2013 STAMP Conference
MIT Partnership for a Systems Approach to Safety

“Evaluating Project Safety (System Engineering and Safety Management) in an Organization”

Lorena Pelegrín
27/03/2013
### Table of Contents

- Background
- Project Outline
- Initial Status Review
- Evaluation
- Lessons
- Outlook
- More Information
Evaluating Project Safety (System Engineering and Safety Management) in an Organization

Background

- Engineering and Consulting Group in Oil & Gas, Water & Environment, Energy & Climate Protection, and Transport & Structures
- ILF Munich leads Oil & Gas Business segment (highest turnover in ILF Group)
- Process facilities (Upstream, Midstream, Downstream, Onshore, Offshore). Core field cross-country Pipeline Systems
- Project and client driven. Different approaches. Not consolidated
- Major incidents continue to happen in the O&G industry, a fundamental change is needed. Oil & Gas industry resistant to change?
Evaluating Project Safety (System Engineering and Safety Management) in an Organization

Project Outline

- Master Thesis supervised by Prof. Leveson
- Perform Initial Status Review
  - Learn about current practice
- Perform analysis of STAMP steps in terms of
  - Current practice
  - Feasibility of step implementation
  - Development of STAMP step for a project example
  - Definition of high-level guidelines for implementation of step
- Define a strategy for implementation of STAMP into the system engineering process
Evaluating Project Safety (System Engineering and Safety Management) in an Organization

Initial Status Review (1/7)

Scope

- Elements of System Safety Engineering
- Project Phases as in O&G Industry
- Levels of Intent Specification
- Elements of Using STAMP
- Related Chapters of “Engineering a Safer World”
Scope: Elements of System Safety Engineering

Management
- Leadership
- Culture
- Behavior
- Safety Control Structure
- Responsibility, Accountability, Authority
- Controls
- Feedback Channels
- Continual Improvement

Engineering Development
- Hazards
- Safety Requirements/Constraints
- Design Rational, Assumptions
- Physical Usage
- Operational Environment
- Human Task Analysis
- System Operations Analysis
- Hazard Analysis and Safety-Guided Design
- Design Decisions
- Hazard Analysis

Operations
- Safety Constraints, Operating Requirements, and Assumptions
- Problems, Experience Investigation Reports

2013 STAMP Conference. MIT Partnership for a Systems Approach to Safety
Leveson (2012)
Evaluating Project Safety (System Engineering and Safety Management) in an Organization

Initial Status Review (3/7)

**Scope: Project Phases**

![Operating Asset Life Cycle Diagram](image)

- **Appraise**
  - Opportunity value identification
  - Feasibility Package preparation
  - Project framing
- **Select**
  - Opportunity framing
  - Conceptual Design Package preparation
  - Project strategy planning
- **Define**
  - Opportunity & venture definition
  - Permit engineering
  - Environmental, Social Impact Assessment
  - Basic Design Package preparation
  - Tendering
  - Project execution planning
- **Execute**
  - Opportunity realization
  - Procurement & contracting
  - Detail, construction & vendor design
  - Construction
  - Commissioning & trial operation
  - Project execution management
- **Operate**
  - Business control
  - Operation
  - Dismantling
  - Optimization
  - Rehabilitation
  - Modification
  - Project contracts close out
Scope: Levels of an Intent Specification

Leveson (2012)
Evaluating Project Safety (System Engineering and Safety Management) in an Organization

Initial Status Review (5/7)

**Scope: Elements of Using STAMP**

- Establishing the Goals of the System
- Defining Accidents
- Identifying System Hazards
- Integrating Safety into Architecture Selection and System Trade Studies
- Documenting Environmental Assumptions
- Generating System-Level Requirements
- Identifying High-Level Design and Safety Constraints
- Performing System Design and Analysis
- Documenting System Limitations
- Considering relevant Operations Experience in the Development
- Delivering Safety Requirements and Constraints to Operations
- Providing Leadership for Safety Matters
- Implementing a Safety Policy
- Implementing a Safety Management Plan
- Implementing a Safety Control Structure
- Implementing a Safety Information System
### Example

<table>
<thead>
<tr>
<th>Element of Engineering Systems</th>
<th>Project Phase (Oil &amp; Gas Terminology)</th>
<th>Intent Spec Level</th>
<th>Element of Using STAMP</th>
<th>Chapter of Engineering a Safer World</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>All</td>
<td>Level 0</td>
<td>Implementing a safety control structure</td>
<td>13.2.6</td>
<td>Is there a group responsible for safety in the projects?</td>
</tr>
<tr>
<td>Development</td>
<td>Functional Design, Basic Design “Define”</td>
<td>Level 1</td>
<td>Generating system-level requirements</td>
<td>10.3.6</td>
<td>Are system-level requirements traceable back to the system goals and/or hazard analysis from where they have been generated?</td>
</tr>
</tbody>
</table>
Review questions adapted to the terminology of O&G industry
Approx. 100 questions categorized
No especial preparation required by participants (Project Managers and Business Unit Directors)
Interviews format
No audit atmosphere, open discussions
Evaluating Project Safety (System Engineering and Safety Management) in an Organization

Evaluation

- Safety Policy seems an Occupational H&S Policy, rather than a policy for designing for safety
- Gap between high-level Safety Policy and Safety Engineering Practice
- Safety Engineering practice driven by client requirements
- HAZID and HAZOP most useful traditional techniques, QRA and SIL quantitative frame aids in decision making
- Managers wish a more proactive approach to Safety Engineering, changing designs after hazards analysis is inconvenient
Evaluating Project Safety (System Engineering and Safety Management) in an Organization

Lessons (1/2)

- STAMP framework provides a comprehensive, detailed and useful frame for evaluating how an organization designs for safety.
- Most of standards available for Safety Management Systems are (i) too general and (ii) not specific to designing for safety, but to Occupational H&S.
- STAMP framework (and the checklist developed in this Project) cannot be used without training.
- STAMP framework and specially Intent Specification Approach useful for improvement and standardization of design philosophies (requirements).
Implementation of complete STAMP framework resource demanding, but less resource demanding measures based on STAMP principles can be implemented little by little and still drive improvement.

STPA powerful tool for generating comprehensive and precise requirements.

Inclusion of STPA elements into traditional techniques such as HAZOP (STPA control flaws as part of CHAZOP?)

STAMP framework aids in solving „old“ engineering management problems (traceability, interface management, documentation of assumptions and limitations, etc.)
Evaluating Project Safety (System Engineering and Safety Management) in an Organization

Outlook (1/2)

- Implementation of Thesis Recommendations
- „ILF Guideline for Safety in Design in O&G Developments“
- Hazards Analyses Recommended Practices considering STPA elements
- „ILF Guideline for Project Risk Management“ based on STAMP framework
Evaluating Project Safety (System Engineering and Safety Management) in an Organization

Outlook (2/2)

- TANAP Trans Anatolia Natural Gas Pipeline

2013 STAMP Conference. MIT Partnership for a Systems Approach to Safety
Evaluating Project Safety (System Engineering and Safety Management) in an Organization

MIT Partnership for a Systems Approach to Safety

- Papers, Masters Theses and Ph.D. Dissertations
  
  http://psas.scripts.mit.edu/home/theses-and-dissertations/

Contact

Lorena Pelegrín, MSc. MSc.
Head of Safety Engineering
Process and Safety Engineering Department
ILF Consulting Engineers
Werner-Eckert-Str. 7
81829 Munich / Germany

Lorena.Pelegrin@ilf.com
+49 (0) 176-171-174-24