AN INDEPENDENT EVALUATION OF THE UK PROCESS INDUSTRY GAP ANALYSIS TOOL FOR ADDRESSING THE USE OF AN OPERATOR AS A SIL LEVEL 1 COMPONENT IN TANK OVERFILL PROTECTION SYSTEMS

David Embrey and Jamie Henderson
Human Reliability Associates, Dalton UK

The UK Process Industry Association (UKPIA) has developed a minimum set of requirements for an operator to be considered part of a SIL1 safety function in relation to tank overfill protection systems at refineries and terminals. The requirements address areas such as system architecture, human factors, communication and alarm management. This set of requirements was used by the UKPIA to develop a self-assessment tool (the SIL 1 Human Factors Self-assessment tool) for organisations to assess an actual or proposed Safety Instrumented System (SIS) that incorporates a human operator.

With the support of the UKPIA, Human Reliability Associates conducted an independent evaluation of the proposed UKPIA approach to assuring the adequacy of the use of a human operator to provide adequate SIL 1 level protection. This required inputs both from human reliability specialists and from engineers with substantial experience of using SIL concepts and standards in engineering risk analyses. As a result of the evaluation, UKPIA's approach was developed into a Gap Analysis Tool (GAT) to evaluate the adequacy of an operator as a SIL 1 component in specific systems. This paper describes the GAT, and outlines the review process that was conducted to verify its usefulness.

1. INTRODUCTION

The UK Process Industry Association (UKPIA) proposed an approach for assessing the use of a human operator to provide SIL 1 level protection in a safety system. The full report [1] and supporting tools can be accessed at the UKPIA website. Human Reliability Associates were asked to provide an independent evaluation of the proposed approach. The terms of reference of the review were that, in accordance with IEC61511, operators may form part of a SIL1 safety function, provided appropriate measures and controls have been implemented. The appropriate measures and controls were set out as minimum compulsory requirements within a self-assessment tool.

The review covered five main areas, addressed within separate work packages (WP):

WP1 Verification that the self-assessment tool addresses all necessary factors or conditions that need to be addressed for an operator to act as part of a safety function.

WP2 Verification that the compulsory requirements identified within the self-assessment tool meet current expectations/good practice as identified in the following standards:

- BS-EN61511
- EEMUA 191
- HSE guidance on alarm handling

WP3 Verification that that the minimum compulsory requirements identified within the self-assessment tool provide a substantiated and defensible case for the inclusion of an operator within a SIL1 safety function as part of the end to end safety function.

WP4 Consideration of the Probability of Failure on Demand (PFD) quotient that may be attributed for an operator, given current guidance taking into account the response time and compliance with the compulsory requirements identified in the assessment.

WP 5 Use of training simulators to validate the predictive capability of the self-assessment tool model.

The review was carried out in consultation with the UKPIA working group that had been established to develop the self-assessment tool. WP2 was carried out in parallel with WP1, and the results of the standards review were incorporated in the overall review of the tool. As a result of the initial review, the original self-assessment tool was restructured into two tools. The first of these is a Gap Analysis Tool (GAT) which allows the focussed evaluation of the most relevant factors necessary to justify the use of an operator as a SIL 1 component in a Safety Instrumented System (SIS). The second is a self-assessment tool that will assess a system against markers of overall excellence in process safety. The project included two site workshops, and the comments from the participants in these workshops were incorporated in the GAT. The subsequent sections of this paper will focus on the GAT structure, the site workshops and the PFD issues.

2. REVIEW OF THE CONTENT OF THE TOOL

The terms of reference for WP1 included the requirement to verify that the self-assessment tool addressed all necessary factors or conditions necessary for an operator to act as part of a SIL 1 safety function. This was interpreted as confirming that all variables that might affect operator response

to an alarm in an overfill scenario, (subsequently referred to as Performance Influencing Factors, PIFs) were included in the tool.

