Can we quantify human reliability in Level 2 PSA?

Lavinia Raganelli[a,b,*], Barry Kirwan[c]
[a] Imperial College, London, United Kingdom
[b] Corporate Risk Associate, London, United Kingdom
[c] Eurocontrol, Brétigny-sur-Orge, France

Abstract: In current safety practice in the nuclear power domain, the demand for Level Two PSA by regulatory organizations has become mandatory, and this has received greater priority after the Fukushima-Daiichi accident in Japan in March 2011. However, there are many challenges in the process of performing a Level Two PSA. Most of the challenges are related to uncertainties in the plant state in such accident scenarios. However, even assuming that it is possible to know the exact extent of damage in a selected scenario, a key question remains: "What level of detail is required for describing the human response?" In reality, damage to equipment and the exact plant status are not predictable; therefore Severe Accident Management Guidelines (SAMGs) and Emergency Operating Procedures (EOPs) offer guidelines for operator behaviour rather than specifying the procedural details of actions. In this paper the appropriate level of detail for the analysis of operator action in Level Two PSA models is discussed, as are the difficulties in conducting Human Reliability Assessment (HRA) for vaguely defined actions. It is found that most current HRA approaches for Level 2 PSA rely heavily on expert judgment, but is such expertise valid? This paper explores potential ways forward for HRA in Level 2 PSA.

Keywords: PRA, Human Factors, Uncertainty, Level 2.

INTRODUCTION

A Severe Accident scenario in a nuclear power plant could lead to loss of containment integrity and a melted core. The consequence is an uncontrolled release of radioactivity into the environment. Level Two PSA is concerned with the progression of accident sequences until the release into the atmosphere and the ability of the containment to withstand overpressurisation. In current PSA practice the modelling of Level Two conditions has assumed greater importance and major regulatory bodies have asked for an updated and improved modelling of severe accident sequences following recent accident history, in particular the Fukushima-Daiichi nuclear power plant accident in Japan on 11th March 2011, which culminated in a meltdown of three of the plant's six reactors, and a large release of radioactive material into the environment. This was the second accident of this magnitude, the first being Chernobyl in 1986 in the Ukraine. These are the only two accidents so far in civil nuclear history to reach a level of 7 on the International Nuclear Event Scale.

In a Severe Accident time-frame the operators play important roles. They need to assess plant status using the information available during the accident sequence, and they then need to operate the available auxiliary systems to maintain or reinstate core cooling to prevent core damage and mitigate plant damage, and avoid atmospheric release once the core has been damaged. The modelling of operator actions in a Level 2 time-frame has not yet been formalized. To date, in a PSA model the practice consists of introducing general, high level actions, and assigning them a probability of failure based on expert judgement. But given the potential severity of such accidents that L2 PSA models, and the given the critical role of the operators during severe accident evolution, both the validity and the utility of the assessment of the human role must come under scrutiny in terms of its validity and utility in assuring reactor safety. This paper therefore discusses the key issue in assessing the human role in severe accidents, namely the large uncertainties that are associated with Level 2 PSA models, especially how they influence human action assessment. The paper then discusses how HRA in L2 PSA is currently done, and explores ways to improve the quality, validity and utility of the process.

* l.raganelli13@imperial.ac.uk

First, Level 2 PSA itself must be outlined in terms of its objectives and its requirements, and this is discussed in the next section.

REQUIREMENTS FOR LEVEL 2 PSA AND ITS OBJECTIVES

In any process involving radioactive materials, the primary requirement is to ensure the protection of the public, the workers and the environment from the harmful effect of ionising radiation. The main safety principle when dealing with an installation containing radioactive materials is to maintain risk As Low As Reasonably Achievable (ALARA). International Atomic Energy Agency (IAEA) safety standards establish specific requirements in terms of risk assessment and risk acceptability. The standards include the requirement to carry out both a deterministic and a probabilistic assessment of risk. Overall, a PSA provides a methodology for identifying accident sequences that originate from various Initiating Events, and it allows a systematic evaluation of accident frequencies and consequences. Internationally, three levels of PSA are generally recognised:

Level 1 PSA, where plant design and operations are analysed to identify possible event sequences that could lead to core damage. Level 1 PSA provides insights into design weaknesses and into accident prevention.

Level 2 PSA, where a quantitative assessment predicts the consequences following reactor fuel damage. Level 2 PSA is concerned with the analysis of how a release of radioactive materials from the reactor core could lead to an environmental release. A Level 2 PSA provides input into assessing the importance of accident sequences leading to core damage and on the importance of mitigation of severe accidents consequences.

