A SYSTEMATIC APPROACH TO ADDRESSING HUMAN FACTORS ISSUES FOR SIL DETERMINATION STUDIES

David Embrey[a] and Mrudhul Raj[b]
[a]Human Reliability Associates, Dalton, UK
[b]Optimus Aberdeen Ltd, Aberdeen, UK

As set out in BS EN 61508 and 61511, Major hazard installations are required to demonstrate the choice of any Safety Instrumented Functions (SIF), and determine and verify the safety integrity level (SIL). Both standards require human factors to be included in the assessment. However, there is a lack of a systematic approach in SIL determination methodology such as Layer of Protection Analysis (LOPA) to both the qualitative modelling and quantification of human reliability.

This paper introduces a novel approach to assess human reliability in SIL determination, based on the integrated use of Hierarchical Task Analysis (HTA) for the identification of critical tasks and the assessment of the contextual factors, called Performance Influencing Factors (PIFs), which determine the likelihood of human failures. A methodology called the Success Likelihood Index Methodology (SLIM) provides a set of models for the factors that influence human error for commonly occurring activities such as alarm response, actions, checking, information retrieval and communication. Evaluation of these factors for a specific situation allows the quantification of human errors for the scenario being subjected to a SIL determination analysis. The method allows site specific information from personnel, such as panel operators and safety engineers, to be incorporated in the analysis. Issues such as dependencies between actions and verification activities, and interactions between the factors (e.g. time stress and experience) that may impact on the resulting error probabilities, can also be addressed by the methodology.

The paper provides a comprehensive case study that illustrates how the methodology can be applied as part of a SIL determination analysis of a ship to shore transfer operation for a flammable liquid overfilling. This analysis shows how the overall SIL level can be determined by combining the hardware layers of protection and the human reliability analyses.

KEYWORDS: SIL Determination, Alarm response, Success Likelihood Index Methodology (SLIM), Human Reliability Assessment, Performance Influencing Factors, Hierarchical Task Analysis

1. INTRODUCTION

The standards BS EN 61508 and 61511 require the process industries to conduct a risk assessment to justify the choice of any safeguard in place. The choice of safety instrumented functions (SIF) depends on the gap between the target risk and the process risk, once the safety integrity level (SIL) has been determined and verified. Almost 80% of accidents may be attributed, at least in part, to the actions or omissions of people throughout the life cycle from design through to operation, maintenance, management and decommissioning (HSE UK, 2007, pp 6).

The research report: 'A review of Layers of Protection Analysis (LOPA) analyses of overfill of fuel storage tanks' (HSE UK, 2009b) was published by HSE following the Buncefield Incident. The report covered findings from 15 plants and included a detailed analysis of seven of these plants. Human factors and human failures were major issues. Examples of the problems identified were:

- Human error probability (HEP) estimates were too optimistic, and were often based on cases taken from published studies, without taking into account the site specific situation.
- Lack of independence of human operators, leading to the double counting of the benefits arising from human interventions
- Only three out of fifteen assessments used a formal quantitative human reliability analysis technique (namely the HEART method).
- There was no systematic treatment of Performance Influencing Factors (PIFs) (also known as Performance Shaping Factors, PSFs), the context specific factors that determine the human error probabilities. For example, even though ship unloading operations take many hours, no consideration was given to PIFs such as the effectiveness of the shift handover regime or operator fatigue.

Human error is therefore a much more frequent initiating cause than the Basic Process Control System (BPCS) loop, regulator and equipment failures which are addressed by engineering risk analysis techniques e.g. HAZOPs, Layer of Protection Analysis (LOPA) and Quantitative Risk Assessment (QRA) applied at the design stage. Whilst both standards require that human factors issues be taken into account in their application, they do not give much guidance on how this should be done.

The use of a probability of failure on demand (PFD) of 0.1 for a response within 20 minutes comes from The Human Reliability Handbook (Swain, A.D. & Guttmann, H.E., 1983). It is interesting to note that this study was carried out 30 years ago for a single alarm response (one scenario) in the nuclear power industry. However, there are substantial differences between nuclear power stations and chemical processing plants. In particular, there are often many more alarms in process plants.

Currently, there is a lack of guidance to demonstrate a risk reduction factor (RRF) of 100 credits or SIL-2 rated equivalent, for an alarm layer as a safety function. An example would be a scenario (where the instruments are SIL 2 rated) that takes a long time to develop and requires the control room operator(s) to press a push-button following an alarm to close a Remote Operated Shut-off Valve (ROSoV).

However, some safety analysts disagree with this, even though Part 2, 8.2.1, Para 7 of BS EN 61511 states the following:

"The credit that can be taken will need to be limited by human factor issues such as how quickly action needs to be taken and the complexity of the tasks involved. Where an operator, as a result of an alarm, takes action and the risk reduction claimed is greater than a factor of 10, then the overall system will need to be designed according to IEC 61511-1. The system that undertakes the safety function would then comprise the sensor detecting the hazardous condition, the alarm presentation, the human response and the equipment used by the operator to terminate any hazard. It should be noted that a risk reduction of up to a factor of 10 might be claimed without the need to comply with IEC 61511. Where such claims are made, the human factor issues will need to be carefully considered. Any claims for risk reduction from an alarm should be supported by a documented description of the necessary response for the alarm and that there is sufficient time for the operator to take the corrective action and assurance that the operator will be trained to take the preventive actions."

2. SCOPE

In order to minimise analytical resources when performing human reliability analysis, it is tempting to quantify a task at a highly aggregated level even when it is complex and contains many subtasks. Techniques such as HEART and THERP, which have predefined task categories, such as valve operations, encourage the analyst to quantify at the same level as this classification. For more complex tasks, this approach has a number of disadvantages. In particular, it does not attempt to model the overall structure of the task in a way that allows the identification of its constituent subtasks and their associated failure modes. Such analyses do not always evaluate the effects of the specific PIFs that may drive human error in particular situations, but which may not be included within the built-in set of factors provided by quantification techniques such as HEART or THERP. (Embrey, D. E., 2012)

This paper aims to provide a methodology which can be applied in SIL determination studies to integrate human reliability analyses with quantitative or semi-quantitative risk assessment (LOPAs). This is done by providing a systematic approach to identifying and quantifying human failures based on a consideration of site-specific human factors issues. For SIL determination analyses in a hazardous event scenario, the human failures in initiating causes and in alarm layers need to be identified and quantified.

