FAULT SCHEDULE DEVELOPMENT

The Fault Schedule (*FS*) should be structured to allow each node of operation to be viewed separately and should match the nodal approach to hazard and fault identification, Deterministic Safety Assessment (*DSA*) and Probabilistic Safety Assessment (*PSA*). The role of the Fault Schedule is specifically to link the hazard identification process to the assessment and justification analysis and documentation. It should provide:

- An auditable trail to the fault and hazard assessment, and identification of the credible faults.
- Identification of the safety measures that are claimed in the safety case.
- An audit trail to the definition and substantiation of safety measures.

The Fault Schedule performs a central safety case configuration management role because of its route map position between the Hazard Identification, and the DSA and PSA. It is the main vehicle that links the various elements within safety cases, between safety cases, and across equipment or responsibility boundaries.

An example process flow diagram is shown in Figure 1 which illustrates the procedure to develop a Fault Schedule as a result of either a new design or a change to an existing design for any item of plant or equipment which is identified as being of nuclear safety significance.

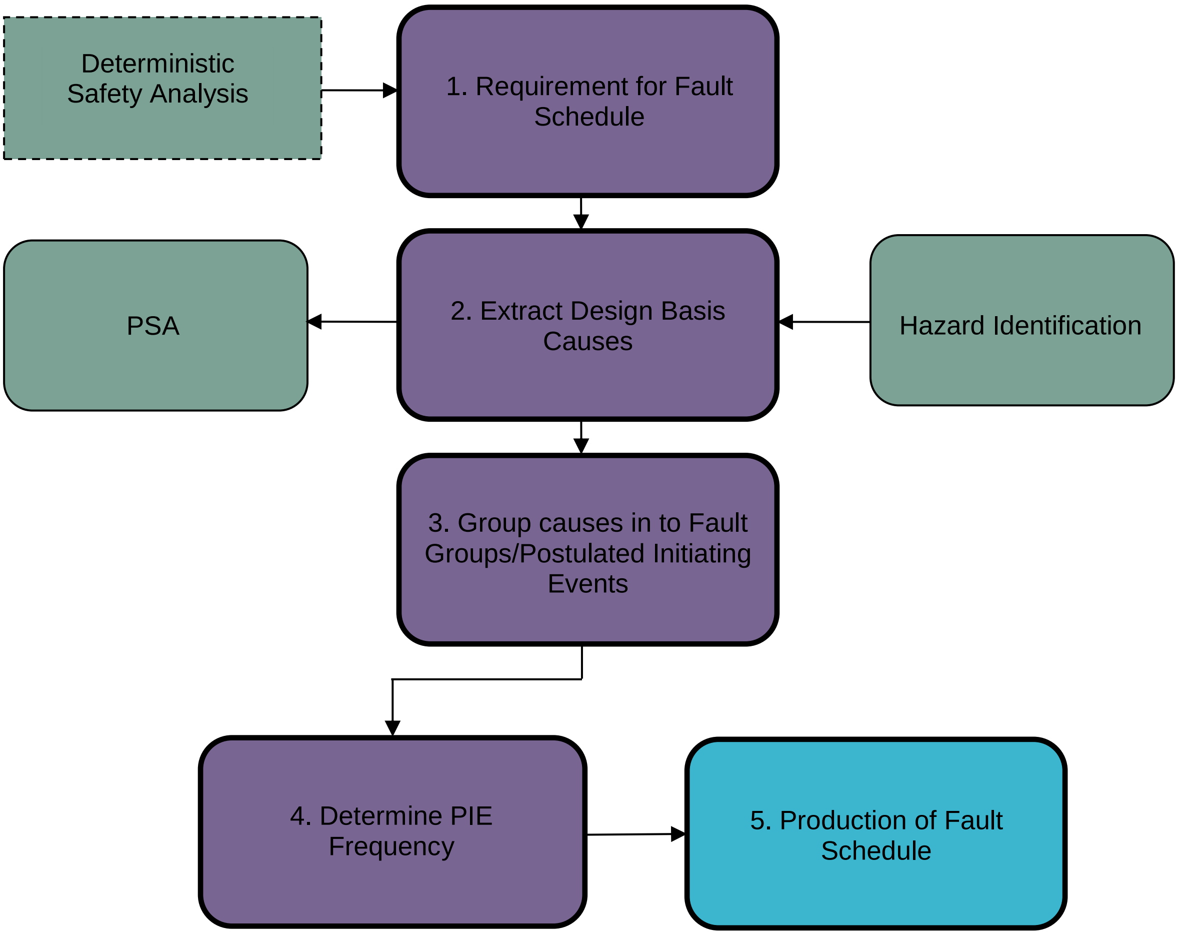
Deterministic Safety Analysis
1. Requirement for Fault Schedule
PSA
2. Extract Design Basis Causes
Hazard Identification
3. Group causes in to Fault Groups/Postulated Initiating Events
4. Determine PIE Frequency
5. Production of Fault Schedule

Figure 1: Fault Schedule development flow diagram

Additional Information & Guidance

- http://www.onr.org.uk/resources.htm