Safety Case Process Diagram

The diagram below presents a high-level outline of the chronology and associations between various key elements in a typical reactor safety case. The approach to constructing a safety case for a non-reactor nuclear facility is similar. The information flow is left to right.

Starting at the left-hand side of the diagram there are two stands which run across the diagram: (a) an assessment of radiological safety associated with normal operation of the plant and (b) an assessment of radiological safety associated with the plant under fault and hazard conditions. The consideration of radiological safety for a normal operating plant is necessary since there will be some exposure of personnel to low levels of radiation when the plant is operational. There is also the potential for radiation exposure to personnel from plant maintenance activities and from stored waste arisings on the site. UK nuclear regulations set specific targets for normal operation dose levels and it is therefore expected that these are addressed separately from radiation doses associated with fault or hazard conditions.

The assessment of radiological safety under fault or hazard conditions necessarily begins with a systematic process of fault and hazard identification. The likelihood of each of these initiating events needs to be characterised, and for those which are considered to be credible, the unmitigated radiological consequences need to be determined. ‘Unmitigated’ in this context means in the absence of engineered safety measures designed to reduce the severity of the radiological consequences.

The fault analysis continues to the right. Design Basis Analysis is a rigorous and demanding method of fault analysis, aimed at providing a robust demonstration of the fault/hazard tolerance of a nuclear facility. Design Basis Analysis typically focuses on faults with frequencies greater than 10^{-5} per year and with off-site consequences greater than 1 mSv. Mitigation of the radiological consequences of Design Basis faults and hazards generally requires the provision protective safety measures whose safety functions are required to be categorised in line with their mitigative capability. The systems which deliver these functions are classified in line with the safety function categorisation. Preventive safety measures should also be considered as part of the fault analysis. Such measures may reduce the likelihood of an initiating event and/or lessen the consequences of the event. Both preventive and protective measures will reduce risk. It is expected that Design Basis Analysis will generally be conservative in its approach.

Probabilistic Safety Analysis (PSA) is carried out to complement Design Basis Analysis. The scope of PSA extends the frequency and consequence range of faults/hazards addressed in the Design Basis Analysis to cover very low frequency events (>10^{-7} per annum) and also low consequence events. PSA is usually carried out on a best-estimate basis so that the relative significance of different faults and safety measures may be determined. Beyond Design Basis Accident Analysis and Severe Accident Analysis are additional areas of analysis typically focused on identifying greater defence in depth for safety measures which may mitigate the consequences of an off-site release of radioactive material.

All strands of safety analysis are subject to the application of the As Low As Reasonably Practicable (ALARP) principle i.e. the duty holder must demonstrate that all reasonably practicable measures to reduce risk have been implemented.

Having carried out the safety analysis, it is the role of the safety case to summarise and present the analysis in a manner which supports the claim that activities on the site are safe and that risks have been reduced in accordance with the ALARP principle.

The arrow at the base of the diagram seeks to emphasise that human factors play a part in all aspects of the analysis and presentation of the safety case.

Safety Case Process Diagram