A Systems Theoretic Approach to Safety Engineering*

Nancy Leveson, Mirna Daouk, Nicolas Dulac, Karen Marais
Massachusetts Institute of Technology

April 19, 2004

1 Introduction

A model or set of assumptions about how accidents occur lies at the foundation of all accident prevention and investigation efforts. Traditionally, accidents have been viewed as resulting from a chain of events, each directly related to its "causal" event or events. The event(s) at the beginning of the chain is labelled the *root cause*. Event-chain models, however, are limited in their ability to handle new or increasingly important factors in engineering: system accidents (arising from dysfunctional interactions among components and not just component failures), software-related accidents, complex human decision-making, and system adaptation or migration toward an accident over time [9, 12].

A systems-theoretic approach to understanding accident causation allows more complex relationships between events (e.g., feedback and indirect relationships) to be considered and also provides a way to look more deeply at why the events occurred. Accident models based on systems theory consider accidents as arising from the interactions among system components and usually do not specify single causal variables or factors [8]. Whereas industrial (occupational) safety models focus on unsafe acts or conditions and reliability engineering emphasizes failure events and the direct relationships between these events, a systems approach to safety takes a broader view of what went wrong with the system's operation or organization to allow the accident to take place. This paper provides a case study of the systems approach to safety by applying it to a water contamination accident in Walkerton, a small town in Ontario, Canada, that occurred in May 2000. About half the people in the town of 4800 became ill and seven died [15].

The general systems-theoretic approach to safety and a specific implementation called STAMP (Systems-Theoretic Accident Model and Process) are first described and then the Walkerton accident is used to show various ways that systems theory can be used to provide important information about accident causation.

2 Safety as a Emergent System Property

In response to the limitations of event-chain models, systems theory has been proposed as a way to understand accident causation (see, for example, Rasmussen [17] and Leveson [12]). Systems theory dates from the thirties and forties and was a response to the limitations of classic analysis techniques in coping with the increasingly complex systems being built [4]. The systems approach

*This research was partially supported by NSF ITR grant CCR-0085829 and by a grant from the NASA Engineering for Complex Systems Program NAG2-1543.

focuses on systems taken as a whole, not on the parts taken separately. It assumes that some properties of systems can only be treated adequately in their entirety, taking into account all facets and relating the social to the technical aspects [16]. These system properties derive from the relationships between the parts of systems: how the parts interact and fit together [1]. Thus, the systems approach concentrates on the analysis and design of the whole as distinct from the components or the parts.

The foundation of systems theory rests on two pairs of ideas: (1) *emergence* and *hierarchy* and (2) *communication* and *control* [4].

2.1 Emergence and Hierarchy

The first pair of basic system theory ideas are emergence and hierarchy. A general model of complex systems can be expressed in terms of a *hierarchy* of levels of organization, each more complex than the one below, where a level is characterized by having *emergent* properties. Emergent properties do not exist at lower levels; they are meaningless in the language appropriate to those levels. The shape of an apple, although eventually explainable in terms of the cells of the apple, has no meaning at that lower level of description. Thus, the operation of the processes at the lower levels of the hierarchy result in a higher level of complexity—that of the whole apple itself—that has emergent properties, one of them being the apple's shape. The concept of emergence is the idea that at a given level of complexity, some properties characteristic of that level (emergent at that level) are irreducible.

Safety is an emergent property of systems. Determining whether a plant is acceptably safe is not possible by examining a single valve in the plant. In fact, statements about the "safety of the valve" without information about the context in which that valve is used, are meaningless. Conclusions can be reached, however, about the reliability of the valve, where reliability is defined as the probability that the behavior of the valve will satisfy its specification over time and under given conditions. This is one of the basic distinctions between safety and reliability: Safety can only be determined by the relationship between the valve and the other plant components—that is, in the context of the whole. Therefore it is not possible to take a single system component, like a software module, in isolation and assess its safety. A component that is perfectly safe in one system may not be when used in another.

