UKpia

UK Petroleum Industry Association Ltd.

Gap Analysis and Self Assessment for -

OPERATORS & SIL1 SAFETY SYSTEMS FOR OVERFILL PROTECTION SYSTEMS

Doc. Type / Title: Gap Analysis & Self Assessment Module Operators & SIL1 Safety Systems for Overfill Protection of Tanks		Project: Process Safety Leadership				
		Issue Date: 15th November 2011				
UKpia		Document identity: UKPIA SIL1 Operators	Lang.: en	Rev. ind.: 1.2	Sheet: 1	No. of sh.: 22

Foreword

As part of its Process Safety Leadership Commitment, UKPIA has developed, through its members, a framework for self assessment in process safety. This document provides detailed guidance on the use of both a self-assessment tool and gap analysis for determining the suitability of an operator within a Safety Instrumented Function (SIF) where an automated interlock is not provided, referred to as 'UKPIA SIL1 Operators'.

This toolset was developed by UKPIA and its member companies. This document is distributed to member companies to allow them to perform self-assessment and gap analysis in accordance with the Process Safety Leadership Commitment.

It is not the intention of this document to specify how human factors processes for SIF's should be developed, nor replace any existing corporate assessment or audit activities. The intent of this document is to:

1. Provide a means by which organisations can perform a gap analysis against high priority requirements when using an operator to form part of a SIF, and
2. Provide a means by which organisations can further assess themselves against a common framework of excellence in process safety when using an operator to form part of a SIF.

It is not the intent of this document to justify the suitability of an operator as part of an Alarm Function that of itself is not or will not be SIL1 rated.

There are no limitations on further distribution of this document to other organisations outside of UKPIA, provided that:

1. It is understood that the UKPIA SIL1 Operators document and associated tools represent UKPIA's view of a common framework
2. UKPIA owns all rights to the UKPIA SIL1 Operators document and associated tools.
3. UKPIA accepts no responsibility in terms of the use or misuse of this document.
4. The UKPIA SIL1 Operators document and associated tools are distributed in a read only format, such that the name and content is not changed and that it is consistently referred to as "The UKPIA Gap Analysis and Self Assessment for Operators and SIL1 Safety Systems for Overfill Protection of Tanks".
5. It is understood that no warranty is given in relation to the accuracy or completeness of information contained in the document except that it is believed to be substantially correct at the time of publication.

Contents

1. Introduction

This is one of a suite of documents prepared by UKPIA as part of their commitment to process safety.

The purpose of this document is to provide the detailed guidance and tools necessary to perform a gap analysis of key factors, and a self-assessment against excellence, of human factors for operators which form part of an overfill protection SIF.

Supporting this document, two tools have been produced:

1. Gap Analysis – provides a mechanism for gap analysis against key factors that are required for an operator to be considered as part of an overfill protection SIF, reference should be made to section 2.1 for a definition of the compliance terms.

2. Self Assessment Module – Further human factors aspects that may wish to be considered by an operator (where appropriate) as a view of process safety excellence in this area.

1.1 Scope

Applicability

Where it has been determined that a Safety Integrity Level of 1 (SIL1) is required (through appropriate hazard analysis and SIL determination techniques, refer to section 1.1.1) as a layer of protection to reduce the overall risk of a tank overflow to As Low As Reasonably Practicable (ALARP), and an operator is identified as a required element of the Safety Instrumented Function (SIF).

It is unlikely that SIL2 or higher can be achieved for any safety instrumented function including an operator – where the risk assessment and SIL determination has identified an additional protection layer greater than SIL1, a fully automated system should be considered.

Tanks within scope

Tanks within the scope of this document are defined as: Bulk storage atmospheric tanks at refineries, terminals and petrochemical facilities.

Usage

It is envisaged that the gap analysis provided as part of this toolset will typically be utilised during Phase 4 (Design and Engineering) of the BS EN 61511 safety lifecycle, which excludes such activities as operation, maintenance and demolition. However, the gap analysis tool does consider the key processes and procedures necessary during the operation and maintenance phases of the safety lifecycle that are a required element for the operator when they form part of the overall SIF.

The gap analysis tool may also be used retrospectively to assess the suitability of existing SIF's which incorporate an operator.

It is intended that this toolset is used by designers of the SIF, and that the designers have the appropriate knowledge, or access to relevant experience, in human factors.

