Risk Analysis in Design and Construction of a Hydropower Station

Svana Helen Björnsdóttir, PhD candidate
4th European STAMP Workshop
INTRODUCTION
Aim of Research

• Seek a generic risk analysis methodology that can be used in different disciplines

• Case Study: Hydropower project – one of six
  – Examine currently used risk analysis methodology
  – Apply STAMP/STPA to investigate whether it can be used as a basis for a generic risk analysis methodology
  – Evaluate and compare
Definition of Risk Analysis in ISO 31000 Risk Management Standard
Main Research Question

What is a generic risk analysis methodology that can be applied in different disciplines?
Research Sub-Questions

• What is a risk analysis methodology?
• What are the commonalities of risk analysis methodologies in different disciplines?
• What are the requirements for a generic risk analysis methodology?
• Can STAMP/STPA fulfill these requirements?
National Power Company

- Owned by the state
- Operates 15 power stations in Iceland
- Emphasis on operations in harmony with environment and society
- One of the largest producers of renewable energy in Europe
- Case Study: Latest Hydro Electro Project (HEP) Búðarháls, built in 2010-2014
Búðarháls HEP 2010-2014
Búðarháls HEP 2010-2014
Current Risk Analysis

- Company own approach
- Written risk assessment procedure
- Bottom-up approach
- Project driven as a part of project management
- Contractors provide own risk information
- Risk information gathered & risk register created
- Focus on avoiding threats and preventing failure
RESEARCH METHOD
Research Method

- Written contract signed by CEO in 2014 – ISO27001 req.
- Questionnaire with 49 questions reg. risk issues
- Answers received
- 6 semi-structured follow-up interviews 1-2 hours long
  - Interview with project risk manager and head of risk mgmt.
  - According to ISO19011 audit standard
  - Data collected, documents received
  - Search for evidence, e.g. processes, procedures, definitions
- Documents reviewed
- Partly conducted as a master’s thesis at Reykjavik University in 2015-2016
APPLICATION OF STAMP/STPA
Why STAMP/STPA?

• Current risk methodology does not capture risk in a holistic way
• Company policy to seek continuous improvements in risk management
• Improve decision making process
• To get a different perspective on risk than currently exists
• Systems approach to risk identification and risk analysis is needed
Project Goals in the HEP

• Project goal is to complete and deliver a hydropower station:
  – In time for planned operation and energy sales
  – In compliance with law, regulations, contracts and standards
  – Without exceeding the approved budget plan
  – For safe operation and delivery of sufficient power
Accidents/Unacceptable Losses

A1: Loss of human lives
A1: Financial loss (overrun of budget or project delay)
A3: Unsafe usage of equipment and other resources
A4: Power plant does not deliver sufficient power
A5: Breach of laws, regulations, contracts, standards
A6: Loss of public policy support
A7: Loss of safety/security/quality when outsourcing
Dotted lines indicate flaws in HCS
Main Hazards and Threats

Three main hazards and threats:

H1: Project not finished in time for operation to start
H2: Injury or loss of human lives
H3: Overrun of budget plan
System-Level Safety Constraints

- Management team must establish a control structure to manage project and project risk
- People working on construction site must not be injured
- Measure must be taken to reduce likelihood of accidents on construction site
- Means must be available and effective to treat risk on site
- Project risk manager must review and monitor risk in project plans
- Operational Management must be involved early enough to supervise and validate system requirements
Control Actions

• Two cases of Control Actions investigated:
  – Involvement of operation in design and development of HEP
  – Involvement of risk manager (or risk management team) in HEP – investigated by a master’s student at Reykjavik University, see workshop poster
Example 1 of UCA

Control Action: Involvement of operation in design and development of HEP

<table>
<thead>
<tr>
<th>Not Providing Causes Hazard</th>
<th>Providing Causes Hazard</th>
<th>Wrong Timing or Order Causes Hazard</th>
<th>Stopped Too Soon or Applied Too Long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation is <strong>not</strong> involved, thus not providing necessary input and information (H1,H2,H3).</td>
<td>If operation is involved but <strong>recommendations are incorrect</strong>, this can cause hazard (H1,H2,H3).</td>
<td>Early involvement provides no hazard. <strong>Late</strong> involvement can cause hazard (H1,H2,H3).</td>
<td>If operation involvement <strong>stops too soon</strong>, this can cause hazard (H1,H2,H3). Too long: No hazard.</td>
</tr>
<tr>
<td>Operation is <strong>not</strong> involved, thus not providing necessary input and information (H1,H2,H3).</td>
<td>If operation is involved but <strong>recommendations are ignored</strong>, this can cause hazard (H1,H2,H3).</td>
<td>Early involvement provides no hazard. <strong>Late</strong> involvement can cause hazard (H1,H2,H3).</td>
<td>If operation involvement <strong>stops too soon</strong>, this can cause hazard (H1,H2,H3). Too long: No hazard.</td>
</tr>
</tbody>
</table>
## Example 2 of UCA