Level 3 PSA, where the consequences of a radioactive release outside of the reactor building are evaluated. In this case the focus is on the environmental contamination and on public and workers' health.

The benefits gained from performing a Level 2 PSA include:

- making sure that systems to mitigate consequences are in place;
- verifying the aptness and the limits of the containment for retaining radioactive materials;
- providing plant personnel with indications for action in case of severe core damage accident sequences.

The Level 2 analysis develops along two trajectories, one is containment response to fuel meltdown through Containment Event Trees (CETs), and the other is progression of the accident sequences through Accident Progression Event Trees (APETs). It is important to be aware of the limitations of modelling. Any limitation affecting the Level 1 PSA will be inherited by the Level 2 PSA. Moreover, if the starting point for a Level 2 assessment is a Level 1 PSA there might be underdeveloped sequences and portions of the Level 1 model. Level 1 PSA is mainly concerned with core damage frequencies, not with the structural safety of the containment and its related systems, thus differences in the development of a station model. If the containment integrity has not been considered in the Level 1 model, the experts need to create a containment model in the Level 1 frame before developing a Level 2 model.

Considering the logic models that need to be developed in a Level 2 scenario, it is important to remain true to the accident sequence chronology. To this end IAEA recommends [1] to divide the accident sequence into three parts:

- Phase 1: Immediate response of the plant to the plant damage state caused by the initiating event through the early period of in-vessel core damage.
- Phase 2: Late period of in-vessel core damage up to failure of the reactor pressure vessel.
- Phase 3: Long term response of the plant.

In a Level 1 analysis numerous sequences and initiating events that lead to core damage frequencies are identified. When the effectiveness of the containment integrity needs to be assessed, there is no

advantage in treating every Level 1 sequence individually after core damage and until release frequency. Hence the IAEA recommends that [1]:

> "Accident sequences should be grouped together into plant damage states (PDS) in such a manner that all accidents within a given plant damage state can be treated in the same way for the purposes of the Level 2 PSA."
>
> "Plant damage states should represent groups of accident sequences that have similar accident timelines and generate similar loads on the containment, thereby resulting in a similar event progression and similar radiological source terms."

THE ROLE OF THE OPERATOR DURING SEVERE ACCIDENTS

IAEA provides international guidelines on management of accidental scenarios following core damage. The Severe Accident Management guidance gives some information on how to manage and organise recovery and mitigation when extremely unlikely events are happening. During these scenarios the role of the operator is a key one, as automatic responses of the plant control and auxiliary systems may no longer be available or reliable. The objectives of severe accident management are given as follows [2]:

- Preventing significant core damage;
- Terminating the progress of core damage once it has started;
- Maintaining the integrity of the containment as long as possible;
- Minimizing releases of radioactive material;
- Achieving a long term stable state.

As Vinh Dang et al (2009) [3] report, the actions the operators are required to perform during Level 2 accident sequences are different to routine ones, and are also different from those that they perform in known emergency conditions. The main differences are outlined below and are taken directly from the paper.
Some of the most significant differences are:

- The prescriptive character of EOPs (Emergency Operating Procedures) vs. the informative nature of SAMGs (Severe Accident Management Guidelines). EOPs represent a plan that should be followed to the extent possible while SAMGs are more akin to a set of options with informative character. This distinction is not completely unambiguous since there are a few areas with scope for the control room operators' judgment in the EOPs and, conversely, some accident measures with clear criteria within the SAMG.
- The optimal response (whether or not to implement the SAM measure) cannot be fully determined in advance. One of the reasons for the informative rather than prescriptive character of SAMG is that the uncertainties concerning accident progressions hinder the determination of the optimal response in advance. Some of these uncertainties will not be eliminated during the accident, such that the determination of the optimal response for the situation "at hand" remains subject to uncertainties.
- The responsible staff for making the decisions within the EOPs and the SAMG. The decision-making responsibility for SAMG actions lies with the head of the Emergency Response Team (ERT), who is advised by the SAMG team, the Emergency Response Organization (ERO), and, in some cases, other external experts. Some SAM measures require the agreement of the authorities.

- The need to consider radiation exposure in assessing the actions to implement the SAM measure, in terms of feasibility as well as constraints on the execution.