It is not the intent of this tool to be used to justify the Probability of Failure on Demand (PFD) of an operator response to an alarm that is claimed as an Independent Protection Layer (IPL) in a risk assessment analysis that does not:

- Require a SIL1 system or greater or
- Has an automated interlock that provides the SIF

The level of rigor is not appropriate over and above the technical assessment of the PFD for the operator response to an alarm. However, where IPL's for operator response to alarm are claimed with PFD of <0.1 then this tool may be used to support those claims.

Limitations on use

For the purpose of overfill protection of a storage tank, this document and associated tools assumes that a single operator action is required to initiate the safety function from a control panel (i.e. remote activation of the final element from a push button). This does not preclude the use of more than one operator within a SIF, however further analysis would be required to determine the nature, role and interaction (and thus the combined reliability) between those operators which form part of the function.

Compliance with the gap analysis, or the self assessment module, does not constitute full compliance with the standards quoted in section 1.2. The tools provided draw only on those elements relevant to the use of operators as part of a SIF, and do not address any further functional safety, alarm system design or human factors requirements.

In the context of the interpretation of the self assessment element of this toolset by the competent authority, it is not aimed at assessing an operator's performance against existing best practice or standards, but instead to put forward a view of excellence, identifying another tier that can be used to enhance what is already done, if appropriate. The value in this tool is in the questions asked, rather than the score produced – challenging operators to look at their existing processes, and determining whether existing systems could or should be improved over and above existing best practice. This also implies that the 'correct' score will be site dependant and not necessarily 100% for specific sections or the totality. Thus, it would be appropriate for an inspector to ask an operator questions such as what did you learn from your self-assessment, and what has come out of it?

1.1.1 Risk Assessment

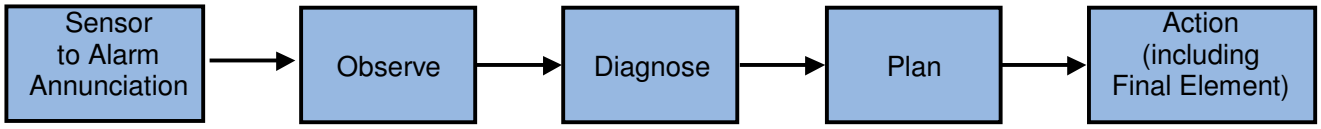
The use of operators within a SIF is recognised within both BS EN 61508 and BS EN 61511.

Before using the UKPIA SIL1 Operators toolset, it is assumed that appropriate risk assessment and SIL determination has been performed, identifying the need for an additional protection layer to SIL 1.

Careful consideration should be given to the use of an operator as part of a Safety Instrumented Function (SIF). Operators should be used where an automated overfill protection system would:

1. Give rise to a more serious safety or environmental consequence, or
2. Is considered ineffectual due to plant or process constraints

A safety instrumented function comprising of an operator can be expressed in block diagram form as follows:



The operator is required to:

- Observe the alarm on the alarm system,
- Diagnose the nature of the alarm or failure,
- Plan what action to take, and
- Perform the necessary action

The period of time for the operator to observe, diagnose, plan and perform the appropriate action is of critical importance when demonstrating that the target SIL has been achieved. Further guidance relating to risk assessment techniques and operator response can be found in the Safety and Environmental Standards for Fuel Storage Sites PSLG final report[1]

As part of the evidence to support the demonstration of SIL achievement, the completed gap analysis tool which forms part of this document, may be referenced.

1.2 Development

This document and associated toolset has been developed through a consultation process with experts from each member organisation. The question set developed is based on existing good practice contained within the references given below, and plant experience of the design and operation of human factors elements and safety instrumented systems. The working group consisted of experts in the following key subjects:

[1] The Process Safety Leadership Group (PSLG) report identifies and provides guidance to duty holders for addressing the recommendations of the Buncefield MIIB Design and Operations Report.

- Safety Instrumented Systems
- Alarm Management
- Human Factors
- Training and Competency
- Process Safety Management

Following the initial development of this document, an independent evaluation was performed by Human Reliability Associates (HRA) to assure the adequacy of the use of a human operator to provide adequate SIL1 protection. The verification process included the following elements:

1. In accordance with BS-EN61511, Operators may form part of a SIL1 safety function. The gap analysis provides a view of the minimum techniques, measures and controls necessary.

2. Ensuring that the gap analysis address all necessary factors to be considered for an operator acting as part of a safety function.

