. Internal Hazards Topic Reports.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: integrity of metal components and structures: analysis EMC.32, Fault analysis: assurance of validity of data and models AV.1-2).
Design Assessment Report (DAR)	This is where the findings of Engineering Design Substantiations are recorded. DARs can be single or multi-discipline depending on the SSCs involved.	Design / Engineering Substantiation. International and national industry codes, standards and best practice. Engineering Schedule. Equipment Technical Reports.	Design Substantiation.	The output is the DAR which should summarise the engineering substantiation findings.	Fault Schedule. SSC Classification. Safety Function Categorisation. Schedule of Initiating Events and Safeguard Reliabilities. Fault Assessment (Unmitigated Radiological Dose). DSRs.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: integrity of metal components and structures: analysis EMC.32, Fault analysis: assurance of validity of data and models AV.1-2).
Design Codes, Standards and Guidance	International and national industry codes and standards applied to the design of the plant. For nuclear safety related SSCs these are typically identified based on the classification of the SSC and the relevant design authority guidance for the type of system. These are generally defined on a discipline basis, for example Control & Instrumentation, Electrical, Mechanical Handling, Civil Structural, and owned by the relevant subject matter experts within the organisation.	International and national industry codes, standards and best practice.	Design Review. International and national nuclear codes and standards. Licensees own design authority standards and guidance.	The output is the generation of all safety case documentation that complies with all relevant Codes and Standards.	Interface with Design Authority guidance and standards defining acceptable codes and standards for use in the design of plant and equipment, including requirements specific to different classes of SSCs.	British Standards, https://shop.bsigroup.com IAEA Safety Standards, https://www.iaea.org/resources/safety-standards
Engineering Schedule	The engineering schedule is a comprehensive list of all Nuclear and Non-Nuclear Structures, Systems and Components within a facility. The list includes the SSC Safety Function, Safety Status, Performance Requirements and the DAR in which it is assessed. The engineering schedule is a concept used in the UK to link the fault schedule to the	Fault and Hazard Identification (HAZID). Fault Assessment (HAZAN Reports). DSRs.	Database tools and techniques.	The output is a fully populated **Engineering Schedule**.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). Fault Schedule. SSC Classification.	

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
	engineering substantiation of the systems requirements specified by the SFRs. An indicative structure for a typical UK Engineering Schedule is provided.				Safety Function. Safety Function Categorisation Performance Requirements. Schedule of Initiating Events and Safeguard Reliabilities. HRA. DSRs.	
Engineering Substantiation Summary Report	This is a summary of the recordings of all the DARs produced for a specific Facility. It provides the overall justification that the Facility's structures and engineered safeguards / SMDCs satisfy their Safety Functions. The DARs form the individual annexes that support the ESSR.	DARs. DSRs.	Design Substantiation.	The output is an Engineering Substantiation Summary Report.	Fault Schedule. SSC Classification. Safety Function Categorisation. Schedule of Initiating Events and Safeguard Reliabilities. Fault Assessment (Unmitigated Radiological Dose). DSRs. Design Assessment Reports (DARs).	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: integrity of metal components and structures: analysis EMC.32, Fault analysis: assurance of validity of data and models AV.1-2).
Equipment Qualification	Equipment qualification is a fundamental requirement of the UKs approach to safety assessment for nuclear facilities. It is a process by which any safety related and safety critical equipment used in the reactor design will function correctly and reliably on demand, within the parameters of the site-specific safety case.	DSRs.	Design Substantiation.	The output of this stage is the production of an Equipment Qualification Schedule.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). Fault Schedule. SSC Classification. Safety Function Categorisation. Schedule of Initiating Events and Safeguard Reliabilities.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: equipment qualification EQU.1, Engineering principles: maintenance, inspection and testing EMT.4, Engineering principles: integrity of metal components and structures: manufacturing, pre- and in-service examination and testing EMC.30).
