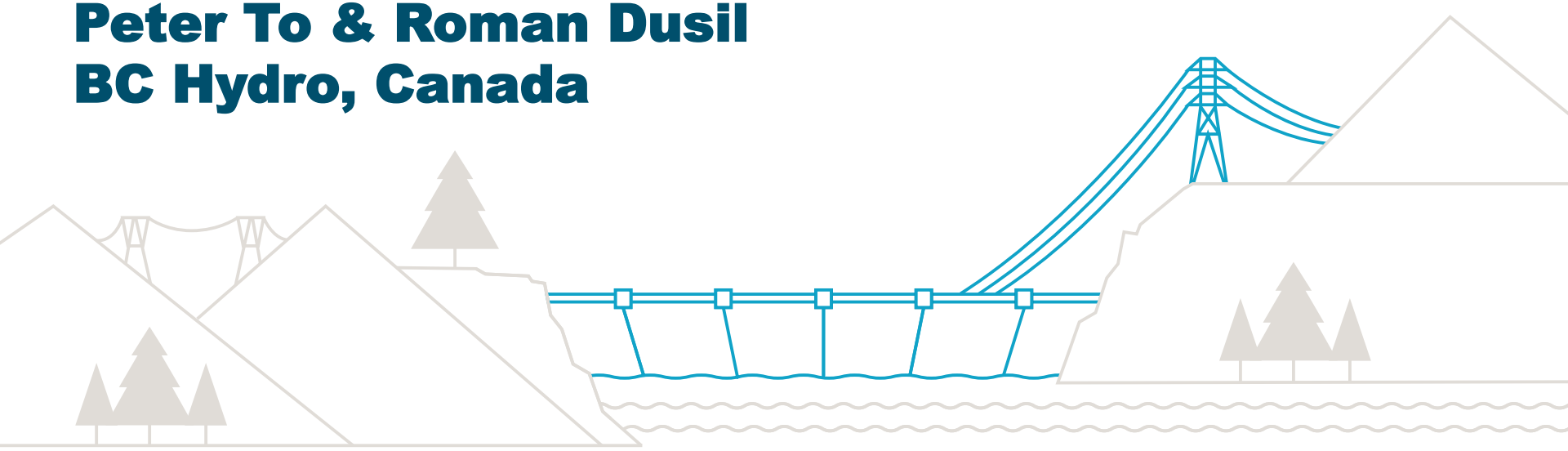
STPA Application in Hydropower – Piloting Experience

Peter To & Roman Dusil
BC Hydro, Canada



March 2018

BC Hydro
Power smart

Presentation Outline

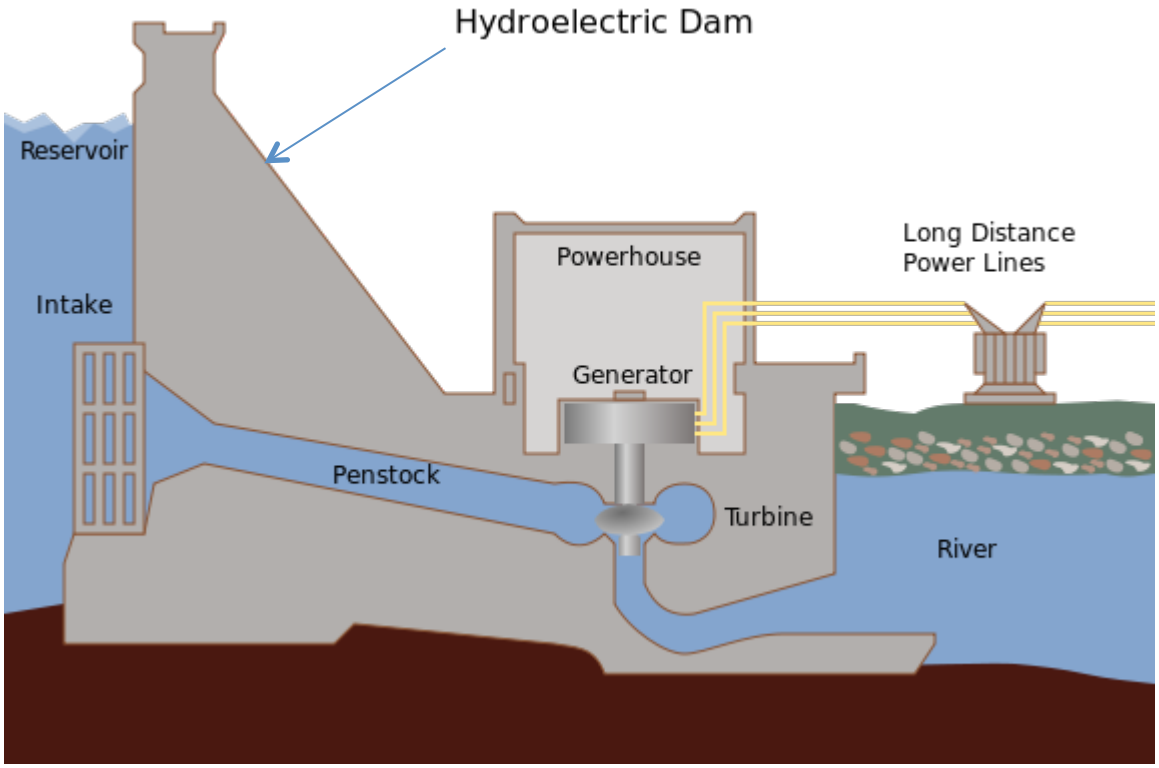
- Intro to Hydropower
- Pilot Applications of STPA:
  - Case 1 - Water Passage System
  - Case 2 - River System
- Applicability of STPA in Hydropower



BC Hydro
Power smart

Hydropower

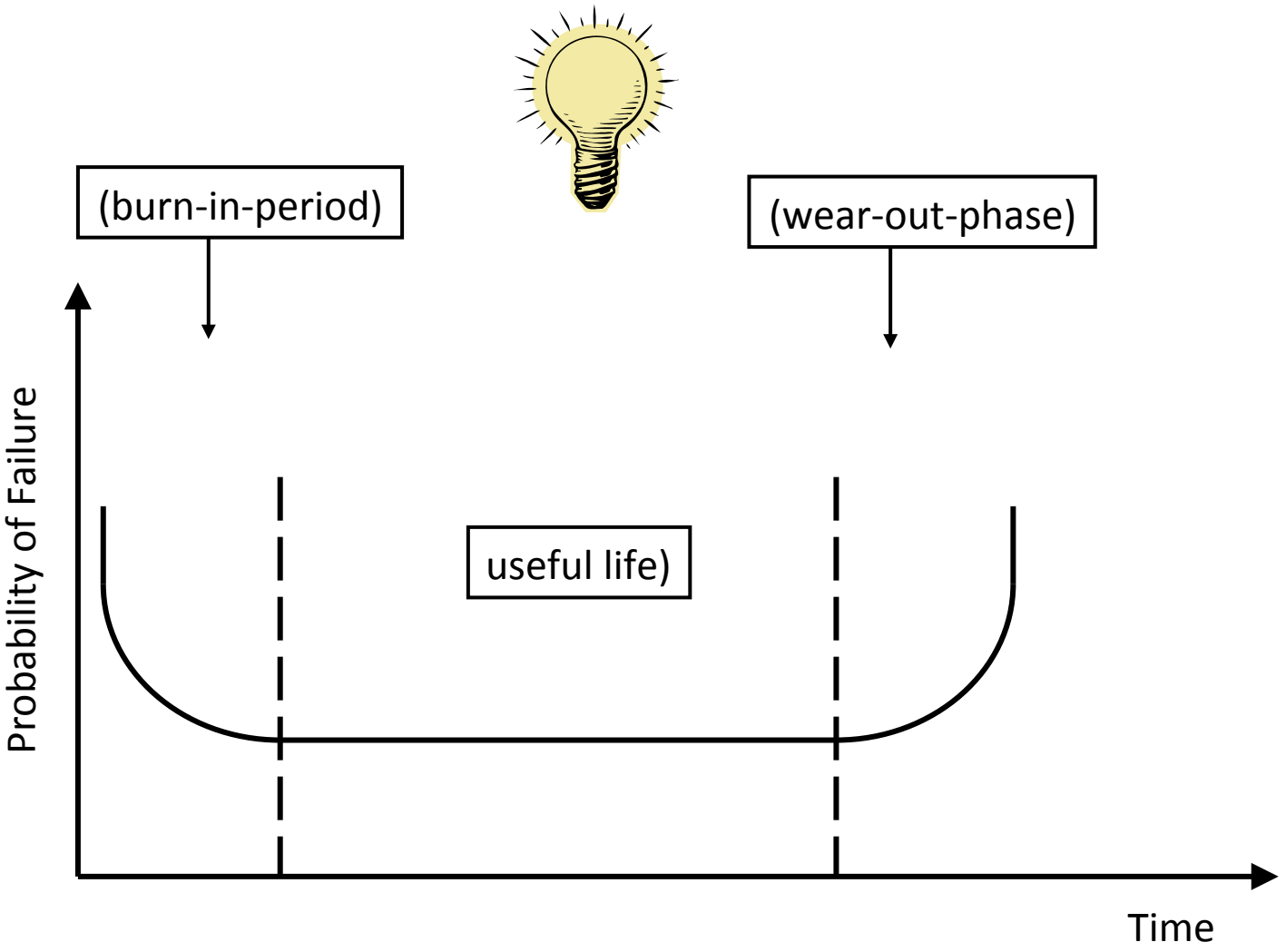
- Convert potential energy in water to electrical energy
- 15% of world electricity
- >130 years - Perceived as robust & mature (not progressive)
- **Focus is on water flow not electrons**