We reviewed the PIFs in the tool using our professional knowledge of human factors issues and their impact on alarm response, based upon 35 years of experience in the oil and gas sector. We also evaluated the items included in the tool against a set of relevant PIF lists relevant to operator response in alarm situations, i.e. HEART [2], ATHEANA [3] and CCPS [4]. HEART and ATHEANA are both human reliability assessment tools that have been developed to provide quantitative assessments of human reliability in nuclear, process and other industries. They contain comprehensive lists of PIFs that are used to generate human error probabilities. CCPS is the textbook 'Guidelines for Reducing Human Error in Process Safety' that was developed by for the Center for Chemical Process Safety. It provides guidance for the process industry regarding relevant PIFs that need to be considered when assessing human reliability. The initial conclusions of the review were that the tool contained a good broad coverage of relevant PIFs. However, some factors, (e.g. shift handover), although important from a general HF perspective, were considered to be less important for operator response to alarms in situations such as tank filling.

Because of the very different nature of the human and hardware components in the chain of response from the initiating event to its successful management, the reviewers felt that it was desirable to separate the human and hardware questions in the tool. The nature of the task(s) that are to be evaluated by the tool needed to be clearly defined. For example it was felt that communication elements should be excluded. This had the effect of eliminating a number of communications related factors from consideration and increased the focus on key issues such as the time required for response. If the scope of the tool is to be extended to consider situations where the remote valve fails to operate, then issues related to communication may become relevant again in terms of recovery. Similarly, the scope of the response may include advising relevant parties (e.g. ships, adjacent sites) of the shutdown and emergency. There may be other risks associated with post-alarm response actions (e.g. advising a ship of action) that are not currently addressed in the tool.

3. RESTRUCTURING THE TOOL

The review concluded that the original draft of the tool included a mix of two distinct groups of factors. The first of these was relevant to achieving best practice with regard to process safety excellence, and the other consisted of specific factors which could be related to alarm response. It was therefore proposed that the tool should be restructured in the form of two separate tools. The first of these is a Gap Analysis Tool (GAT), which allows the focussed evaluation of the most relevant factors necessary to justify the use of an operator as a SIL 1 component in a SIS. The second should be a self-assessment tool that will assess a system from the point of demonstrating overall excellence in process safety. These tools are now included as Appendices 1 and 2 in the UKPIA document 'Operators and SIL 1 Safety Systems for Overfill protection of Tanks' [1].

In developing the format for the GAT, the following criteria were applied:

- The analysis should be concerned solely with the probability of the operator responding in a timely fashion to a SIL1 alarm
- The structure of the tool should be based on an end to end process that includes the specific functions of alarm detection and response that are central to the SIL requirement
- The tool should not include any subsequent emergency response tasks (e.g. raising a site alarm in the event of overfill) or recovery actions (e.g. response to failure of a valve to close). It does however include the detection of such a failure
- The revised tool should be based on those factors in the original tool that are specific to the response to tank level alarms
- The revised GAT should include any additional factors not currently included in in the original tool but considered to be relevant

The requirement to structure the tool as an end-to-end process led to the use of a standard human factors model of operator response in alarm response conditions. This can be represented in the form shown in Figure 1:

The assessment factors contained in the GAT were therefore organised to comply with this model. Each of these topics has a comprehensive set of evaluation questions. The detailed content of the GAT including the full question set is provided in Appendix 1. The main elements of the GAT are shown in Figure 2. The human factors questions were developed partly from the experience of both the engineering and human factors specialists in the project team. Some specific sources of relevant PIFs were the documents cited previously [2, 3, 4]. The final version of the GAT, described in [1], is in the form of a spreadsheet, where the analyst evaluates the compliance to the question set of the system being assessed by means of a yes/no score.