Hierarchy theory deals with the fundamental differences between one level of complexity and another. Its ultimate aim is to explain the relationships between different levels: what generates the levels, what separates them, and what links them. Emergent properties associated with a set of components at one level in a hierarchy are related to *constraints upon the degree of freedom* of those components. In a systems-theoretic view of safety, the emergent safety properties are controlled or enforced by a set of *safety constraints* related to the behavior of the system components. Safety constraints specify those relationships among system variables or components that constitute the non-hazardous or safe system states—for example, the power must never be on when the access door to the high-voltage power source is open; pilots in a combat zone must always be able to identify potential targets as hostile or friendly; and the public health system must prevent the exposure of the public to contaminated water. Accidents result from interactions among system components that violate these constraints—in other words, from a lack of appropriate constraints on system behavior.

2.2 Communication and Control

The second pair of basic systems theory ideas is communication and control. Regulatory or *control* action is the imposition of constraints upon the activity at one level of a hierarchy, which define the "laws of behavior" at that level yielding activity meaningful at a higher level. Hierarchies are characterized by control processes operating at the interfaces between levels. Checkland writes:

> Control is always associated with the imposition of constraints, and an account of a control process necessarily requires our taking into account at least two hierarchical levels. At a given level, it is often possible to describe the level by writing dynamical equations, on the assumption that one particle is representative of the collection and that the forces at other levels do not interfere. But any description of a control process entails an upper level imposing constraints upon the lower. The upper level is a source of an alternative (simpler) description of the lower level in terms of specific functions that are emergent as a result of the imposition of constraints [4, p.87].

Control in open systems (those that have inputs and outputs from their environment) implies the need for *communication*. Bertalanffy distinguished between *closed systems*, in which unchanging components settle into a state of equilibrium, and *open systems*, which can be thrown out of equilibrium by exchanges with their environment [3].

In systems theory, open systems are viewed as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control. Systems are not treated as a static design, but as a dynamic process that is continually adapting to achieve its ends and to react to changes in itself and its environment. For safety, the original design must not only enforce appropriate constraints on behavior to ensure safe operation (the enforcement of the safety constraints), but it must continue to operate safely as changes and adaptations occur over time. Accidents in systems-theoretic accident models are viewed as the result of flawed processes involving interactions among system components, including people, societal and organizational structures, engineering activities, and physical system components.

2.3 STAMP: A Systems-Theoretic Model of Accidents

Rasmussen and Svedung [17, 18] have added some features of system theory into the classic event chain model by adding hierarchical control levels above the basic event chain. As shown in Figure 1, at the social and organizational levels they use a hierarchy, with levels for government, regulators and associations, company, management, and staff. At all levels, they map information flow. The model concentrates on the operations component of the socio-technical system: information from the system design and analysis process is treated as input to the operations process. At each level, they model the factors involved using event chains, with links to the chain at the level below. Woo and Vicente applied this model to the same water contamination accident we use in this paper [20], which allows a comparison of the two approaches.

While the Rasmussen/Svedung model adds some systems theory concepts to the basic event-chain model, Leveson has defined an accident model, called STAMP (Systems-Theoretic Accident Modeling and Processes) that uses pure systems theory [12]. In STAMP, accidents are conceived as resulting not from component failures, but from inadequate control or enforcement of safety-related constraints on the design, development, and operation of the system. In the Space Shuttle *Challenger* accident, for example, the O-rings did not adequately control propellant gas release by sealing a tiny gap in the field joint. In the Mars Polar Lander loss, the software did not adequately control the descent speed of the spacecraft—it misinterpreted noise from a Hall effect sensor as an indication the spacecraft had reached the surface of the planet.