Standard Operating Procedures (SOP) / Emergency Operating Procedures (EOP)	A Standard Operating Procedure (SOP) is a set of step-by-step instructions compiled by an organization to help workers carry out complex routine operations. SOPs aim to achieve efficiency, quality output and uniformity of performance, while reducing miscommunication and failure to comply with industry regulations.	International and national industry codes, standards and best practice. Equipment Technical Reports.	Review of Operational Experience. Hazard Identification.	The output of this stage is the production of a set of SOPs and EOPs.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). Fault Schedule.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: commissioning ECM.1, Engineering principles: human factors EHF.9).

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
	An Emergency Operating Procedure (EOP) is a plan of actions to be conducted in a certain order or manner, in response to a specific class of reasonably foreseeable emergency, a situation that poses an immediate risk to health, life, property, or the environment.	Operational Experience.			Equipment Qualification. Maintenance Schedule. External Hazards Topic Reports. Internal Hazards Topic Reports.	ONR, NS-TAST-GD-035, Limits and Conditions for Nuclear Safety (Operating Rules), March 2018.
Maintenance Schedule	A maintenance schedule is a record of any maintenance that is required to be carried out ahead of time and within a predetermined period. It can either be a recurring task done at regular time intervals or a one-time task. Scheduled maintenance includes inspections, adjustments, regular service, and planned shutdowns.	International and national industry codes, standards and best practice. Equipment Technical Reports. Operational Experience.	Review of Operational Experience. Hazard Identification.	The output of this stage is the generation of the **Maintenance Schedule**.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). Fault Schedule. Equipment Qualification. SOPs / EOPs.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: maintenance, inspection and testing EMT 1-8). ONR, NS-TAST-GD-009, Examination, Inspection, Maintenance and Testing of Items Important to Safety, May 2019.
As Low As Reasonably Practicable (ALARP)	ALARP measures are the necessary measures to avert risk taken until, or unless, the cost of the measures (whether in money, time of trouble) is grossly disproportionate to the risks that would thereby be averted.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). International and national industry codes, standards and best practice. External Hazards Topic Report. Internal Hazards Topic Report. Operational Experience. Equipment Technical Reports. DSRs.	ALARP Meetings. Optioneering.	The output of this stage is an **ALARP** report.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). Fault Schedule. Equipment Qualification. Maintenance Schedule. External Hazards Topic Reports. Internal Hazards Topic Reports. SOPs / EOPs.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition. ONR, NS-TAST-GD-005, Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable), December 2019.
Defence in Depth (DiD)	The Defence in Depth principle requires that facilities are designed and operated so that defence in depth against potentially significant faults is achieved by provision of multiple independent barriers to fault progression.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose).	Balanced approach to reactor design (to prevent core damage, containment failure, and mitigation of accident consequences). Common Cause Failure Analysis.	The output is the refinement of the **PSA** and a specific chapter within the PSR/PCSR etc. discussing what defence in measures have been employed in the design.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose).	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: key principles EKP.3).

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
		International and national industry codes, standards and best practice. Operating Experience. External Hazards Topic Report. Internal Hazards Topic Report. Equipment Technical Reports. DSRs.			Fault Schedule. DBA. PSA.	
Normal Operation Dose Assessment	A demonstration of the means of achieving effective radiological protection and control is an essential part of the licensee's nuclear safety submissions. The provision of adequate protection for persons against ionising radiations is required during normal operations and also under fault and accident conditions.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose).	Radiological Dose Assessment.	The output is the Normal Operational Dose Assessment which should demonstrate that the dose to workers and members of the public will meet the required ONR Dose Targets (Targets 1, 2 and 3 of the ONR SAPs).	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). Fault Schedule. DBA. PSA.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition. ONR, NS-TAST-GD-043, Radiological Analysis – Normal Operation, July 2019.