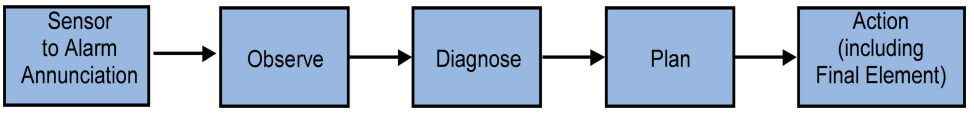

Figure 1. Simple sequential model of operator response to an alarm

Phase		Elements for assessment
1.Hardware 1	**1.1 Sensor**	Assessed using the criteria in 61511
	1.2 Alarm	Assessed using the criteria in 61511
2. Human Factors	**2.1 Alarm detection**	2.1.1 Availability of staff to hear alarm
		2.1.2 Ease of alarm detection
	2.2 Alarm Response	2.2.1 Awareness of tank status
		2.2.2 Available time for response
		2.2.3 Ease of deciding appropriate response
		2.2.4 Ease of control panel operation
		2.2.5 Operating culture (willingness to act)
	2.3 Response confirmation	2.3.1 Confirmation of response from instrumentation
		2.3.2 Confirmation of response from other sources
3. Hardware 2	**Final element**	Assessed using the criteria in 61511

Figure 2. Structure of the GAT

4. VERIFICATION OF THE SELF-ASSESSMENT TOOL CONTENT BY SUBJECT MATTER EXPERTS

The first criterion for assessing the validity of the tool was completeness of coverage: did it address the most important factors that determine the likelihood of effective operator response to an alarm? A second criterion was credibility: are the factors included in the tool considered to be reasonable by operators and other personnel working in situations where responding to alarms is a daily occurrence? The content of the GAT was checked against standards and relevant literature by experienced human factors professionals and revised where appropriate. As a further level of assurance, we carried out a verification exercise at two refineries. The basic assumption of the exercise was that front line operating personnel, with direct experience in responding to process alarms, would provide valid opinions regarding the comprehensiveness of the factors contained in the tool and their validity as a set of criteria for including an operator as part of a SIL 1 safety function.

The participants in the first workshop were a group of process safety specialists and panel operators with 20+ years of experience. The second workshop included the refinery's human factors specialist and two experienced panel operators, with 17 and 20 years of experience respectively. The participants in both workshops were given a list of the factors included in the GAT and also shown the detailed questions used for assessing these factors. The team was then asked to comment on the factors, and also to indicate if there were any significant omissions from the list, i.e. other areas that needed to be covered in order to assess the likelihood that there would be an effective human response to a process alarm. The discussion concluded that the list of factors was comprehensive, and no additional factors were proposed. These results provided an assurance that the factors included in the GAT were appropriate, comprehensive and valid indicators of the extent to which an operator could be included as part of a SIL 1 safety function.

5. EVALUATING THE PFD FOR AN OPERATOR

Establishing the PFD quotient, or a human error probability (HEP), for a task of this type, is difficult for a number of well documented reasons (see, for example, Kirwan [5], and Embrey, [6]). A major problem is the lack of available, reliable data in this area. Where data does exist, other issues, such as how nominal data in a HEP database should be modified to take into account context specific Performance Influencing Factors need to be considered. For example, the HEP for an operator in a given situation will be influenced, both negatively and positively, by a number of factors (e.g. quality of training, presence of distractions, and level of fatigue). A related issue is the transferability of data from one setting to another. For example, a HEP probability obtained for a task in a nuclear power station

may not apply in an oil refinery, where the pressures on operator performance are likely to be different.

As shown in Appendix 1, the GAT provides a number of yes or no questions, which if answered affirmatively, specify the optimal conditions for minimising the PFD for an operator in a SIL level 1 system. However, even if the system cannot be scored as a yes on all questions, the PFD may still be within the SIL level 1 target PFD range of $\geq 10^{-2}$ to 10^{-1} . In its current form, the GAT does not provide any explicit process to link variations in scores for the factors in the GAT to a PFD. This capability would obviously be very useful in that it would enable a specific PFD to be determined for the system being evaluated. If the GAT scores for the system indicated that the predicted PFD was outside the acceptable range for a SIL 1 component, the use of scales to rate the quality of the factors in the GAT would enable the safety analyst to identify the problem areas that needed to be improved in order to achieve an acceptable predicted PFD.