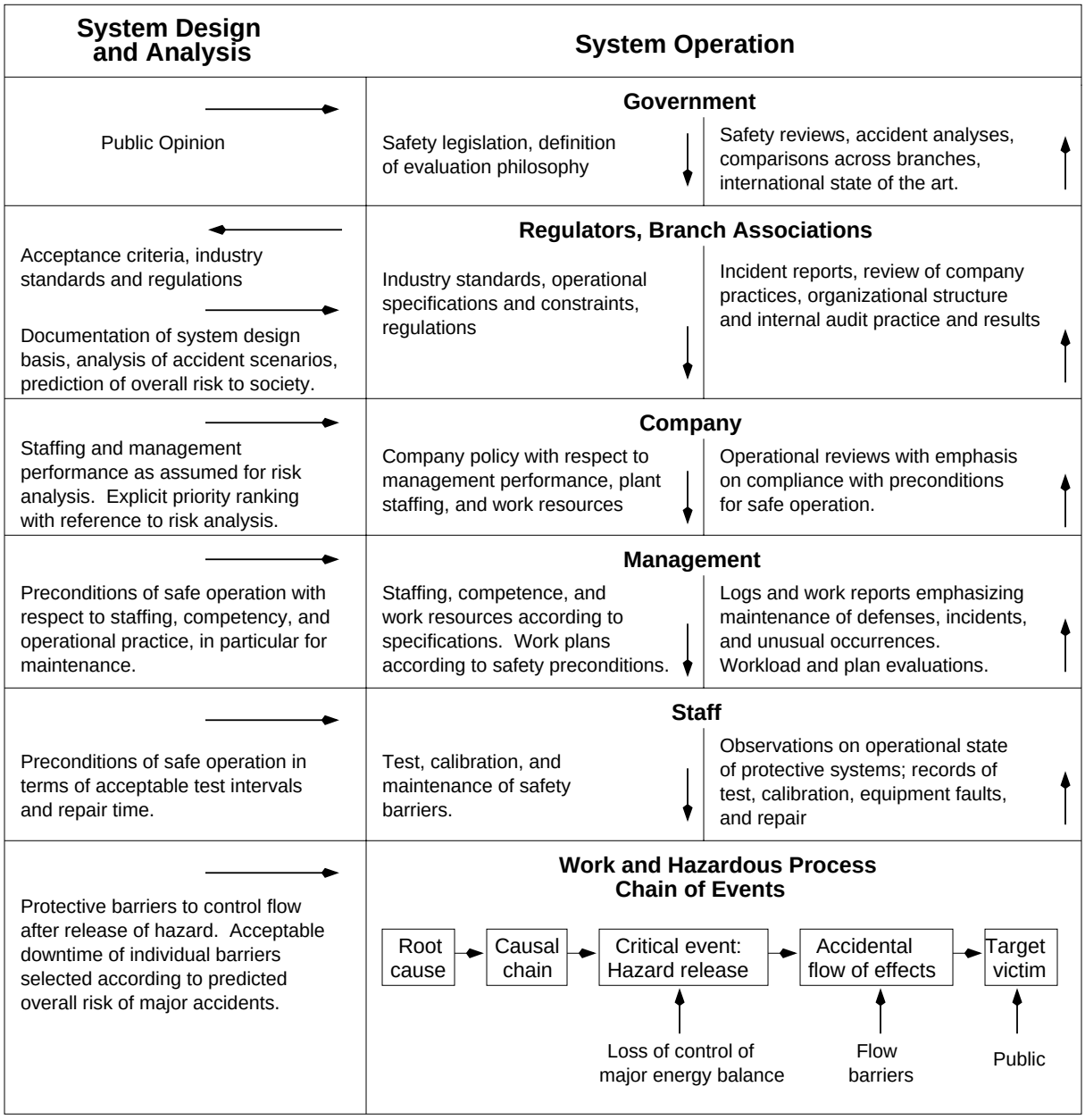


Figure 1: The Rasmussen/Svedung Model of Risk Management

Accidents such as these, involving engineering design errors, may in turn stem from inadequate control over the development process, i.e., risk is not adequately managed in the design, implementation, and manufacturing processes. Control is also imposed by the management functions in an organization—the *Challenger* accident involved inadequate controls in the launch-decision process, for example—and by the social and political system within which the organization exists.

A systems-theoretic approach to safety, such as STAMP, thus views safety as a *control problem*: accidents occur when component failures, external disturbances, and/or dysfunctional interactions among system components (including management functions) are not adequately handled. Instead of viewing accidents as the result of an initiating (root cause) event in a series of events leading to a loss, accidents are viewed as resulting from interactions among components that violate the system safety constraints. While events reflect the *effects* of dysfunctional interactions and inadequate enforcement of safety constraints, the inadequate control itself is only indirectly reflected by the events—the events are the *result* of the inadequate control. The system's hierarchical control structure must be examined to determine why the controls for each component at each hierarchical level were inadequate to maintain the constraints on safe behavior and why the events occurred—for example, why the designers arrived at an unsafe design and why management decisions were made to launch despite warnings that it might not be safe to do so.

STAMP is constructed from three basic concepts: constraints, hierarchical levels of control, and process models. These concepts, in turn, give rise to a classification of control flaws that can lead to accidents. Each of these is described below.