3. APPLICATION OF THE METHODOLOGY TO INITIATING CAUSES

Human initiating causes can be defined as those human failures which either by themselves or in combination with equipment failures lead to a demand on any Independent Protection Layers (IPL) or safety functions. This is quantified in terms of frequency per year.

3.1 BREAK DOWN THE TASK OBJECTIVE INTO THE FIRST LEVEL SUBTASKS AND TASK STEPS REQUIRED TO ACHIEVE THE OVERALL TASK OBJECTIVE

Hierarchical Task Analysis (HTA) is a well-established methodology that has been used extensively in applications such as COMAH Safety Reports (Embrey, D. E. & Henderson, J., 2011). It involves a top down breakdown of a task from its main objectives at the top level of the analysis to more detailed subtasks and ultimately task elements. Figure 1 shows the top level of a HTA for a ship unloading operation, and Figure 2 shows subtask 3 'Line-up Tank A for receipt of substance' broken down to illustrate the successive re-description of a task into subtasks and ultimately individual actions linked by plans.

3.2 SCREEN THE LOWEST LEVEL OF THE HTA (USING A RISK RANKING PROCESS) TO SPECIFY THE SUBTASKS OF THE POTENTIAL HAZARDOUS EVENT UNDER STUDY

In order to minimise the analysis effort, it is useful to prioritise which of the subtasks should be selected for analysis and quantification. A simple method for prioritising the analysis process is to develop a risk ranking score for each of the subtasks. This uses a coarse evaluation of the likelihood of failure e.g. based on a subjective judgement of the likelihood of error, combined with the severity of the consequences (overfilling in the case study). Assessing these parameters on a three point scale High = 3, Medium = 2 Low = 1 and multiplying them together gives a simple risk index ranging from 1 to 9 (9 = highest risk). If required, the likelihood of error recovery (before the consequences of the error are realised) can also be included in this index (where High = 1, medium = 2 and low = 3, since increases in the likelihood of recovery reduce the overall risk), in which case the index ranges from 1 to 27.

Table 1 summarises the results of the screening analysis for the ship unloading scenario, including steps not shown in Figures 1 and 2. Based on this analysis, task

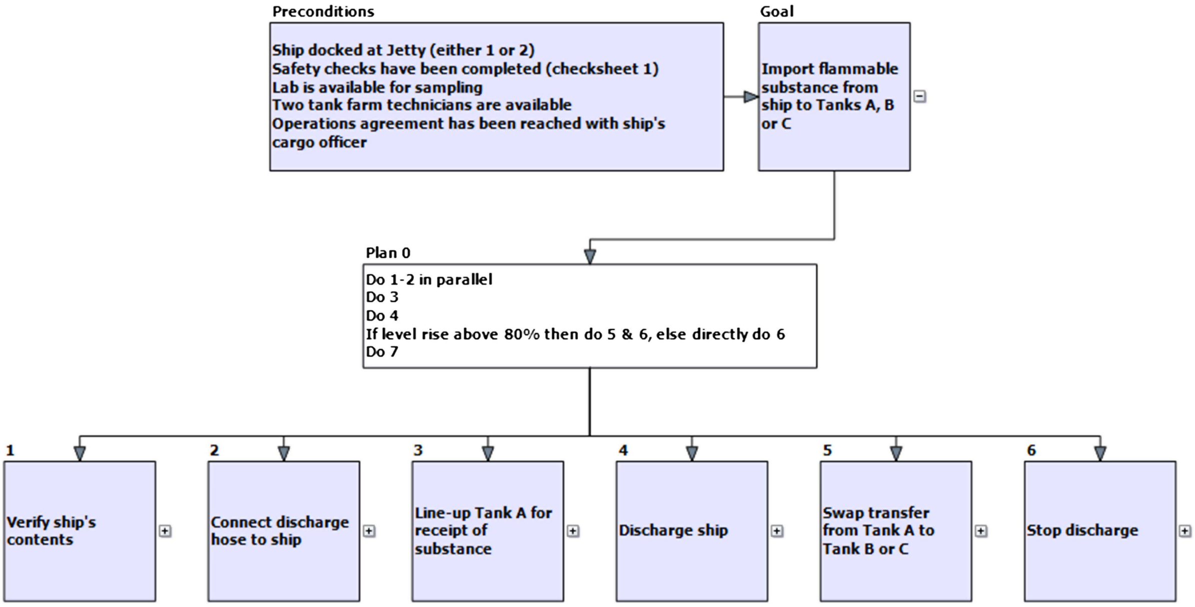

Preconditions
Ship docked at Jetty (either 1 or 2)
Safety checks have been completed (checksheet 1)
Lab is available for sampling
Two tank farm technicians are available
Operations agreement has been reached with ship's cargo officer
Goal
Import flammable substance from ship to Tanks A, B or C
Plan 0
Do 1-2 in parallel
Do 3
Do 4
If level rise above 80% then do 5 & 6, else directly do 6
Do 7
1
Verify ship's contents
2
Connect discharge hose to ship
3
Line-up Tank A for receipt of substance
4
Discharge ship
5
Swap transfer from Tank A to Tank B or C
6
Stop discharge

Figure 1. Top level of a Hierarchical Task Analysis for a Ship Unloading Task

elements 2.1, 3.1, 4.6 5.1 and 5.2 were selected for detailed analysis.

3.3 CLASSIFY THE TASK ELEMENTS INTO A CATEGORY IN THE TASK ACTIVITY CLASSIFICATION TAXONOMY AND IDENTIFY FAILURE MODES AND PIF'S

Once the task has been broken down to the level of detail required, and task elements have been selected for HEP evaluation, they are then classified using a Task Activity Classification Taxonomy (TACT). TACT is classification of the main types of activity that are encountered in safety critical tasks, together with an associated set of failure modes for each activity. A simplified version of TACT taxonomy and generic PIFs that determine the probability of each of the failure modes is summarised below in Table 2. The analyst can evaluate the situation to decide whether one of the specific failure modes within each category (e.g. Action Omitted or, Right Action on wrong object) is