There are usually several choices the plant manager and the operators need to face in order to reach a long term stable state, and a few points are highlighted below, see [2] for further reading. The operators need to be aware that auxiliary and support system could be used for a different purpose than originally intended. Also the option of restoring failed equipment should be considered. All levels of personnel present at the station need to collaborate fully with any external authority or with new personnel reaching the power station. The station manager needs to be aware of how the management hierarchy changes, e.g. whether an emergency team arrives at station, and how to best secure the exchange of information between the new arrivals and the plant team.

The potential for wrong diagnosis by the operators should be minimised by providing redundancy and diversity of signals and feedback. However, the signals should not be confusing and it should be possible for the operator to detect if the signals are giving a wrong warning. In an ideal scenario the operators will have been trained through simulator exercises to respond and react to severe accident conditions. Guidelines such as SAMGs or similar, should also be provided to help taking decision. The SAMGs should always outline both advantages and disadvantages of any mitigation actions.

UNCERTAINTIES IN LEVEL 2 PSA

Uncertainties Due To Physical Model

To obtain a suitable PSA model the dynamics of a Severe Accident need to be understood. However, Severe Accidents, by definition, are extremely unlikely to happen; if the design of the station is effective the probability of its occurrence is practically eliminated ($<10^{-7}$ events per reactor year). Due to this definition, very few SA sequences have been observed so far, the most notable examples being at Fukushima-Daichi station and Chernobyl.

The lack of a sufficient number of observed events means a scarcity of data that would demonstrate the evolution of a Severe Accident. Thus, to understand the development of a Severe Accident the analysts use integrated system computer codes that portray the evolution of the accident from the molten core condition to containment failure. The codes are able to simulate possible plant scenarios, using as input physical parameters describing plant conditions.

Given the lack of data and the difficulties in validating the codes, the models are affected by high uncertainties. It is practical to divide uncertainties related to any physical process into *epistemic* and *aleatory* uncertainties. The first is due to lack of sufficient information while the second is tied to the statistical variation of recurring phenomena. Therefore, in a Severe Accident scenario aleatory uncertainties stemming from the different possible accident developments limit the accuracy of the model. At the same time epistemic uncertainty on the signal and plant feedback impacts on the effective management of the accidental conditions.

To develop an effective time-dependent model in an integral system code (MAAP, MELCOR) the engineers should identify the parameters that regulate the development of the accident sequence. The dominant parameters are related to the following:

- Degree of core damage and configuration of debris/molten core
- Core/corium coolability
- Hydrogen release into the containment
- Reactor Coolant System integrity
- Operator actions that could change the event sequence.

Practically speaking the dominant phenomena usually influence the core coolability, affecting the classical thermal hydraulic parameters: pressure, heat transfer coefficient, temperature, viscosity, etc.

Any mechanism that avoids bypass or failure of the Reactor Cooling System (RCS) is certainly influencing the outcome of an accident scenario. However, if the RCS fails, a successful containment of radionuclides could be still achieved if there are mitigating features that keep the radioactivity in the containment. So the first logical step would be to understand if there are phenomena that allow the core to be cooled inside the Reactor Pressure Vessel.

Once the dominant parameters have been identified, MAAP or similar codes can run different analyses, varying these parameters, namely the heat exchange coefficient of a partially molten core, or the size of the of the primary circuit leak. The variation range of the parameters is usually given by experimental results or theoretical models. Once a sufficient number of simulations have been run, it is possible to extrapolate uncertainties of the parameters conditioning each event in an accident sequence.

The issues in uncertainty evaluation for instrumentation feedback have not been solved. In the ASTEC (Ref) 2013 report it is stated how the instrumentation available during the Fukushima-Daichi accident did not provide sufficiently reliable feedback on cores and spent fuel ponds even weeks after the accident. Also the lack of reliable signals for longer than the first year did not allow precise location of core debris. Unreliable instrumentation renders SAMG implementation difficult, because if the plant status in not well diagnosed, it is impossible to successfully manage the accident sequence. Appropriately performing instrumentation needs to be developed. As an alternative, already-existing instruments need to be positioned diversely or redundantly to allow a better follow-up of core degradation and cooling conditions. These uncertainties influence the operator knowledge of the plant status and so they impact the probability of operators performing the correct action.

Although the uncertainties introduced in a Level 2 PSA due to inaccurate instrumentation feedback are not necessarily considered explicitly when evaluating the Human Error Probability, they could be. The impact of inaccurate instrumentation feedback on operator performance can be quantified using HRA techniques such as NARA (Nuclear Action Reliability Assessment) or SPAR-H (Standardised Plant Assessment of Risk – HRA). Both these techniques contain a specific performance shaping factor related to feedback. The maximum effect on the Human Error Probability for this factor can range from x30 (NARA) to x50 (SPAR-H). It should be noted that in the recent Empirical Benchmark of HRA techniques led by the USNRC [4] that the size of this factor was found to be appropriate. One of the scenarios used in the Benchmark included misleading instrumentation, which had a significant impact on human performance in realistic real-time simulations with licensed operators and industry EOPs.