Possible techniques that can be used for this approach include the Success Likelihood Index Method (SLIM) which is described in a detail in a companion paper in this conference [7] and the IDEAS approach (Influence Diagram Evaluation and Assessment System) [8] which uses a Bayesian approach to gathering evidence from experienced operators regarding their perceptions of error probabilities under varying operational conditions. A trial application of this method was carried out as part of the two refinery workshops, and is described in detail in the main report [1]. The results of this exercise were inconsistent, and confirmed that there was a need to collect actual field data on PFDs from operating plants in order to verify the effectiveness of the wide the range of quantification techniques that are available. The feasibility of using simulators and data from SCADA systems in operating plants was the focus of the final workpackage of the project.

6. USE OF TRAINING SIMULATORS AND OTHER SOURCES OF DATA TO VALIDATE THE PREDICTIVE CAPABILITY OF THE SELF-ASSESSMENT TOOL MODEL

Two types of data collection systems could be used to develop a comprehensive and defensible body of evidence from which to estimate PFDs. Training simulators provide an attractive method for collecting such data, as they are already employed extensively process plants, and the data recording functions can easily be adapted to collect information that can be used to generate PFDs. Another advantage of using training simulators is that the conditions which affect the PFD, such as the time available, quality of the information, and other contextual factors evaluated in the GAT, can be systematically varied as part of a planned experimental programme. This would allow the impact of these factors on the PFDs to be measured, and could be used to develop a model to predict PFDs.

Data collection using the SCADA system has the advantage that it can allow large volumes of data to be accumulated from plant DCS systems. The feasibility of this approach had been demonstrated at Refinery 2, where the SCADA system had been interrogated to determine the proportion of operator responses to an alarm which were considered to be within an acceptable time interval. Another advantage of this approach is that data are collected under real operational conditions, which are difficult to replicate realistically in a training simulator. The main disadvantage is that data on the conditions under which successful or unsuccessful responses to alarms occurred cannot easily be collected by DCS systems. An approach was proposed to address this problem by setting up a parallel manual data collection system to record these operational conditions, which could be used in conjunction with the SCADA based process to provide contextualised data.

7. CONCLUSIONS

The overall conclusion of this review is that the revised GAT comprehensively addresses the conditions that need to be assessed to verify that an operator can act as part of a safety function. The tool has been subject to a comprehensive review by human factors specialists, the UKPIA steering committee, and operating personnel. In order to maximise consistency in the use of the tool, it is recommended that further background information is provided to assist users in answering the assessment questions. This could be in the form of links to appropriate Web resources and other relevant documentation

There would clearly be value in applying the tool widely in a reasonably large sample of sites in order to obtain feedback on both its usability and also to compare its predictions with operational data. Because of the difficulty of obtaining such data, it is recommended that use of training simulators and SCADA based data collection methods be explored further.

REFERENCES

1. SIL1 Human Factors Assessment Tool Review: Final Report November 2011 UKPIA website: http://www.-ukpia.com/process-safety/tools/self-assessment-tools.aspx Understanding Hazards & Risks.
2. Williams J. C. 1986 *HEART A proposed Method for Assessing and Reducing Human Error*) In: Proceedings of the 9th Advances in Reliability Technology Symposium University of Bradford.
3. Cooper, S. E., Ramey–Smith, A. M., Wreathall, J., Parry, G. W., Bley, D. C. Luckas, W. J., Taylor, J. H., Barriere, M. T. 1996 A Technique for Human Event Analysis (ATHEANA) – Technical Basis and Methodological Description. NUREG/CR- US Nuclear Regulatory Commission 6350 Brookhaven National Laboratory, Upton, NY.
4. Embrey, D. E., Kontogiannis, T. and Green, M. 1994. *Guidelines for Reducing Human Error in Process Safety*

Center for Chemical Process Safety American Institute for Chemical Engineers New York: Wiley.
5. Kirwan, B. 1994 *A Guide to Practical Human Reliability Assessment* Taylor and Francis: London.
6. Embrey, D. (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 Publishing London UK (2004).
7. Embrey, D., Mrudhul, R. 2012 A systematic Approach to Addressing Human Factors issues for SIL Determination Studies This Conference.
8. Phillips, L. D., Embrey, D., Humphreys, P. and Selby, D. L. 1990 *A Socio-technical approach to assessing human reliability*. In Oliver, R. M., and Smith, J. A. *Influence Diagrams. Belief Nets and Decision Making: Their Influence on Safety and Reliability* Wiley, New York.