2.4 Constraints and Hierarchical Levels of Control

The most basic concept in STAMP is not an event, but a constraint. In systems theory or control theory, systems are viewed as hierarchical structures where each level imposes constraints on the activity of the level beneath it—that is, constraints or lack of constraints at a higher level allow or control lower-level behavior [4]. Safety-related constraints specify those relationships among system variables that constitute the nonhazardous or safe system states—for example, the power must never be on when the access door to the high-voltage power source is open; pilots in a combat zone must always be able to identify potential targets as hostile or friendly; and the public health system must prevent the exposure of the public to contaminated water. The control processes that enforce these constraints must limit system behavior to the safe changes and adaptations implied by the constraints.

This definition of accidents fits both classic component failure accidents as well as system accidents. Note that a separate "controller" is not required. Component failures may be controlled through design, e.g., redundancy, interlocks, and fail-safe design methods. They may also be controlled through process, e.g., manufacturing processes and procedures or maintenance procedures. But it does imply the need to enforce the safety constraints in some way, and it includes system components that do not "fail" in the way that physical components do..

Figure 2 shows a generic hierarchical control model. Accidents result from inadequate enforcement of constraints on behavior (e.g., the physical system, engineering design, management, and regulatory behavior) at each level of the socio-technical system.

The model in Figure 2 has two basic hierarchical control structures—one for system development (on the left) and one for system operation (on the right)—with interactions between them. An aircraft manufacturer, for example, might only have system development under its immediate control, but safety involves both development and operational use of the aircraft, and neither can be accomplished successfully in isolation: Safety must be designed into the system, and safety during operation depends partly on the original design and partly on effective control over opera-

tions. Manufacturers must communicate to their customers the assumptions about the operational environment upon which the safety analysis was based, as well as information about safe operating procedures. The operational environment, in turn, provides feedback to the manufacturer about the performance of the system during operations.

Between the hierarchical levels of each control structure, effective communication channels are needed, both a downward *reference* channel providing the information necessary to impose constraints on the level below and a *measuring* channel to provide feedback about how effectively the constraints were enforced. For example, company management in the development process structure may provide a safety policy, standards, and resources to project management and in return receive status reports, risk assessment, and incident reports as feedback about the status of the project with respect to the safety constraints.

The safety control structure often changes over time, which accounts for the observation that accidents in complex systems frequently involve a migration of the system toward a state where a small deviation (in the physical system or in human operator behavior) can lead to a catastrophe. The foundation for an accident is often laid years before. One event may trigger the loss, but if that event had not happened, another one would have. Union Carbide and the Indian government blamed the Bhopal MIC (methyl isocyanate) release (among the worst industrial accidents in history) on human error—the improper cleaning of a pipe at the chemical plant. However, the maintenance worker was, in fact, only a minor and somewhat irrelevant player in the loss [9]. Instead, degradation in the safety margin occurred over time and without any particular single decision to do so but simply as a series of decisions that moved the plant slowly toward a situation where any slight error would lead to a major accident:

> The stage for an accidental course of events very likely is prepared through time by the normal efforts of many actors in their respective daily work context, responding to the standing request to be more productive and less costly. Ultimately, a quite normal variation in somebody's behavior can then release an accident. Had this 'root cause' been avoided by some additional safety measure, the accident would very likely be released by another cause at another point in time. In other words, an explanation of the accident in terms of events, acts, and errors is not very useful for design of improved systems [17].

Degradation of the safety-control structure over time may be related to *asynchronous evolution* [8], where one part of a system changes without the related necessary changes in other parts. Changes to subsystems may be carefully designed, but consideration of their effects on other parts of the system, including the control aspects, may be neglected or inadequate. Asynchronous evolution may also occur when one part of a properly designed system deteriorates. In both these cases, the erroneous expectations of users or system components about the behavior of the changed or degraded subsystem may lead to accidents. The Ariane 5 trajectory changed from that of the Ariane 4, but the inertial reference system software did not [13]. One factor in the loss of contact with the SOHO (SOlar Heliospheric Observatory) spacecraft in 1998 was the failure to communicate to operators that a functional change had been made in a procedure to perform gyro spin-down [14]. One factor in the accidental friendly fire shootdown of a U.S. Army Blackhawk helicopter by the U.S. Air Force fighter over northern Iraq in 1996 was that the Air Force had upgraded their radio technology while the Army had not, thus violating the safety constraint that U.S. forces would be able to communicate by radio [10].

