Human Reliability Assessment for 'Flex' Equipment

Martin Reid[a]
[a] EDF Energy, Gloucester, UK

Abstract: The 2011 Fukushima Daiichi incident exposed potential vulnerabilities of nuclear power plants to loss of cooling following severe hazards. In response the world nuclear community re-evaluated the potential for off-site hazards of all types and introduced equipment that could be useful in the event of an unforeseen incident. Making formal nuclear safety case claims on such 'flex equipment' is very difficult because the hazard being addressed is, by definition, unknown. However, when flex equipment is claimed to address specific hazards and faults Human Reliability Assessments can be carried out to ensure that the design of the equipment and arrangements for use are optimised and to allow a formal claim to be made on the equipment in the safety assessment.

This paper describes

- Optimisation of equipment for the unknown
- How standard Task Analysis tools can be used for assessment of tasks using flex equipment
- How the feasibility of such tasks can be substantiated
- The types of task that need to be assessed
- How these tasks may fail and how they can be assessed
- The effect of extreme environment on task reliability and timing

Flex equipment provides an important and flexible response to both known and unknown hazards. For known hazards conventional task and error analysis can provide evidence that a task is feasible and allow an estimate of reliability to be made. Where equipment is provided to address the 'unknown unknown' it is not possible to prove that the equipment is operable. It is however practical to take a user centred approach considering ergonomics to optimise the design so that it is intuitive to use, error tolerant and usable in the widest possible range of conditions.

Keywords: Flex equipment, Human Reliability, Back up equipment

1 INTRODUCTION

In order to facilitate efficient control of large systems, such as power stations, railway signalling, air traffic control and process plants control is centralised into a dedicated Main Control Room (MCR). This means that most control is carried out from a single room were the Human Machine Interface (HMI) can be well designed, the environment controlled and the users can be selected and trained to achieve a very high competence level. Most post fault actions required for nuclear safety and therefore claimed in a Nuclear Power Station safety case or Probabilistic Safety Assessment (PSA) are carried out in the MCR. In addition there are generally a small number of post fault actions that have to be carried out local to the plant being controlled.

In some cases, to back-up installed systems and to address some low frequency event sequences simple flexible systems are provided. Operation of these 'flex' systems has been assessed and included in safety cases for many years. For example, on some stations, in order to provide diverse cooling when the reactor is shutdown fire hose connection points have been provided to key heat exchangers and can be deployed if primary and secondary systems were to fail. Deployment of these systems is fully assessed and modelled in our safety cases.

The need for diverse, redundant and hazard resilient back-up systems was highlighted by the 2011 Fukushima Daiichi incident [1] where because of a very large earthquake and subsequent tsunami all

station power and cooling was lost. In response [2] EDF Energy invested in a number of work streams, for example:

- To give options to manage unforeseen incidents a flexible set of Deployable Back Up Equipment (DBUE, see Figure 1) was designed and procured. The DBUE is held partly on site, for quick deployment but most DBUE is stored off site so it is remote from any hazard affecting stations and includes robust vehicles to get the systems on site.
- The potential for off-site hazards was re-assessed to ensure that installed and on site back up equipment was sufficient to address all foreseeable hazards.

In order to assess the reliability of response to a hazard the magnitude of the hazard must be estimated. For example, although the vehicles that transport the DBUE to station are very capable, with an unlimited potential hazard they would not be able to reach site. This means that making a formal claim on the DBUE in response to an *unknown* event is **not** possible. However, it is possible to make claims for use of this equipment for extreme events as long as the event magnitude is defined and the task is shown to be feasible.

Figure 1 EDF Energy DBUE

In order to optimise the usability of the DBUE Human Factors and Ergonomics processes and data were used to ensure that the equipment was designed with the user in mind considering possible extreme weather conditions, and good usability is now built into the design.

The re-evaluation of off-site hazard identified a small number of areas where the frequency of significant natural hazards was determined to be greater than previously assessed. The revised hazard intensity and frequencies challenged the existing safety cases.

Figure 2 New Flood Wall

The concept of a hierarchy of control is well known and is integrated into EDF Energy processes [4]. This states that protective systems should have characteristics as near to the top of the following list as long as it is reasonably practicable:

- Passive safety measures that do not rely on control systems, active safety systems or human intervention,
- Automatically initiated active engineered safety measures,
- Active engineered safety measures that need to be manually brought into service in response to the fault,
- Administrative safety measures.