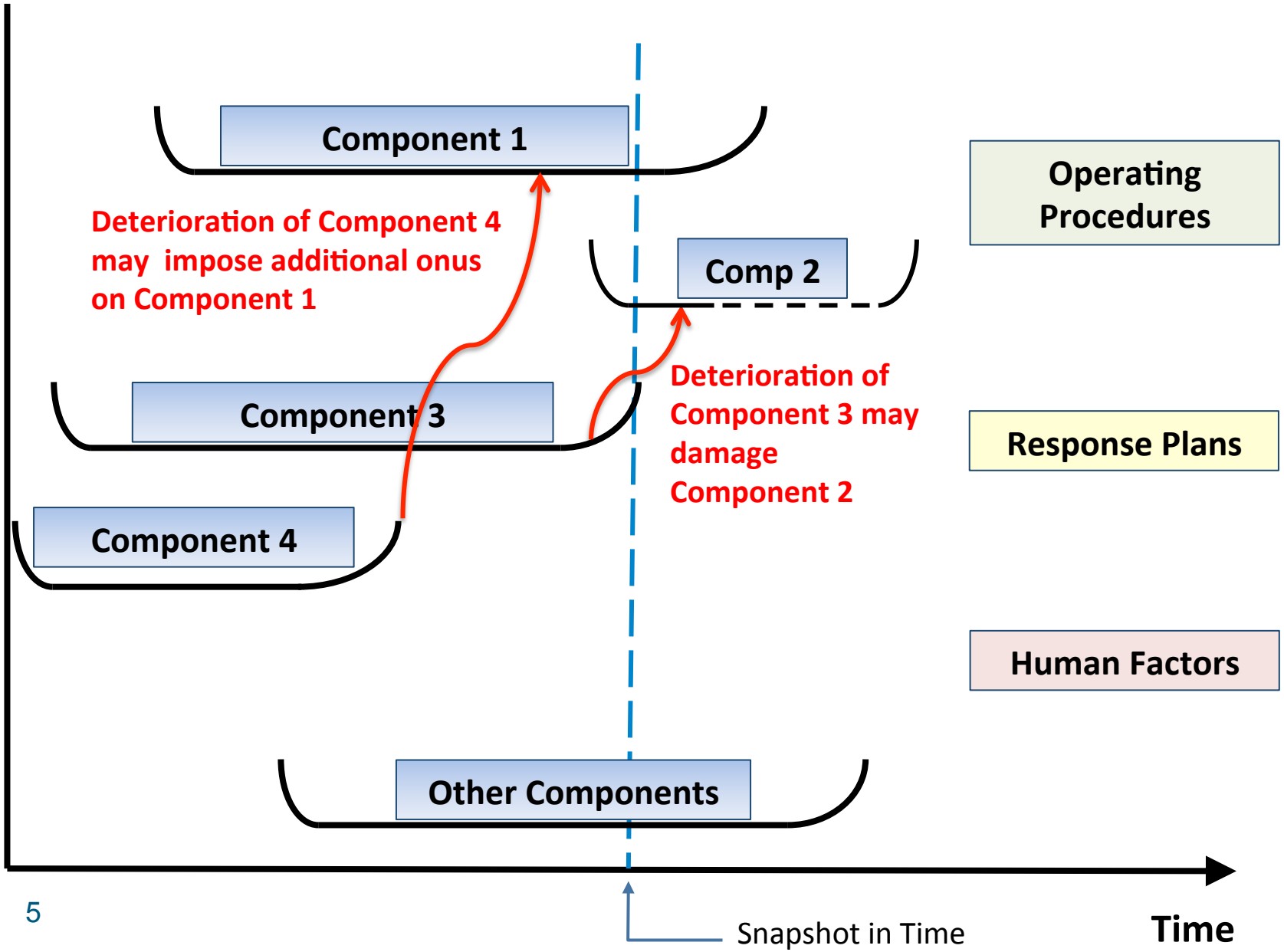
BC Hydro
Power smart

Traditional Approach

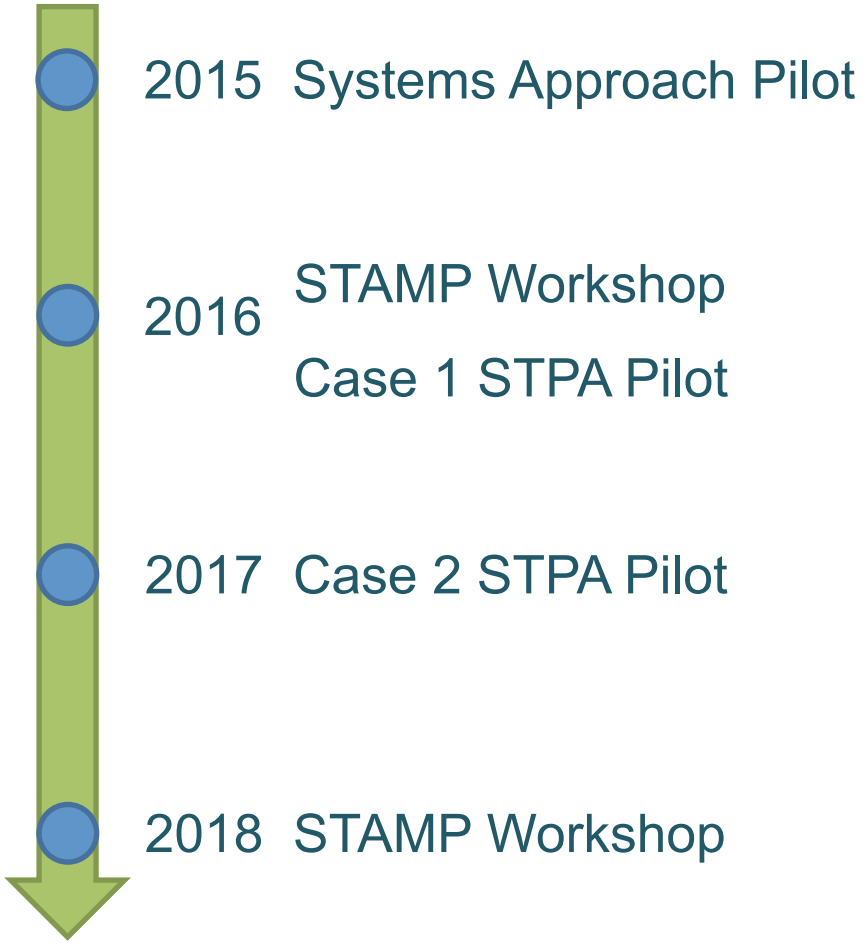
- Bottom up, component-based analysis



Multiple Components in Diverse System

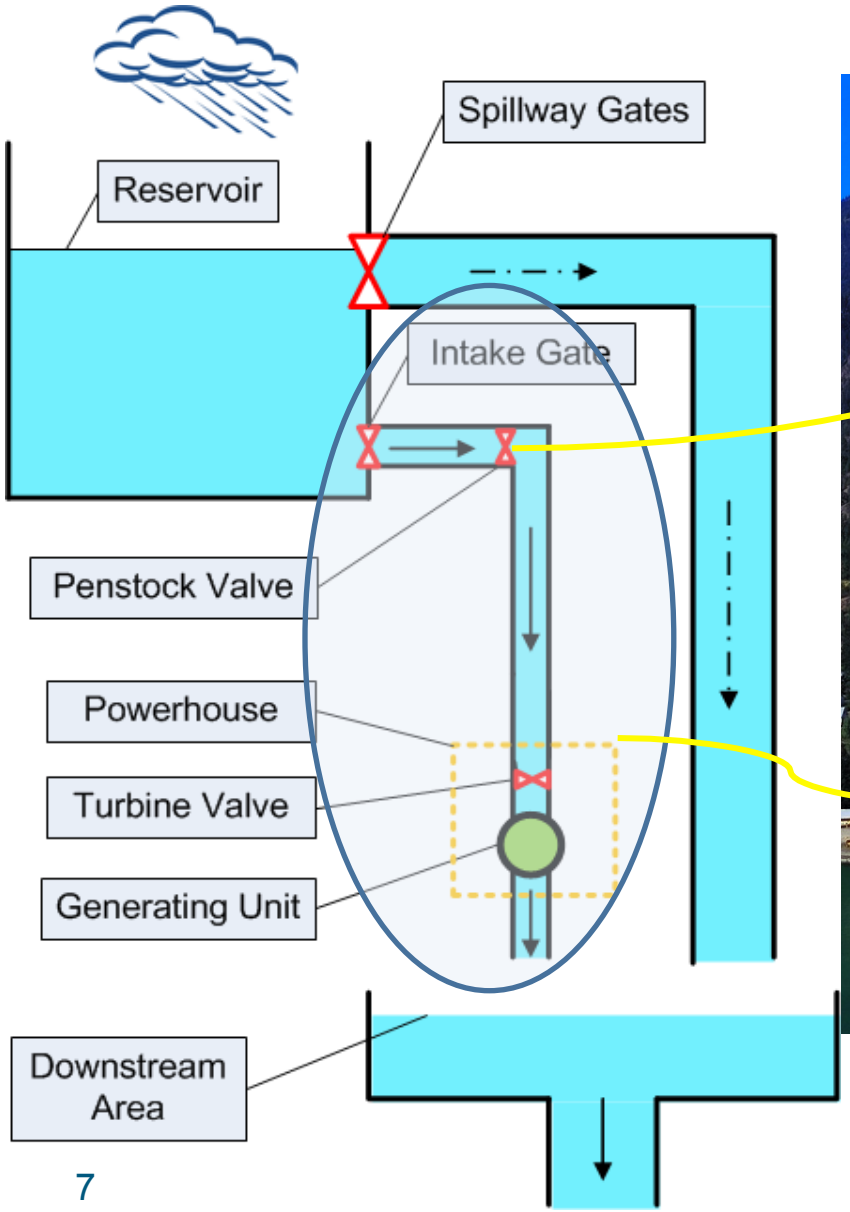


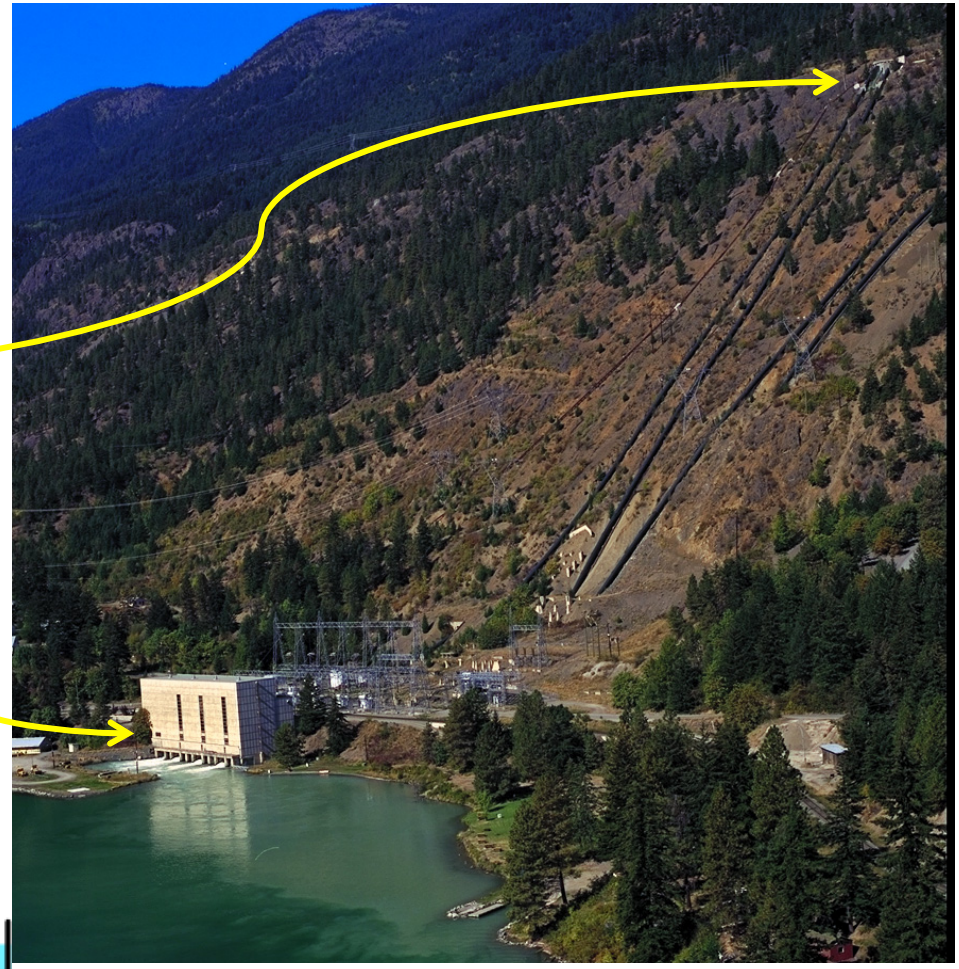
Our Systems Approach Journey



BC Hydro
Power smart