In the analysis of an accident using STAMP, the required constraints to provide safe behavior are first identified for each level of the control structure and then the socio-technical control structure is examined to determine if and how the constraints were to be enforced and why the controls

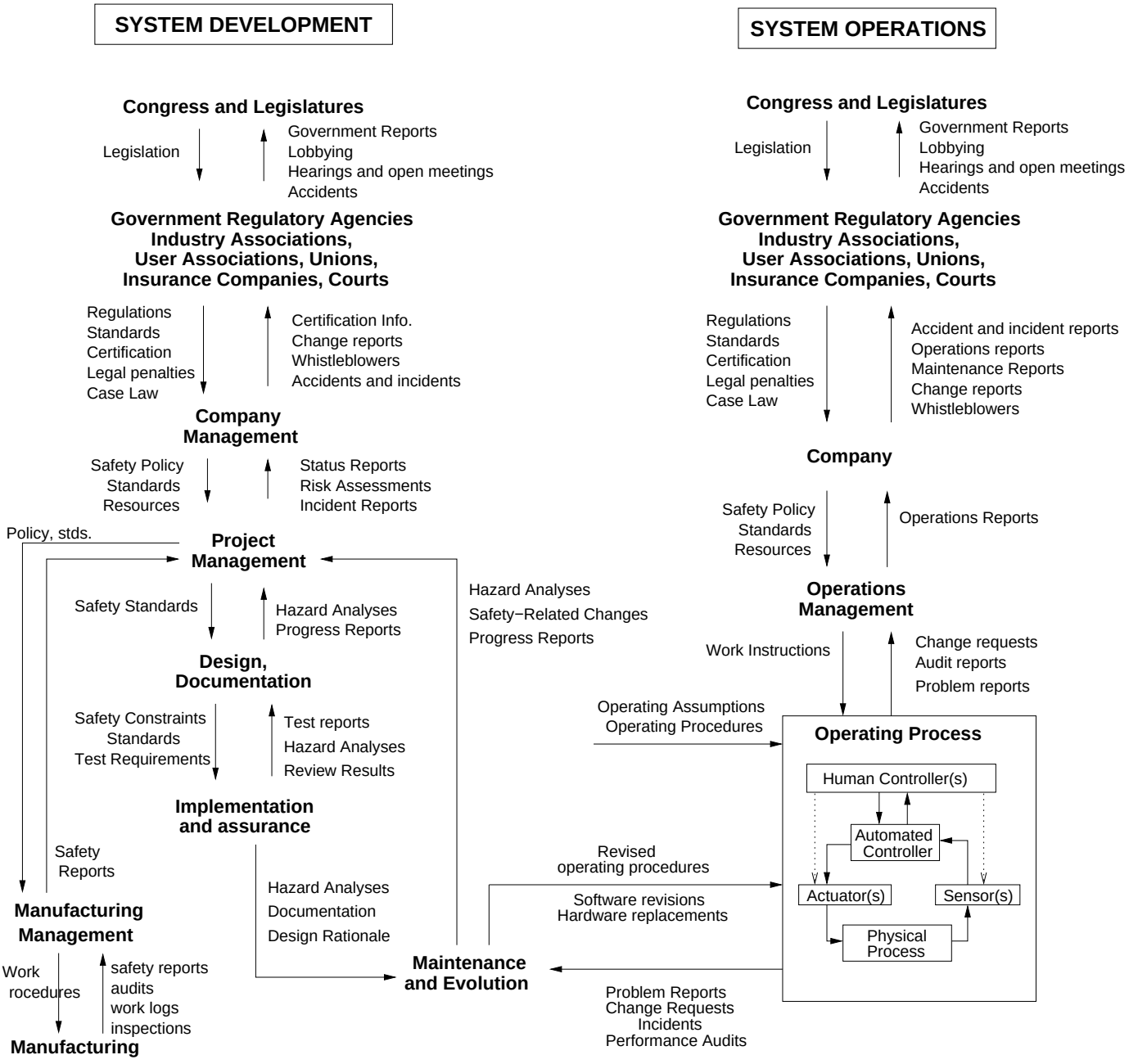


Figure 2: General Form of a Model of Socio-Technical Control.

established to enforce them were ineffective in that particular instance. If the controls had once been potentially effective but had degraded over time, the reasons for that degradation are identified.