Flex systems are near the bottom of this list and passive measures are therefore preferred over flex systems where the time and cost of providing the passive protection is not disproportional to the risk mitigated. Where the hazard re-evaluation showed the current arrangements were inadequate new safety cases were developed. In the short term flex systems where claimed but in the longer term more passive measures were used, for example a new flood wall (Figure 2).

Despite the preference for passive protection flex systems can provide a reasonably practical means of providing additional barriers or to address lower frequency events. If they are to be credited in the safety case (and PSA) they need to be shown to be functionally capable and sufficiently reliable.

At around the same time, new flex equipment was being developed for other licensees and approaches were developed in parallel with the approach described in this paper for assessment of the reliability of their deployment. For example, MacLeod et al [3] report a Human Reliability Assessment (HRA) method for assessment of such equipment. This uses a set of screening human error values and a decision tree to develop a task human error probability. For high wind the decision tree considers the following; base Human Error Probability (HEP), whether there are obstructions, if the action can be taken after the event, if the wind is below safety limits, what time margin is available and if independent verification would be available. This approach is analogous to our approach but is more structured and less flexible as it uses a limited number of factors to determine the overall HEP.

Our approach is to demonstrate that the actions are feasible in the postulated conditions and then use standard HRA tools, applying Performance Shaping Factors (PSFs) to reflect the conditions to determine the HEP.

This paper describes how HRA was used for claimed flex equipment, some of the challenges, potential failure mechanisms and lessons learnt.

2 APPROACH FOR THE HUMAN RELIABILITY ASSESSMENT OF FLEX EQUIPMENT OPERATION

If a system is to be claimed it needs to be shown to be functionally capable, its deployment feasible and sufficiently reliable. Flex systems can be assessed in the following steps:

1. Document the identified hazard;
2. Identify the systems that will be used from detection through decision making to system deployment;
3. Qualitative assessment of system operation;
4. Task error probability assessment;
5. Finalise the assessment.

These steps are discussed in the sections below.

2.1 Document the initiating fault or hazard

While this is not part of the HRA it is key to its success. In order to perform the HRA it is essential that the hazard and fault sequence is defined. It is essential to identify:

- Fault sequence and symptoms
- The intensity of the hazard, for example the wind speed, on site flood depth etc.
- The duration of the hazard.
- Pre-warning of the hazard.
- The geographical spread of the hazard and potential for off-site support.

Predicting possible hazard strength and duration for a 1 in 1000 or 1 in 10,000 year event will inevitably be difficult and open to debate. It would be easy to shortcut such assessment by taking a conservative approach. While this makes justifying the hazard assessment easier it makes assessing the potential response to such an event more difficult and should be avoided. The hazard assessment should therefore be on a best estimate basis and not be overly conservative.

In some elements of our response to the events at Fukushima Daiichi we spent time considering ‘what if’ scenarios. Including more extreme wind and flooding than is predicted as a 1 in 10,000 year event. These ultimately proved fruitless because there is always another more extreme possibility. For the most part environmental conditions in the UK are relatively benign compared to other parts of the world but the historical record does show severe storms causing extensive flooding and damage. It was this type of event we conceded were possible. Such storms would be accompanied by very high

winds. We carried out research to determine if we could be confident that staff would be able to work in the predicted wind. Our conclusion was that making claims on staff during such extreme conditions is **not** generally reasonable and efforts are better spent on assessment and optimisation of pre- and post- event response where the conditions would be more benign.

2.2 Identify the systems that will be used from detection through decision making to system deployment

Having documented the fault sequence an appropriate risk mitigation strategy can be selected considering the hierarchy of control discussed above. Flex systems are low on the hierarchy but are suitable for low frequency events, as additional protection or as a short term measure. For example, at one of our sites, the reassessment of hazards identified that on-site flooding was possible with a return frequency which required, according to our safety rules, two lines of protection. That is two independent, functionally capable systems to maintain nuclear safety. A strategy was developed to achieve these two lines in the short and medium term. In the short term the lines were:

1 Hazard warning, shutdown, plant preparation and maintenance of near normal post trip reactor cooling systems
2 No warning, reliance on pre-installed flood protection measures on a small number of key systems.

Line 1 required a detailed procedure for hazard warning, decision making, pre flood preparation and post flood recovery. All of these actions needed to be shown to be feasible and sufficiently reliable and were subject to a formal HRA.