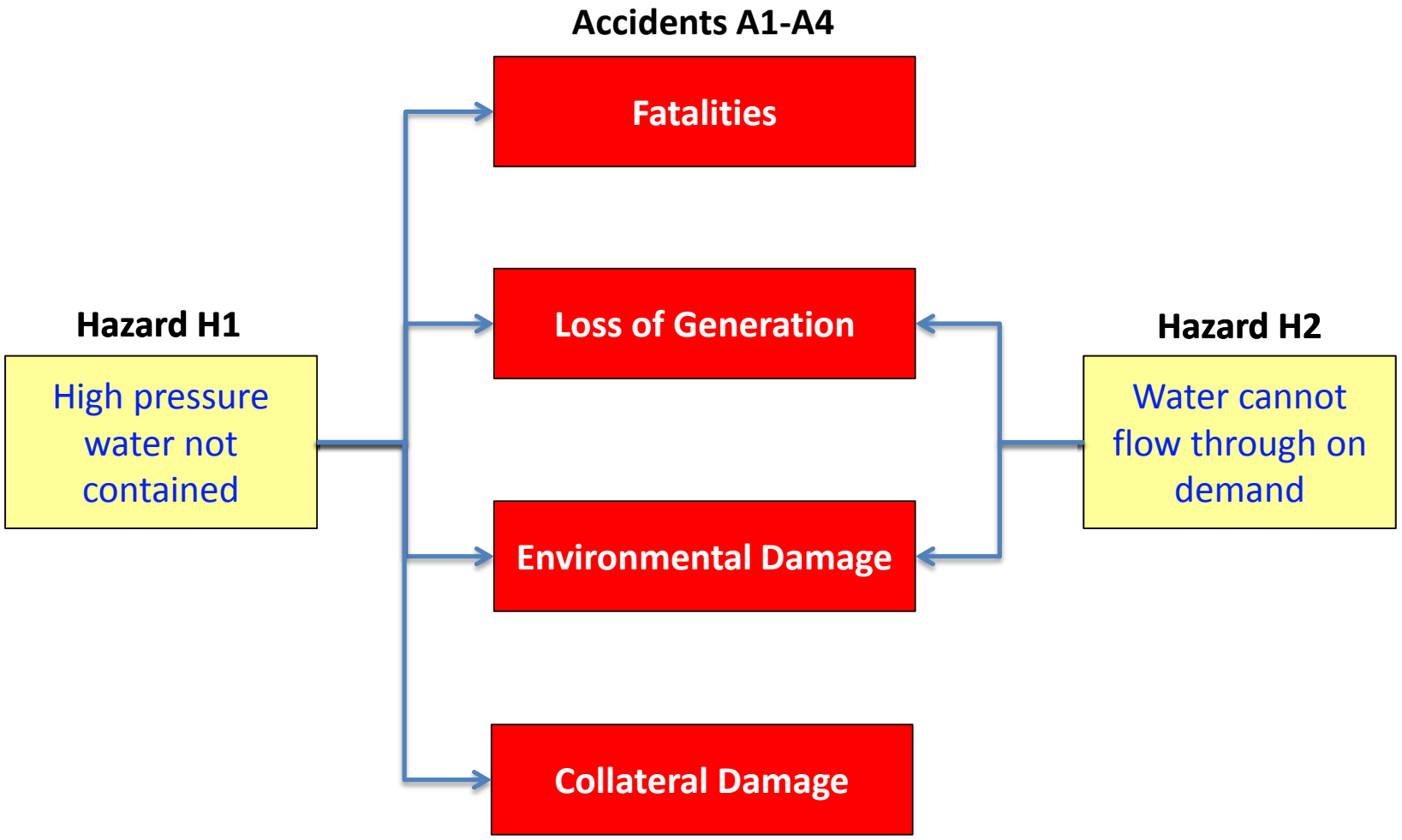
Case 1 – Water Passage System





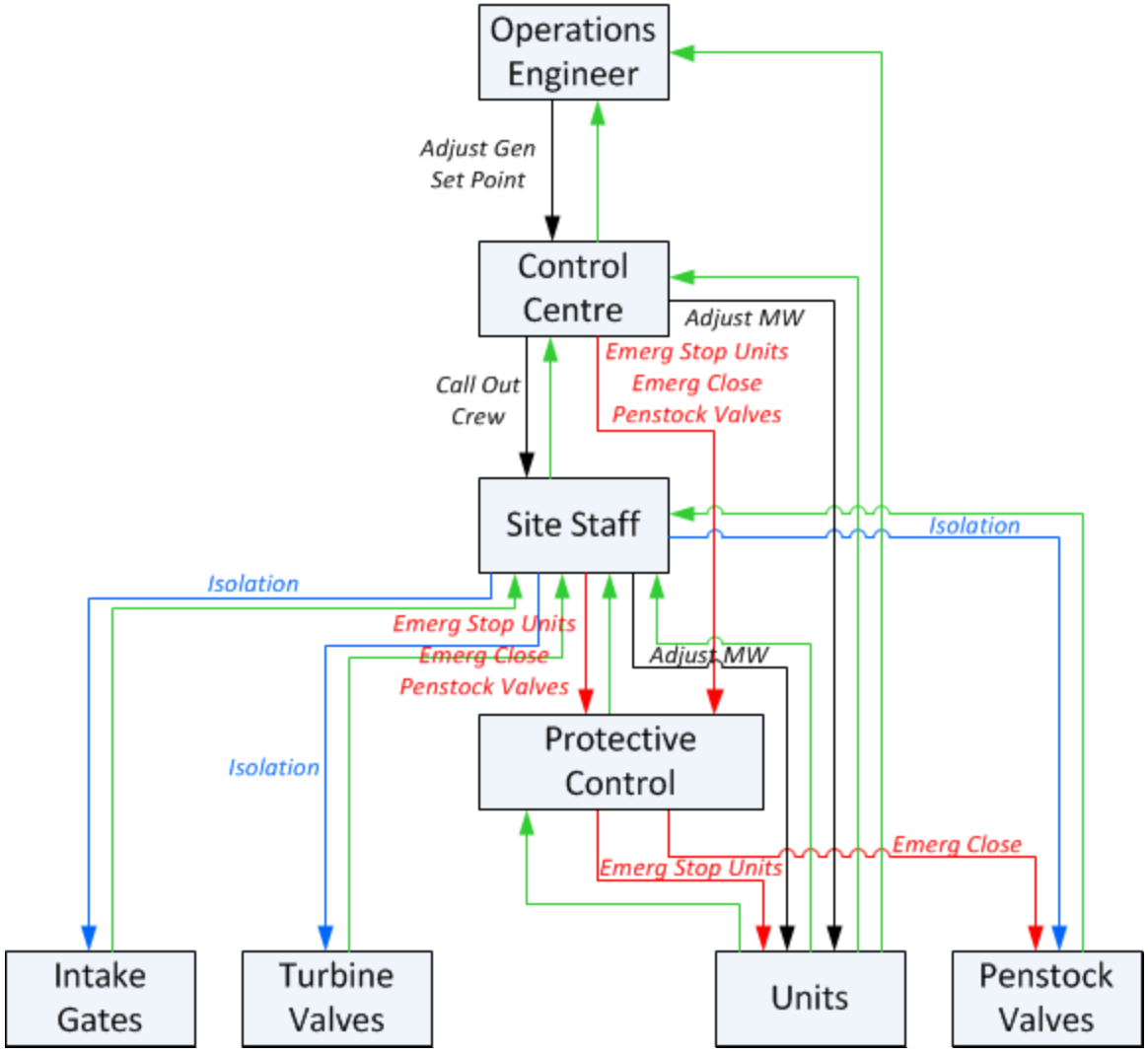
BC Hydro
Power smart

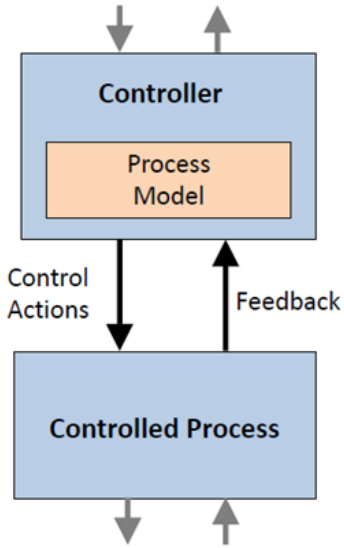
Case 1 - Hazards & Accidents



BC Hydro
Power smart

Case 1 - STPA Control Structure



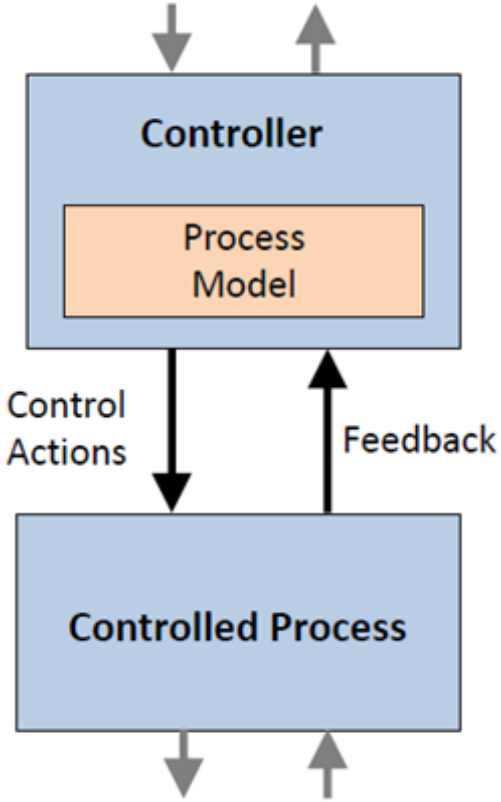


Not our conventional way of thinking!

BC Hydro