2.5 Process Models

Besides constraints and hierarchical levels of control, a third basic concept in STAMP is that of process models. In basic systems theory, to effect control over a system requires four conditions [2, 5]:

- **Goal Condition**: The controller must have a goal or goals, e.g., to maintain the setpoint or to maintain the safety constraints.
- **Action Condition**: The controller must be able to affect the state of the system in order to keep the process operating within predefined limits or safety constraints despite internal or external disturbances. Where there are multiple controllers and decision makers, the actions must be coordinated to achieve the goal condition. Uncoordinated actions are particularly likely to lead to accidents in the boundary areas between controlled processes or when multiple controllers have overlapping control responsibilities.
- **Model Condition**: The controller must be (or contain) a model of the system. Accidents in complex systems frequently result from inconsistencies between the model of the process used by the controllers (both human and automated) and the actual process state; for example, the software thinks the aircraft is climbing when it is actually descending and as a result applies the wrong control law or the pilot thinks a friendly aircraft is hostile and shoots a missile at it. Whether the model is embedded in the control logic of an automated controller or in the mental model of a human controller, it must contain the same type of information: the required relationship among the system variables (the control laws), the current state (the current values of the system variables), and the ways the process can change state.
- **Observability Condition**: The controller must be able to ascertain the state of the system from information about the process state provided by *feedback*. Feedback is used to update and maintain the process model used by the controller.

Using systems theory, accidents can be understood in terms of failure to adequately satisfy these four conditions:

1. Hazards and the safety constraints to prevent them are not identified and provided to the controllers (goal condition);
2. The controllers are not able to effectively maintain the safety constraints or they do not make appropriate or effective control actions for some reason, perhaps because of inadequate coordination among multiple controllers (action condition);
3. The process models used by the automation or human controllers (usually called mental models in the case of humans) become inconsistent with the process and with each other (model condition); and
4. The controller is unable to ascertain the state of the system and update the process models because feedback is missing or inadequate (observability condition).

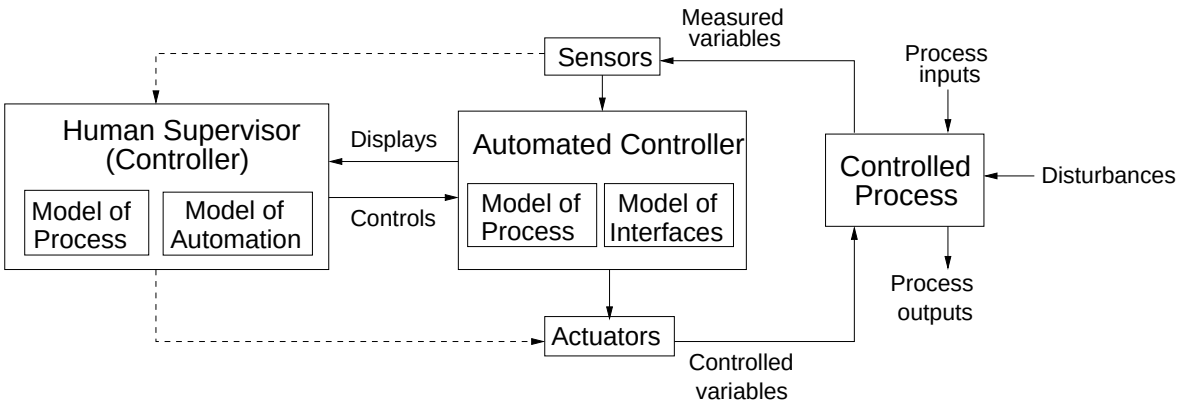


Figure 3: A standard hierarchical three-level control loop. The hierarchy is turned on its side, which is a more common notation in control theory.