As line 2 is essentially passive, the HRA associated with it is very limited and was largely concerned with ensuring that installation of the new flood protection to key buildings was optimised so that it remained in place. This was achieved by ensuring that building access was still available and by providing administrative control to warn staff and to provide mechanisms for necessary temporary removal and restoration of the flood protection.

It was recognised that these lines are complex and open to gradual erosion through procedural violation and low on the hierarchy of control and judged not to meet safety case requirements [4]. It was therefore decided to build a new site flood wall (shown in Figure 2). Once installed this reduced the reliance on plant preparation but in the meantime line 1 actions had to be substantiated.

2.3 Qualitative assessment of system operation;

The required tasks to achieve the claims need to be systematically documented. In the example above a whole site, extreme weather Hierarchical Task Analysis (HTA) was developed (see Figure 5). This identified what actions would be required in the postulated events, their order and priority. It was then necessary to assess and demonstrate that the actions would be:

- Feasible,
- Sufficiently reliable,
- And, to identify any reasonably practical options for improving operability and therefore reliability.

These aims can be achieved by using a task analysis based HRA process. The HRA assessment of any task should be based on a firm understanding of the task, its context and the capabilities of the people carrying it out. There is therefore no reason not to use the same techniques that are used for CCR tasks for deployment of flex equipment. An application of such techniques was presented in [5]. The approach is summarised in Figure 4 and summarised in the sections below.

2.3.1 Task and Error Analysis

Conventional task and error analysis can be used for the assessment of flex equipment operation. A HTA describing the task goals, task and task order provides a framework for a Tabular Task Analysis (TTA). The TTA describes the tasks in detail and allows the analyst to record their judgements on

task feasibility. For example, the controls are within reach and do not require excessive strength and are operable in the required personal protective equipment – e.g. gloves.

The TTA can then be used as the basis for error analysis. In the error analysis, potential errors are postulated, their consequence identified and recovery modes identified. This leads to a set of credible errors that could lead to system failure. Efforts can be made to reduce or mitigate these errors by changing the design or providing improved procedures/training.

2.3.2 Data collection

The task analysis should be based on robust information. Such data can come from task demonstrations, walk throughs, talk throughs and interviews with task subject matter experts.

The data collection programme should identify; the required tasks, PSFs, observed errors, checking tasks, task feedback and other opportunities for recovery.

Often potential errors would be revealed. For example, hose coupling errors are easy to see and may be recovered. These types of errors delay deployment rather than cause an unrecoverable failure. A key part of the data collection is therefore to identify task times, so that a base task time can be established and models of potential task recovery developed.

Figure 3 Task Demonstration

2.3.3 Time to respond

Plausible errors in deployment of flex equipment are generally simple and often recoverable. The main effect of errors is therefore to slow deployment and to take staff away from other potentially important tasks.

A timeline should be developed that shows the required tasks in order and uses task times to build a representation of the whole task. The timeline should consider potential errors and show there is margin for recovery. For example, in a task where many hoses are connected it is very unlikely that all connections fail but possible that one fails. Recovery of the possible error should be included in the task timeline. This would include the time to determine flow has failed, to walk the hose line, rectify the problem and restart the system.

Data for task times can be obtained through task simulation and observation or expert judgement. In some cases these times may need to be changed to account for poor environmental conditions. Previous work by Umbers and Reierson [6] identified a set of time multiplication factors that account for poor working conditions. We used these to alter base times to reflect the postulated conditions. For example, nominal time is multiplied by 2 for laying hose over rubble.

The task timelines can then be combined with other task assessments to determine a whole site response.

2.4 Task error probability assessment;

The primary reason for the assessment of these tasks is to ensure that risk reduction measures have been taken and then to show that the tasks are feasible and sufficiently reliable. Feasibility is shown through the qualitative task assessment which will also identify options for task improvement. These improvements should be addressed if reasonably practical to do so; it is here that real safety improvements can be made which is clearly more important than a demonstration of theoretical safety. Having shown that a task is feasible the task reliability can be considered.

The tasks may fail because of:

- Running out of time.
- Decision making before starting the task.

- Un-recoverable errors.

In some cases preparation for extreme weather requires early plant shutdown. In which case, staff have a difficult decision to make. Either shutdown, with the inevitable financial cost and make the plant safe against the possibility of a significant weather event which may never arrive or hope that the predicted conditions do not occur. Ideally such conflicts would be avoided by ensuring that suitable measures can be taken without early reactor shutdown. This is one reason a new flood wall was built (Figure 2). HRA of decision making is possible but outside the scope of this paper.