Power smart

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

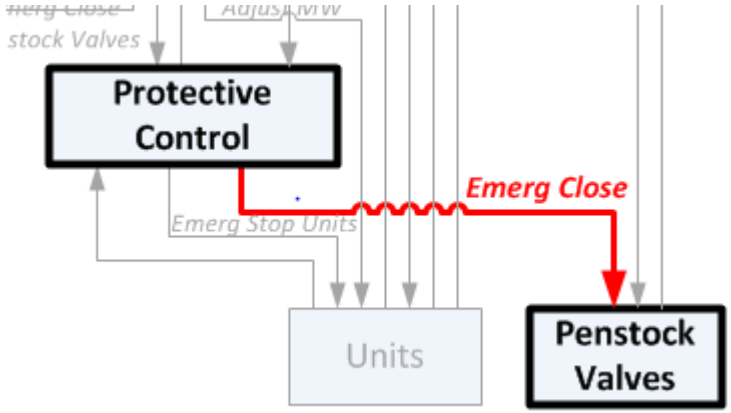


BC Hydro
Power smart

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).

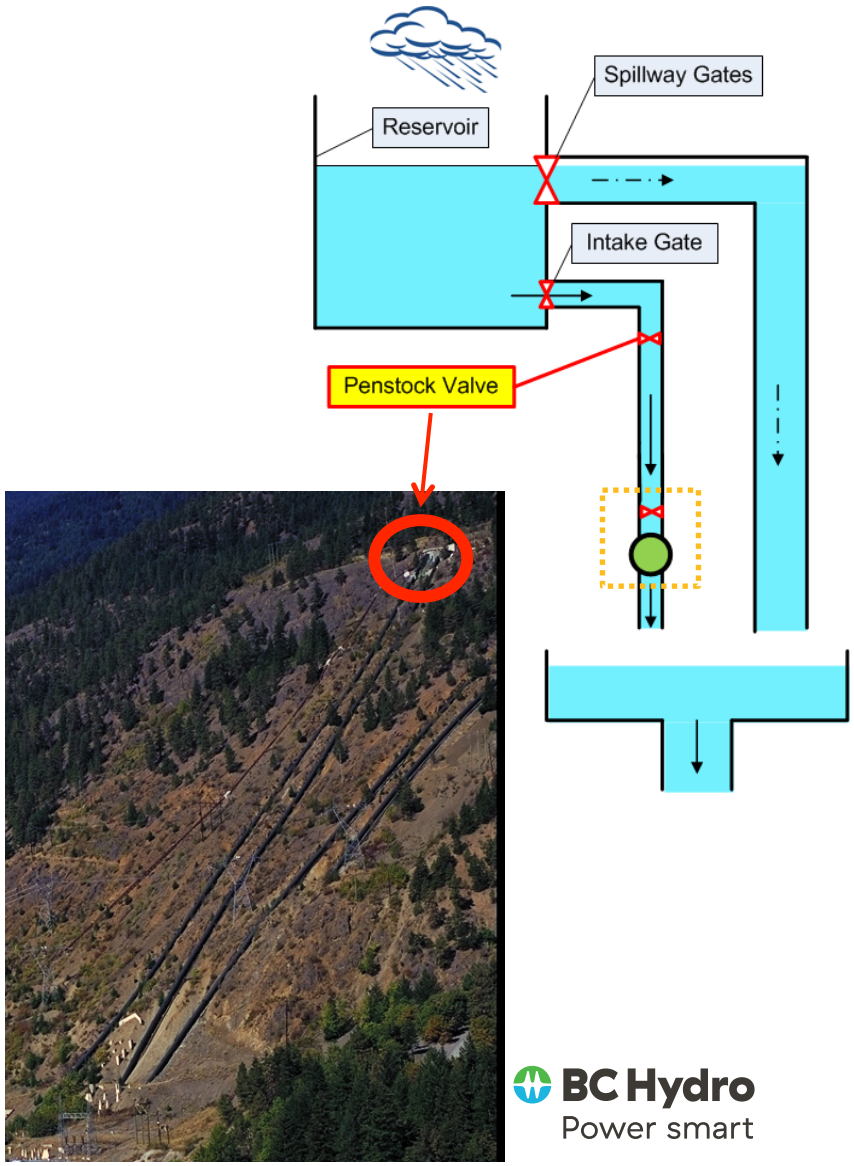
Case 1 – Findings – Penstock Valves



BC Hydro
Power smart

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.