Control Action: Involvement of risk manager (or risk management team) in HEP

<table>
<thead>
<tr>
<th>Not Providing Causes Hazard</th>
<th>Providing Causes Hazard</th>
<th>Wrong Timing or Order Causes Hazard</th>
<th>Stopped Too Soon or Applied Too Long</th>
</tr>
</thead>
<tbody>
<tr>
<td>If risk manager is <strong>not involved in design and development</strong> of project, this may cause hazards (H1,H2,H3).</td>
<td>If risk manager is involved but his work is <strong>ineffective</strong> (incorrect or insufficient), this may cause hazard (H1,H2,H3).</td>
<td>Early involvement causes no hazards. <strong>Late</strong> involvement may cause hazards (H1,H2,H3).</td>
<td>If <strong>stopped to soon</strong> may cause hazard (H1,H2,H3). Applied too long causes no hazard.</td>
</tr>
<tr>
<td>If risk manager is <strong>not involved in construction phase on site</strong>, this can cause hazard (H1,H2,H3).</td>
<td>If risk manager is involved but his work is <strong>ineffective</strong> (incorrect or insufficient) this may cause hazard (H1,H2,H3).</td>
<td>Early involvement causes no hazards. <strong>Late</strong> involvement may cause hazards (H1,H2,H3).</td>
<td>If <strong>stopped to soon</strong> may cause hazard (H1,H2,H3). Applied too long causes no hazard.</td>
</tr>
</tbody>
</table>
Identifying Causal Scenarios in Ex.1
# Examples of Potential Causes of UCA

<table>
<thead>
<tr>
<th>No.</th>
<th>Potential Causes of Hazards and Threats to a HEP Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a</td>
<td>Management Team does not allocate enough resources from Operation</td>
</tr>
<tr>
<td>1b</td>
<td>The involvement of Operation is incorrectly scheduled by Head of Operation</td>
</tr>
<tr>
<td>2a</td>
<td>Incorrect understanding of project scope, project plans and procedures</td>
</tr>
<tr>
<td>2b</td>
<td>Estimation of Operations man-hours is incorrect, more resources is required in the project</td>
</tr>
<tr>
<td>2c</td>
<td>Required competence of Operations staff in the project is underestimated or incorrect</td>
</tr>
<tr>
<td>3</td>
<td>Operations staff get their instructions too late when alignment with contractors need to start</td>
</tr>
<tr>
<td>4a</td>
<td>Operations staff is not available when required start of working with contractors</td>
</tr>
<tr>
<td>4b</td>
<td>Operations staff is replaced during initial development of project, loss of know-how and experience</td>
</tr>
<tr>
<td>5</td>
<td>Lack of resources by Operations, Head of Operation requires support of staff members in another project at the same time</td>
</tr>
<tr>
<td>6a</td>
<td>Incorrect information is given to contractors</td>
</tr>
<tr>
<td>6b</td>
<td>Correct information provided to contractor is not considered</td>
</tr>
<tr>
<td>7a</td>
<td>Operation report start of alignment with contractor although it has effectively not yet started</td>
</tr>
<tr>
<td>7b</td>
<td>Operation report start of alignment with contractor too late</td>
</tr>
</tbody>
</table>
FINDINGS AND EVALUATION
Findings and Evaluation

• Búðarháls HEP was a successful project
  – Time and budget plans were met
  – No major accident, however near-to losses
  – Risk management processes were followed

• Comparison of two risk registers:
  – Risk register from 2011 has 149 risks
  – Risk register from 2013-2014 has 154 risks

• Risk management strategy in Búðarháls HEP:
  – Define goals
  – Risk matrix approach with contribution from contractors
Findings and Evaluation

• STAMP/STPA takes a different approach:
  – Create HCS and define roles and responsibilities
  – Define unacceptable losses
• STAMP/STPA framework is a more structured approach
• Clear methodology and process for analyzing risk
• Traceability ensured
• Justification and rationale are available
• Identification of causes of unsafe or inadequate Control Actions
• CAs and causes of UCA or ICAs in the case study are credible
Findings and Evaluation

- Risk Management in Búðarhálsl HEP
- Risk Management Planning
- Risk Identification
- Risk Evaluation – Effect on: Safety/Cost/Time/Business Multiplication
- Risk Register
- Risk Treatment with Mitigating Controls
- Risk Acceptance

- STAMP/STPA in a Hydropower Project
- Goals
  - Unacceptable Losses
  - Hiararchical Control Structure
- High Level Hazards
- High Level Safety Constraints
- High-Level Safety Req. Control Actions
- STPA Step 1: Unsafe Control Actions
Findings and Evaluation

• With STPA more detailed and precise risk mitigation strategies can be developed
• The bottom-up risk approach in Búðarháls HEP proves to be practical in many ways – contractors are able to understand, share and participate
• Two types of project risk investigated
  – High level project risk
  – Risk in the risk management process itself
• STPA can be used independently by an analyst with knowledge of techniques and project context
Findings and Evaluation

• Not all risks in a hydropower project can be identified with project based bottom-up risk analysis methodology
• With STPA we get another perspective that helps us identify previously unidentified risks
• Flaws in the control structure were identified with STPA – but not by current method
Findings and Evaluation

• Request for combined use of STPA and bottom-up risk analysis
• ISO standards require well defined risk analysis methodology – but don’t tell how
• In long term STAMP/STPA will influence:
  – Development of ISO risk management standards
  – Project management standards, e.g. requirements and checklists
  – Contracts, compliance requirements
CONCLUSIONS
Conclusions

• No generic risk analysis methodology has yet been defined as such, but STAMP/STPA has been applied in many different disciplines
• Risk terms not yet properly defined as science requires – depends on industry sector and research field
• Risk based thinking now required in ISO9001 quality management standard
• Risk analysis methodologies need to be defined for scientific use
Conclusions

• There are commonalities of risk analysis requirements in different industries, e.g. when using ISO31000

• The requirements for a generic risk analysis methodology must be investigated further

• No limitation found to the applicability of STAMP/STPA other than it requires training, understanding – and preferably a software tool to support use
Thanks to ...

Landsvirkjun
Páll Jensson
Robert Jan de Boer
Katrín Dögg Sigurðardóttir
Lorene Pelegrín
Questions and further information?

Svana Helen Björnsdóttir
svana@stiki.eu