3. Ensuring that the gap analysis meets current expectations/good practice, identified in BS-EN61511, EEMUA 191 , HSE guidance as found on: http://www.hse.gov.uk/humanfactors/comah/alarmhandlinginfo.htm

4. The self assessment module identifies further human factors aspects that may wish to be considered by an operator (where appropriate) as a view of process safety excellence in this area.

Refer to Appendix 3 of this document for a description of the verification process adopted by HRA.

Following the development of the tool, a series of dry run tests were performed to verify the adequacy of the question set, and to ensure that the tool can be consistently applied and interpreted. Front line operational personnel were involved as part of these tests to ensure that factors relating directly to the control room operators had been effectively captured.

2. UKPIA Gap Analysis – SIL1 Operators

The gap analysis tool is included in Appendix-1 of this document.

2.1 Gap Analysis Guidance

The gap analysis is performed by individual UKPIA members, and may utilise such techniques as review of procedures, supporting documentation and individual change records, and discussions with those personnel directly involved in the use of the procedure.

For each question asked, a mark of 1 should be given in the appropriate column (one column only):

- Not Implemented. The hardware, management system or process does not meet the requirement
- Partially Implemented. The hardware, management system or process partially meets the requirement, there is a need/intent to carry out further work
- Fully Implemented. The hardware, management system or process fully meets the requirement
- Implemented SFAIRP. The hardware, management system or process meets the requirement so far as is reasonably practicable, no intent to carry out further work as this not justified on the grounds of reasonable practicability
- Not Applicable. The hardware, management system or process for this requirement is not applicable

Where appropriate, document references may be added in support of the responses provided.

2.2 SIF Overview

A description of the safety function should be provided, together with the parameters which determine the nature and operation of the function. This may be a reference to the applicable Safety Requirements Specification.

2.3 Attendance Record

The attendance record may be used to provide a record of those involved in the gap analysis process.

Note that:

1. Those involved in the gap analysis process should have knowledge of Human Factors and SIS, and wider corporate management systems.

2.4 Reference Documents

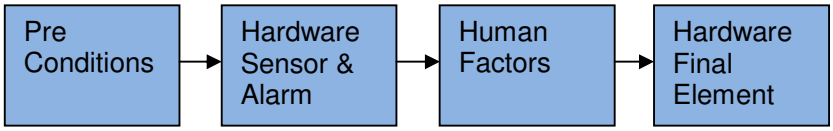
Where appropriate, a record of relevant documents reviewed as part of the gap analysis process should be provided. This may include:

1. Hazard and Risk Analysis
2. Design documents
3. Operational procedures and instructions
4. Training records
5. Audit records
6. Action plan for improvements

Note that individual document references may also be included as appropriate when responding to each gap analysis question.

2.5 Gap Analysis Worksheet

The gap analysis worksheet is structured such that it prescribes an end to end process that includes the specific functions of alarm detection and response that are central to the SIL requirements, this can be described as follows:



- Preconditions
- Hardware
  - Sensor
  - Alarm
- Human Factors
  - Alarm Detection
    - *Availability of staff to hear alarm*
    - *Ease of alarm detection*
  - Alarm Response
    - *Awareness of tank status*

        - *Available time for response*
        - *Ease of deciding appropriate response*
        - *Ease of control panel operation*
        - *Operating culture*
    - Response Confirmation
        - *Confirmation of response from instrumentation*
        - *Confirmation of response from other sources*
- Hardware
    - Final Element
    - End to End Functionality

3. UKPIA Self Assessment Module – SIL1 Operators

The self-assessment tool is included in Appendix-2 of this document. The self-assessment is divided into two phases, each related to a specific aspect of Human Factors when applied to Safety Instrumented Systems:

1. Alarm Detection
2. Alarm Response

The self assessment tool builds on the foundations of the gap analysis described in section 2, and provides further challenging questions to the user in order to assess against excellence in process safety, those areas of Human Factors development that can be worked toward to demonstrate excellence in the field. As each phase is completed, the self-assessment tool calculates a percentage score based on metrics agreed as part of tool development. A level of implementation, ranging from 0 (Awareness Building) to 4 (Optimising) is attributed to each percentage score as follows:

Phase		
Alarm Detection	0%	Awareness Building
Alarm Response	0%	Awareness Building
Average	0%	Awareness Building

Score	Level of Implementation	Attributes and Evidence
4	Optimising (best practice)	Effective and efficient. Visible continuous improvement culture/efforts in place. "We are systematically applying lessons learned and best practices to improve performance".
3	Managed	Documented and effectively implemented. "We consistently follow our programs and procedures".
2	Implementing	Documented. Implementation ongoing/not effective. "We have established programs and procedures and are working on implementation effectiveness".
1	Program Development	Some evidence that the practice exists (limited or no documentation of processes or practices). "We are aware of our gaps and are developing programs and procedures".
0	Awareness Building	Practice is essentially non-existent, or ad-hoc. Reliance on key people. Reliance on initiative. Processes & procedures minimal.