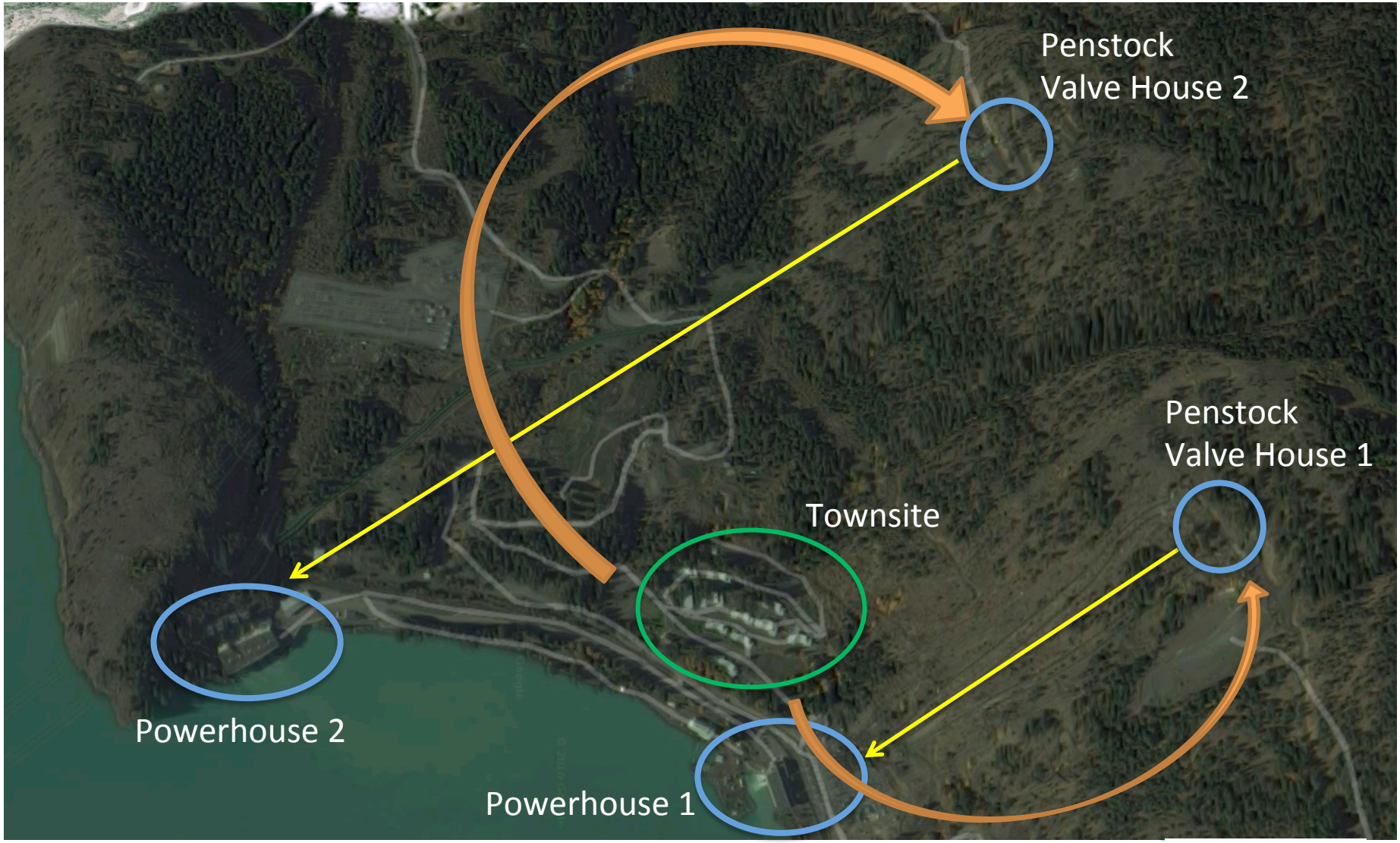


BC Hydro
Power smart

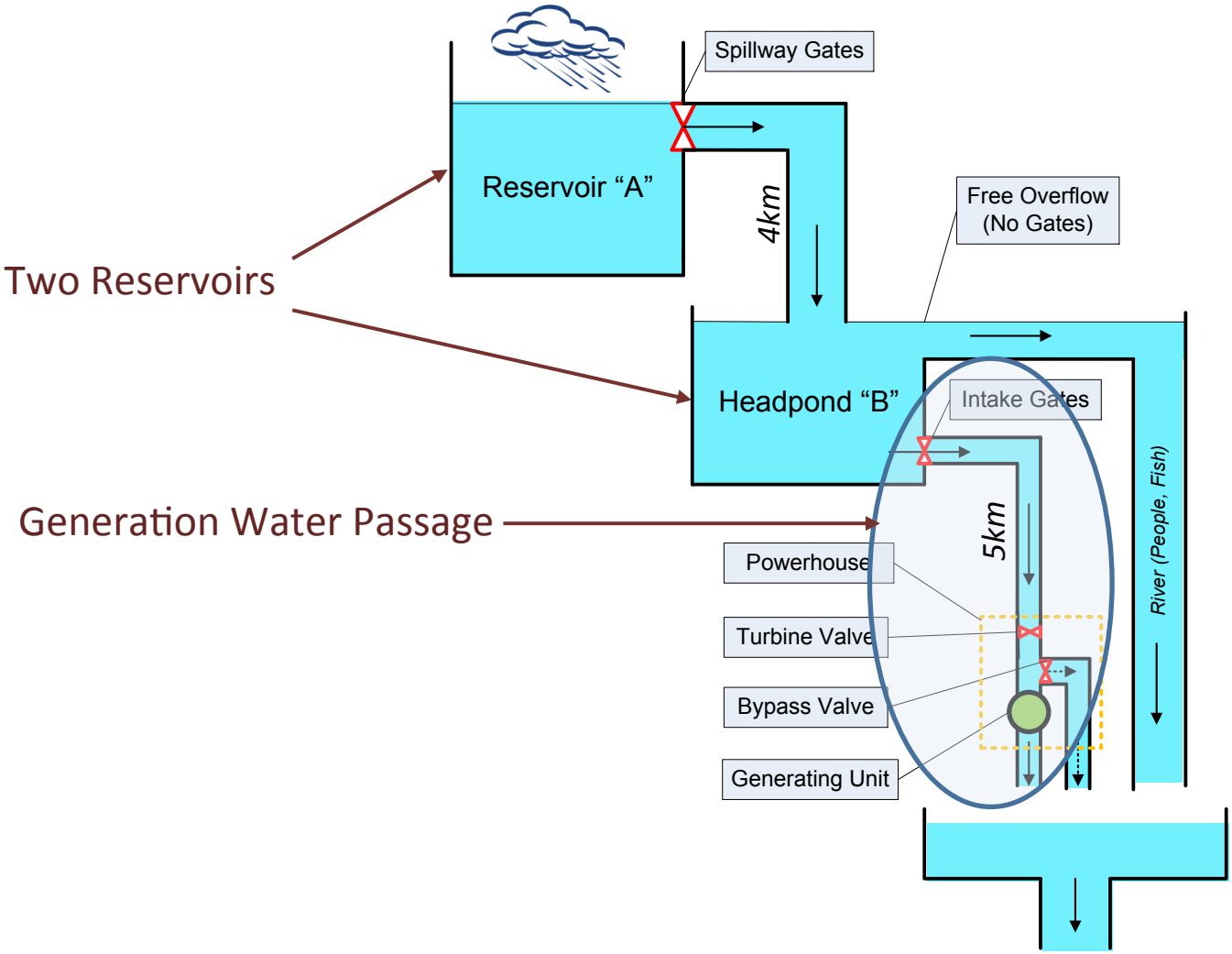
Case 1 – Findings – Penstock Valves

- **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

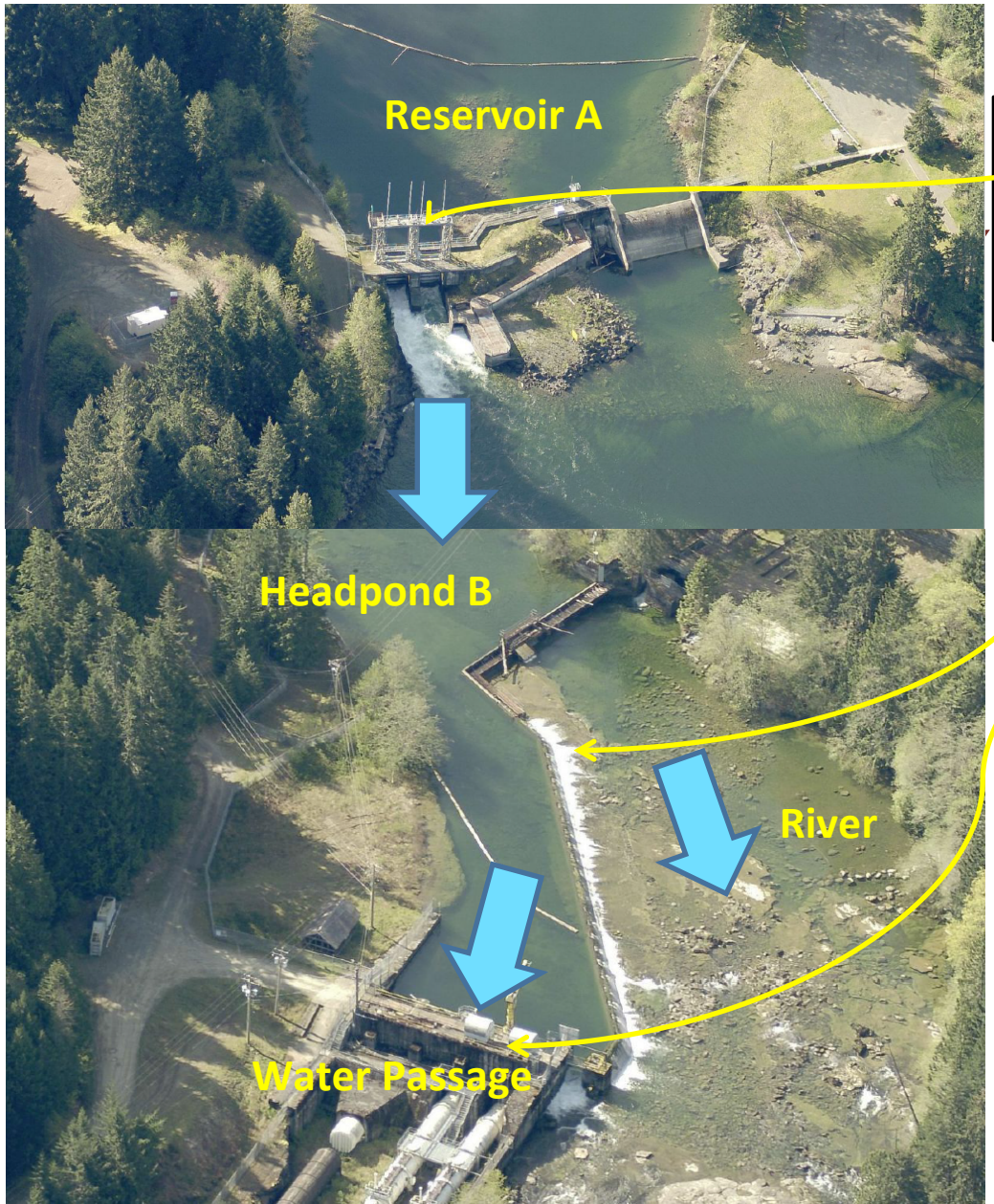


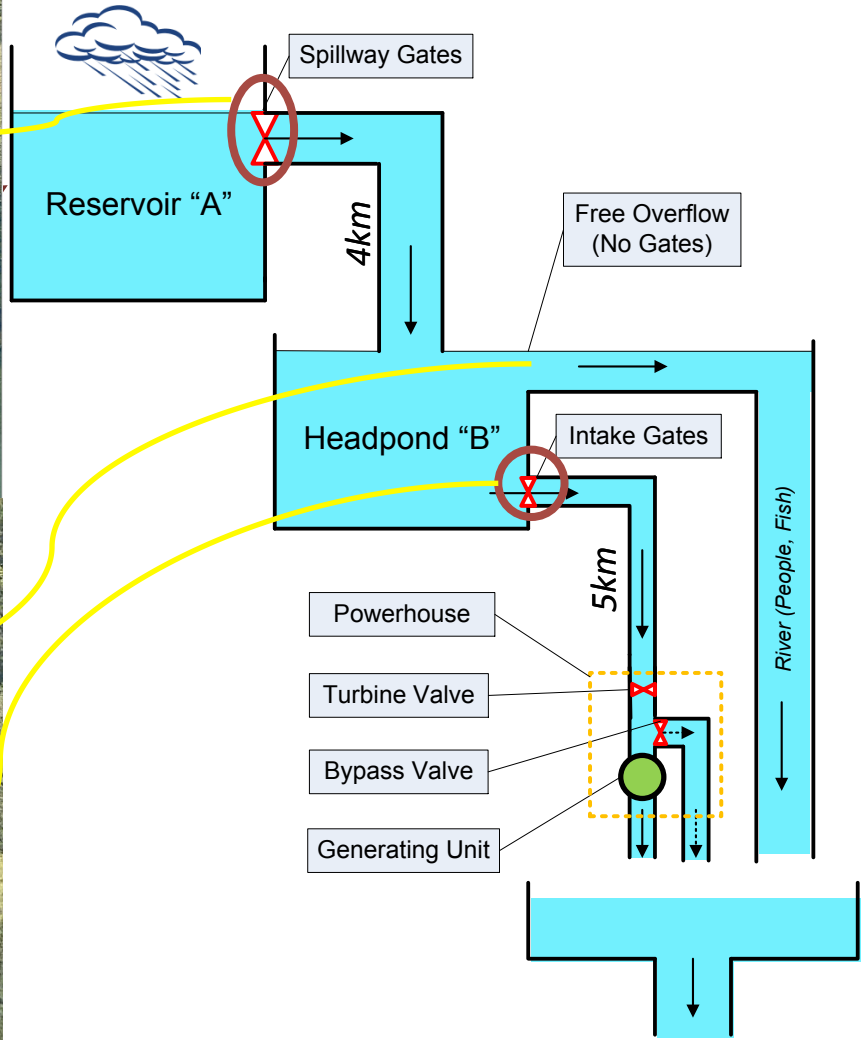
Case 2 – River System



BC Hydro
Power smart

Case 2 – River System





BC Hydro
Power smart

Case 2

Water Passage

River (calm)







Case 2

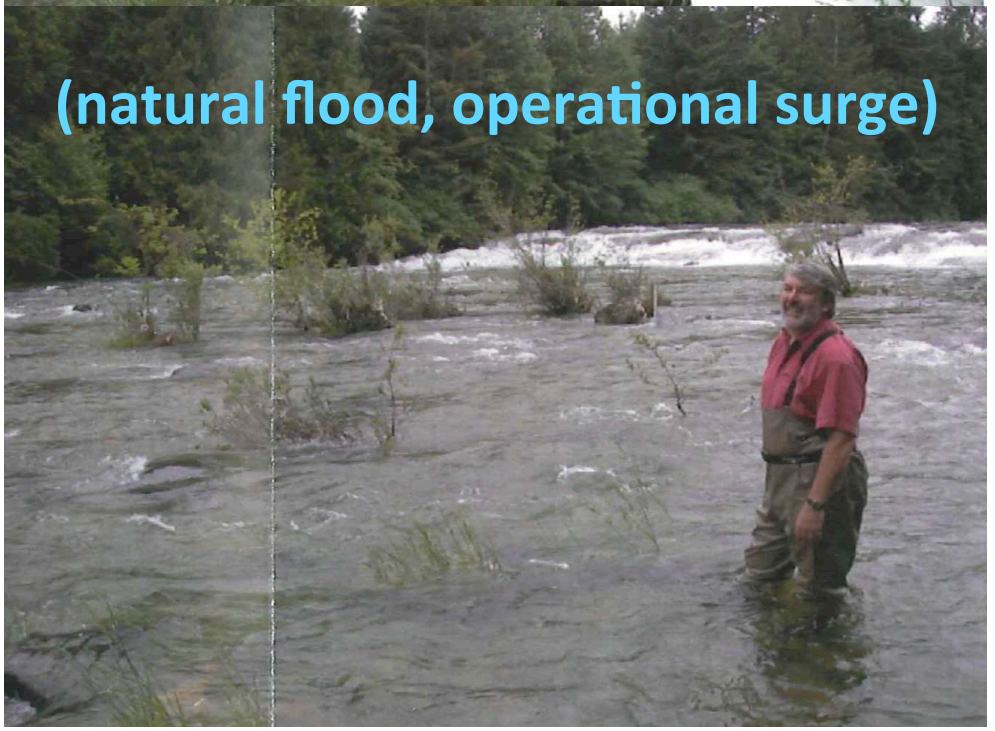