Generally flex equipment is claimed after either an infrequent hazard or a combination of faults. In either case the required reliability is generally modest. For example, at one of our stations failure of the external power grid and all station power is conceded to be possible but as it is the result of an off-site fault and an un-specified common cause failure its frequency is very low. A flex emergency petrol driven boiler feed system is available to provide sufficient boiler feed to cool the reactor. The claim on the system is 0.1 per demand which, given the low demand frequency, is sufficient to make the fault sequence non-dominant i.e. the fault sequence becomes insignificant. This is typical; the claims on flex systems are either unspecified or modest. This means that if it is possible to show that use of the flex equipment is feasible, justifying the modest reliability claim is straightforward. This could be achieved by expert judgement but we tend to use a normal Human Reliability Quantification (HRQ) tool such as NARA [7].

Human reliability data for use of systems in extreme environments is, of course limited. Using conventional HRQ tools in conditions which are postulated to be extreme is difficult to justify. To overcome this we take a two-step approach, demonstrate that the task is feasible and only if it is quantify the reliability. We therefore filter out scenarios which require operations in the midst of severe hazards and would take the conditions outside what is reasonable for the HRQ tools. In order to make claims on flex systems we have had to consider what are conservative limits of human performance in hazards. For example:

- Floods - we do not claim wading through water because:
    - Underwater obstructions or holes may not be seen
    - Even a shallow but fast moving water can be impassable
- Winds – High winds can make communication difficult, deploying equipment hazardous and cause wind blown missiles. The feasibility of the task will depend on the nature of the task and the wind. For a very simple action that simply required external access it may be possible to make a claim in a wind of up to force 11 beyond this claiming external access is difficult. For more complex tasks such as flex deployment the point when a claim is feasible is less clear and needs further work.

Having qualitatively assessed the task and shown it is feasible it is then reasonable to use a conventional HRQ tool such as NARA to quantify the potential errors.

NARA requires tasks to be qualitatively assessed so that Performance Shaping Factors (PSFs) are understood and potential errors identified before error probability is quantified. The tasks identified in the task analysis are grouped to a level of task decomposition that matches one of NARA's 13 Generic Task Types. PSFs are identified from the task analysis and used to modify the base task reliability to reflect the expected task and environmental conditions. The resulting assessment is based therefore on a qualitative judgement of feasibility and an assessment of the task and PSFs to derive an HEP. The resulting HEP may be used directly in the safety assessment or used to support a rounded up figure.

2.5 Finalising the Assessment

The last step is to document the assessment and ensure it is correct. The documentation will depend on the nature of the hazard or faults being addressed by the flex equipment but should include sufficient information for the judgements made to be confirmed by an independent review and to be re-evaluated if they need to be updated later. Just like any other claim the assessment should be subject to independent valuation.

3 CONCLUSIONS

Flex equipment can provide an important and flexible response to both known and unknown hazards but it should be recognised that passive or automatic systems are more reliable and should be used when reasonably practical.

For known hazards conventional task and error analysis can provide evidence that a task is feasible. Having shown that a task is feasible it is, by definition, within the capability of staff and it is then reasonable to use normal Human Reliability quantification methods to estimate the reliability of deployment and operation of such systems. It is however important to recognise that in extreme conditions it may not be reasonable to claim deployment of flex equipment and the claim may need to be limited to pre-deployment or post hazard deployment.

There are a number of areas where further research would strengthen the assessment of the use of flex systems and provide insights into optimising its design and use. These include:

- The limiting weather conditions – wind, temperature etc;
- Limiting flood depth, particularly of moving water;
- Data on the effect of poor conditions on flex system deployment in terms of time delay and error causation.

Such data would help to increase the scope of the use of flex equipment for low frequency – high intensity events. However, where flex equipment is provided to address the 'unknown unknown' it is not possible to prove that the operation of the equipment is feasible in all conditions as whatever you design it for a more severe event can be postulated. It is however practical to take a user centred approach considering ergonomics to optimise the design so that it is intuitive to use, error tolerant and usable in the widest possible range of conditions.

