- How to test hypotheses in an appropriate way: To update mental models, human controllers often use hypothesis testing to understand the system state better and update their process models. Such hypothesis testing is common with computers and automated systems where documentation is usually so poor and hard to use that experimentation is often the only way to understand the automation behavior and design. Such testing can, however, lead to losses. Designers need to provide operators with the ability to test hypotheses safely and controllers must be educated on how to do so.

Finally, as with any system, emergency procedures must be overlearned and continually practiced. Controllers must be provided with operating limits and specific actions to take in case they are exceeded. Requiring operators to make decisions under stress and without full information is simply another way to ensure that they will be blamed for the inevitable loss event, usually based on hindsight bias. Critical limits must be established and provided to the operators, and emergency procedures must be stated explicitly.

12.7 Creating an Operations Safety Management Plan

The operations safety management plan is used to guide operational control of safety. The plan describes the objectives of the operations safety program and how they will be achieved. It provides a baseline to evaluate compliance and progress. Like every other part of safety program, the plan will need buy-in and oversight.

The organization should have a template and documented expectations for operations safety management plans, but this template may need to be tailored for particular project requirements.

The information need not all be contained in one document, but there should be a central reference with pointers to where the information can be found. As is true for every other part of the safety control structure, the plan should include review procedures for the plan itself as well as how the plan will be updated and improved through feedback from experience.

Some things that might be included in the plan:

- General Considerations
  - Scope and objectives
  - Applicable standards (company, industry)
  - Documentation and reports
  - Review of plan and progress reporting procedures
- Safety Organization (safety control structure)
  - Personnel qualifications and duties

- Staffing and manpower
- Communication channels
- Responsibility, authority, accountability (functional organization, organizational structure)
- Information requirements (feedback requirements, process model, updating requirements)
- Subcontractor responsibilities
- Coordination
- Working groups
- System safety interfaces with other groups, such as maintenance and test, occupational safety, quality assurance, and so on.

• Procedures
- Problem reporting (processes, follow-up)
- Incident and accident investigation
  · Procedures
  · Staffing (participants)
  · Follow-up (tracing to hazard and risk analyses, communication)
- Testing and audit program
  · Procedures
  · Scheduling
  · Review and follow-up
  · Metrics and trend analysis
  · Operational assumptions from hazard and risk analyses
- Emergency and contingency planning and procedures
- Management of change procedures
- Training
- Decision making, conflict resolution

• Schedule
- Critical checkpoints and milestones
- Start and completion dates for tasks, reports, reviews
- Review procedures and participants

• Safety Information System
- Hazard and risk analyses, hazard logs (controls, review and feedback procedures)

  - Hazard tracking and reporting system
  - Lessons learned
  - Safety data library (documentation and files)
  - Records retention policies
- Operations hazard analysis
  - Identified hazards
  - Mitigations for hazards
- Evaluation and planned use of feedback to keep the plan up-to-date and improve it over time

12.8 Applying STAMP to Occupational Safety

Occupational safety has, traditionally, not taken a systems approach but instead has focused on individuals and changing their behavior. In applying systems theory to occupational safety, more emphasis would be placed on understanding the impact of system design on behavior and would focus on changing the system rather than people. For example, vehicles used in large plants could be equipped with speed regulators rather than depending on humans to follow speed limits and then punishing them when they do not. The same design for safety principles presented in chapter 9 for human controllers apply to designing for occupational safety.