Water Passage



River (calm)

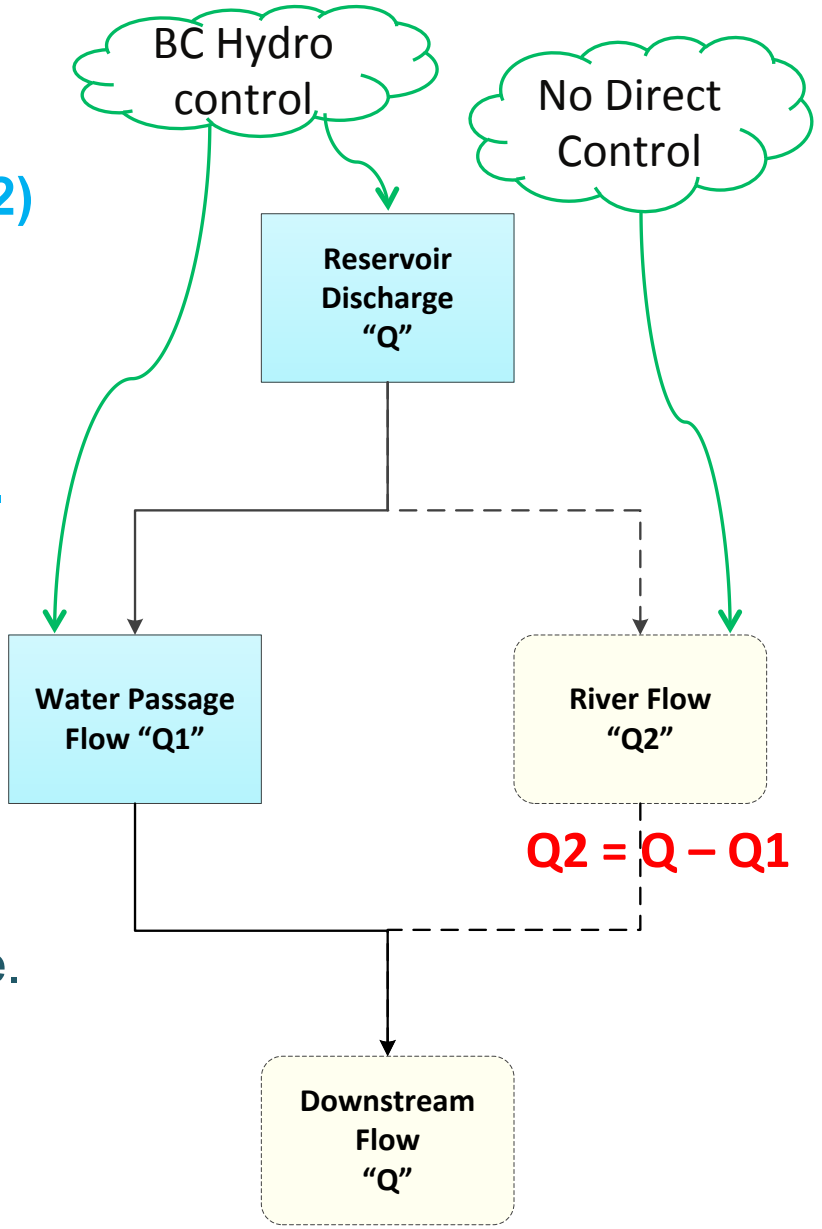


(natural flood, operational surge)



Case 2 - Flow Control

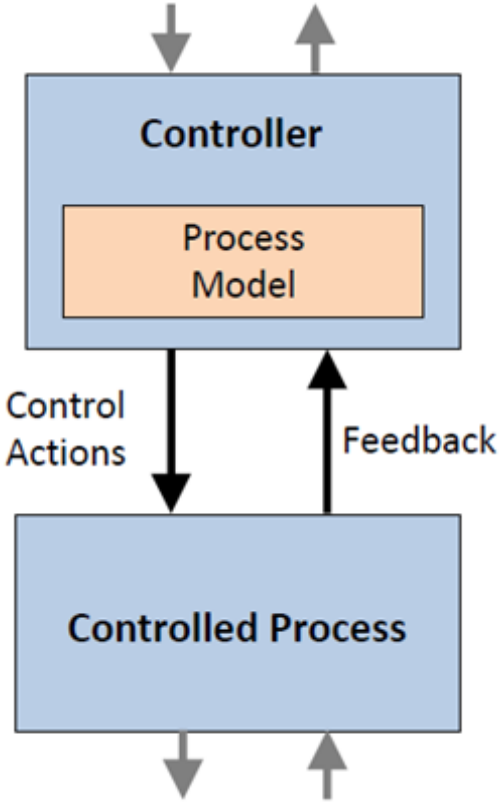
- **Most Critical: Control River Flow (Q2)**
  - Public safety
  - Fish habitat
- **Can only control indirectly (Q & Q1).**
  - Q & Q1 are independently managed.
  - Operator dependent.
- **Numerous regulatory violations**
  - Q ↑↓ or Q1 ↑↓ all susceptible.
  - Wrong move may not be recoverable.



