HEALTH & SAFETY LABORATORY

HFC Meeting

Human Factors in Operational Risk Management With Focus on Barrier Management

HSE Experience of Incorporating Human Reliability into LOPA and SIL Analysis from an Engineers Viewpoint

Dr Colin Chambers CEng MIET

27th & 28th April 2016

© Crown Copyright, HSL 2016

HSE Experiences of Incorporating Human Reliability into LOPA and SIL Analysis from an Engineers Viewpoint

HEALTH & SAFETY LABORATORY

- Introduction.
- My background.
- Introduction to LOPA.
- Human reliability in LOPA
- Operator involvement in LOPA
- Example Buncefield LOPA operator tasks.
- Human factors issues in LOPA and SIL determination.
- Guidance associated with LOPA and Human Factors.

HSL: HSE's Health and Safety Laboratory

© Crown Copyright, HSL 2016

My Background

Dr Colin Chambers CEng MIET

- Background
  - Degrees in Electronic Systems, Control Engineering and Computer Science.
- Worked at HSL since 1996
  - Development of risk assessment methodologies.
  - COMAH safety report technical assessor EC&I.
  - SIL determination assessor & LOPA specialist.
  - Served on Process Safety Leadership Group (PSLG) LOPA sub-group.
    - Helped develop PSLG guidance on LOPA.
  - Member of competent authority (CA) group who assessed all post Buncefield LOPA studies for the UK bulk fuel storage sector.

© Crown Copyright, HSL 2016

Introduction

- My experience of working in HSE and with the UK petrochemical industry is that EC&I engineers and Process Safety engineers have been tasked with determining and reviewing Safety Integrity Levels (SIL) using methods such as Layer Of Protection Analysis (LOPA).
- It is also my experience that many processes within the petrochemical industry rely on operator involvement to perform critical control tasks and implement risk reduction measures.
- This talk presents a brief picture of HSE's experience of how engineers have accounted for human reliability in LOPA used for SIL determination.

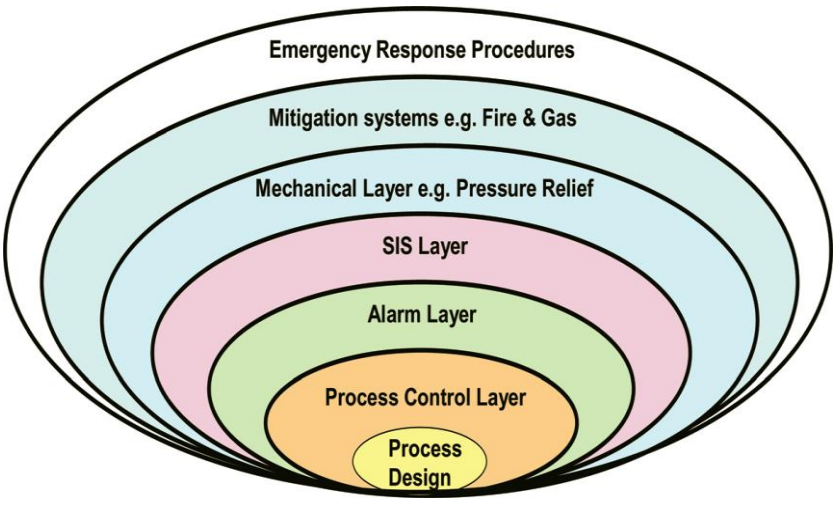
© Crown Copyright, HSL 2016

What is LOPA

- LOPA can be thought of as a method of assessing the balance between process risk and its risk reduction factors.
- LOPA represents the process safety Onion Layer Model of process risk reduction.
- The output from a LOPA is a mitigated event frequency, which is compared to a target frequency.

© Crown Copyright, HSL 2016

Onion Layer Model: Layers Of Protection



© Crown Copyright, HSL 2016

LOPA rules and their application to operator actions

LOPA rules support the requirements of IEC 61511 for SIL determination and guard against dependent failures.

- Independence.
  - Between independent protection layers (IPL), initiating event (IE) and conditional modifiers (CM) for each initiating event.
- Effectiveness.
  - The IPL is able to prevent the process entering an unsafe state without relying on any other risk reduction measure.
  - Layer completeness – 'detect – think – do'.
- Auditability.
  - Must be able to demonstrate, with documented evidence, all of the above issues associated with an IPL.