Uncertainties the PSA model

Once a Severe Accident development is understood, the next step is to build Event Trees that cover the possible paths of the accident sequences. The ETs, as noted earlier, are Accident Progression Event Trees and Containment Event Trees. During the transition from L1 to L2 the frequencies resulting in a damaged core are grouped into Plant Damage States. Then the APETs are developed, showing the possible evolutions of an accident sequence. The evaluation of each accident sequence frequency is carried out explicitly considering the dependent probabilities of all the events occurring in the sequence. The probabilities related to each branch are conditional probabilities, thus the calculation tools need to be accurately set. In each APET (or CET) branching node the possible outcome path is dependent upon multiple parameters. Deterministic calculations need to assess the value range the parameters could assume for a certain path to be taken. The input is a probability distribution or a point value with a range of uncertainty. The analyst then chooses the best way to represent the uncertainty.

Before and after running a Monte-Carlo simulation, in order to identify the relevant parameter sensitivity studies can be carried out, it would help to select the critical input data influencing the release frequency and intensity. Sometimes, if a certain parameter is subject to high uncertainties, the

easiest route is to assign it a subjective probability distribution and then verify the influence it has on the overall release frequency distribution through Monte-Carlo simulation.

CURRENT LEVEL 2 PSA MODELLING PRACTICE

Once the Level 2 PSA model has been built, the frequencies or probabilities in each event tree node need to be assigned. The probabilities result from expert judgement, software outputs, plant walk downs and simulator experiments. They can be updated during the plant lifetime if new data becomes available. The whole evaluation process needs to be recorded for future reference. In recent years, Level 2 PSA has been requested by regulatory bodies in many nations having a developed nuclear program. Internationally, for Level 2 PSA the reference models are the already cited IAEA standards and the NRC NUREG-1150 report.

In 2013, the EURATOM consortium has conducted a report relating the state of the art for Level 2 PSA performed in various European countries [5]. The scope of the study is to provide an update of differently implemented Level 2 PSAs and to encourage the reduction of such differences. Most of the level 2 models are somewhere between a full scope PSA model and a limited scope one. As a matter of fact, the different national regulatory bodies have pushed the developers towards prioritising different aspects in the modelling, and thus different levels or detail. As a result, the general IAEA guidelines and the NRC NUREG-1150 have been followed to different levels.

In the Sizewell B Level 2 PSA [6] the process of assigning probabilities to the nodes of the different trees is showed in detail. Because of the peculiarity of post melt core scenarios the branching ratios of the phenomena are not known in detail, so expert judgment is heavily relied upon. The probability of failure, and of success, assigned to each node results usually from an informed decision made by experts. The knowledge could come from different sources; multi-physics computer codes, literature, experiments, other expert judgements, other plants. Unfortunately due to imperfect recording procedures it is not always possible to trace how the choices are made, so it is difficult for subsequent analysts to form an idea on how information leading to a certain choice was gathered.

CURRENT PRACTICE IN MODELLING OPERATOR'S ACTIONS

The role played by the operators during Severe Accidents becomes part of the Level 2 PSA model, because operator actions can significantly influence the outcomes of recovery and mitigation. However the choices made by practitioners on how to include human performance in a PSA Level 2 model differ depending on the resources available and modelling choices. Thus there is a continuous exchange of information between PSA model, SAMGs and thermal hydraulic analyses.

During Severe Accidents the operators are expected to intervene and bring the station to the safest possible state. The Level 2 PSA model needs to reflect the possible choices of operators and how they achieve their goals. The dependencies between actions performed in Level 1 and those that should be performed in Level 2 also have to be explored.

The development of Severe Accident Management Guidelines (SAMGs) is strongly encouraged by IAEA and international regulatory bodies. The scope of such guidelines is to help operators perform the necessary interventions in case of Severe Accidents. As noted earlier, there are substantial differences between the description of mandatory actions given to operators in a Level 1 PSA context and that given during a Level 2 Severe Accident scenario. The SAMGs are informative in nature, describing the context in which the operator should act. The informative approach to management guidelines is justified by considering the following factors:

- The operators have received at least some training for reacting to Severe Accident scenarios
- The operators know in depth the plant response in standard conditions as well as the plant peculiarities and characteristics
- There is uncertainty on the feedback available to the operators and which alarms and signals are going to be available

- It could be necessary to operate systems outside their standard functions and objectives
- Some support from Emergency Response Team will be available.