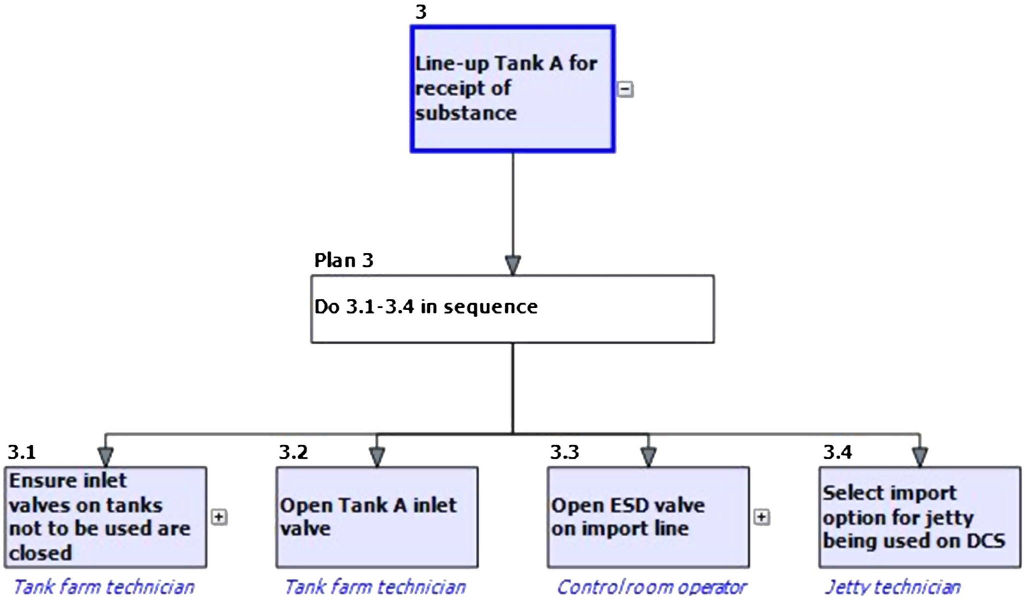

3
Line-up Tank A for receipt of substance
Plan 3
Do 3.1-3.4 in sequence
3.1
Ensure inlet valves on tanks not to be used are closed
Tank farm technician
3.2
Open Tank A inlet valve
Tank farm technician
3.3
Open ESD valve on import line
Control room operator
3.4
Select import option for jetty being used on DCS
Jetty technician

Figure 2. Breakdown of Subtask 3 'Line-up Tank A for receipt of substance'

Table 1. Results Risk screening process used in HTA

Task		Severity of Consequence	Likelihood of Error	Likelihood of Recovery	Risk Index
ID	Description				
1*	Verify ship's contents	Low (1)	High (3)	Medium (2)	6
2*	Connect discharge hose to ship	High (3)	High (3)	Medium (2)	18
2.1**	Ensure sufficient ullage available in tanks A, B & C to meet ship	High (3)	High (3)	Medium (2)	18
2.2	Fill the import line with substance from Tank A	Low (1)	Medium (2)	High (1)	2
2.3	Attach hose to crane (JT)	Medium (2)	Medium (2)	High (1)	4
2.4	Connect hose to ship manifold (JT)	Medium (2)	Medium (2)	High (1)	4
2.5	Open hose butterfly valve (JT)	Low (1)	Low (1)	Low (3)	3
2.6	Open jetty head manifold valve (JT)	Low (1)	Medium (2)	Medium (2)	4
3*	Line-up Tank A for receipt of substance	High (3)	Medium (2)	Low (3)	18
3.1**	Open Tank A inlet valve (TFT)	High (3)	Medium (2)	Low (3)	18
3.2	Open ESD valve on import line (CRO)	Low (1)	Medium (2)	Medium (2)	4
3.3	Select appropriate import option on DCS for jetty	High (3)	Low (1)	High (1)	3
4*	Discharge ship	High (3)	Medium (2)	Low (3)	18
4.1	Start the pump	Low (1)	Medium (2)	Medium (2)	4
4.2	Ensure hose pressure does not exceed 4 barg	Medium (2)	Medium (2)	Medium (2)	8
4.3	Reduce pumping rate from ship (ship)	Medium (2)	Low (1)	Medium (2)	4
4.4	Manage hose height as level of vessel changes	Low (1)	High (3)	High (1)	3
4.5	Monitor rates and pressure (CRO/JT)	Medium (2)	Medium (2)	Medium (2)	8
4.6**	Monitor the increase in level	High (3)	Medium (2)	Low (3)	18
5*	Swap transfer from Tank A to Tank B or C	High (3)	Medium (2)	Low (3)	18
5.1**	Open the inlet valve on the new receiving tank	High (3)	Medium (2)	Low (3)	18
5.2**	Close the inlet valve on Tank A	High (3)	Medium (2)	Low (3)	18
6*	Stop discharge	Low (1)	Medium (2)	Medium (2)	4
7*	Complete pre-departure administration	Low (1)	Medium (2)	High (1)	2

* Indicates Results of risk ranking procedure applied to first level of the HTA

** Indicates task elements subjected to Predictive Human Error Analysis (See Figure 4)

TFT = Tank Farm Technician, CRO = Control Room Operator, JT = Jetty Technician

likely to be present. Another approach is to consider the consequences under study that could arise in the situation as a result of human error, and then to decide on which of the failure types could give rise to this consequences.

3.4 ASSIGN HEPs TO FAILURE MODES

To calculate Human Error Probabilities (HEPs) for the failure modes, we recommend a methodology called the Success Likelihood Index Methodology (SLIM). This derives the HEPs from an assessment of the PIFs in the situation being assessed. The methodology is described in detail in Embrey, D. E., 2012 & 1986. SLIM derives an estimate of the HEP by combining the ratings of the quality of the PIFs in a situation (weighted if necessary to reflect their relative importance) to give an overall index called the Success Likelihood Index (SLI). Since this represents a measure of the overall quality of the factors that drive the HEP, it can be converted to an HEP, if at least two suitable calibration values are available.

In principle, other techniques such as THERP or HEART could also be applied to generate the required HEPs. However, these techniques do not provide a method for addressing PIFs other than those provided within the technique itself. The main advantage of SLIM is that it can calculate the HEP based on numerical ratings of the specific set of PIFs associated with each failure type. The analyst also has the option to include other context specific factors if they are deemed to have a major impact on the HEP being evaluated. SLIM uses a graphical representation, called an Influence Diagram (ID), to represent the relationship between the SLI and the HEP. An example of a SLIM model connecting PIFs to HEPs for the Action failure modes in TACT is shown in Figure 3. The numbers in the top right hand panes of the boxes are the relative weights of the factors and those in the bottom left panes the ratings of the quality of the factors. The minus signs indicate that as the rating of the factor increases, it also increases the HEP at the top of the model (see discussion below). Similar models are available for the other TACT Activity types shown in Table 2.

