Evolution of HIPS & Using Risk Analysis Tools to Define SIL
(Prevention First 2012)

Steven T. Maher, PE CSP

Risk Management Professionals
www.RMPCorp.com
Key Topics

• Evolution of Offshore Facility SMS Regulatory Requirements
• Hazards Analysis SEMS Requirements
• Key Design Guidelines
• Offshore Facility Protection Systems Evolution & Interface with Other SMS & Analysis Techniques
• References & Resources
• Questions
Evolution of Offshore Facility SMS Regulatory Requirements
How Did We Get Here?
Observations from Major Incidents

Safety Management Systems Concepts

• Major Accidents have Caused Significant Loss of Life and Property, as well as Significant Indirect Costs, e.g.:
  – Business Interruption
  – Lost Confidence and Contracts
  – Increased Regulation

• Typical Characteristics of Major Accidents:
  – Relatively-Simple Precursors & Initiating Events
  – Root Causes – Failure to Maintain Design Intent (first line of defense)

• MOST EFFECTIVE MECHANISM FOR IMPROVEMENT – Not by Addressing Specific Actions, but by Effecting Changes in the Way Business is Done (i.e., SAFETY CULTURE & “MANAGEMENT SYSTEMS”)
Evolution of SMS Guidelines & Regulations to Performance (Goal) – Based Standards

Onshore Process Safety (USA)
- 1987 – CCPS
- 1990 – API RP 750
- 1992 – PSM
- 1996 – RMP

Offshore Safety Management Systems (USA)
- 1989 – PSSDS
- 1991 – SEMP Concept
- 1993 – API RP 75
- 2004 – API RP 75
- 2006 – SEMS Concept
- 2009 – SEMS Prop. Rule
- 2010 – SEMS Final Rule

Offshore Safety Management Systems (UK)
- 1992 – UK Safety Case
- 2005 – UK SC Update
- 2009 – MODU HSE Case
SEMS Elements

- General Provisions
- Safety & Environmental Information
- Hazards Analysis
- Management of Change
- Operating Procedures
- Safe Work Practices
- Training
- Mechanical Integrity
- Pre-Startup Review
- Emergency Response & Control
- Investigation of Incidents
- Audit of SEMS Elements
- Records & Documentation
- Employee Participation
- Contractor Safety
Hazards Analysis
SEMS Requirements
§250.1911 General Clarifications

- Offshore Facility Definition
  - All Types of Offshore Structures Permanently or Temporarily Attached to the Seabed (i.e., Mobile Offshore Drilling Units; Floating Production Systems; Floating Production, Storage and Offloading Facilities; Tension-leg Platforms; and Spars)
  - DOI-Regulated Pipelines

- Two Types of HA Requirements
  - Facility-Level Hazards Analysis
  - Job Safety Analysis (operations/task level)
§250.1911 General Clarifications

- Analysis & documentation must be maintained for the life of the operation of the facility.
- Applicability to similar systems/processes is allowable.
- HA must be completed by 15Nov11.
- HA must be periodically updated and at the same time as compliance audit performance – At 3-year Intervals Starting on the Second Year After Initial SEMS Program Completion
- JSA must be completed/approved “prior to the commencement of the work.”
Facility-Level HA Techniques

• §250.1911(a) “... must be appropriate to the complexity of the operation and must identify, evaluate, and manage the hazards involved in the operation.”

• API RP 14J identifies the following methods as acceptable:
  – What-If
  – Checklist
  – Hazard and Operability (HAZOP) Study
  – Failure Modes and Effects Analysis (FMEA)
  – Fault Tree Analysis
  – An Appropriate Equivalent Methodology

Effective applications capitalize on the unique characteristics of these methods.
Facility-Level HA Techniques

• The HA shall address:
  – Hazards of the process/operation
  – Previous incidents
  – Engineering and administrative controls
  – Qualitative evaluation of consequences (safety/health, human/marine environments, equipment) of failure of controls
  – Human factors (also addressed via JSA)

• System to promptly address Team findings & recommendations

• Other Objectives – QUALITY
Facility-Level HA Team

• The Team must be made up of representatives from:
  – Engineering
  – Operations
  – Other specialties, as needed

