STPA Application in Hydropower – Piloting Experience

Peter To & Roman Dusil
BC Hydro, Canada
Presentation Outline

- Intro to Hydropower
- Pilot Applications of STPA:
  - Case 1 - Water Passage System
  - Case 2 - River System
- Applicability of STPA in Hydropower
**Hydropower**

- Convert potential energy in water to electrical energy
- 15% of world electricity
- >130 years - Perceived as robust & mature (not progressive)
- **Focus is on water flow not electrons**
Traditional Approach

- Bottom up, component-based analysis

![Graph showing probability of failure over time with phases: burn-in-period, useful life, wear-out-phase.]
Multiple Components in Diverse System

Deterioration of Component 4 may impose additional onus on Component 1

Deterioration of Component 3 may damage Component 2

Operating Procedures

Response Plans

Human Factors
Our Systems Approach Journey

- **2015**: Systems Approach Pilot
- **2016**: STAMP Workshop
  - Case 1 STPA Pilot
- **2017**: Case 2 STPA Pilot
- **2018**: STAMP Workshop
Case 1 – Water Passage System

Reservoir

Spillway Gates

Intake Gate

Penstock Valve

Powerhouse

Turbine Valve

Generating Unit

Downstream Area

BC Hydro
Power smart
Case 1 - Hazards & Accidents

Accidents A1-A4

- Fatalities
- Loss of Generation
- Environmental Damage
- Collateral Damage

Hazard H1

High pressure water not contained

Hazard H2

Water cannot flow through on demand
Case 1 - STPA Control Structure

Not our conventional way of thinking!
Case 1 - STPA Analysis & Output

- Team - 2 full time
- Used XSTAMPP
- Step 1 – Identify Unsafe Control Actions
  - 26 Unsafe Control Actions/Safety Constraints
- Step 2 – Determine Casual Scenarios
  - 120 Causal Scenarios
  - Consolidated into 18 issues
    - 10 were previously known
    - 8 were newly identified by STPA
Case 1 – Seismic Scenario

- BC Hydro operates in a seismically active zone.
- A seismic event causes penstock rupture.
- Must be able to mitigate damage by shutting off flow (closing valves).
Case 1 – Findings – Penstock Valves
Case 1 – Findings – Penstock Valves

- **UCA-1**: Protective control system does not close penstock valve during rupture
  - Device - Inability to close under rupture flows
  - Post-seismic functionality uncertain
    - No consistent seismic standards

- **UCA-2**: Protective control system closes penstock valves when there is no emergency
  - Should we make control logic failsafe (i.e. bias to close)?
    - Downside - Surge shafts may overflow.
Case 1 – Findings – Penstock Valves

- **UCA-3**: Remote Operator does not close penstock valve during rupture
  - Control Centre response is rule-based.
    - Rules/response actions are not always clear.

- **UCA-4**: Local staff do not close penstock valve during rupture
  - Emergency training adequate?
  - Access…
Case 1 – Findings...cont’d
Case 2 – River System

Two Reservoirs

Generation Water Passage

Reservoir “A”

4km

Spillway Gates

Free Overflow (No Gates)

Headpond “B”

Intake Gates

5km

Powerhouse

Turbine Valve

Bypass Valve

Generating Unit

River (People, Fish)
Case 2 – River System

Reservoir A

Headpond B

Water Passage

Reservoir “A”

Spillway Gates

Free Overflow (No Gates)

Headpond “B”

Intake Gates

Powerhouse

Turbine Valve

Bypass Valve

Generating Unit

River (People, Fish)

5km

4km

17km

River System Diagram with Reservoirs A and B, Headpond B, Water Passage, and Various River Components.
Case 2

Water Passage

River (calm)
Case 2

Water Passage

River (calm)

(natural flood, operational surge)
Case 2 - Flow Control

- Most Critical: Control River Flow (Q2)
  - Public safety
  - Fish habitat
- Can only control indirectly (Q & Q1).
  - Q & Q1 are independently managed.
  - Operator dependent.
- Numerous regulatory violations
  - Q ↑↓ or Q1 ↑↓ all susceptible.
  - Wrong move may not be recoverable.
Case 2 – FMEA, STPA

- **2015-2016**
  - Commenced with FMEA
  - Overwhelmed by complexity

- **2016-2017**
  - STPA
  - Small Team – 2 full time, 6 part time
  - Top down *(really helped!)*
    - 2 Hazards
    - 4 Accidents
Case 2 - Control Structure

- 26 Control Actions

Operations Engineer

- Instruct Operations
- (Actual Conditions, Daily Op Schedule, Operating Orders)