Note that accidents caused by basic component failures are included here. Identifying the failure events themselves, however, does not provide enough information about why they occurred to prevent similar accidents in the future. Component failures may result from inadequate constraints on the manufacturing process; inadequate engineering design such as missing or incorrectly implemented fault tolerance; lack of correspondence between individual component capacity (including humans) and task requirements; unhandled environmental disturbances (e.g., EMI); inadequate maintenance, including preventive maintenance; physical degradation over time (wearout), etc. STAMP goes beyond simply blaming component failure for accidents and requires that the reasons be identified for why those failures can occur and lead to an accident. STAMP also provides a model for accidents that result from interactions among the components and not from individual component failure.

Figure 3 shows a typical control loop. Control actions will, in general, lag in their effects on the process because of delays in signal propagation around the control loop: an actuator may not respond immediately to an external command signal (called *dead time*); the process may have delays in responding to manipulated variables (*time constants*); and the sensors may obtain values only at certain sampling intervals (*feedback delays*). Time lags restrict the speed and extent with which the effects of disturbances, both within the process itself and externally derived, can be reduced. They also impose extra requirements on the controller, for example, the need to infer delays that are not directly observable. Accidents can occur due to inadequate handling of these delays.

In STAMP, the four control flaws identified above, plus time lags, are used in understanding and preventing accidents. Figure 4 shows the factors that can lead to these control flaws. We are using these factors to create a new type of hazard analysis based on the STAMP accident model [11].

The rest of the paper provides a case study of the application of a systems-theoretic approach to safety using the STAMP model of accidents.

3 The Basic Events at Walkerton

The accident occurred in May 2000 in the small town of Walkerton, Ontario, Canada. Some contaminants, largely Escherichia coli O157:H7 (the common abbreviation for which is E. coli)

- **Inadequate Control Actions**
  - Design of control algorithm (process) does not enforce constraints
  - Process models inconsistent, incomplete, or incorrect (lack of linkup)
    - Flaw(s) in creation or updating process
    - Inadequate or missing feedback
      - Not provided in system design
      - Communication flaw
      - Inadequate sensor operation (incorrect or no information provided)
    - Time lags and measurement inaccuracies not accounted for
  - Inadequate coordination among controllers and decision−makers (boundary and overlap areas)
- **Inadequate Execution of Control Actions**
  - Communication flaw
  - Inadequate "actuator" operation
  - Time lag

Figure 4: General accident causal factors based on the STAMP model of accidents, that is, the factors leading to inadequate enforcement of the safety constraints.

and Campylobacter jejuni entered the Walkerton water system through a well of the Walkerton municipal water system.

The Walkerton water system was operated by the Walkerton Public Utilities Commission (WPUC). Stan Koebel was the WPUC's general manager and his brother Frank its foreman. In May 2000, the water system was supplied by three groundwater sources: Wells 5, 6, and 7. The water pumped from each well was treated with chlorine before entering the distribution system.

The source of the contamination was manure that had been spread on a farm near Well 5. Unusually heavy rains from May 8 to May 12 carried the bacteria to the well. Between May 13 and May 15, Frank Koebel checked Well 5 but did not take measurements of chlorine residuals, although daily checks were supposed to be made.[1] Well 5 was turned off on May 15.

On the morning of May 15, Stan Koebel returned to work after having been away from Walkerton for more than a week. He turned on Well 7, but shortly after doing so, he learned a new chlorinator for Well 7 had not been installed and the well was therefore pumping unchlorinated water directly into the distribution system. He did not turn off the well, but instead allowed it to operate without chlorination until noon on Friday May 19, when the new chlorinator was installed.

On May 15, samples from the Walkerton water distribution system were sent to A&L Labs for testing according to the normal procedure. On May 17, A&L Labs advised Stan Koebel that samples from May 15 tested positive for E. coli and total coliforms. The next day (May 18) the first symptoms of widespread illness appeared in the community. Public inquiries about the water prompted assurances by Stan Koebel that the water was safe. By May 19 the scope of the outbreak had grown, and a pediatrician contacted the local health unit with a suspicion that she was seeing patients with symptoms of E. coli.