The SLI is calculated by adding together the products of the relative importance weights and the assessed quality rating for each of the PIFs. The calculation formula for this process is:

$$\mathrm{SLI_j} = \Sigma \mathrm{R_{ij}} \cdot W_\mathrm{i} \tag{1}$$

Table 2. TACT Activity and Failure mode classification and corresponding generic PIFs

Actions	Checking	Communication
A1 Operation too long/short	C1 Check omitted	I1 Information not communicated
A2 Operation mistimed	C2 Check incomplete	I2 Wrong information communicated
A3 Operation in wrong direction	C3 Right check on wrong object	I3 Information communication incomplete
A4 Operation too little/too much	C4 Wrong check on right object	I4 Information communication unclear
A5 Operation too fast/too slow	C5 Check too early/late	
A6 Misalign	**Information retrieval**	**Selection**
A7 Right operation on wrong object	R1 Information not obtained	S1 Selection omitted
A8 Wrong operation on right object	R2 Wrong information obtained	S2 Wrong selection
A9 Operation omitted	R3 Information retrieval incomplete	
A10 Operation incomplete	R4 Information incorrectly interpreted	
A11 Operation too early/late		
A12 Operation in wrong order		
A13 Misplacement		

Failure modes	Performance Influencing Factors (PIFs)
Action errors	• Clarity of signal that action is required • Likelihood of previous incorrect diagnosis • Barriers to prevent action error • Quality of procedures • Time pressure • Distractions • Training
Checking errors	• Cue/signal to initiate checking • Perceived importance of check relative to other Demands • Perceived redundancy
Communications errors	• Strength of cues/signal to initiate communication • Use of formal communication protocols • Degree of shared understanding between sender & receiver • Complexity of information to be communicated • Level of redundancy in communication channels
Information retrieval errors	• Strength of cues/signal to initiate information retrieval • Quality of information organization/presentation • Accuracy of source information • Ambiguity of source information
Selection (when choosing between alternatives, e.g. selecting one from several valves)	• Strength of cues/signal to initiate selection • Labelling of items from which selection is to be made • Degree of colour or shape coding of items • Physical proximity of items

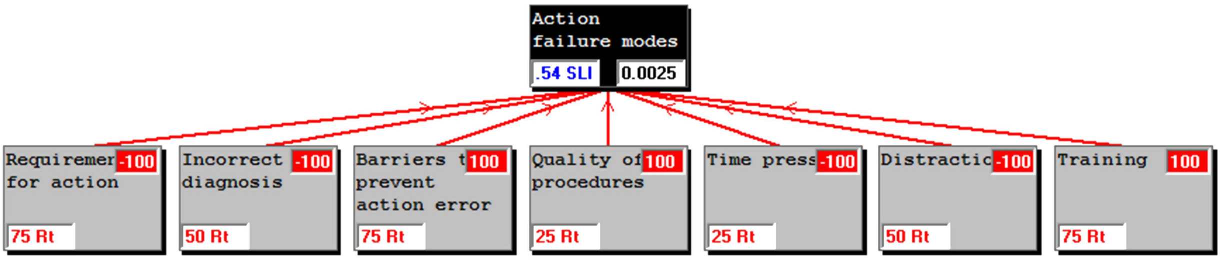


Figure 3. SLIM Model with generic PIFs for Action failure modes

Where

SLI_j = SLI for task j
W_i = Normalised importance weight for the ith PIF (weights sum to 1)
R_{ij} = Rating of the jth task on the ith PIF

In order to obtain the ratings, which are the values in the lowest level boxes, the analyst assigns a numerical value which reflects the state of each PIF in the model. This is normally on a scale from 1 (corresponding to worst case conditions) to 100, corresponding to best case conditions. For some PIFs, (called reverse scales) such as time pressure or distractions, increasing the ratings (e.g. from low time pressure, rating 5 to high time pressure, rating 95) will increase the error probability. For these types of PIFs, the rating values are subtracted from 100 in order to reverse direction of the scale.

The products of each rating with its corresponding weight are then added to give an overall Quality score (the SLI) for the PIFs, which is then rescaled to fall within the range 0-1.00. This is the number shown in the left hand window (0.54) in the top box of the Action failures model shown at the top of Figure 3. This score can be transformed to a HEP (the value of 0.0025 shown in the adjacent window) by means of a calibration relationship shown in Equation 2:

$$\text{Log (HEP)} = \text{A SLI} + \text{B} \qquad (2)$$

Where HEP = human error probability and A, B are constants. (Embrey, D. E., 2012)

In order to calculate the constants A and B in the equation, at least two tasks with known SLIs and error probabilities must be available in the set of tasks being evaluated. Ideally, the relationship between the SLI and error probabilities should be obtained from data collected from the domain of interest. For the example calculations we make the following assumptions:

When the SLI = 1.0 (Best case conditions for all PIFs) → HEP = 0.0001 (10^{-4}) Log HEP = -4

When the SLI = 0.0 (Worst case conditions for all PIFs) → HEP = 0.1 (10^{-1}) Log HEP = -1

Substituting these values in Equation (2) enables the constants A and B to be calculated and this gives a general equation for converting SLI values to HEPs:

$$\text{Log (Failure Probability)} = -3 \times \text{SLI} - 1 \qquad (3)$$

In the case study, for the failure mode ‘A9 Operation omitted’ it assumed that each PIF has the same influence or weight. Since ther are seven factors, each weight is $W_i = 1/7$. If the PIF weights are assumed equal, they will always be the reciprocal of the number of factors being considered in the analysis.

The failure rating, Rt (given in bottom left corner of each PIF in Figure 3) is based on the judgements of an experienced analyst or discussions with plant personnel who have carried out the task.

Following the same method for other PIF’s and substituting these Rt values in Equation (1) gives the following (Note the correction for reversed scales for PIFs 1, 2, 5 and 6):

$$\begin{aligned}\text{SLI} = [&(1-0.75)+(1-0.50)+0.75\\&+0.25+(1-0.25)+(1-0.50)\\&+0.75)]\times(1/7)=0.54\end{aligned}$$

Substituting the calculated SLI value of 0.54 (at the top of the ID in Action failure modes of Figure 3) into Equation (3) gives a predicted HEP of 0.0025 for this action error. Although these calculations may appear tedious, software tools are available which perform the HTA analyses, enable the user to construct the SLIM models and populate them with appropriate ratings to calculate the HEPs (Embrey, D. E., & Zaed, S., 2010). This enables the qualitative modelling and the numerical evaluation of HEPs to be carried out relatively quickly.