APPENDIX 1
DETAILED CONTENT OF THE GAP ASSESSMENT TOOL (GAT)

	Preconditions
R1.1	As part of the hazard analysis, have relevant human factors aspects been considered, including identification of potential human error both as initiating event and in responding to alarms/emergency response?
R1.2	Is there a single operator response required to initiate the SIL1 safety function from a control panel (i.e. remote activation of the final element from a push button)?
R1.3	The SIL1 safety function does not rely on further communication (i.e. The operator does not need to seek advice from others relating to clarification of alarm, or to clarify the appropriate action to take)?
R1.4	The course of action that the operator is required to take in the event of an alarm initiating the SIL1 safety function is pre-specified (this should be a single action, such as stopping the flow into the tank)?
R1.5	If alternative actions are permissible by the operator in the event of an alarm initiating the SIL1 safety function (for example closing an inlet valve OR diverting flow by actuating multiple valves) the alternative options should be limited to no more than five?
R1.6	Where alternative actions may be taken by the operator, where feasible, a checklist or job aid is available in a prominent position at the control panel. The checklist or job aid should clearly specify the required action based on input conditions (in the format If Condition X, then do Action Y)?
R1.7	Where a checklist or job aid is used, operators required to carry out the SIL1 safety function action are trained in emergency response using this checklist or job aid?
R1.8	For the operator initiating the SIL1 safety function, whether by initiation of a single action, or by determining an appropriate alternate action, no additional diagnosis for which knowledge of operating principles is necessary (i.e. The operator does not require any additional information before initiating the trip)?

		Hardware
Sensor	R2.1	Is the Safety Instrumented Functions (SIF) sensor separate and independent from the Basic Process Control System (BPCS - for example, ATG, DCS, SCADA) alarm?
	R2.2	Has the Probability of Failure on Demand (PFD) for the sensor been drawn from plant experience or from other recognised sources when demonstrating SIL achievement, and does this meet the target failure measure for the SIL?
	R2.3	Does the Safe Failure Fraction (SFF) and Hardware Fault Tolerance (HFT) of the sensor subsystem meet the architectural constraints of BS EN61511 for the target SIL?
Alarm	R2.4	Is the response to the SIS alarm sufficiently independent from the Basic Process Control System (BPCS - for example, ATG, DCS, SCADA)?

		Human Factors: Alarm Detection
Availability of staff to hear alarm	R3.1	Are there sufficient resources to ensure there will always be an operator in the vicinity of the control panel to respond to an alarm within the required time (i.e. Cover for tea/food/toilet/rest breaks)?
	R3.2	Have work patterns been assessed and balanced to minimise fatigue?
	R3.3	Are procedures in place to manage the working hours of operators in safety critical roles to comply with the Working Time Regulations and minimise the risk of fatigue?
Ease of alarm detection	R3.4	Does the alarm management procedure have clearly defined process for inhibiting and reinstating an alarm which is readily accessible to the operator?
	R3.5	The alarm management procedure have a clear mechanism to define the category and priority of alarms?
	R3.6	Is there a clearly defined process to control changes to the alarms?
	R3.7	Are SIL1 alarms clearly displayed to the operator?
	R3.8	Does the system provide different audible tones for different priorities of alarm?
	R3.9	Are audible warnings clear and distinguishable between operator stations?
	R3.10	Are SIL1 alarms differentiated clearly from other lower priority alarms?
	R3.11	Does operator training include training on the alarm system?