BC Hydro
Power smart

Case 2 – FMEA, STPA

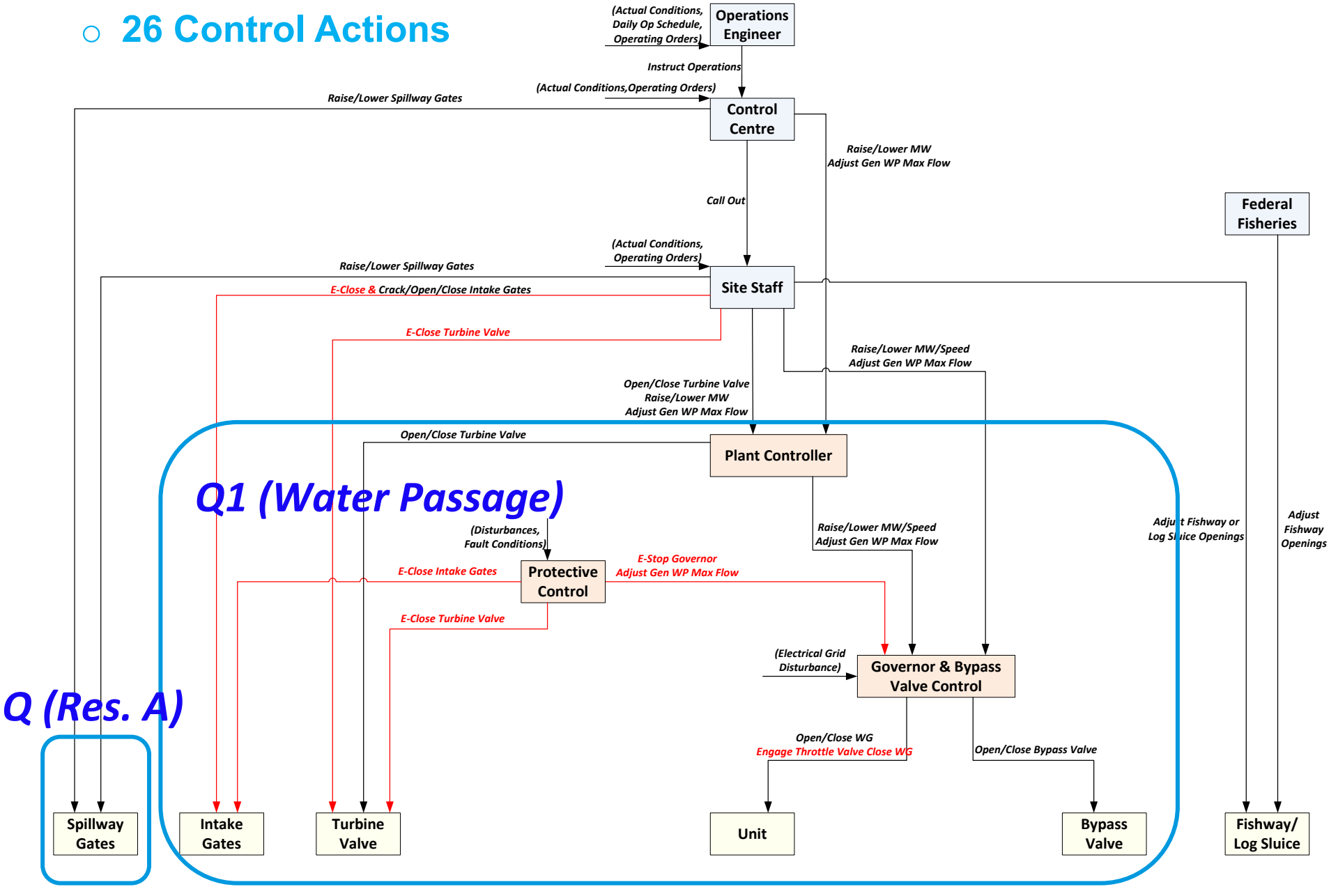
- **2015-2016**
  - Commenced with FMEA
  - Overwhelmed by complexity
- **2016-2017**
  - STPA
  - Small Team – 2 full time, 6 part time
  - Top down *(really helped!)*
    - 2 Hazards
    - 4 Accidents