3.5 INCLUDE ANY RECOVERY STEPS OR VERIFICATIONS AND CONSIDER POSSIBLE DEPENDENCIES

Figure 4 Shows how both actions and verifications in the HTA can be broken down into their constituent failure modes for quantification. Plan 3.1 shows that the Task element ‘Close inlet valves’ has an associated verification activity: ‘Check inlet valves are closed’ which is intended to recover an error made at step 3.1.1.1. These task elements are in turn broken down into their constituent failure modes with their associated HEPs, which are combined using ‘OR’gates. The action (3.1.1) and checking (3.1.2) task elements are combined using an ‘AND’ gate to give an overall failure probability of 0.0002. The use of an ‘AND’ gate assumes that the action and checking elements are independent, and this assumption of independence is emphasised by Plan 3.1 which specifies that the check is carried out by an independent operator. However, it is often necessary to take into account possible dependencies that may exist if checking or verification activities are included in an analysis.

Dependencies can arise due to coupling mechanisms between same person, same crew, same procedure, same procedure step, similar action and actions that are close in time. A dependency model to take into account these interactions is illustrated below using an example of two dependent events of potential human errors: A (previous) and B (following). The probability of making an error A and error B (potentially dependent) is evaluated as follows (Swain, A.D., & Guttmann, H.E., 1983);

$$P(A \cdot B) = P(A)P(B|A) = (1-\beta_H)QAQB + \beta_H QA \quad (4)$$

Where; P(A) = QA and P(B) = QB are probabilities of relevant failure events; and β_H is a factor linked with the degree of dependency with values given in Table 3.

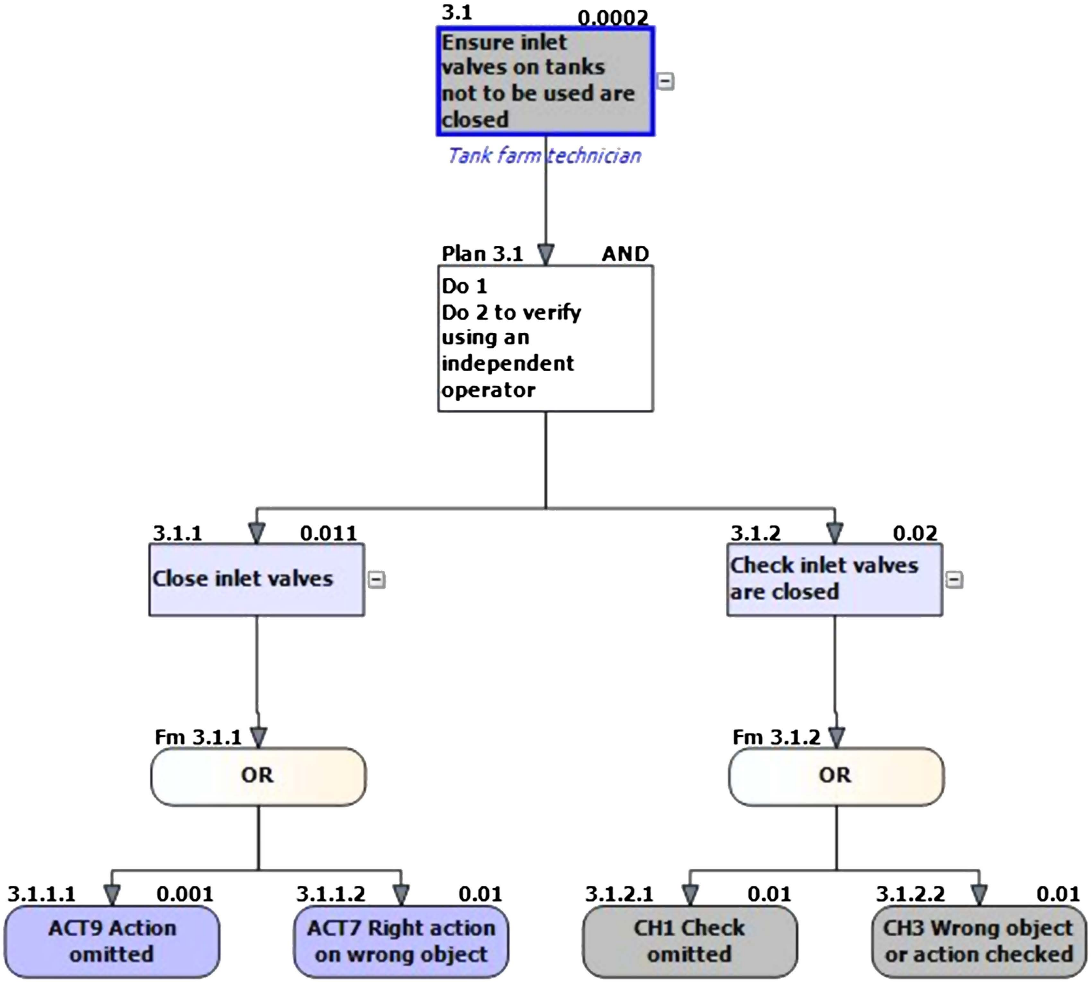
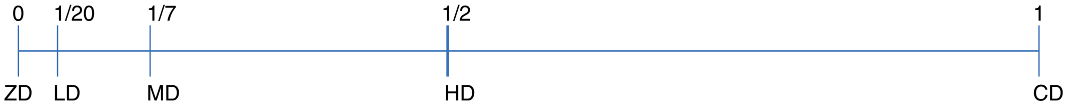

3.1
0.0002
Ensure inlet valves on tanks not to be used are closed
Tank farm technician
Plan 3.1
AND
Do 1
Do 2 to verify using an independent operator
3.1.1
0.011
Close inlet valves
3.1.2
0.02
Check inlet valves are closed
Fm 3.1.1
OR
Fm 3.1.2
OR
3.1.1.1
0.001
ACT9 Action omitted
3.1.1.2
0.01
ACT7 Right action on wrong object
3.1.2.1
0.01
CH1 Check omitted
3.1.2.2
0.01
CH3 Wrong object or action checked

Figure 4. Combining HEPs within the HTA and addressing recovery

3.6 COMBINE THE HEPs OF FAILURE MODES OR INITIATING CAUSES

Using an 'OR Gate' combine the HEPs of failure modes or the initiating causes with common layers of protection to find the overall HEP for the task above (see Figure 4). Care needs to be taken to ensure that same IPL's are effective for the all the combined failure modes or initiating causes.