When the SAM actions are modelled in a L2 PSA, usually the level of detail remains unvaried, as there is no task breakdown. Then, HRA analysts are called to evaluate a very general action, e.g. starting HP feed.

Figure 1 Severe Accident mitigation actions for Maanshan NPP

The Major Mitigation Actions in SAGs and SCGs

SAGs	Major Mitigation Actions	SCGs	Major Mitigation Actions
SAG-1 Inject into the SG	Inject into the SG by using auxiliary feedwater, condensate, and firewater pumps.	SCG-1 Reduction of radionuclide releases	Use containment sprays and fan cooler system, etc., to reduce the fission product release.
SAG-2 Depressurize the RCS	Open pressurizer PORVs and RPV head vent to depressurize the RCS.		
SAG-3 Inject into the RCS	Inject into the RCS by using high head safety injection, low head safety injection, and accumulators.	SCG-2 Containment depressurization	Use containment sprays, fan cooler system, and containment venting strategy to prevent containment overpressurization.
SAG-4 Inject into containment	Inject into containment by every possible path to cool RPV and allow recirculation.		
SAG-5 Reduce the fission product release	Use containment sprays and fan cooler system, etc., to reduce the fission product release.	SCG-3 Control hydrogen flammability	Stop containment heat sinks, operate H_2 recombiner, and resort to containment venting to prevent H_2 burn.
SAG-6 Control containment conditions	Use containment sprays and fan cooler system to control containment pressure and temperature.		
SAG-7 Reduce containment hydrogen	Reduce H_2 concentration by operating H_2 recombiner and igniter.	SCG-4 Containment vacuum control	Stop containment heat sinks and open pressurizer PORVs to pressurize containment.
SAG-8 Flood containment	Flood containment by every possible path to cool melt core debris.		

Currently, HRA practitioners mostly rely to expert judgement, using different frameworks and approaches to justify their evaluations. The external factors, pertaining to the environment, are probably similar to those considered in a Level 1 methodology. However, it is plausible that the external factors influence is going to be different due to the different operator mind-set in a Severe Accident, especially since the operators are expected to act according to their knowledge and deductions, and not simply abide by the procedures.

In some cases existing Level 1 methodologies have been adopted (e.g. use of THERP in Spanish PWRs [5]). If so, some degree of expert judgement is required, as Level 1 techniques do not provide descriptors fully applicable to a Level 2 scenario. The argument for doing so is that the systems claimed in a Level 2 scenario are not different from those used in Design Basis Accident (DBA) scenarios. In the Level 2 PSA for Beznau (Switzerland) power station [7] the author remarks that in the human error the diagnosis and the execution phase were assigned and the overall error probability was obtained by adding the two values. Due to scarcity of date some general HEP were assigned using THERP and ASEP.

Another source of uncertainty in a Level 2 framework which clearly influences the analyst's ability to evaluate the Human Error Probability is the dependency between Level 1 and Level 2 actions. The issue with modelling dependencies is due to difficulty in understanding how actions performed in a Level 1 time-frame influence those performed in a Level 2 time-frame. Also the dependency could be tied to the operators' mental state. For example, if an operator performs an action that does not achieve the expected outcome, he may become stressed and under more time pressure, resulting in an increased likelihood of error in any future performance. At the moment the authors are unaware of an explicit model that links the dependency between Level 1 and Level 2 operator actions.

POSSIBLE APPROACHES TO IMPROVE MODELS FOR HUMAN BEHAVIOUR IN L2 PSA

As introduced above, in a HRA context, the basic issue with modelling and quantifying human reliability in Level 2 PSA is thus one of uncertainty, first over what the operators will face in terms of exact sequence progression(s), plant state, instrumentation availability and reliability, etc., and second in terms of how the operators might react in extreme circumstances (faced with fatalities, fires, etc.). The first is uncertainty in the modelling, and (in theory) could be addressed by developing a number of specific and contextualised scenarios (using experts) to give a description of how one of these scenarios would look in real life. This is similar to what simulator training developers do today, albeit taking it dramatically forward. Nevertheless, this could result in some 'bounding scenarios' which are best engineering guesses about scenario progression and what the operators would see and have available, all in an unfolding timeline. These would be contextualised stories, similar to the CICAs used in the HRA technique MERMOS, but from them it would be possible to develop detailed task analyses and then apply HRA techniques to those task analyses.