4 REFERENCES

[1]. http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/fukushima-accident.aspx

[2]. https://www.edfenergy.com/sites/default/files/japanese_earthquake_response_programmes_final_report_to_the_onr.pdf

[3]. Simplified Human Reliability Analysis Process for Emergency Mitigation Equipment (EME) Deployment Don MacLeod, Gareth Parry, Barry Sloane, Paul Lawrence, Eliseo Chan, and Alexander Trifanov. Probabilistic Safety Assessment and Management. PSAM 12, June 2014, Honolulu, Hawaii

[4]. EDF Energy (2017). ALARP Decision Making for Safety Cases and Implementation of Modifications BEG/SPEC/DAO/003 Revision 004

[5]. Davies, A and Reid M. Qualitative Task Assessment in support of Human Reliability Assessment and Task Optimisation (pre-NARA assessment). Presented at IFE Norway 2017

[6]. Umbers, I.G. and Reierson, C.S. (1995) Task analysis in support of the design of a nuclear power plant safety system, ergonomics, 38, 3, pp. 443-54.

[7]. Kirwan B., Gibson H., Kennedy R., Edmunds J., Cooksley G., Umbers I. (2004) Nuclear Action Reliability Assessment (NARA): A Data-Based HRA Tool. In: Spitzer C., Schmocker U., Dang V.N. (eds) Probabilistic Safety Assessment and Management. Springer, London