The results of the self-assessment can be used by the member to determine where best to focus improvement plans for this module.

3.1 Analysis

The results of the elements of excellence in process safety may be used by the UKPIA Process Safety Programme Manager (PSPM) to perform peer-to-peer analysis of the results, and where appropriate, provide feedback to individual member organisations.

Through repeat self-assessments, percentage scores and levels of implementation can be charted over time, providing indication of increasing levels of process safety excellence, within the scope of this module.

Refer to UKPIA_PSL_006[2], guideline for peer-to-peer analysis for further information.

3.2 Self-Assessment Guidance

The self-assessment is performed by individual operators, and may utilise such techniques as review of procedures, supporting documentation and individual change records, and discussions with those personnel directly involved in the use of the procedure.

For each question asked, a score of between 0 and 4 should be awarded for the current level of implementation, where:

0 – Awareness Building

1 – Program Development

2 – Implementing

3 – Managed

4 – Optimising

Where appropriate, document references may be added in support of the responses provided.

3.3 Attendance Record

The attendance record may be used to provide a record of those involved in the self-assessment process.

Note that:

1. Those involved in the self-assessment process should have knowledge of Human Factors and SIS, and wider corporate management systems.

2. An independent UKPIA witness can attend the self-assessment on request.

3.4 Reference Documents

Where appropriate, a record of relevant documents reviewed as part of the self-assessment process should be provided. This may include:

1. Hazard and Risk Analysis

[2] The Guideline for Peer-to-Peer Analysis provides detailed information relating to how data captured through assessment is quantified, compared and reported back to each member, and the controls that are in place to maintain confidentiality of this information.

2. Design documents
3. Operational procedures and instructions
4. Training records
5. Audit records
6. Action plan for improvements

Note that individual document references may also be included as appropriate when responding to each self-assessment question.

3.5 Alarm Detection

Alarm detection relates to the mechanisms and processes in place that may assist the operator in detecting the alarm. As part of the self assessment, this addresses the following key topics:

- Availability of staff to hear the alarm
    - Determined as essential factors for the operator as part of the SIF, Key topics are addressed as part of the Gap Analysis, refer to section 2
- Ease of alarm detection
    - Alarm Detection
    - Alarm system design
    - Implementation of the alarm management system procedures
    - Performance metrics
    - Record keeping
    - Training

3.6 Alarm Response

Alarm response relates to the mechanisms and processes in place that may assist the operator in responding to the alarm. As part of the self assessment, this addresses the following key topics:

- Awareness of tank status
    - Shift handover
    - Status of all tanks
- Available time for response

- Determined as essential factors for the operator as part of the SIF, Key topics are addressed as part of the Gap Analysis, refer to section 2

- Ease of deciding appropriate response
  - Procedures and training
  - Resources/Operator wellbeing
- Ease of control panel operation
- Operating culture

Appendix-1 UKPIA Gap Analysis Tool – SIL1 Operators

Appendix-2 UKPIA Self Assessment Module – SIL1 Operators

Appendix-3 Verification Process

The verification process adopted by HRA is defined by four work packages, WP1 to WP4.

WP1 – Verification that the toolset addresses all necessary factors to be considered for an operator acting as part of a SIF

Perform a review of control room response tasks to assess the comprehensiveness of the factors identified in the toolset. In addition, a short literature review to establish whether there are any other factors that may require consideration when examining control room response tasks.

WP2 – Verification that the requirements identified within the gap analysis tool meet current expectation/good practice

An analysis undertaken to evaluate the requirements stipulated in the tool against the three specified standards and guidelines: BS-EN61511, EEMUA 191, and the HSE guidance on alarm handling. Where additional potential requirements, not currently mentioned in the toolset, are identified, these are captured and included in the recommendations returned to UKPIA. Similarly, any compulsory requirements not mentioned in the standards are also highlighted. Finally, a summary report will detail where references to the requirements can be located in the standards and guidelines. The SIL specialists in the team focus on BS-EN61511, the EEMUA 191 aspects evaluated jointly by both the engineering and the human factors specialists, who take the lead on the HSE alarm standards.