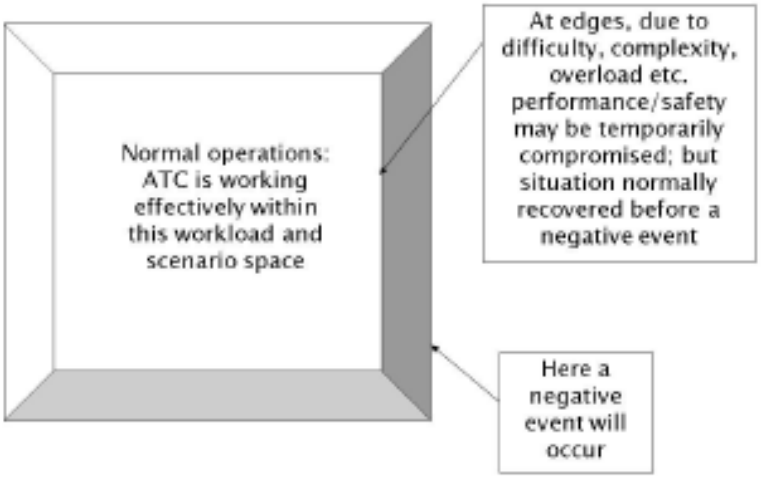
For this to work, the HRA techniques must be able to address the second uncertainty problem, namely that of determining how people would react in such scenarios. HRA techniques from an early age considered 'stress' (e.g. THERP, 1983), and then later the concept of 'burden', which concerns the emotional stress associated with, e.g. fatalities, or having to make decisions that have grave and non-recoverable consequences. The effect of burden can be very real, and can even emerge in realistic simulations and emergency exercises, leading to (temporary) decision impairment and delay in action execution. This is well understood in military situations, where the counter-measure is a high degree of training and a very strongly disciplined command control hierarchy (the latter is not appropriate to civil nuclear installations).

The determination of the impact of burden on operator behaviour is difficult due to the lack of good psychological models in this area. The factor of stress can be used, but the derivation of the stress factor in most HRA techniques has not always considered burden in this way, instead focusing on time pressure and workload. A first and obvious solution is to consider utilising expert judgement (e.g. in the framework of a HRA technique such as ATHEANA or MERMOS), but then the question is one of whether we have experts who possess *substantive expertise* (i.e. they have experienced such burdensome scenarios themselves), because if not, then frankly it is not expertise we are eliciting but engineering judgment or even opinion, and it is likely that two different expert groups may differ significantly in their assessments. However, the use of a model to elicit expert judgement whatever the model may be, should allow to estimate uncertainties surrounding those estimates.

Human Performance Envelope approach

Another way to consider the issue is in terms of what is being called the *Human Performance Envelope* [8] in the aviation field. This new concept in human performance borrows from the engineering concept of a flight performance envelope for an aircraft: within the envelope (defined by a set of key parameters such as speed, thrust, angle, etc.) the aircraft performs as expected. Outside the envelope the aircraft will stall and fall out of the sky (if it is put into a deep stall, this is irrecoverable). This is illustrated below for air traffic control (ATC) operations.

Figure 2 Human Performance Envelope Model



This concept can be applied to the nuclear power plant context, with the central 'plateau' area representing normal performance. The 'slopes' then represent off-normal conditions, as would be considered in Level 1 PSA. Here, behaviour is affected by conditions (including stress) but the operators are capable of dealing with these conditions, and HRA techniques can predict the outcome reasonably well.
Level 2 scenarios would either be on the lower edges of this slope or off it, at which point we are less certain of how operators would behave. Fukushima can certainly be considered to be such an extreme event. Yet the operators did try their best to recover from the situation, exhibiting a degree of heroism (i.e. personnel risking irradiation, as also seen in Chernobyl) and ingenuity (e.g. using car batteries to power up key instruments to better understand plant conditions). Fukushima was a very difficult and burdensome event, but did not result in the human equivalent of a 'stall'.

One advantage of the approach is that it can be used to develop behavioural 'markers' for operating crews and supervisors to help them understand when they are under-performing due to stress or burden, and help them get back to a better performance state. Concepts like the Human Performance Envelope therefore might help to address the safety of operator performance in Severe Accidents, even if it doesn't help with the actual quantification of that performance.

Using a performance envelope approach could be interesting, and increase the utility of the overall HRA approach, but the justification for it in front of regulatory bodies might require some explanations and more details, as it is a far cry from current accepted practice. Most likely it would only be countenanced as part of the qualitative analysis or functions provided to determine how to support operators in Severe Accidents.