Table 3. Degree of Dependency and its beta-H factor



Degree of Dependency	Example	beta-H factors β_H Value
ZD- zero dependence		0
LD- low dependence	Certified by independent body	1/20 → 0.05
MD- moderate dependence	Independent company	1/7 → 0.14
HD- high dependence	Different team, within the company	1/2 → 0.5
CD- complete dependence	Within same team	1

3.7 EVALUATE THE OPPORTUNITIES FOR FAILURE OR FREQUENCY OF TASK PERFORMANCE PER YEAR

Using plant documents or past operational records, evaluate the opportunities for failure or frequency of task performance per year. This frequency per year is multiplied by the HEP for the initiating cause to obtain the failure rate per year. Table 4 shows how several initiating causes and their associated HEPs from other parts of the task analysis illustrated in Figures 1–4 are combined with differing task frequencies.

4. APPLICATION OF THE METHODOLOGY TO AN ALARM LAYER

The alarm layer is an IPL that includes an alarm to alert the operator. It comprises elements such as sensors, annunciators, the operator response to prevent the hazardous event and the final element (e.g. a valve). This is quantified in terms of the Probability of Failure on Demand (PFD). The demand on this IPL is after the initiating cause and before the activation of the SIF (e.g. trips, if any). The success of this layer depends mainly on the operator response to the alarm, which in turn is highly dependent on PIFs which affect the three successive stages of detection, diagnosis / planning and action.

4.1 VALIDATE THE OPERATOR RESPONSE TIME TO AN ALARM

This stage is to define the alarm response task required and verify that the operator is capable of doing the task. This involves checking the records of past simulation drills, which are normally conducted least once in year. These data are used to verify that the Operator Response time during testing (MAORT is the theoretical combined time for detection of an alarm, diagnosis/planning of a response, and carrying out the action), and the Process dead Reaction Time (PRT) (e.g. time for valve closure) is less than the Process Safety Time (PST) (Bridges, W., 2011):

$$T_{PST} > T_{ORT} + T_{PRT} \text{ or } T_{MAORT} > T_{ORT} \qquad (5)$$

This is illustrated in the Figure 5 and typical validation data are given in Table 5.

4.2 CALCULATE THE HEP OF AN OPERATOR ALARM RESPONSE

Figure 6 provides a generic model for evaluating the HEP for the overall operator alarm response. This model combines three separate SLIM models for the stages of Detection, Diagnosis/Planning, and Action respectively. The failure HEPs for each of these stages are combined using an 'OR' gate, as failures in any of these stages could give rise to an overall failure to respond to the alarm within the required time period. The use of an integrated model allows common PIFs to be taken into account, such as degree of time pressure, which affects the HEPs for both the Diagnosis and Action stages of the alarm response. Figure 6 shows the direct and indirect PIFs which affect the overall probability of failure at the top of the tree. As discussed previously, the values in the lower left windows of the boxes in Figure 6 are failure ratings which represent the state of the PIFs in the situation being evaluated. The PIFs in the UKPIA gap analysis tool (Embrey, D. E. & Henderson, J., 2012) could also have been used. It is assumed that all of the factors are equally weighted, and hence a value of 100 is appended to all of the top right hand boxes The two bottom level PIFs, were excluded from the analysis as not being relevant, and hence were weighted as zero.

The three sub-models used in the calculation (Detection, Diagnosis/Planning, Action) were each calibrated using the process described in Section 3.4 with Table 6.

Table 4. Frequency of human initiating causes

Task ID & description (Initiating Cause)	Failures Mode (Table 2)	SLI	HEP (Contituent failure modes are combined using 'OR' gates)	Frequency for task carried out 100 times a year
2.1 Ensure sufficient capacity available in tanks A, B & C to meet ship [CRO omits the check or incorrectly calculate the ullage]	C1 Check omitted I2 Wrong information obtained	0.46 0.49	0.0042 + 0.0033 = 0.0075	0.75/year
3.1 Open Tank A inlet valve [TFT diverts to the wrong tank]	S2 Wrong selection	0.59	0.0017	0.17/year
4.6 Monitor the increase in level [TFT fails to monitor the level of the tank]	C1 Check omitted	0.46	0.0042	0.42/year
5 Swap transfer from Tank A to Tank B or C [TFT fails to swap]	S2 Wrong selection A9 Action omitted	0.60 0.54	0.0025 + 0.0025 = 0.005	0.5/year
Section Reference: 3.2	**3.3**	**3.4**	**3.4 & 3.5/3.6**	**3.7**

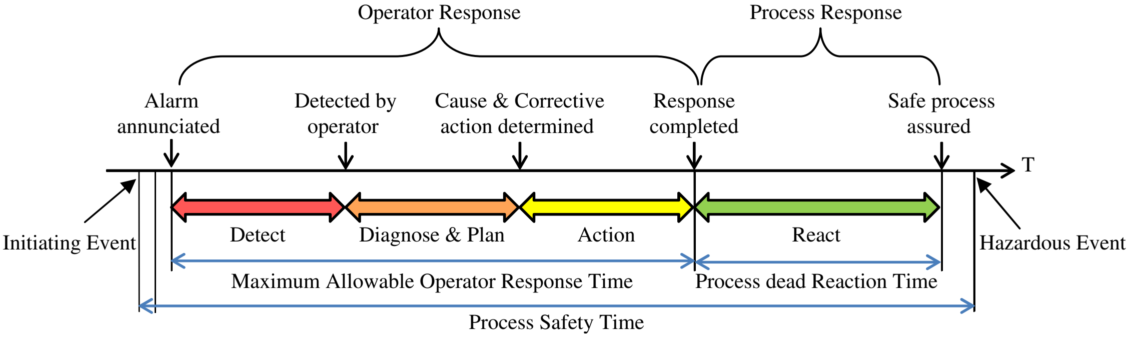


Figure 5. Maximum allowable operator response time (MAORT)

Table 5. Validation of operator response time (ORT)