• and must include:
  – Person with experience & knowledge specific to the process being evaluated
  – Person with experience & knowledge in the HA methodology
Key Design Guidelines
API RP 14C/14J Overview

- Representative Safety System Designs
  - Component Configurations
  - Process Flow Diagrams
  - P&IDs
  - Alarm Features
  - Associated Safety Analysis Checklist
- **Safety Analysis Methods & Development of SAFE Charts**

- **API RP 14J** – “Design and Hazards Analysis for Offshore Production Facilities”
- Details for Support of Two Critical SEMP Elements
  - Safety & Environmental Information
  - Hazard Analysis
- Identification of Good Design Practices
- Primary Applicability – Offshore Production Facilities and Production Processing Systems of Mobile Offshore Units
IEC 61508/61511 Overview

- **IEC 61508** – “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems”
  - Provides a Risk-Framework for the Identification of Hazards
  - Risk Analysis Using the “Familiar” Likelihood/Severity/Risk-Ranking
  - Defines Safety Integrity Level

  - Focus on Safety Instrumented Systems (SIS)
    - Electrical, Electronic, and Programmable Electronic Equipment
    - Electronic Logic Solvers
    - Also Addresses Pneumatic or Hydraulic Systems to Manipulate Final Elements
  - Primary Applicability – Process Industries
  - Key Elements
    - Requirements
    - Application Guidelines
    - SIL Determination
  - Stresses the Importance of a Management System
Offshore Facility Protection Systems Evolution & Interface with Other SMS and Analysis Techniques
Focusing on the Objective
(The “Big Picture”)

- **RISK** = PROBABILITY * CONSEQUENCES
  - Probability = Likelihood of Occurrence
  - Consequences = Effects of Occurrence
- For Engineered Systems:
  - Risk = \( \Sigma P_i \times C_i \)
### Risk/SIL Ranking

<table>
<thead>
<tr>
<th>Frequency (1/yr)</th>
<th>Severity</th>
<th>Level 1 Risk (first priority)</th>
<th>Level 2 Risk (tolerable if ALARP)</th>
<th>Level 3 Risk (acceptable)</th>
<th>Level 4 Risk (target w/o SIS)</th>
<th>Level 5 Risk (start w/ SIS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Likely (&gt; 10^{-2})</td>
<td>Moderate (E)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(2) Unlikely (10^{-2}–10^{-3})</td>
<td>Serious (D)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(3) Very Unlikely (10^{-3}–10^{-4})</td>
<td>Major (C)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(4) Extr. Unlikely (10^{-4}–10^{-5})</td>
<td>Catastrophic (B)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(5) Remote (&lt; 10^{-5})</td>
<td>Disastrous (A)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Severity:**

- E: Moderate
- D: Serious
- C: Major
- B: Catastrophic
- A: Disastrous

**Note:** Risk/SIL Ranking bases typically come from operating company.
Tandem Advances in Protection System Design Architectures & Analysis

Protection System Design Evolution

1986 - API RP 14C
1996 - ANSI/ISA S84.01
1999 - IEC 61508-1
2004 - IEC 61511-1
2004 - ANSI/ISA S84.00.01

Reliability Criteria & Design Architecture Specifications

<table>
<thead>
<tr>
<th>SIL-1</th>
<th>SIL-2</th>
<th>SIL-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>(10^{-2} \leq \text{PFD}_{\text{AVG}} &lt; 10^{-1})</td>
<td>(10^{-3} \leq \text{PFD}_{\text{AVG}} &lt; 10^{-2})</td>
<td>(10^{-4} \leq \text{PFD}_{\text{AVG}} &lt; 10^{-3})</td>
</tr>
</tbody>
</table>

Safety Integrity Levels
Control/Protection System

Spectrum – BPCS & SIS/HIPS

Increasing Reliability & Larger SIL (SIS-Only, ANSI/ISA-S84.01 & ANSI/ISA-S84.00.01)

- Smart Sensors
- Redundancy
- Voting Logic
- Electronic Sensing & Sig. Processing
- Diversity
- Separation of Control & Protection
- High Pedigree Devices
- End Device Feedback Loops
- Single-Element Analog Devices
- Decreased Cost
- Increased Redundancy, Diversity, Pedigree

BPCS = Basic Process Control System, SIS = Safety Instrumented System, HIPS = High Integrity Protection System
Safety Instrumented Systems (SIS)

• Concept
  – Diversity
  – Redundancy
  – Separation

• Objectives
  – Highly reliable safety features should have a low Probability of Failure on Demand (PFD)
  – Ensure that the likelihood of high/medium consequence events have an acceptably low risk contribution.