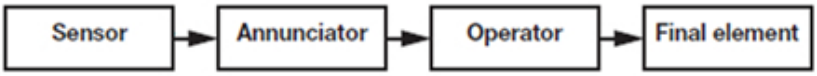
© Crown Copyright, HSL 2016

LOPA limitations with respect to operator involvement

- Requires independence between all layers of protection and the process control system for each initiating event.
  - Operator performs control and risk reduction tasks.
- LOPA is not well suited to complex systems.
  - Significant levels of dependent failure will violate LOPA independence assumptions.
  - Implementing and demonstrating independence of operator and operator tasks is problematic.
  - HSE has in-house human factors specialists who help determine whether independence has been implemented and demonstrated.

© Crown Copyright, HSL 2016

HSE operational guidance for engineers applied to LOPA



- This diagram represents a truly independent layer of protection.
  - What if the operator initiates the final element from another IPL.
  - What if the operator relies on the BPCS sensor and annunciator.
  - What if the operator has other demands on his/her time.
  - LOPA does not consider these 'what if's' so HSE does.
  - Each case above invalidates LOPA rules hence the IPL is not independent, hence HSE would not accept claims for credit in the LOPA.

© Crown Copyright, HSL 2016

Human reliability in LOPA

- Within a LOPA study the assessment of operator contributions to process risk and risk reduction can be performed 'offline' using established methods.
  - Human reliability assessments, e.g. HSE is keen to see qualitative task analysis used in conjunction with a human reliability estimation tool such as HEART.
  - Fault tree analysis or reliability block diagram analysis to model failure logic.
- These methods can be used to determine the error rates/probabilities for the initiating events or risk reduction measures.
- There are difficulties in how do we establish whether an operator(s) maintains their estimated initial integrity?

© Crown Copyright, HSL 2016

Human error rates/probabilities in LOPA

- For initiating events/causes in LOPA.
  - Equipment based initiating events use annual equipment failure rate.
  - Operator based initiating events use an annual operator error rate.
- For risk reduction measures (IPL).
  - Equipment based risk reduction measures use PFD_{avg}.
    - Average probability of failure on demand.
  - Operator based risk reduction measures HEP.
    - Human Error Probability .

© Crown Copyright, HSL 2016

Simplified error probability calculation used for SIL determination in LOPA

1. $PFD_{avg} = \lambda du\ (\frac{Ti}{2})$
2. $PFD_{avg}\ (operator) \approx HEP?$
   - HEP is generally considered to be the operator equivalent to PFD_{avg}.

- Where.
  - 'PFD_{avg}' is the average probability of failure on demand.
  - 'λdu' is the dangerous undetected failure rate per year.
  - 'Ti' (hours) is the proof test interval.
  - 'HEP' is the human error probability per demand.

© Crown Copyright, HSL 2016

Human reliability data quality issues

- Assumptions implicit in data quality.
  - Site and circumstance factors not accounted for, e.g. EPC/PSF .
- Optimistic claims, especially for human reliability.
  - Even historical performance data may not be enough.
- Data sources used.
  - Same process same site historical performance data.
  - Same site similar process historical performance data.
  - Same or similar process historical performance different site.
  - Predicted failure rate from human reliability estimation method such as HEART, THERP etc.
  - Generic data (unsupported published data).

© Crown Copyright, HSL 2016

Basic Process control system (BPCS) definition

- A BPCS has been defined as all arrangements required to implement basic process control (PSLG final report).
- This includes operator actions.
- Performance limits placed on the BPCS in IEC 61511.
  - The IEC 61511 performance limit for a BPCS when claimed as an initiating event is 1E-5 dangerous failures per hour.
  - When claimed as a layer of protection a risk reduction factor of less than 10 can be claimed.
  - IEC 61511 references human factors but gives little or no help in how they should be incorporated into LOPA.

© Crown Copyright, HSL 2016

Operator as a layer of protection

- The PSLG guidance defined operator crosschecks to formalise operator intervention to address LOPA requirements.
- Operator crosschecks are independent protection layers that are.
  - Designed to prevent initiating events leading to dangerous failures.
  - Independent from the BPCS and from other independent protection layers.
  - Effective in performing the stated task.
    - Be able to detect a hazard and perform an appropriate action – often claims only consider detecting the hazard,
  - Supported by auditable records of their performance,
  - IEC 61511 IPL requirements.