Claims, Arguments, Evidence (CAE)	Having carried out the safety case development, the demonstration that the plant analysis, systems design, operational safety measures and safety management arrangements are all in place and ALARP must be presented in a clear, coherent manner. Safety cases are based on a Claims, Arguments and Evidence (CAE) approach, even if this has tended to be implicit within the text of the safety case. More recently there has been a move towards explicitly structuring the safety case around set of defined claims as to why the risk associated with the plant or process in question is ALARP, supported by relevant arguments and evidence substantiating the claims. The benefits of the CAE approach vary depending on the application being considered, with it being better suited to applications like C&I systems than to claims on human action. However, it	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). International and national industry codes, standards and best practice. Operating Experience. External Hazards Topic Report. Internal Hazards Topic Report. Operational Experience.	CAE Methodology.	The output is a clear, concise, and logically structured safety case.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). International and national industry codes, standards and best practice. External Hazards Topic Report. Internal Hazards Topic Report. Equipment Technical Reports. DSRs.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition.

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
	can be used to provide clear and auditable links from what the plant, processes and people are claimed to do to maintain safety and why, down to the supporting analysis and other evidence that demonstrates that the relevant requirements can be met, with the required reliability and integrity.	Equipment Technical Reports. DSRs.				
General Design / Plant Description (includes Operating Modes)	Basic description of the reactor design and layout, such as the Main Plant Systems (e.g. Reactor Core and Reactor Coolant System, Safety Systems, Main Auxiliary Systems, Power Conversion Systems, Instrumentation and Control Systems, Electric Power Systems i.e. Offsite electric power system, onsite electric power system and Black Out electric power system. Plant operating modes are defined during the design development. Typically these include: Power Operation, Start-up, Hot Shutdown, Cold Shutdown and Refuelling.	Design Organisation. International Guidance. ONR Regulatory Expectation. Operational Experience.	There are distinct phases in the design development corresponding to different stages in the plant lifecycle. These are: Concept design (Pre-PSR). Preliminary / Scheme Design (Pre-PCSR). Detailed design (PCSR onwards). The design continuously evolves throughout the life of the plant in response to changing requirements, standards, ageing and degradation mechanisms, regulatory expectation etc.	The output is the production of the General Design / Plant Description Safety Case Chapter. See GDA Guidance Step 1.2 below for suggested contents list of this chapter.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). International and national industry codes, standards and best practice. External Hazards Topic Report. Internal Hazards Topic Report. Equipment Technical Reports. DSRs.	ONR, NS-TAST-GD-057, Design Safety Assurance, November 2017.
Site Layout	The site layout is developed taken account of a variety of drivers including: Design requirements, Operational requirements / logistics, Geographical constraints, Internal hazards and External hazards.	Concept / Preliminary Design Reports. Fault and Hazard Identification (HAZID). Operational Requirements Report.	Optioneering. HAZID.	Approved Site Layout and Generic Site Characteristics Safety Case Chapter.	Fault and Hazard Identification (HAZID).	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: layout ELO.1-4). ONR, CNS-TAST-GD-6.6, Nuclear Construction Sites, March 2017.
Design Life	The design life is the specified lifetime for which the plant has been designed to deliver its functional requirements. This may be different to operational life if the plant closes early or its life is extended. The design is required to demonstrate that components that are difficult to replace or that cannot be economically replaced are capable of lasting for the duration of the design life. For components that are not capable of surviving for the design life, it is necessary to plan in replacements and it may be necessary to have adequate stocks of components available.	Design organisation, informed by licensee requirements.	Licensee guidance on meeting design life requirements.	Fully justified design life of plant.	Fault and Hazard Identification (HAZID).	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: civil engineering: design ECE.9).
Fundamental / Nuclear Safety Principles	Principles that form the basis of the licensees' safety management system and underpin the safe delivery of nuclear activities on the site.	Safety Management System - based on regulatory and international guidance	Licensee guidance on producing Nuclear Safety Principles and implementing a Safety Management System.	The output is a comprehensive set of safety management arrangements to ensure the	International and national industry codes, standards and best practice.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition.

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
		and standards (ONR and IAEA).		delivery of the safety principles at all times.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose).	ONR, NS-TAST-GD-004, Fundamental Principles, April 2019.
