The Risk of LOPA and SIL Classification in the process industry

Mary Kay O’Connor Process Safety Center
International Symposium
Beyond Regulatory Compliance, Making Safety Second Nature
October 28-29, 2008

Chris Pietersen
Safety Solutions Consultants BV
pietersen@safety-sc.com
Chris Pietersen

*Director SSC  (before : TNO SSC)*

> TU Delft, Shell (Process Control)
> 25 year in safety, TNO senior Research Fellow
> Accident investigation (e.g. Bhopal, Mexico LPG)
> Member Dutch Advisory Council for Hazardous Material
> Leader Module ‘Industrial Safety’ of official Dutch Safety Education Program

Process Safety Philosophy

- Technical:
  
  HAZOP, SIL, LOPA, QRA

- Organisational
  
  Safety Management,
  Learning from incidents

- Culture
  
  Safety Culture Assessment (SCM)
  Behaviour
International SIL Standards:

IEC 61508/ 61511: Risk Based Approach

- Evaluate the **Risk** of a (HAZOP derived) scenario
- Determine the required **Risk** reduction magnitude
  - Design or Verify the **Risk** Control Measure
  - Implement in Safety Management System
Potential Pitfalls (1)

• The quality of the HAZOP study
  – Team composition/ experience
  – As built drawings
  – Project budget/ planning
  – Inherent Safety
  – Credibility, information of LOC scenario’s for SIL/ LOPA

• The risk analysis capability of the team
  – Consequence / frequency assessment
  – (In) dependencies in causes and control measures
Potential Pitfalls (2)

• The SIL verification:
  – Functionality check
  – (In) dependencies
  – PFD calculations

• Safety management of SIL
  – Plan, Do, Check, Act approach
  – Procedures and Workinstruction
The need for a SIS

The risk of overfilling a vessel

*Examples from disasters*

- *Buncefield explosion (UK): Overfilling of storage tank* (December 2005)

- *Texas City disaster: Overfilling of distillation tower* (March 2005)

- *Mexico City LPG Disaster: Overfilling a storage sphere* (November 1984)
Overfilling Tank 912
Buncefield Depot 11 December 2005

> Filling (from pipeline) with ‘motorfuel’ (550-890 m3/hr)
> Start filling tank: 19.00 hr, overfilling/release: 5.20 hr
> Explosion: 06.01 hr

> **Automatic Overfill protection system failed (levelswitch):**
IEC 61511: Reliability of (overfill) protection system
> Main Problem: Safety Management, no risk based approach.
Explosion Texas Refinery, 23 March 2005

- **Continued overfilling** of the raffinate splitter in the isomerisation during start-up (closed outlet)

- Opening Relief valves to Blowdown drum and Loss of Containment (200 m3) via ventstack at 36 meter height.

- Explosion and fire, temporary trailers: 15 fatalities/ >170 injured persons
Texas disaster aspects

- **Inherent Safety: vent to non-safe location**
  - Proposed modification not implemented.
  - Post disaster reaction industry: SIL protection overfilling!
    - IEC 61508: always consider inherent safety first
    - Effort to be put at safe design/controlled system; remaining risk: SIL

- **HAZOP start-up not performed**
  - Common practice in industry: only continuous process
  - IEC 61508: A systematic Hazard Identification for all Life Cycle phases is required before the SIL approach is applied.
Inherent Safety Example

SIL Runaway reaction killing system
Venting to non-safe location
Texas disaster aspects (2)

• Level instrumentation bottom splitter (Texas)

  – Level transmitter voor Level Control (**not functional**).
  – Level indication (control room) via transmitter: **failed**
  – High Level Alarm (72%, 2,3 m): **normal functioning**
  – Separate, redundant, hardwired high level alarm
  – Level Sight Glass: **not functional** (dark residue)
  – **No automatic overfill protection**

  – IEC 61511 SIL Approach: SIS required
  – Operator dependence (alarms, sight glass)
  – Maintenance of safety critical equipment
Mexico City LPG depot  19 November 1984
Overfilling storage sphere
Consequences of overfilling

500 people killed

BLEVE phenomenon

- No HAZOP
- No MOC
- No Overfill protection
IEC 61508/ 61511 SIL approach

• Perform a systematic hazard identification study
  – HAZOP study

• Evaluate the risks of the identified hazards :
  – Risk matrix, Risk Graph, LOPA

• Determine the need for risk reduction :
  – Compare with acceptable Risk level

• Determine the required SIL of the SIS

• Verify the SIL for the SIS
Overfill Example

HAZOP: overfilling can lead to an explosion: 1 fatality

Liquid from Unit 100
Liquid from Recovery unit

Separator V1

Gas

Liquid

Safety Solutions Consultants BV
www.safety-sc.com
Risk reduction for overfill scenario: Result SIL 1