		Human factors: Alarm response
Awareness of tank status	R3.12	Does the shift handover include formal updates on the status of SIL1 tanks and their alarms (e.g. if maintenance is being performed)?
	R3.13	Is tank status information available to operators?
Available time for response	R3.14	Is there a Basic Process Control System (BPCS - for example, ATG, DCS, SCADA, operator monitoring of tank levels) in place that will take corrective action in response to a high alarm? (where operator monitoring is in place, is there sufficient time for the operator to observe, diagnose, plan and action the alarm
	R3.15	Have SIL1 alarm levels been set at a level to allow sufficient time for the operator to observe, diagnose, plan and action the alarm prior to an overflow occurring?
	R3.16	Are there alarm response procedures (or Job Aids) in the immediate vicinity of the alarm control panel for SIL1 alarms? (Only applicable if more than one alternative response)
	R3.17	Do the SIL1 alarm response procedures (or job aids) give clear, concise account of action to be taken in response to each individual alarm? (Only applicable if more than one alternative response)
	R3.18	Is workload managed so that there will always be sufficient resource available to respond to alarms?
	R3.19	Do operators ever run the tanks at levels above the highest non-SIL alarm level? (threat of reduced time for response)
Ease of deciding appropriate response	R3.20	Does operator training cover the defined response to safety related alarms? (including understanding the consequences of failure to respond and action to be taken)
	R3.21	Does the operator receive refresher training on the defined response to safety related alarms?
	R3.22	Do alarms give sufficient information to enable operator to easily identify equipment and nature of the problem
	R3.23	Does the system have the facility to bring up a detailed graphical display in relation to the latest alarm?
Ease of control panel operation	R3.24	Does all equipment on the Basic Process Control System (BPCS - for example, ATG, DCS, SCADA) have unique, clearly defined ID labels to prevent confusion between similarly tagged equipment?
	R3.25	Does the Basic Process Control System (BPCS - for example, ATG, DCS, SCADA) give sufficient feedback on the status of equipment to allow operator to identify if corrective action has been successful?

Operating culture (willingness to act)	R3.26	Do operators practice regular emergency response drills, including desk-top exercises?
	R3.27	Are specific measures in place for ensuring that SIL1 alarms have a very low probability of false operation e.g. arising from equipment faults
	R3.28	Is the culture and training regime such that operators do not have any inhibition from responding to a SIL1 alarm, even if this response could have a significant negative impact on production, down time or other profit related issue
	R3.29	Operators do not feel that they need to seek confirmation or clarification from their supervisors or any other staff before acting on SIL1 alarms

Human Factors: Response Confirmation		
Confirmation of response from instrumentation	R3.30	Does the Basic Process Control System (BPCS - for example, ATG, DCS, SCADA) page showing the affected equipment also display alarm status as a double check to ensure intervention performed on correct equipment?
Confirmation of response from other sources	R3.31	Is there any other confirmation that the response has been successful (e.g. remote operator, feedback from associated process variables such as flow)

Hardware		
Final Element	R4.1	Is the SIS final element (including initiating pushbutton) separate and independent from the Basic Process Control System (BPCS - for example, ATG, DCS, SCADA)?
	R4.2	Has the PFD for the final element been drawn from plant experience or from other recognised sources when demonstrating SIL Achievement, and does this meet the target failure measure for the SIL?
	R4.3	Does the Safe Failure Fraction (SFF) and Hardware Fault Tolerance (HFT) of the final element subsystem meet the architectural constraints of BS EN61511 for the target SIL?
End to End Functionality	R4.4	Does the end to end Safety Instrumented Function (SIF) meet the target SIL1 in terms of target failure measure (PFD) and architectural constraints?
	R4.5	During the design of the Safety Instrumented Function (SIF), have failure modes for each element been considered, and that these failures are revealed to the operator where possible (for example instrument failures)
	R4.6	Have the loss of utilities (for example power, air supply) been considered as part of the demonstration of SIL Achievement?