Design Functional Requirements	Functional requirements of the design, include things like reactor output, efficiency etc. These will impact on the safety requirements of the plant.	Plant specification document.	Define the set of design requirements that are required to achieve the appropriate reliability of the systems to perform their safety functions. Define the seismic requirements of the design i.e.: 1. Operability – capability of an active component including all necessary auxiliary supporting and energy supply systems to perform its intended functions and to meet the safety objective. 2. Functional capacity – ability of all pressure-bearing parts of components to safety withstand the specified loadings at the given frequency of occurrence throughout the service life of the component. 3. Integrity – ability of all pressure-bearing parts of components to safety withstand the specified loadings at the given frequency of occurrence throughout the service life of the component. 4. Stability – ability of a component to withstand loads which tend to change the orientation or location of the component.	The output is a set of Design Functional Requirements.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). General Design / Plant Description (includes Operating Modes). Site Layout. Fundamental / Nuclear Safety Principles.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition. ONR, NS-TAST-GD-057, Design Safety Assurance, November 2017.
Safety Functions	A high level statement of the functions to be implemented by safety measures to either safeguard or mitigate against a particular fault sequence. High level safety functions are developed during the design and safety case development informed by the hazard identification and fault assessment.	Fault Assessment (Unmitigated Radiological Dose). Derive from plant fundamental safety functions and nuclear safety principles.	Licensee guidance on development of safety functions.	The output of this stage is a further development of the Fault Schedule, which should include a list of High Level Safety Functions (should not typically be solution specific).	The design and safety process is an iterative process used to develop safety functions and feedback into the more detailed design.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: key principles EKP.4). ONR, NS-TAST-GD-003, Safety Systems, March 2018.

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
Safety Function Categorisation	Safety function categories are assigned based on the contribution the function makes to nuclear safety, which is typically determined by the consequences of failure to deliver the function. There are generally three categories for Safety Functions: Category A – any Safety Function that plays a principal role in ensuring nuclear safety; Category B – any Safety Function that makes a significant contribution to nuclear safety; Category C – any other Safety Function contributing to nuclear safety. Categories are applied to all Safety Functions whether provided by engineered systems, structures, components, operating procedures or administration rules.	Safety Functions. Fault Assessment (Unmitigated Radiological Dose).	Licensees SMS. Regulatory and international guidance and standards.	The output of this stage is a further development of the Fault Schedule, which should now include the Safety Function Category A, B or C. This determines the minimum number and Class of the Structures Systems and Components (SSCs) required to deliver it.	Fault and Hazard Identification (HAZID). Safety Functions.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: safety classification and standards ECS.1-2). ONR, NS-TAST-GD-094, Categorisation of Safety Functions and Classification of Structures, Systems and Components, July 2019.
Safety Functional Requirements (SFRs)	A statement of the performance requirements of the design that are required to adequately fulfil the safety function. It provides a technical requirement definition, which may be used in combination with other SFRs to fully specify the required performance measures to fulfil any specific Safety Function. SFRs consist of safety limits, operating limits, monitoring requirements, administrative controls, operating instructions, procedures etc.	Safety Functions. Fault Assessment (Unmitigated Radiological Dose). Design Requirements.	Derived from deconstruction of the safety functions during the fault assessment.	The output of this stage is a further development of the Fault Schedule, which should now include the SFRs. The Engineering Schedule will also require to be updated and the SSC Specification Report generated.	Fault and Hazard Identification (HAZID). Engineering Schedule / Substantiation.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: maintenance, inspection and testing EMT.7, Engineering principles: civil engineering ECE.1, 7, 12 & 20). ONR, NS-TAST-GD-094, Categorisation of Safety Functions and Classification of Structures, Systems and Components, July 2019.
Structures, Systems and Components (SSCs)	This is a collective term relating to structures, systems and components whose failure could impact on nuclear and/or non-nuclear safety.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). Safety Functions. SFRs.	Candidate SSCs identified by safety SQEP in conjunction with design team via: Optioneering. HAZID.	The output of this stage is a further development of the Fault Schedule, which should now include the SSCs. The Engineering Schedule will also require to be updated.	Fault and Hazard Identification (HAZID). Engineering Schedule / Substantiation.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition. ONR, NS-TAST-GD-094, Categorisation of Safety Functions and Classification of Structures, Systems and Components, July 2019.