• Design Guidelines
  – 1996 - ANSI/ISA S84.01 (United States)
  – 2004 - ANSI/ISA S84.00.01 (United States)
  – 1999 - IEC 61508-1 (International)
  – 2004 - IEC 61511-1 (International)

• Safety Integrity Level (SIL) – Measure of SIS reliability
Layer of Protection Analysis (LOPA)

- LOPA was created as a bridge between a detailed QRA and HAZOP.

  - Increased Complexity
  - Increased Insights
  - HAZOP
  - LOPA
  - QRA

- LOPA uses relatively standard initiating cause frequencies and independent protection layer PFDs to keep the analysis simple, but to yield quantitative results.
LOPA Ratio Calculation

- LOPA is a subset of the QRA Framework; however, it has its own set of acronyms and terminology to focus the analysis:
  - IC – Initiating Cause (i.e., Initiating Event)
  - ICL – Initiating Cause Likelihood (Frequency)
  - IPL – Independent Protection Layer
  - PFD – Probability of Failure on Demand
  - TF – Target Frequency
  - VF – Vulnerability Factor – Conditional Modifiers

\[
LOPA \text{ Ratio (Safety)} = \frac{TF_{Safety}}{ICL \times PFD_1 \times PFD_2 \times PFD_3 ... \times VFi \times VFp}
\]
## Using LOPA Results

- Calculated LOPA Ratio is the primary decision-making basis.
  - To meet safety targets, if no SIS features exist, adjust BPCS to increase the LOPA Ratio to be $\geq 1$ or add SIS feature.
  - To determine SIS pedigree, safety targets may be achieved by assigning SIL Allocation Target (see previous SIL Matrix).
  - Related integrity levels for environmental (EIL) and commercial (CIL) issues can be defined.

<table>
<thead>
<tr>
<th>LOPA Ratio (w/o SIS)</th>
<th>SIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^{-0} - 10^{-1}$</td>
<td>No special integrity requirements</td>
</tr>
<tr>
<td>$10^{-1} - 10^{-2}$</td>
<td>SIL 1</td>
</tr>
<tr>
<td>$10^{-2} - 10^{-3}$</td>
<td>SIL 2</td>
</tr>
<tr>
<td>$10^{-3} - 10^{-4}$</td>
<td>SIL 3</td>
</tr>
</tbody>
</table>
LOPA Summary

• LOPA utilizes a simplified quantification process to:
  – Determine if risk targets are met (e.g., acceptability of high-risk scenarios.
  – Determine adequacy of BPCS and SIS/HIPS protection features.
  – Compare the benefit-cost associated with improvements.
  – Identify if risk targets can be achieved with BPCS rather than SIS/HIPS.
  – Determine SIL Allocation Target for SIS/HIPS features.

• Implementation
  – Initial LOPA during HAZOP Study can reinforce SIL.
  – More-detailed LOPA can provide a more formal basis for scenario risk and needed SIS/HIPS SIL.
Simple SIS/LOPA Example

2-50% capacity relief valves exist on downstream LP vessel.
## LOPA Ratio Calculation Details

<table>
<thead>
<tr>
<th>IC</th>
<th>Chain of Events (Consequences)</th>
<th>IPL 1</th>
<th>IPL 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>LV-1 malfunctions open, possibly due to a failure of LT/LIC-1, or bypass valve inadvertently open.</td>
<td>Gas blow-by resulting in overpressurization of downstream equipment and resultant release of hydrocarbons and H2S, Potential for severe injury or fatality.</td>
<td>LAL-1, if LT/LIC-1 is not the cause of the malfunction.</td>
<td>2-50% capacity relief valves on downstream LP vessel</td>
</tr>
<tr>
<td>0.1/yr</td>
<td>----</td>
<td>2*0.01/demand</td>
<td></td>
</tr>
</tbody>
</table>