WP3 – Verification that the toolset provides a substantiated case for the inclusion of an operator within a SIL1 SIF

WP1 and WP2 consider the range and appropriateness of issues identified in the toolset. WP3 is a more fundamental review of the toolset approach. The expectation is that, if applied correctly, the user toolset will, with confidence, be able to demonstrate that an operator can be included as part of a SIL1 safety function.

Part of this expectation will be met if the criteria discussed in WP1 and WP2 are satisfied. However, a more fundamental issue is whether a self-applied, checklist-based approach is sufficient for ensuring that an operator can be included as part of a SIL1 safety function. For example, a simple human factors analysis of the alarm response situation would normally consider the following stages in the response process:

- Detection of the alarm (influenced by factors such as the design of the alarm system, operator alertness, presence of an operator in the control room)
- Interpretation (influenced again by the nature of the information provided by the alarm system design, and factors such as the perceived reliability of the alarm system, level of training and experience)
- Action (including simply allowing the automatic trip systems to operate) (influenced by the control system design, situation awareness, training and experience)

The extent to which a more detailed consideration of the alarm response task would provide a more substantiated justification of the use of an operator to provide Level 1 SIL protection is addressed in this work package.

A review of the toolset approach is undertaken, and comparison with other possible approaches for undertaking this type of analysis, ensuring that the tool is implemented in the most effective way.

WP4 – Consideration of the Pfd quotient that may be attributed for an operator

The development of a predictive pfd model based upon the factors included in the toolset. This is accomplished by means of interactive workshop sessions facilitated by consultants from the HRA team.

References

The following table provides references to documentation used to develop the gap analysis and self-assessment module.

Description	Reference
Functional safety of electrical/electronic/programmable electronic safety-related systems	BS-EN61508
Functional safety. Safety instrumented systems for the process industry sector	BS-EN61511
Guide to the design, management and procurement of alarm systems	EEMUA 191
Safety and Environmental Standards for Fuel Storage Sites. Process Safety Leadership Group Final Report	ISBN-978-0-7176-6386-6
HSE Guidance – 'More information on alarm handling'	N/A

The following table provides details of applicable UKPIA process safety leadership documents that should be referenced where indicated within this self-assessment module.

Description	Reference
Overview Self Assessment Framework	UKPIA_PSL_002
Guideline for Peer to Peer Analysis	UKPIA_PSL_006

Abbreviations

Abbreviation	Description
ATG	Automatic Tank Gauging
CA	Competent Authority
DCS	Distributed Control System
EEMUA	Engineering Equipment and Materials Users Association
HEP	Human Error Probability
HFT	Hardware Fault Tolerance
HSE	Health and Safety Executive
HRA	Human Reliability Associates
IPL	Independent Protection Layer
LOPA	Layer of Protection Analysis
PFD	Probability of Failure on Demand
PSPM	Process Safety Programme Manager
PSLG	Process Safety Leadership Group
RA	Risk Assessment
SCADA	Supervisory Control and Data Acquisition
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SIF	Safety Instrumented Function
SIS	Safety Instrumented System
UK	United Kingdom
UKPIA	United Kingdom Petroleum Industry Association

Acknowledgements

This assessment module was created as part of UKPIA's Process Safety Leadership Commitment, under the direction of the Process Safety Leadership Network (PSLN).

PSLN and UKPIA wish to record their appreciation to the working group members who were responsible for creating this toolset:

Carole Egner	INEOS Manufacturing Scotland Ltd.
Daniel Brain	Murphy Oil
Peter Davidson	UK Petroleum Industry Association
David Kelly	PetroPlus
John Donald	Total
Linda Dixon	Chevron
Mark Manton	Shell (Chair)
Mike Boothman	Conoco Phillips
Richard Tinkler	Conoco Phillips
Robert Martin	PetroPlus
Dr David Embrey	Human Reliability Associates
Jamie Henderson	Human Reliability Associates
Dr Tony Foord	Human Reliability Associates
Dr Mark Sujan	Human Reliability Associates

Revision History

Rev.	Section	Description	Date	Changed By
0	All	First Issue	7-Aug-2009	PSD
1	All	Updated following HRA Review	24-Mar-2010	PSD
1.1	All	Updated following working group final comments	16-Apr-2010	PSD
1.2	All	Updated following trial runs at member sites	15-Nov-2011	PSD