SSC Classification	SSC classifications are assigned based on the required integrity of the SSC. There are generally three categories for SSCs: Nuclear Safety Class 1 – any structure,	Licensee Categorisation and Classification Process.	Licensees SMS - based on regulatory and international guidance and standards. Derived from category of corresponding safety function and	SSC Class 1, 2 or 3 that will define the integrity requirements, such as single failure tolerance, redundancy, Quality Assurance arrangements etc.	Fault and Hazard Identification (HAZID). Engineering Schedule / Substantiation.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition. ONR, NS-TAST-GD-094, Categorisation of Safety Functions and Classification of

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
	system or component that forms a principal means of fulfilling a Category A Safety Function; Nuclear Safety Class 2 – any structure, system or component that makes a significant contribution to fulfilling a Category A Safety Function, or forms a principal means of ensuring a Category B Safety Function; Nuclear Safety Class 3 – any other structure, system or component contributing to nuclear safety.		the contribution that the SSC is claimed to make to delivery.			Structures, Systems and Components, July 2019.
Safeguards / Safety Measures	Engineered or Operational (including administrative, managerial or procedural) controls and/or protection comprising hardware, software and/or persons, or a combination of these, available for a given failure demand (initiated internally or externally) which eliminate or reduce the potential for harm.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). Fault Schedule.	HAZID. DBA. PSA.	The output is a Schedule of Safeguards that have been identified to protect against the fault scenarios.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). External Hazards Topic Report. Internal Hazards Topic Report. Equipment Technical Reports. DSRs. Fault Schedule. Engineering Schedule / Substantiation.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: key principles EKP.5). ONR, NS-TAST-GD-003, Safety Systems, March 2018. ONR, NS-TAST-GD-010, Early Initiation of Safety Systems, November 2017.
Safety Mechanisms, Devices and Circuits (SMDCs)	These are physical items which provide a function (actively or passively) which act in response to a fault to prevent or mitigate a radiological consequence. These items take no part in operational control and if their function were to be removed normal operations would not be affected.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). Fault Schedule.	HAZID. DBA. PSA.	The output should be a set of procedures which ensure that the safety case clearly identifies any necessary SMDCs and the permitted configurations of them necessary to assure safety.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). External Hazards Topic Report. Internal Hazards Topic Report. Equipment Technical Reports. DSRs. Fault Schedule. Engineering Schedule / Substantiation.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition.

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
Computational Analysis Codes, Standards and Techniques	These relate to the analysis codes and techniques used to develop the design. For example, civil structural and fluid dynamic assessment codes, burnup analysis codes, transient analysis packages, seismic codes. These require to verified, validated and accepted by the licensee as suitable for use in each specific applications.	International, national and industry codes, standards and best practice.	Design Review.	The output should be a set of approved codes and standards for use in the safety analysis.	Interface with Design Authority guidance and standards defining acceptable codes and standards for use in the design of plant and equipment, including requirements specific to different classes of SSCs.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: safety systems ESS.27). ONR, NS-TAST-GD-042, Validation of Computer codes and Calculation Methods, March 2019. ONR, NS-TAST-GD-046, Computer Based Safety Systems, April 2019.
Reliability Requirements	The reliability requirements on SSCs are generally related to the contribution that they make to ensuring nuclear safety through delivery of the fundamental safety functions. For the DBA specific reliability targets for SSCs are not generally used, as the required reliability is delivered through the application of appropriately robust design and analysis, driven by the SSC classification, ultimately derived from its contribution to delivery of the safety functions. However, to satisfy the overall risk reduction targets associated with DBA a target reliability of around $1x10^{-3}$ failures per year for Class 1 and 2 equipment can generally be inferred. Reliability targets may also be specified by standards or the licensees own arrangements, for C&I the Cat and Class approach defined in IEC 61226 is generally adopted by licensees in their own arrangements, as well as the safety lifecycle approach from IEC 61513 / 61508.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). Fault Schedule. SSCs. SSC Classification.	Derived from fault assessment based on safety function and cat and class.	The output should be a set of reliability requirements for each SSC.	Fault and Hazard Identification (HAZID). Fault Assessment (Unmitigated Radiological Dose). DSRs. Fault Schedule. Engineering Schedule / Substantiation. SSCs. SSC Classification.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: design for reliability EDR.1-4, Engineering principles: reliability claims ERL.1-4, Engineering principles: maintenance, inspection and testing EMT.6 & 8, Engineering principles: integrity of metal components and structures: highest reliability components and structures EMC.1-3, Engineering principles: safety systems ESS.21 & 27, Engineering principles: essential services EES.3).