© Crown Copyright, HSL 2016

Buncefield examples of operator tasks assessed by LOPA

- Operator typically performs the following control tasks:
  - calculates tank ullage.
  - line up the relevant tank.
  - check that the correct tank is filling.
  - monitor the tank filling progress.
  - Switch over to next tank in filling sequence for large deliveries.
  - tank fill termination.
  - tank level control valve can be manually/electrically activated.
- Operator performs the following risk reduction tasks:
  - Regularly check tank levels
  - Responds to process alarms
  - Responds to critical alarms

© Crown Copyright, HSL 2016

Buncefield incident UK: Operator tasks before and after

- Pre Buncefield tank filling operations relied on:
  - Operator control of the process.
  - Operator risk reduction measures.
- Post Buncefield tank filling operations relied on:
  - Operator control of the process.
  - Operator risk reduction measures.
  - Electromechanical final layer of protection.

© Crown Copyright, HSL 2016

Operator error analysis problems associated with LOPA

- Only operator considered, not equipment they use.
- Data taken from sources not relevant to situation being considered.
- Task analysis rarely done, so HRA and hence HEP not supported.
- Data taken from published source without considering actual cause of error.
- Uncertainly regarding the definition of a BPCS.
  - Defined in the PSLG final report as 'All equipment and arrangements required to affect normal process control.

© Crown Copyright, HSL 2016

Assumptions about the operator

- Assumptions made about all parts of the assessment from the process, its operation, the number of persons involved.
- Assumptions can be optimistic or pessimistic and can balance out in the assessment, but this is not acceptable.
- Incorrect assumptions about operator rolls and performance are a significant source of error in a LOPA.
- Erroneous assumptions can be made because the LOPA was desk based.
  - Lack relevant information on how operator tasks are performed and what factors can affect operator.
  - The assessment team might not be representative in terms of relevant experience and expertise.

© Crown Copyright, HSL 2016

Supporting evidence for operator involvement

- Within LOPA studies submitted to HSE supporting evidence, HSE sought includes.
- Adequate description of the process
- Adequate description of operator tasks who's failure could lead to a hazardous event occurring.
- Adequate description of operator based layers of protection and other measures for which credit is claimed.
- Reference to company procedures, if present, to support expected operator tasks.
- HSE asks can the evidence be verified, to what degree can it be verified – if poorly, then it might not be acceptable.

© Crown Copyright, HSL 2016

Problems when incorporating operator actions within a LOPA

- Engineering standards such as IEC 61511 are based on the quantification of factors used to determine SIL.
  - Hence an engineers need to quantify.
- Concentrating on human reliability estimation numerically can divert focus from identifying barriers to mitigate identified human error possibilities.
- Engineers work to find ways of thinking about operator performance in a similar way to an item of equipment in terms of how their contribution to risk and risk reduction can be estimated.

© Crown Copyright, HSL 2016

Guidance on Human Factors for LOAP and SIL determination

- Process Safety Leadership Group Final (PSLG) report (HSE) – Safety and Environmental Standards for Fuel Storage Sites.
- HSE Operational Guidance. Operator Response within Safety Instrumented Systems in the Chemical, Oil & Gas, and Specialist Industries http://www.hse.gov.uk/foi/internalops/og/og-00047.htmPSLG Guidance.
- Engineering Equipment and Materials Users' Association (EEMUA) Publication '191': Alarm Systems – A Guide to Design, Management and Procurement. (ISBN 0 85931 076 0) (Edition 3).
- Contract Research Report 373/2001 – Proposed Framework for Addressing Human Factors in IEC 61508.
- IEC 62508: Guidance on Human Aspects of Dependability (currently draft).

© Crown Copyright, HSL 2016

Conclusions

- This talk has presented an engineers experience of how HSE and industry deal with some common human factors issues in LOPA and SIL determination.
- Industry attempts to find ways of accounting for operator performance and demonstrating this in LOPA studies has been problematic.
- Human reliability data and its applicability by industry has been problematic but is slowly improving.
- An approach has been to use task analysis and HRA methods such as HEART and incorporate the outcome into a LOPA analysis.
- There is guidance out there and HSE contributes to this guidance.
- We as engineers need to be more human factors aware.

© Crown Copyright, HSL 2016

Thank you for listening

HSL is the commercial arm of The Health and Safety Executive, HSE. Our commercial work delivers high quality science to meet the needs of industry and government in the UK and overseas. Our commercial customers can commission services and research using our state-of-the-art scientific laboratory in Buxton, as well as analytical expertise from other parts of HSE's science base.

© Crown Copyright, HSL 2016