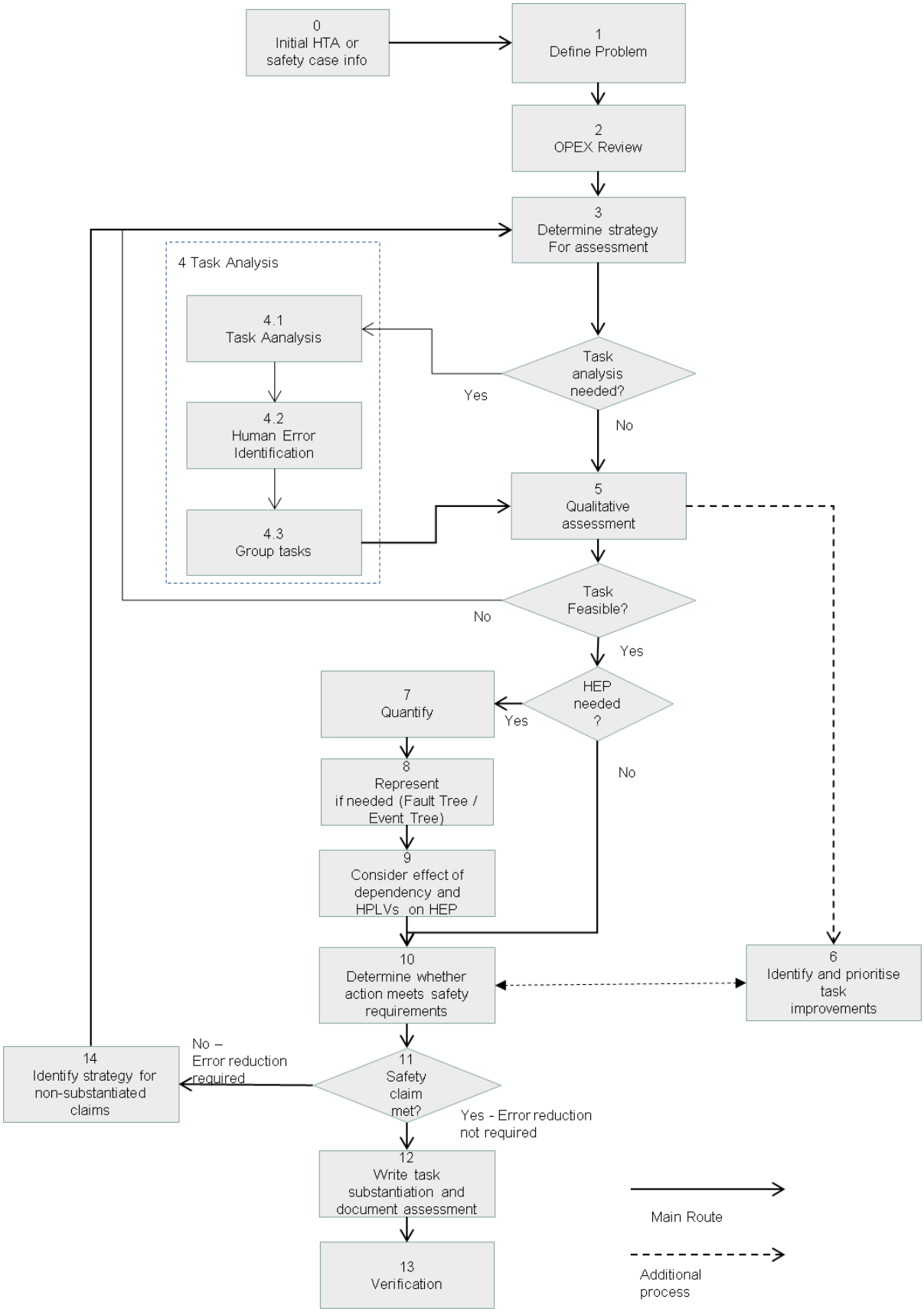

Figure 4 Generic Human Reliability Process

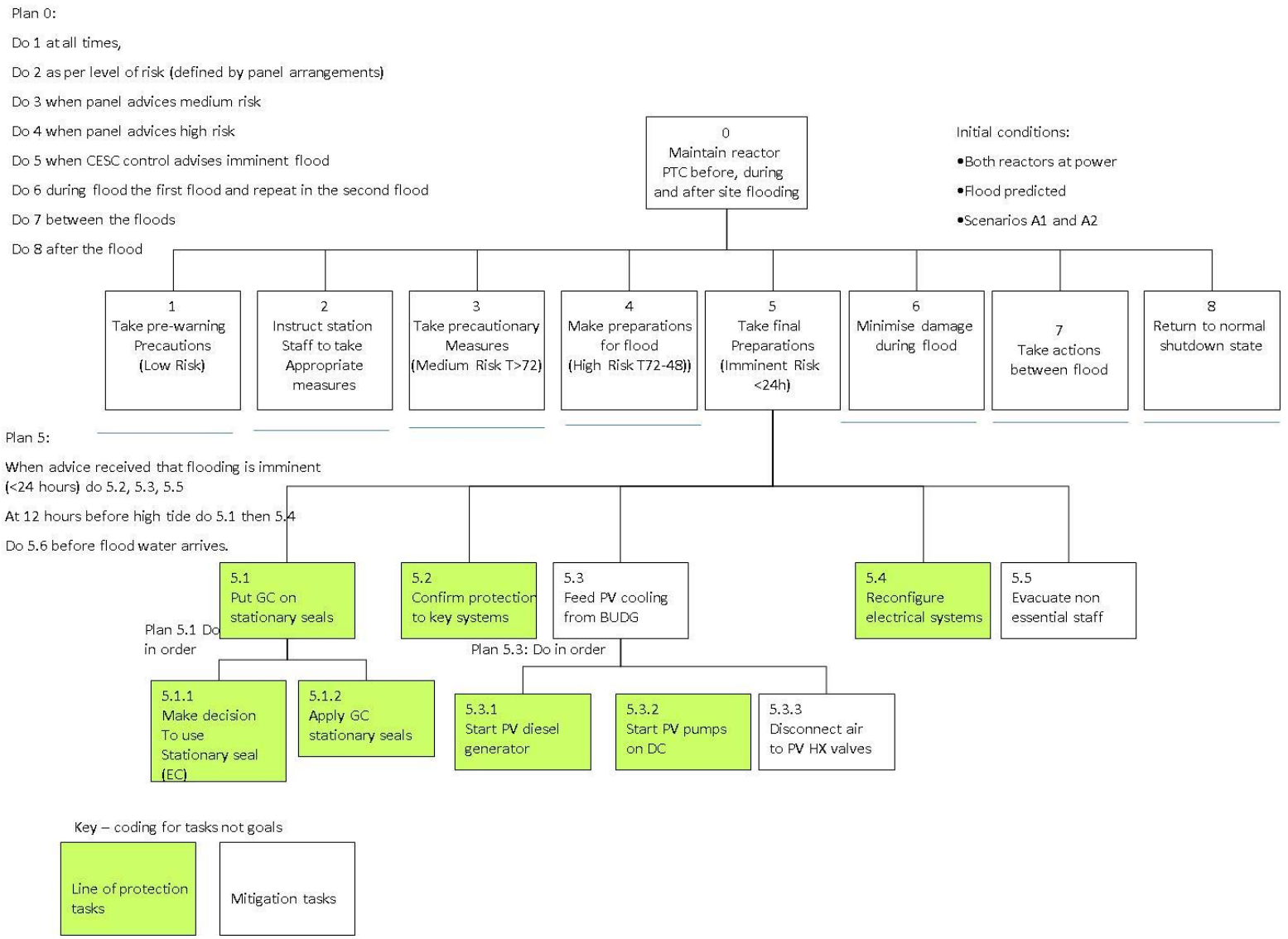

Figure 5, Extract from a Whole Site HTA for Site Flooding