External Interfaces	This should define and explain how the plant interfaces with the external environment. This may include grid supply, ultimate heatsink, essential consumables (diesel fuel, gases etc.), support from offsite emergency services etc.	Design Requirements.	Feasibility Studies.	The output should be an assessment of the plant and its interface with the external environment i.e. with the national grid.	DSRs.	
Source Term	Types and amounts of radioactive or hazardous material released to the environment following an accident.	Generated from specifics of fuel and reactor chemistry regime.	Approved burnup analysis codes. Conservative approach as will be used for shielding analysis. The following source terms will be derived: ♦ Primary coolant source term - This is mainly used for system design and radiation protection. ♦ Secondary Coolant Source Term	The output is a series of source terms which will be used in the fault assessment / consequence assessment.	Fault Assessment (Unmitigated Radiological Dose). Radiological Shielding and Zoning. Radioactive Waste Arising / Management.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Fault analysis: PSA FA.13 & 15 & Target 9).

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
			- This is used as input for gaseous and liquid effluent release assessment, shielding and zoning design. ♦ Derived Source Term - This is the source term of different systems in different buildings that is used for radiation shielding and zoning design, dose assessment and equipment qualification in safety case. ♦ Gaseous and liquid effluent release from Nuclear Power Plant during normal operation as input for the environmental impact assessment. ♦ Airborne activity in the nuclear island buildings. This is used to estimate the resulting internal exposure to workers and internal exposure caused by finite cloud shine. ♦ Accident Source Term.			
Radiological Shielding and Zoning (incorporates Radiological Protection)	Initial radiological zoning, identifying areas of the plant in which radiological material will be stored, handled, processed and moved.	Radiation Protection Subject Matter Expert (SME). Ionising Radiation Regulations and Approved Code of Practice.	Shielding Assessment Tools and Computer Codes.	The output should be a hierarchy of protective measures that protect against receiving a radiation dose. Such as: ♦ Passive engineered safety measures. ♦ Active engineered safety measures. ♦ Administrative safety measures.	Civil Design. Control & Instrumentation.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: containment and ventilation: import and export of nuclear material ECV.9, Radiation Protection RP.6 & 7). ONR, NS-TAST-GD-002, Radiation Shielding, June 2019.
Quality Assurance / Quality Management System	Demonstration that the QA / QMS implemented for the reactor design are appropriate and will meet UK regulatory expectations. Document Control Arrangements – to ensure all major GDA submissions are appropriately developed, checked, reviewed and approved. Competence Arrangements – to ensure personnel (all staff and contractors) are competent in their roles with records to demonstrate competence and experience commensurate with the responsibility of the assigned tasks. Interface between Design, Safety, Security and Environmental Protection.	Quality Plan.	Licensees QMS / QA processes.	The output is a Company Quality Manual / Quality Management System.	All other safety case data.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: safety classification and standards ECS.3, Engineering principles: maintenance, inspection and testing EMT.5, Engineering principles: civil engineering: construction ECE.17, Fault analysis: assurance of validity of data and models AV.1-2).

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
	Control of Procurement – including evaluation and selection of the supplier, procurement document preparation and acceptance will be implemented based on the Quality Management Manual. Control of Non-Conformances – governance arrangements in place to report, manage and rectify non-conformances during procurement of goods and services. Management and Control of the Design Reference. Management of the Master Document Submission List Interface Arrangements with the ONR and the Environment Agency.					