Operator Response to Alarm Validation by Test/Drill		
Response Task: Jetty technician (JT) detects the alarm and closes the ROSoV by pressing a push-button	Test Date: 15/08/2012	Employee No: 8983
	$T_{ORT} = 1.5$ minutes	$T_{PRT} = 1$ minutes
$T_{PST} > T_{ORT} + T_{PRT}$ PASSED	$T_{PST} = 25$ minutes	$T_{MAORT} = 24$ (25-1) minutes

Substituting the calibration values in Equation (2) enables the constants A and B to be calculated and this gives a general equation for converting SLI values to HEPs:

$$\text{Log (Failure Probability)} = -3.0043 \times \text{SLI} - 0.4771 \quad (6)$$

Converting the failure rating to rating on the PIF's as mentioned in the Section 3.4 and substituting in Equation (1), gives the SLIs for the Detection, Diagnosis and Action sub-models. Then substituting the calculated SLI values (0.67, 0.70, 0.71) into Equation 6 gives predicted HEPs for each of these stages as (0.0033, 0.0027, 0.0025) respectively.

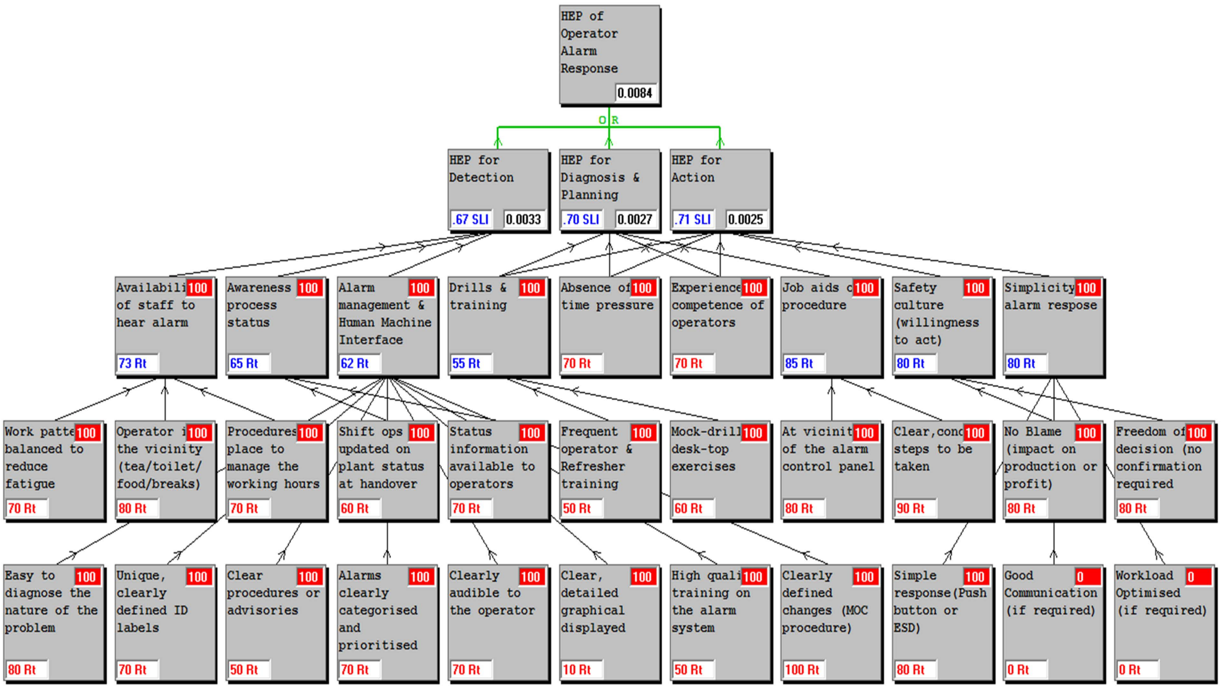

HEP of Operator Alarm Response
0.0084
OR
HEP for Detection
.67 SLI
0.0033
HEP for Diagnosis & Planning
.70 SLI
0.0027
HEP for Action
.71 SLI
0.0025
Availabili of staff to hear alarm 100 73 Rt
Awareness process status 100 65 Rt
Alarm management & Human Machine Interface 100 62 Rt
Drills & training 100 55 Rt
Absence of time pressure 100 70 Rt
Experience competence of operators 100 70 Rt
Job aids c procedure 100 85 Rt
Safety culture (willingness to act) 100 80 Rt
Simplicity alarm respose 100 80 Rt
Work patte balanced to reduce fatigue 100 70 Rt
Operator i the vicinity (tea/toilet/ food/breaks) 100 80 Rt
Procedures place to manage the working hours 100 70 Rt
Shift ops updated on plant status at handover 100 60 Rt
Status information available to operators 100 70 Rt
Frequent operator & Refresher training 100 50 Rt
Mock-drill desk-top exercises 100 60 Rt
At vicinit of the alarm control panel 100 80 Rt
Clear,conc steps to be taken 100 90 Rt
No Blame (impact on production or profit) 100 80 Rt
Freedom of decision (no confirmation required 100 80 Rt
Easy to diagnose the nature of the problem 100 80 Rt
Unique, clearly defined ID labels 100 70 Rt
Clear procedures or advisories 100 50 Rt
Alarms clearly categorised and prioritised 100 70 Rt
Clearly audible to the operator 100 70 Rt
Clear, detailed graphical displayed 100 10 Rt
High quali training on the alarm system 100 50 Rt
Clearly defined changes (MOC procedure) 100 100 Rt
Simple response(Push button or ESD) 100 80 Rt
Good Communication (if required) 0 0 Rt
Workload Optimised (if required) 0 0 Rt

Figure 6. SLIM model for Operator Alarm response

Table 6. Proposed Calibartion of SLI depending on T_{MAORT}

Range of T_{MAORT}	SLI	HEP of Sub-models	Log HEP
$T_{MAORT} \leq 20$ minutes	1	0.00333	−2.4771
	0	0.33333	−0.4771
$20 < T_{MAORT} \leq 60$ minutes	1	0.00033	−3.4771
	0	0.33333	−0.4771
$60 < T_{MAORT} \leq 1000$ minutes	1	0.000033	−4.4771
	0	0.333333	−0.4771

Therefore, from the SLIM models in Figure 6:

$$\text{HEP for Operator alarm response in the case study} \\ = 0.0033 + 0.0027 + 0.0025 = 0.0084$$