Taking this qualitative perspective, the over-riding question becomes one of how to support operators in such events, since we will never be able to predict all the things that can happen in their various combinations and permutations. There is a need to focus on the collective *capability* of the shift team to respond, and understanding the principal factors that drive performance in Severe Accident situations. One study that addressed this, to an extent, is the DORRET approach.

The DORRET Approach

In the mid-90s, a nuclear R&D project called DORRET [9] (Determination of Operator Recovery Reliability over Extended Timescales) considered human performance in deteriorating situations over long timescales. To explain the context, at the time the UK had (and still has) mainly gas-cooled reactors rather than Light Water Reactors (LWRs). The accident dynamics of such reactors includes scenarios slower than those considered for the LWRs, e.g. up to 24 hours. The research also addressed not only reactors but reprocessing facilities, which also have some long timescale scenarios. No HRA

technique at the time, other than expert judgement, addressed such scenarios (typically HRA was focused on scenarios ranging from 30 seconds up to 2-3 hours).

The DORRET Project gathered together a group of experts to consider human performance in such scenarios, which could include those that went outside the existing procedures and training system; hence the relevance of DORRET to Level 2 PSA. The DORRET team also analysed 78 relevant incidents (out of an initial dataset of >5400 incidents). Towards the end of the DORRET project a six-stage model of the operator-led recovery process was suggested:

1. Recognition of the need for action
2. Recognition of the recovery options
3. Nature of the complexity of the recovery options and their consequences
4. Decision making and support
5. Organisational capability to respond
6. Check/feedback on success of the task

For such events therefore, there needs to be continuous recognition of the need for action. This can be elaborated following Fukushima, since there was apparently a focus on the reactor area and less focus on the fuel cooling ponds; therefore recognition needs to extend to all major threat conditions (so there are no 'blind spots'). The second stage is recognition of recovery actions – because if the operators cannot think of anything to do, then they cannot act to mitigate on-going risks. The third stage is a recognition of the complexity of the recovery options, e.g. given that there could be fire/flooding/rubble/irradiated areas/communication or instrumentation difficulties, etc. that impede normal execution of actions. The fourth refers to the collective decision-making intelligence at the heart of the recovery effort. Most nuclear facilities that experience severe accidents will have either onsite or remote technical assistance (or both) within a couple of hours or less, and this is useful because it can help moderate decisions that may have to be made 'in the heat of the moment'. The organisational capability to respond is of course critical, and incorporates the training, selection and safety culture of personnel as well as the sufficiency of qualified and experienced personnel, whether during day or night shift, and the effective organisation of communications. The last stage of verifying task success links back to the first stage, closing the feedback loop.

From DORRET to NARA

The DORRET work was used to inform the NARA [10] (Nuclear Action Reliability Assessment) HRA technique, which has an 'Extended Timescale Factors' (ETFs) module, which also potentially has relevance to Level 2 PSA. The ETF module is based around five factors related to the DORRET recovery stages:

- **Information** – e.g. prioritised alarm system, diverse communication systems, diverse monitoring of key parameters/critical functions
- **Scenario characteristics** – amount of time available (segmented between 2 and 24 hours), environmental conditions local at the plant (e.g. fire, storm, rubble after explosion, etc.), confusion due to misleading indicators
- **Guidance** – quality of procedural guidance available (e.g. EOPs, SAMGs, etc.; shift changeover protocols (for > 6hrs)
- **Stress** – e.g. burden of coping with fatalities or operator concern about worsening the environment or causing major capital damage by extreme recovery measures
- **Teams** – the degree of team training in simulators and site incidents, support by technical support centre, etc.

At the moment the ETFs are not specifically for Level 2 PSA, but they could be developed for such a purpose. More generally, such work as in DORRET and NARA can be a starting point for deciding the most critical factors needed to quantify human reliability in Level 2 PSA scenarios, and also how

to build a strong operating personnel capability in our nuclear facilities to respond to rare and extreme events.

Level 2 Event Training

Of all the factors considered, two seem to be dominant: information, and operator team preparedness (training/teamwork). Information available is primarily a design issue, so that as far as practicable there are good information systems that can highlight what is going wrong, and ensure that the operators can 'see the wood for the trees', and are diverse in nature so that misleading indications can be detected and compensated for by the operators.

