Practical Methods for Process Safety Management

Putting Process Safety Management
“At The Heart Of Our Lives”

Canadian Chemical Engineering Conference 2006

Sherbrooke, Quebec, Canada
October 18, 2006
“Concern for man himself and his safety must always form the chief interest of all technical endeavors. Never forget this in the midst of your diagrams and equations”

~Albert Einstein

Quote taken from “Five Past Midnight in Bhopal”
Agenda

- Introduction
- Standard Overview
- Defining Risk and Risk Reduction
  - Determining if an SIS is required
- Proof Testing
  - Long Term Maintenance
- Discussion/Questions
Sam Kozma, C.E.T., CFSE
Certified Functional Safety Expert

- Certified Functional Safety Expert (CFSE) with TÜV Accreditation
- Instrument and Controls for over 18 years, specializing in SIS, SIL & IEC/ISA
- Experience with many systems including Siemens, HIMA, and Honeywell
- Member:
  - Task Force on Functional Safety
  - Canadian National Committee (IEC/SC 65A)
What are the IEC/ISA Standards?

- A performance based project execution method
  - Uses a “Lifecycle” from “cradle to grave”
  - Sets targets based on your own risk tolerances
  - Quantitative analysis to measure success
  - Non-prescriptive - Tailor to your own specific needs

- Primary objectives to protect humans and the environment
  - Also Successful in Asset Protection, Corporate Image, etc.
What are the IEC/ISA Standards?

- Developed to help prevent incidents
  - Flixborough
  - Seveso
  - Bhopal
  - Texas City
How Many Standards Are There?

IEC 61508

IEC 61513 Nuclear

IEC 62061 Machine Safety

IEC 61511 Process Industry

ISA 84 Process Industry
Where Does it all Start?

- Management
  - Top down approach:
    - Management support
    - Procedures and policies shall reflect the implementation on all projects
    - Develop a Safety Management Plan
Primary Objective

- Inherently Safer Designs

A good design process will use a Safety Instrumented System (SIS) as a last resort to lower the likelihood of an occurrence.
Agenda

- Introduction
- Standard Overview
- Defining Risk and Risk Reduction
  - Determining if an SIS is required
- Proof Testing
  - Long Term Maintenance
- Discussion/Questions
IEC PSM Lifecycle

Stage 1 - SRS Assessment

Stage 2 - SIS Validation

Stage 3 - PSSR - Required

Stage 4 - Regular Periodic Assessment

Stage 5 - Validate Modification

Conceptual Design & Overall Scope Definition

Process Hazard Assessment

SIL Determination & Assessment

Safety Requirements Specification

Stage 1 SRS Assessment

External Risk Reduction: Protection/Mitigation

Other Safety Related Systems

Overall Planning

Installation & Commissioning Planning

Safety Validation Planning

Operations & Maintenance Planning

ANALYSIS PHASE

REALIZATION PHASE

OPERATIONAL PHASE
Application

Process Example
- High Pressure Hazard
- Undersized Flare

CSChE Conference 2006
Sherbrooke, Quebec, Canada
PHA (HAZOP)

- Potential Failure: PIC-100
- Result: Overpressure, possible explosion and fire, toxic gas release
- Recommendation: Review vessel design, independent alarms, SIL analysis

### Inlet Area Node: Inlet Separator

<table>
<thead>
<tr>
<th>Dev.</th>
<th>Cause</th>
<th>Consequence</th>
<th>Safeguards</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>More Pressure</td>
<td>- Increasing pressure will cause stress on Inlet Sep., causing rupture, explosion and resulting fire. - Risk to personnel. - Risk to Environment (Toxic Gas)</td>
<td>Pressure Relief Valve on Inlet Sep.</td>
<td>- Review vessel design. - Investigate possible independent alarms. - Conduct SIL analysis to determine if HIPPS is required.</td>
</tr>
</tbody>
</table>

| 1.2.1 | Failure of Inlet Pressure Controller PIC-100 | - Increasing pressure will cause stress on Inlet Sep., causing rupture, explosion and resulting fire. - Risk to personnel. - Risk to Environment (Toxic Gas) | Pressure Relief Valve on Inlet Sep. | - Review vessel design. - Investigate possible independent alarms. - Conduct SIL analysis to determine if HIPPS is required. |
What is SIL?

- **SIL - Safety Integrity Level**

IEC 61511 Defines SIL as follows:

- Discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the SIS. Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest.
What Does That Mean?

- Determine **risk** and measure it against your risk tolerance.
- **Risk:**
  - the measure of the **consequence** and **frequency** of an unwanted incident.
- The gap is the **intolerable risk**.
- Apply Layers of Protection to reduce the exposure to risk.
- Remaining gap requires an SIS.
Risk

The measure of the consequence and frequency of an unwanted incident

$= \text{RISK}$
Reducing The Gap

- Tolerable Risk
- Protective Layers
  - Design
  - Relief Valves
  - Procedures
- Mitigation
  - Fire and Gas Systems
  - Evacuation Procedures
- Safety Instrumented Systems
Layers Of Protection

- PROCESS
- BPCS
- MECHANICAL PROTECTION SYSTEMS
- MECHANICAL MITIGATION SYSTEMS
- SAFETY INSTRUMENTED MITIGATION SYSTEMS
- OPERATING PROCEDURES
- PROCESS ALARMS
- PROCESS ALARMS WITH EXECUTIVE ACTION
- OPERATOR SUPERVISION
- OPERATOR INTERVENTION
- SAFETY INSTRUMENTED PROTECTION SYSTEMS
- FIRE AND GAS SYSTEMS
- COMMUNITY EMERGENCY RESPONSE
- PLANT EMERGENCY RESPONSE
Application

Process Example
- High Integrity Pressure Protection System (HIPPS)
Agenda

- Introduction
- Standard Overview
- Defining Risk and Risk Reduction
  - Determining if an SIS is required
- Proof Testing
  - Long Term Maintenance
- Discussion/Questions
Proof Testing

- Testing and maintaining an SIS is critical to meeting risk reduction targets throughout the entire lifecycle.

- Impact of Testing on SIL
  - Probability of Failure on Demand (PFD) increases over time without functional proof testing and can result in a declining SIL rating of your SIF thus leaving the process at risk.
Impact of Testing on SIL

- SIL 2 Device
- 80% Test coverage
- Yearly Test Interval
- 10 Year Mission Time

LEGEND
- PFD without Proof Testing
- PFDavg without Proof Testing
- PFD with Yearly Test Interval
- PFDavg with yearly Test Interval

PFDavg (w/Testing) = 0.007
RRF = 143

PFDavg (No Testing) = 0.02
RRF = 50

PFDavg (w/Testing) = 0.007
RRF = 143

PFDavg (No Testing) = 0.02
RRF = 50
Maintenance

- Breakdown vs. Preventative
- Follow manufacturer’s recommendations
- Procedures and intervals should be included in the Safety Requirements Specification (SRS)
- Replace/refurbish to “as new” condition before “wear-out”
- Audit to measure if goals are being met
- Regular PHA (HAZOP, FMEA, etc.)
Thank you!

Questions

Contact Information:
Sam Kozma, C.E.T., CFSE
Phone: (403) 333-8118
Fax: (403 637-2870
Email: sam.kozma@spectraldesign.ca
Website: www.spectraldesign.ca