Control Centre

- Raise/Lower MW
- Adjust Gen WP Max Flow

Site Staff

- Raise/Lower MW/Speed
- Adjust Gen WP Max Flow

Plant Controller

- Raise/Lower MW/Speed
- Adjust Gen WP Max Flow

Governor & Bypass Valve Control

- Open/Close WG
- Engage Throttle Valve Close WG

Q1 (Water Passage)

- E-Close & Crank/Open/Close Intake Gates
- E-Close Turbine Valve

Protective Control

- (Disturbances, Fault Conditions)
- E-Stop Governor
- Adjust Gen WP Max Flow

Spillway Gates

Intake Gates

Turbine Valve

Q (Res. A)

Bypass Valve

Fishway/Log Sluice

Federal Fisheries
Case 2 - STPA Analysis & Output

- **Step 1 – Identify Unsafe Control Actions**
  - 95 Unsafe Control Actions/Safety Constraints

- **Step 2 – Determine Casual Scenarios**
  - 129 Causal Scenarios
    - 85 already known through FMEA (66%)
    - 44 additional ones identified during STPA (34%)
Case 2 - Finding 1 Spillway Gates

- **Water Conveyance Functions:**
  - Normal Operation - Regulate Flow.
  - Unusual Condition - Flood Routing (Dam Safety).

- **Operational Modes:**
  - Primary - Remote Control Centre
  - Backup - Local Site Staff
  - No Auto
Case 2 - Finding 1: Spillway Gates

- **Not Operated Causing Hazard:**
  - Equipment condition.
  - System reliability concerns.

- **Operation Causing Hazard:**
  - Spurious opening – downstream.
  - No upstream inspection when gate opening called for.
    - No protocol.
    - No monitoring.
Case 2 - Finding 2
Water Passage Emergency Close

- 4 Flow Control Devices
  - Intake Gates
  - Turbine Valve (TIV)
  - Generating Unit
  - Bypass Valve

- Scenarios that will “Emergency Close” all 4 Devices
  - Penstock Low Pressure
  - Powerhouse Flood
  - Unit Mechanical Trip (High Bearing Temperature, Vibration)
  - Unit Overspeed
  - Others Observed by Site Operator
Case 2 - Finding 2
Water Passage Emergency Close

- Will “Emergency Close” work?
  (Not Provided Causing Hazard)
  (Too Late)
  (Wrong Sequence)
- Safety Constraint:
  Protective Control must provide “Emergency Close” command when the above scenarios occur.
- Is it appropriate?
  (Provided Causing Hazard)
Case 2 - Finding 2
Water Passage Emergency Close
(i) Not Provided Causing Hazard
Case 2 - Finding 2

Water Passage Emergency Close

(ii) Provided Causing Hazard

- Traditional engineering – Protect asset from damage.
  - “Safety” is defined as cutting off water to the water passage.
    - Is this correct?
    - What about abrupt flow changes in river (people, fish)?
    - Should generation equipment protection come before natural river flow change violations and public safety concerns?
To Perform STPA.....

- Need to Change Our (Traditional) Way of Thinking - *Tough!*

<table>
<thead>
<tr>
<th>STPA</th>
<th>Traditional (in Hydropower)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System view.</strong></td>
<td></td>
</tr>
<tr>
<td>- Get out of organizational silos.</td>
<td><strong>Discipline-based.</strong></td>
</tr>
<tr>
<td></td>
<td>- Electrical, mechanical, etc.</td>
</tr>
<tr>
<td><strong>Scenarios.</strong></td>
<td></td>
</tr>
<tr>
<td>- Include unusual combination of usual events.</td>
<td><strong>Failures.</strong></td>
</tr>
<tr>
<td></td>
<td>- Often equipment.</td>
</tr>
<tr>
<td></td>
<td>- Chain of event.</td>
</tr>
<tr>
<td><strong>Process model flaws.</strong></td>
<td></td>
</tr>
<tr>
<td>- Importance of monitoring &amp; feedback.</td>
<td></td>
</tr>
<tr>
<td><strong>Procedural flaws.</strong></td>
<td></td>
</tr>
<tr>
<td>- Inadequate response plans.</td>
<td><strong>May receive less attention than physical assets.</strong></td>
</tr>
<tr>
<td>- Human factors.</td>
<td><strong>May be decoupled from designs &amp; assessments.</strong></td>
</tr>
<tr>
<td>- Organizational factors.</td>
<td></td>
</tr>
</tbody>
</table>
With STPA

- Can see the big picture.
  - Can answer ‘Why’ and ‘So What’ when preparing business cases.
- Caution:
  - Findings & corrective actions not easily mapped back to our existing organizational setup or business processes.
Conclusions

1. System Thinking
   o Not established practice in hydropower business…
   o But is necessary because hydropower system is complex.

2. STPA - Great Tool for Complex Systems
   o Complement traditional asset-based approaches.
• peter.to@bchydro.com
• roman.dusil@bchydro.com