4.3 CALCULATE THE PFDavg OF AN ALARM LAYER

If the failure of a BPCS loop is not the initiating cause of the scenario, then the independent sensor can be connected to the Distributed Control System (DCS) for alarm purposes and credit may be also taken for other SIF's (including alarm & ESD layers) with separate final elements. However, if a BPCS loop in the DCS is the initiating cause, then no more than one SIF in a SIS for a single scenario can be taken, and credit should be taken for the alarm layer only if it is separate from DCS loop. The PFDavg of Alarm layer is an 'OR Gate' between PFD of Sensor to annunciator, the HEP of Operator alarm response and the PFD of the final element (HSE UK, 2009a).

$$\begin{aligned} \text{PFDavg}_{\text{Alarm layer}} = {} & \text{PFD}_{\text{Sensor to Annunciator}} \\ & + \text{HEP}_{\text{Operator alarm response}} \\ & + \text{PFD}_{\text{to Final element}} \end{aligned} \quad (7)$$

For the case study:
$\text{PFDavg}_{\text{Alarm layer}} = 0.0003$ (level radar) + 0.0001 (DCS Hardwired) + 0.0084 (HEP from Section 4.2) + 0.0002 (Push-button) + 0.0004 (ROSoV) = 0.0094 ~ equivalent to RRF of 100 or SIL-2 rating.

Reducing the test intervals of the sub-elements will achieve a more conservative PFD value for the alarm layers in above example.

5. CONCLUSION

In this paper we have not considered a mitigation layer such as an escape to a temporary refuge or a safe assembly point (King, A.G., 2007). The success of this layer may prevent a fatality even though a hazardous consequence still occurs. The emergency evacuation procedure differs for each plant and hence this layer is not considered in the current paper. Human failures during testing and maintenance (King, A.G., 2007), for example, failure to put a trip back to operational mode from testing mode after calibration, testing or maintenance, resulting in not achieving the required safety function, are are also not considered. However, the same approach described in this paper can also be used for these types of human failures.

Section 3 of this paper emphasised the need for a comprehensive qualitative modelling of the task or system prior to quantification. The process described above provides a systematic framework to achieve this to address both human initiating events and responses to alarms. For human initiating events, the modelling approach decomposes a task to the most appropriate level for the specific type of assessment being performed. The more detailed the modelling, the less likely it is that a significant human initiating causes will be missed, but the greater the analytical effort required.

As discussed in Section 3.5 and Figure 4, verification, checking, and possible dependency issues can be addressed within this framework. The HTA also readily maps on to the fault tree structure, which will be familiar to engineering reliability and safety analysts. The use of HTA to structure the task modelling has the advantage that it allows task elements to be screened and prioritised prior to quantification being applied, thus minimising the analysis resources required. By breaking down the task to a greater level of detail and using systematic search process to identify possible failure modes, it is likely that a more realistic estimate of the HEP will be developed. In addition, the qualitative analysis will provide improved insights into the ways in which the overall HEP could be reduced by identifying the PIFs that are driving the HEPs (Embrey, D. E., 2012). In order to address human failures effectively, the approach set out in Section 3 is recommended for SIL determination in both the design stage and for existing plants.

Figure 6 is a generic model that should be applicable to alarm responses in most process plants. However, when a complex or multiple alarm response is required, Steps 3.1 to 3.3 outlined in Section 3 can be used to identify the appropriate PIFs. This paper also shows that in order to achieve a SIL-2 equivalent alarm layer it is necessary to take into account both the human and engineering reliability aspects of the system in a systematic manner. The Section 4 approach is more relevant for the SIL determination of existing plants without automated trip functions. Thus, a lower human initiating cause frequency and even a risk reduction factor of 100 or SIL-2 equivalent for the alarm layer may be possible by improving the PIFs.

ACKNOWLEDGEMENTS

We would like to acknowledge the many conversations with thier colleagues, Alan G King and William Bridge that have helped in the formulation of the ideas put forward in this paper.

REFERENCES

1. Bridges, W., 2011, LOPA and Human Reliability – Human Errors and Human IPLs (Updated), 7th Global Congress on Process Safety, Chicago, Illinois.
2. BSI, March 2003, BS EN 6151:2004 – Functional safety. Safety instrumented systems for the process industry sector.
3. BSI, June 2010, BS EN 61508:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems.
4. Embrey, D. E., & Henderson, J., 2011, The UK Experience in Managing Risks Arising from Human Error. Proceedings of the 7th Global Congress on Process Safety American Institute of Chemical Engineers, Chicago, USA.
5. Embrey, D. E., & Henderson, J., 2012, An independent evaluation of the UK process industry association gap analysis tool for addressing the use of an operator as a SIL 1 component in tank overfill protection systems. IChemE Hazards XXIII conference, Stockport, UK.
6. Embrey, D. E., & Zaed, S., 2010, A set of computer-based tools for identifying and preventing human error in plant operations, Proceedings of the 6th Global Conference on Process Safety American Institute of Chemical Engineers, San Antonio, USA.
7. Embrey, D. E., 1986, SHERPA: A Systematic Human Error reduction and prediction approach. Paper presented at the American Nuclear Society International Meeting on Advances in Nuclear Power Systems, Knoxville, TN, USA.
8. Embrey, D. E., 2004, Human Reliability Assessment In: Human Factors for Engineers Sandom, C. and Harvey R. S. (Eds.) ISBN 0 86341 329 3 Institute of Electrical Engineers, London, UK.
9. Embrey, D. E., 2012, SHERPA Revisited - A Systematic, Human Error Reduction and Prediction Approach to modelling and assessing human reliability in complex tasks, 2012 PSAM 11 & ESREL 2012 Conference, Helsinki, Finland.
10. HSE UK, 2007, HSG 48: Reducing error and influencing behaviour.
11. HSE UK, 2009a, Process Safety Leadership Group Final report: Safety and environmental standards for fuel storage sites.
12. HSE UK, 2009b, RR716: A review of Layers of Protection Analysis (LOPA) analyses of overfills of fuel storage tanks.
13. King, A.G., 2007, Inclusion of Human Failure In Risk Assessment, IChemE Symposium Series No. 153, UK.
14. Swain, A.D., & Guttmann, H.E., 1983, Handbook of human reliability analysis with emphasis on nuclear power plant applications. Report No. NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, DC, USA.