Training needs to 'push the envelope' for operators, occasionally placing them in severe conditions that are not clear, and where normally available resources are compromised. Some nuclear power related organisations and institutions have indeed carried out such simulations and exercises, and operators usually find them challenging, but also rewarding, giving them the confidence that should such an event occur in reality, they stand more chance of 'keeping a cool head'.

CONCLUSIONS

Severe Accidents are rare but do happen, and we don't know where they might happen, given that they can be due to internal events (e.g. Chernobyl) or external events (e.g. Fukushima, triggered by a tsunami). Since operator action and resourcefulness is critical in such events, there is a dual need to prepare the operators as far as is reasonably practicable for such events via instrumentation, procedural guidance and training, and to assess the likely operator response via HRA in PSA in order to determine and mitigate vulnerabilities.

The main problem in developing a quantification approach for human action in a Level 2 PSA framework is linked to the uncertainty in how Severe Accidents develop. In answer to the question 'Can we quantify human reliability in Level 2 PSA?' the answer is a tentative 'yes': we can 'have a go' with some of the existing tools, and these can include both first and second generation tool s such as THERP and ASEP, NARA, ATHEANA and MERMOS. But we are largely at the stage of making educated guesses, since in all cases such tools have not been designed for Level 2 PSA, and/or rely heavily on expert judgment, either via analysts or subject matter experts, when in reality we have very few experts who really know what it is like in such scenarios.

What is missing is a valid psychological model of operator behaviour in such conditions, or at least a better understanding of the key factors and how they drive human performance in L2 scenarios. The DORRET approach, or a similar study, could be revised to inform the expert judgment process when using HRA techniques in L2 PSAs. More L2 real-time simulations where operating crews are pushed well beyond the normal scenario boundaries, as have been carried out in some NPPs, could be useful starting points to understand how operating crews react, and how behaviour alters when transitioning from a L1 scenario into a L2. Insights like this could also help in the development of better dependence modelling for L2 PSAs.

In conclusion, what is needed is a programme of work that seeks first to understand the limits of PSA modelling for L2, and then to understand human behaviour in such scenarios. From such understanding, factors can be extracted either to guide experts participating in or conducting HRAs for L2 PSAs, or to inform HRA techniques and models themselves. Given the inevitable limitation of modelling for L2 PSA, a related branch of work needs to focus on strengthening the operating crew capability, both via advanced simulator training and also by consideration of other Human Factors approaches (e.g. Human Performance Envelope) that may help operators continue to cope when everything appears to be failing around them.

REFERENCES

[1] IAEA (2010) Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, Austria

[2] IAEA (2009) "Severe Accident Management Programmes for nuclear power plants", Vienna Austria

[3] V. N. Dang, G. M. Schoen, B. Reer (2009) "Overview of the Modelling of Severe Accident Management in the Swiss Probabilistic Safety Analyses" ISAMM 2009, October 26 - 28, 2009 Böttstein, Switzerland

[4] Bye, A., Lois, E., Dang, V., Parry, G., Forester, J., Massaiu, S., Boring, R., Braarud, P., Broberg, H., Julius, J., Männistö, I. and Nelson, P. (2012) "International HRA Empirical Study – Phase 2 Report Results from Comparing HRA Method Predictions to Simulator Data from SGTR Scenarios." NUREG IA-0216 Vol 2, USNRC, Washington DC 20555.

[5] E. Raimond et al (2013) ASAMPSA2 "Best-Practices Guidelines For Level 2 PSA Development And Applications", April 2013

[6] M. L. Ang, N. E. Buttery (1997), "An approach to the application of subjective probabilities in level 2 PSAs" Reliability Engineering & System Safety, Vol 58, Pages 145–156, November 1997

[7] Martin Richner (2006) "Modelling of SAMG operator actions in Level 2 PSA" PSAM-8, May 2006, New Orleans, USA

[8] Edwards, T., Sharples, S., Wilson, J. R., Kirwan, B. (2010). "The need for a multifactorial human performance envelope model in air traffic control" *Presented at the HCI-Aero 2010 conference, 3rd-5th November, Cape Canaveral: USA*

[9] "Manual for the DORRET technique" Vectra Report No. 1005-215-TD01. Revision 1. October 1997.

[10] Kirwan, B., Gibson, H., Kennedy, R., Edmunds, J., Cooksley, G., and Umbers, I. (2004) "Nuclear Action Reliability Assessment (NARA): A data-based HRA tool. In Probabilistic Safety Assessment and Management" 2004, Spitzer, C., Schmocker, U., and Dang, V.N. (Eds.), London, Springer, pp. 1206 – 1211