Radioactive Waste Arising / Management	Qualitative information about the radioactive waste arising / management. Information about the types of waste handled i.e. gaseous, liquid and solid radioactive wastes generated in the operation of the plant. Development of an inventory (volume and activity), timescales of arising and arrangements for storage, packaging, transport and disposal of radioactive wastes such as spent fuel, operational wastes and decommissioning wastes. Development of a route map, programme and management plan for identifying and resolving data omissions and attaining the waste management approvals required for each of the higher activity wastes.	Radiological Assessments. Radiation Protection SME.	Radiological Dose Assessment. Waste Management Plan.	The output should be a record of all radioactive waste arising through the full life cycle of the plant and the management of the waste both in the interim period and its long term storage / disposal.	Fault Assessment (Unmitigated Radiological Dose). Radiological Shielding and Zoning. Source Term.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: civil engineering: design ECE.26, Radioactive waste management RW.1-7). ONR, NS-TAST-GD-024, Management of Radioactive Material and Radioactive Waste on Nuclear Licensed Sites, September 2019.
Operating Modes	Plant operating modes are defined during the design development. Typically these will include: ♦ Power Operation. ♦ Start-up. ♦ Hot Shutdown. ♦ Cold Shutdown. ♦ Refuelling.	Design Organisation. International Guidance. ONR Regulatory Expectation. Operational Experience.	Detailed Design.	The output should be a list of operating modes and definitions, including details of requirements for transition between modes.	Control & Instrumentation. SOPs / EOPs.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Engineering principles: control and instrumentation of safety related systems ESR.4, Engineering principles: human factors EHF.3, Engineering principles: reactor core ERC.1).
Dose Targets	Corporate dose targets for normal operations and fault conditions. Generally these are captured in the nuclear safety principles as deterministic and probabilistic criteria and are	Relevant national and international standards, guidance	Licensee SMS - based on regulatory and international guidance and standards.	The output should be a set of dose acceptance criteria for workers and the public in normal operations and fault conditions.	Fault Assessment (Unmitigated Radiological Dose). Radiological Shielding and Zoning.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see Target 6 & 8).

Safety Case Data	Description of Safety Case Data	Input - Source of Safety Case Data	Approach (Tools / Techniques)	Output	Interfaces & Dependencies	Guidance Links
	based on international and regulatory guidance and legal limits.	and best practice (e.g. ONR and IAEA).			Radioactive Waste Arising / Management. Source Term.	
Availability, Reliability, Maintainability (ARM) Assessment	Reliability, availability, and maintainability (RAM) are three system attributes that are of interest to systems engineers, logisticians, and users. Collectively, they affect economic life-cycle costs of a system and its utility. Reliability is defined as the probability of a system or system element performing its intended function under stated conditions without failure for a given period of time. A precise definition must include a detailed description of the function, the environment, the time scale, and what constitutes a failure. Maintainability is defined as the probability that a system or system element can be repaired in a defined environment within a specified period of time. Increased maintainability implies shorter repair times. Availability is the probability that a repairable system or system element is operational at a given point in time under a given set of environmental conditions. Availability depends on reliability and maintainability. A failure is the event(s), or inoperable state, in which any item or part of an item does not, or would not, perform as specified. The failure mechanism is the physical, chemical, electrical, thermal, or other process that results in failure. In a computerized system, a software defect or fault can be the cause of a failure and the failure may have been preceded by an error which was internal to the item. The failure mode is the way or the consequence of the mechanism through which an item fails. The severity of the failure mode is the magnitude of its impact.	DSRs. DARs.	ARM Assessment Methodology.	The output should be an ARM assessment which will demonstrate satisfactory ARM performance of the plant items. The ARM assessments should also include fault recovery and reliability assessment in support of safety requirements.	Basis of Design.	ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition (see The regulatory assessment of safety cases SC.1, Engineering principles: key principles EKP.5, Engineering principles: safety classification and standards ECS.3, Engineering principles: design for reliability EDR.1-3, Engineering principles: reliability claims ERL.1-4, Engineering principles: maintenance, inspection and testing EMT3, 5-8).