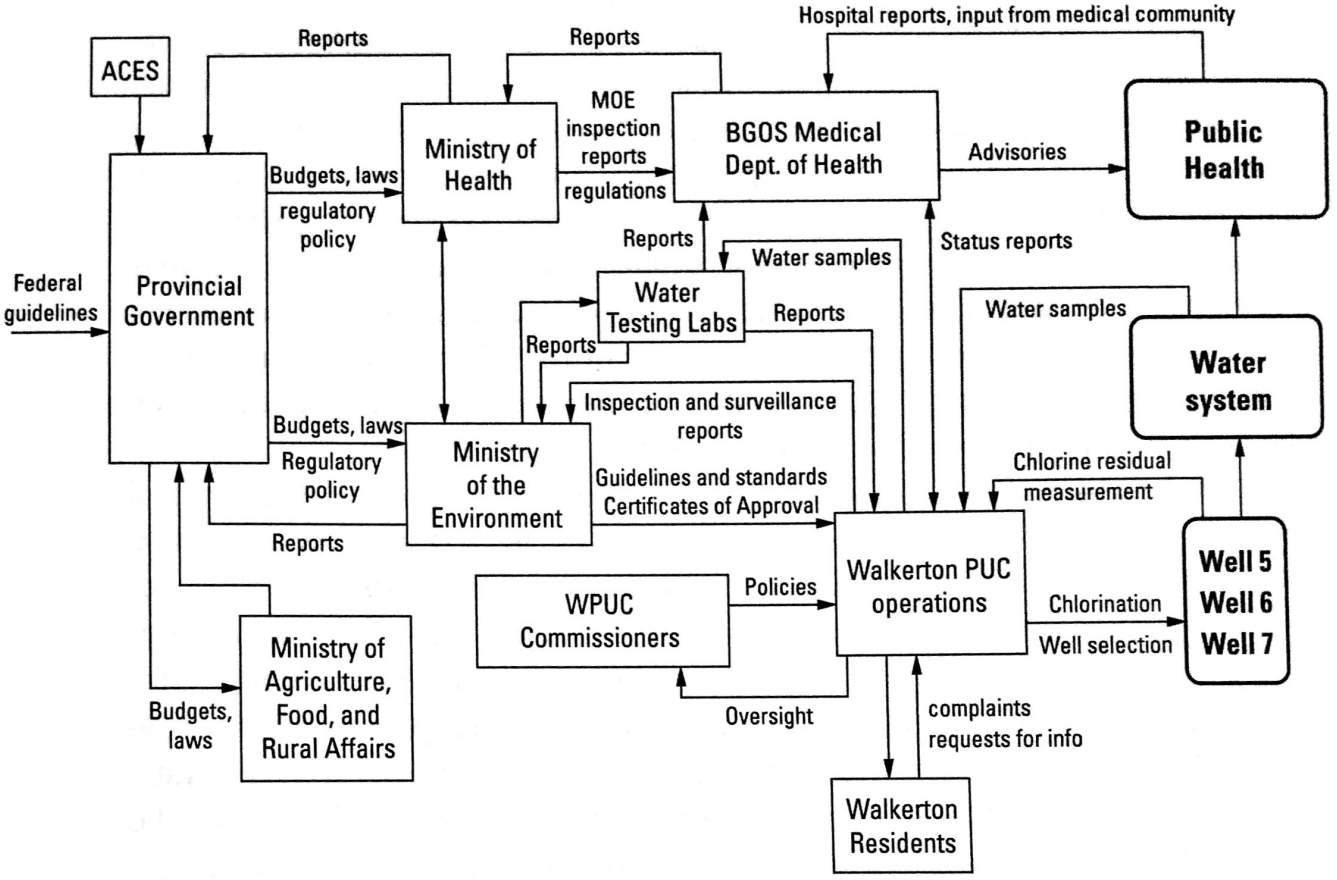
With the increasing complexity and automation of our plants, the line between occupational safety and engineering safety is blurring. By designing the system to be safe despite normal human error or judgment errors under competing work pressures, workers will be better protected against injury while fulfilling their job responsibilities.

System Hazard: Public is exposed to *E. coli* or other health related contaminants through drinking water.

System Safety Constraints: The safety control structure must prevent exposure of the public to contaminated water.

(1) Water quality must not be compromised.

(2) Public health measures must reduce risk of exposure if water quality is compromised (e.g., notification and procedures to follow)



Safety Requirements and Constraints:

Federal Government

- Establish a nationwide public health system and ensure it is operating effectively.

Provincial Government

- Establish regulatory bodies and codes of responsibilities, authority, and accountability
- Provide adequate resources to regulatory bodies to carry out their responsibilities.
- Provide oversight and feedback loops to ensure that provincial regulatory bodies are doing their job adequately.
- Ensure adequate risk assessment is conducted and effective risk management plans are in place.

Ministry of the Environment

- Ensure that those in charge of water supplies are competent to carry out their responsibilities.
- Perform inspections and surveillance. Enforce compliance if problems found.
- Perform hazard analyses to identify vulnerabilities and monitor them.
- Perform continual risk evaluation for existing facilities and establish new controls if necessary.
- Establish criteria for determining whether a well is at risk.
- Establish feedback channels for adverse test results. Provide multiple paths.
- Enforce legislation, regulations and policies applying to construction and operation of municipal water systems.
- Establish certification and training requirements for water system operators.

ACES

- Provide stakeholder and public review and input on ministry standards

Ministry of Health

- Ensure adequate procedures exist for notification and risk abatement if water quality is compromised.

Water Testing Labs

- Provide timely reports on testing results to MOE, PUC, and and Medical Dept. of Health

WPUC Commissioners

- Oversee operations to ensure water quality is not compromi

WPUC Operations Management

- Monitor operations to ensure that sample taking and report is accurate and adequate chlorination is being performed.

WPUC Operations

- Measure chlorine residuals.
- Apply adequate doses of cholorine to kill bacteria.

BGOS Medical Department of Health

- Provide oversight of drinking water quality.
- Follow up on adverse drinking water quality reports.
- Issue boil water advisories when necessary.

Figure C.1
The basic water safety control structure. Lines going into the left of a box are control lines. Lines from or to the top or bottom of a box represent information, feedback, or a physical flow. Rectangles with sharp corners are controllers, while rectangles with rounded corners represent plants.