Scenario Frequency = 0.1/yr * 2*0.01/demand  
Vulnerability Factor = 0.5 (People are present in the hazard zone for less than 12 hours/day.)  
Target Frequency = $1 \times 10^{-5}$/yr

**Departure From Target (LOPA Ratio) = 0.01**

**Conclusions:** Need a factor of 100 improvement in safeguard reliability, e.g.:
- Installing a separate emergency isolation valve fed by an independent level transmitter (if SIS, SIL 2 target)
- Reconfiguring LV-1 to include a separate SIS closure feature (SIL 2)
Overlap Between Key Risk Analysis Tools

- **QRA**
- **Bow-tie**
- **SIL**
- **HA** (HAZOP, "What-If?", FTA, FMECA, HAZID)
- **LOPA**
Interdependency of Design, Analysis, and Standards
What-If/Checklist | Checklist
---|---
JSA | What-If/Checklist
API RP 14C Review | FMECA
HAZID | HAZOP

Each of these tools provides a different perspective & different insights.

Less Effort | Increased Effort, with Increased Insights

Hazards Analysis Tool Spectrum

Allows Risk Quantification

- Bow-tie
- LOPA
- ETA
- FTA
References & Resources
Recent Webinars in Offshore Facility Process Safety Series

- **July 22, 2010** – Offshore Facility Process Safety Overview (Risk Management Professionals + Guest Speaker, Mark Steinhilber)
- **September 14, 2010** – Effective Creation & Appropriate Application of Safety Cases (Risk Management Professionals + Guest Speaker, Ian Sutton)
- **October 14, 2010** – Offshore Facility Process Safety Systems Overview (SEMS – A New Paradigm)
- **November 18, 2010** – SEMS Update and HAZOP Study, LOPA, & SIL Assessment Integration Made Easy
- **December 14, 2010** – Practical SEMS Mechanical Integrity (MI) Program Implementation
- **January 12, 2011** – SEMS Update, Hazards Analysis Basics, and Practical Approaches
- **March 3, 2011** – Safety & Environmental Information Tips (Including Quality P&IDs)
- **March 8, 2011** – Paradigm Shift in the Regulatory Application of SMS
Recent Webinars in Offshore Facility Process Safety Series

- **May 5, 2011** – Sensible Operating Procedures for Offshore Facilities
- **June 2, 2011** – Application of Bow-tie Analysis to Offshore Facilities
- **June 7, 2011** – Practical Approaches to Implementing Management of Change and Pre-Startup Reviews for Offshore Facilities
- **July 21, 2011** – SEMS Program Elements, Audit Requirements, Practical Approaches, Gap Analysis, and Audit Tips
- **October 18, 2011** – SEMS Program Elements, Hazards Analysis Basics, and Practical Approaches
- **October 27, 2011** – Practical SEMS Mechanical Integrity (MI) Program Implementation
- **December 8, 2011** - Practical SEMS Implementation, Auditing Techniques and Gap Analysis
- **June 12, 2012** – Contractors and Operations - The SEMS Rule
- **September 6, 2012** – Paradigm Shift in the Regulatory Application of SMS to Offshore Facilities
Other Resources

- [www.BSEE.gov](http://www.BSEE.gov) – Bureau of Safety and Environmental Enforcement
- [www.RMPCorp.com](http://www.RMPCorp.com) – RMP Home Site with Offshore Facility SEMS Series & Other Training Tracts
- [www.SEMS-Solution.com](http://www.SEMS-Solution.com) – Broad-Spectrum SEMS-compliance Software System
- [www.oilspillcommission.gov](http://www.oilspillcommission.gov) – National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling
- [www.API.org](http://www.API.org) – American Petroleum Institute Publications & Recommended Practices
Questions?

Steven T. Maher, PE CSP

Steve.Maher@RMPCorp.com

877/532-0806
www.RMPCorp.com