BC Hydro
Power smart

Case 2 - Control Structure

- 26 Control Actions



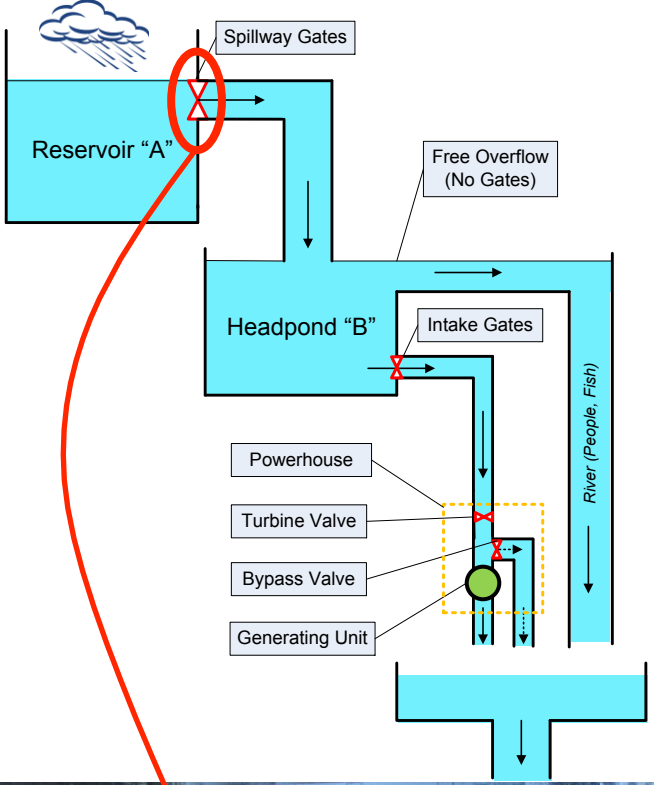
Case 2 - STPA Analysis & Output

- **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

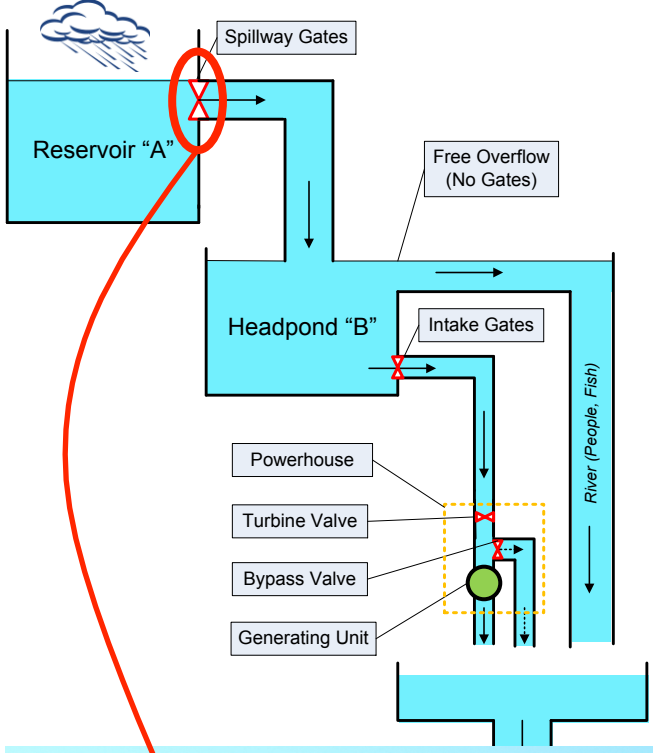




Case 2 - Finding 1
Spillway Gates

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

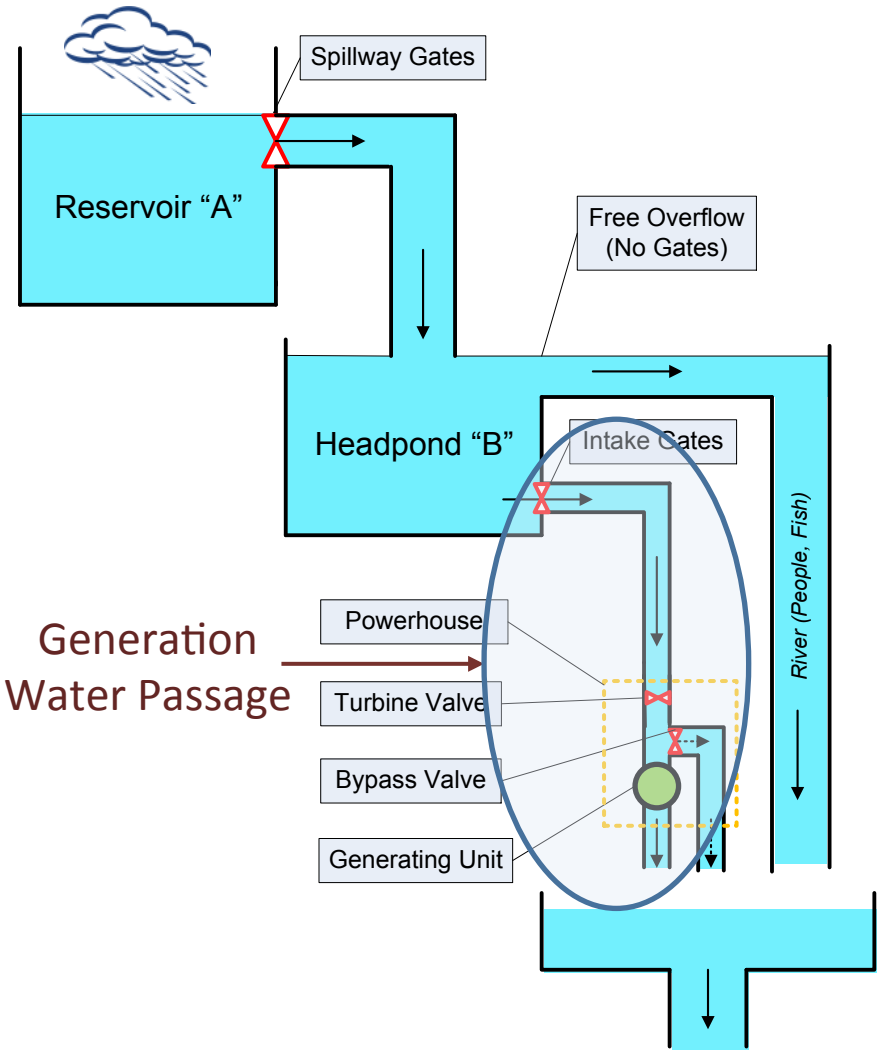
- **Operation Causing Hazard:**
  - Spurious opening – downstream.
  - No upstream inspection when gate opening called for.
    - No protocol.
    - No monitoring.





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



BC Hydro
Power smart

Case 2 - Finding 2
Water Passage Emergency Close

- **Will "Emergency Close" work?**

  (Not Provided Causing Hazard)

  (Too Late)

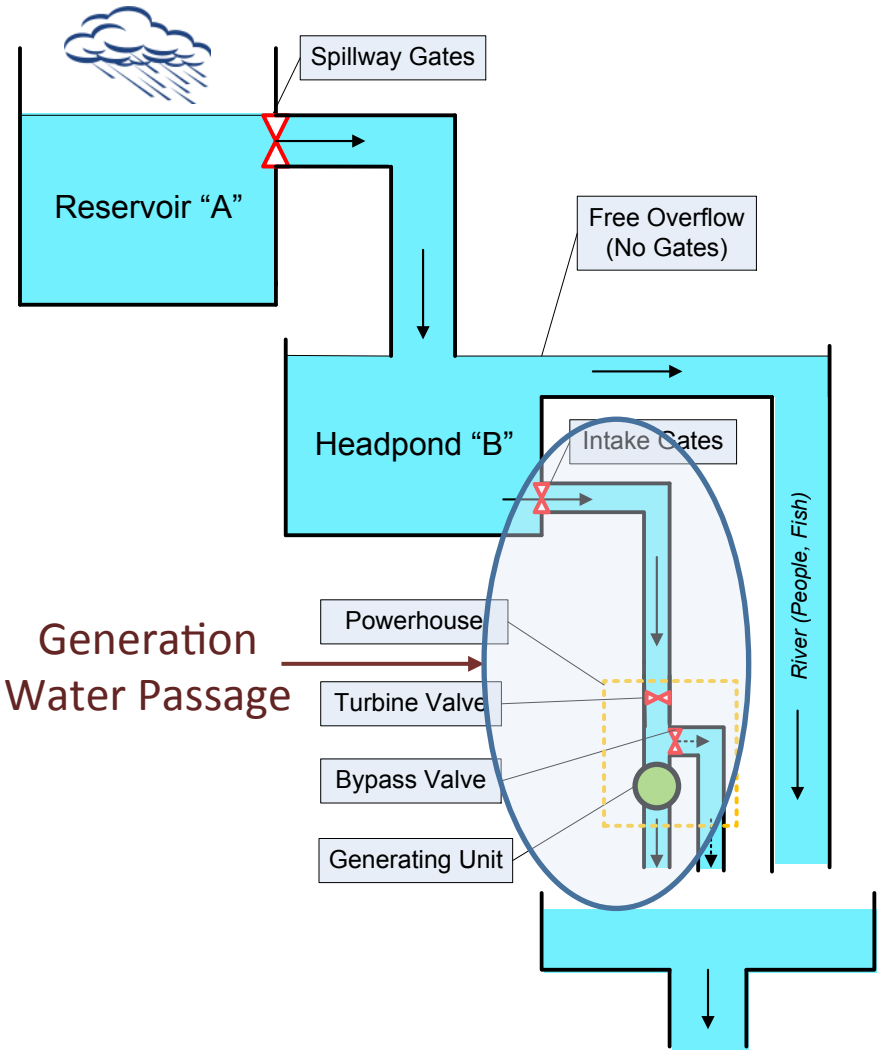
  (Wrong Sequence)

  - Safety Constraint:

    Protective Control must provide "Emergency Close" command when the above scenarios occur.

- **Is it appropriate?**

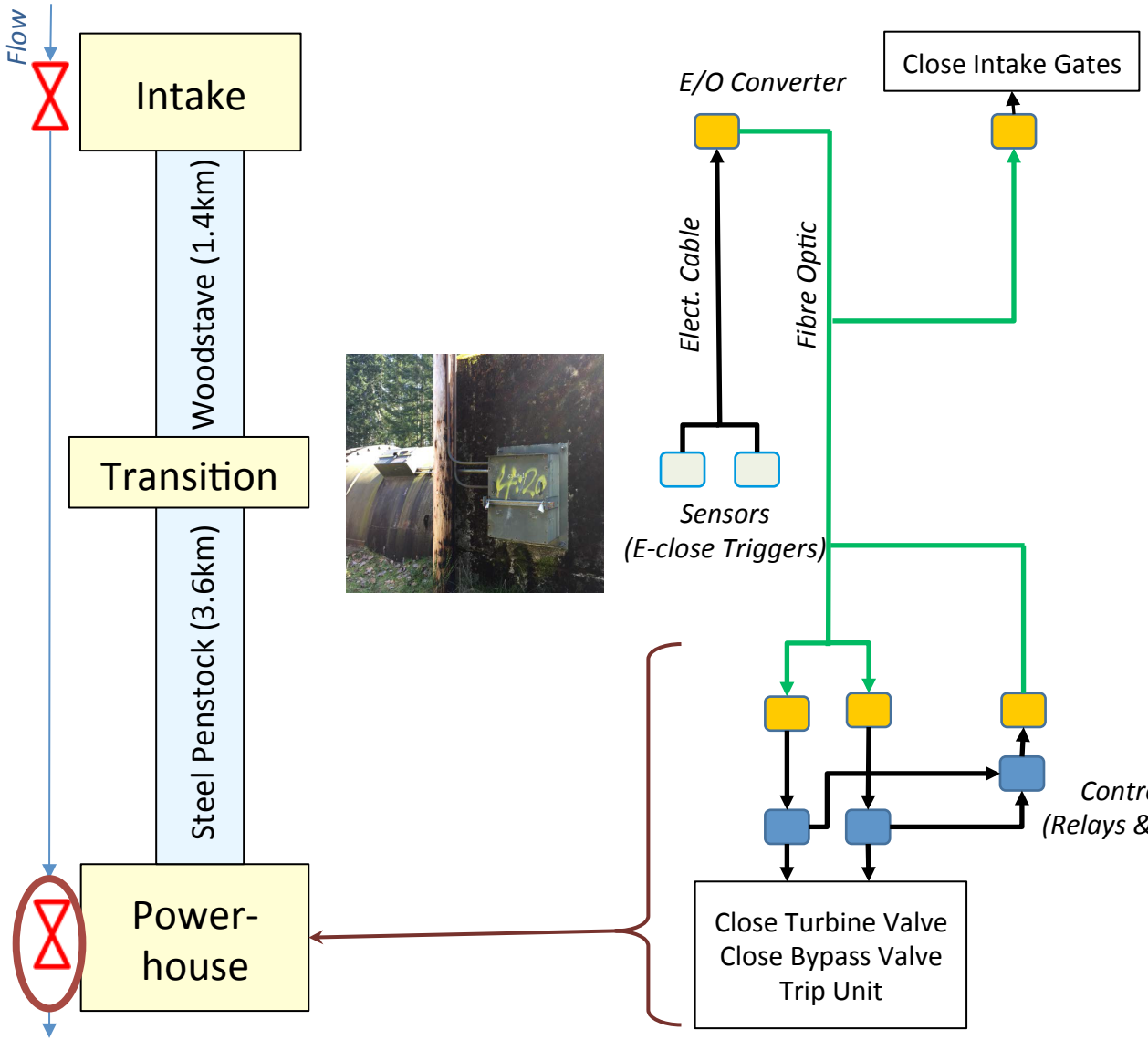
  (Provided Causing Hazard)



BC Hydro
Power smart

Case 2 - Finding 2
Water Passage Emergency Close

(i) Not Provided Causing Hazard



- Complex
- Convoluted
- Inconsistent
- Vulnerable

BC Hydro
Power smart

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!***

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

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
   - Not established practice in hydropower business…
   - But is necessary because hydropower system is complex.

2. STPA - Great Tool for Complex Systems
   - Complement traditional asset-based approaches.



- peter.to@bchydro.com
- roman.dusil@bchydro.com

BC Hydro
Power smart