<table>
<thead>
<tr>
<th>Consequences ?</th>
<th>People present?</th>
<th>Escape possible?</th>
<th>Frequency of occurrence?</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td></td>
<td></td>
<td>W3 W2 W1</td>
</tr>
<tr>
<td>C2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1</th>
<th>a</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>a</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>a</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>na</td>
<td>4</td>
<td>3</td>
</tr>
</tbody>
</table>

- Team requirements
- Company Risk Policy
Proposed Overfill protection system

4 verification requirements:

- Functionality
- Independence of Control
- Architectural constraints
- Probabilistic requirement
Often limited to Probabilistic requirement

Failure frequency verification for SIL 1: PFD < 10\(^{-1}\)
(PFD=Probability of Failure on Demand)

\[
PFD_{SIS} = PFD_{Sens} + PFD_{ls} + PFD_{PLC} + PFD_{valve} + PFD_{pump}
\]

\[
PFD \approx \frac{1}{2} \lambda_{DU} \cdot T
\]

\[
\lambda = \text{failure frequency/ hr}
\]

\[
T = \text{Proof test interval}
\]
PFD calculation

Level transmitter \( \lambda_{DU} = 6,0 \cdot 10^{-7} / h \) Source: Sintef
Isolator \( \lambda_{DU} = 1,5 \cdot 10^{-7} / h \) Source: Exida
MCC relais \( \lambda_{DU} = 2,0 \cdot 10^{-7} / h \) Source: Sintef
Solenoid valve \( \lambda_{DU} = 9,0 \cdot 10^{-7} / h \) Source: Sintef
Valve+ actuator \( \lambda_{DU} = 2,1 \cdot 10^{-6} / h \) Source: Exida
PLC PFD = 5,0 \cdot 10^{-3} Source: TÜV
Prooftest interval T 4 year
Result: \( PFD_{SIS} = 7,8 \cdot 10^{-2} \)

PFD < 10^{-1}; Conclusion: SIL 1 probabilistic requirement fulfilled.

Remarks:

• Only one of the four verification requirements
• Only if failure rate field data are collected over the lifecycle
• Often narrowed to ‘calculations’
The Hitchhiker's Guide to the Galaxy
(Douglas Adams)

- Calculate The Ultimate Answer to The Great Question of Life, the Universe, and Everything.
- Answer after seven and a half million years' work:

42

- Computer: answer is correct : may be you never actually know what the question is!
LOPA aspect: IPL?

Failure level control LC-1: Failure (LOC) V7

- Design pressure V7: 10 bar
- Pressure V7 on loss of level V1: 60 bar

Causes:
- IC1: Failure of level transmitter
- IC2: Opening of manual valve HV-1

- Possible Protection Layers, IPL’s):
  - Relief valve at V7: PSV-7
  - Low level alarm of LC-1
  - Operator training/ procedure: action after alarm
LOPA results

IC1: failure LC control:
Frequency: 0.1 /yr

IC2: Operator error:
Frequency: 0.8 /yr

Is operator an IPL?

Frequency correction:
- Presence of the risk (Ptr): 1.0
- Exposure (Pp): 0.5
- Ignition (Pi): 1.0
- Vulnerability human: 1.0

Total: 0.5 * 10^-3 /yr

Failure V7 (LOC)
Total:
1.3 * 10^-3 /yr
Determining SIL with LOPA

- LOC frequency: $1,3 \times 10^{-3}$ /yr
- Consequences: 5 fatalities
- Acceptation criterium: $10^{-6}$ /yr

Required PFD of a SIS:
\[
PFD_{\text{SIS}} = \frac{10^{-6}}{1,3 \times 10^{-3}} = 0,8 \times 10^{-3}
\]
\[
(PFD_{\text{SIS}} = 10^{-6}/ 0,85 \times 10^{-3}= 1,2 \times 10^{-3} \text{ with operator IPL})
\]

Result: PFD < $10^{-3}$ \hspace{1cm} SIL 3
(Result: PFD < $10^{-2}$ \hspace{1cm} SIL 2 \hspace{1cm} with operator IPL)

Operator should generally not be seen as an IPL!
Before and after
Furnace
Explosion in furnace, 2003

- 3 people died
- HAZOP/ SIL Classification/ -verification: OK
- The Safety System was wrongly still in override during the start up of the furnace.

SIL standard not fully implemented:
Plan, Do, Check, Act in Safety Management System was lacking.
Summary/ Conclusions

- The SIL concept (including the use of LOPA) is often narrowed down to SIL Classification and PFD calculations.
- It is a danger that the SIL/LOPA approach becomes the objective in itself, instead of a means to reach high safety levels.
- The following main problem areas haven been considered:
  - The tendency to go for safety systems instead of more inherent safety
  - The quality of the HAZOP/ SIL/ LOPA team
  - The unjustified over dependency of operators in safety systems
  - The too large emphasis on PFD calculations, losing the real meaning behind it.
  - The lack of implementation of HAZOP/ SIL/ LOPA in the companies Safety Management System.

Overall:
The risk exists that our safety standards and risk analysis methods are becoming counterproductive. The effectiveness for safety should be monitored continuously.