The Bruce-Grey-Owen Sound (BGOS) Health Unit (the government unit responsible for public health in the area) began an investigation. In two separate calls placed to Stan Koebel, the health

[1] Low chlorine residuals are a sign that contamination is overwhelming the disinfectant capacity of the chlorination process.

officials were told that the water was "okay." At that time, Stan Koebel did not disclose the lab results from May 15, but he did start to flush and superchlorinate the system to try to destroy any contaminants in the water. The chlorine residuals began to recover. Apparently, Mr. Koebel did not disclose the lab results for a combination of two reasons: he did not want to reveal the unsafe practices he had engaged in from May 15 to May 17 (i.e., running Well 7 without chlorination), and he did not understand the serious and potentially fatal consequences of the presence of E. coli in the water system. He continued to flush and superchlorinate the water through the following weekend, successfully increasing the chlorine residuals. Ironically, it was not the operation of Well 7 without a chlorinator that caused the contamination; the contamination instead entered the system through Well 5 from May 12 until it was shut down May 15.

On May 20, the first positive test for E. coli infection was reported and the BGOS Health Unit called Stan Koebel twice to determine whether the infection might be linked to the water system. Both times, Stan Koebel reported acceptable chlorine residuals and failed to disclose the adverse test results. The Health Unit assured the public that the water was safe based on the assurances of Mr. Koebel.

That same day, a WPUC employee placed an anonymous call to the Ministry of the Environment (MOE) Spills Action Center, which acts as an emergency call center, reporting the adverse test results from May 15. On contacting Mr. Koebel, the MOE was given an evasive answer and Mr. Koebel still did not reveal that contaminated samples had been found in the water distribution system. The Local Medical Officer was contacted by the health unit, and he took over the investigation. The health unit took their own water samples and delivered them to the Ministry of Health laboratory in London (Ontario) for microbiological testing.

When asked by the MOE for documentation, Stan Koebel finally produced the adverse test results from A&L Laboratory and the daily operating sheets for Wells 5 and 6, but said he could not produce the sheet for Well 7 until the next day. Later, he instructed his brother Frank to revise the Well 7 sheet with the intention of concealing the fact that Well 7 had operated without a chlorinator. On Tuesday May 23, Stan Koebel provided the altered daily operating sheet to the MOE. That same day, the health unit learned that two of the water samples it had collected on May 21 had tested positive for E. coli.

Without waiting for its own samples to be returned, the BGOS health unit on May 21 issued a boil water advisory on local radio. About half of Walkerton's residents became aware of the advisory on May 21, with some members of the public still drinking the Walkerton town water as late as May 23. The first person died on May 22, a second on May 23, and two more on May 24. During this time, many children became seriously ill and some victims will probably experience lasting damage to their kidneys as well as other long-term health effects. In all, seven people died and more than 2300 became ill.

Looking only at these proximate events and connecting them by some type of causal chain, it appears that this is a simple case of incompetence, negligence, and dishonesty by WPUC employees. In fact, the government representatives argued at the accident inquiry that Stan Koebel or the Walkerton Public Utilities Commission (PUC) were solely responsible for the outbreak and that they were the only ones who could have prevented it. In May 2003, exactly three years after the accident, Stan and Frank Koebel were arrested for their part in the loss. But a systems-theoretic analysis using STAMP provides a much more informative and useful understanding of the accident besides simply blaming it only on the actions of Koebel brothers.

4 A Systems-Theoretic Explanation of the Walkerton Accident

The first step in creating a STAMP analysis is to identify the system hazards, the system safety constraints, and the hierarchical control structure in place to enforce the constraints.

The system hazard related to the Walkerton accident is public exposure to E. coli or other health-related contaminants through drinking water. This hazard leads to the following system safety constraint:

> *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., boil water advisories).*

Each component of the socio-technical public water system safety control structure (shown in Figure 5) plays a role in enforcing this general system safety constraint and will, in turn, have its own safety constraints to enforce that are related to the function of the particular component in the overall system. For example, the Canadian federal government is responsible for establishing a nationwide public health system and ensuring it is operating effectively. Federal guidelines are provided to the Provinces, but responsibility for water quality is primarily delegated to each individual Province.

The provincial governments are responsible for regulating and overseeing the safety of the drinking water. They do this by providing budgets to the ministries involved—in Ontario these are the Ministry of the Environment (MOE), the Ministry of Health (MOH), and the Ministry of Agriculture, Food, and Rural Affairs—and by passing laws and adopting government policies affecting water safety.

According to the report on the official Inquiry into the Walkerton accident [15], the Ministry of Agriculture, Food, and Rural Affairs in Ontario is responsible for regulating agricultural activities with potential impact on drinking water sources. In fact, there was no watershed protection plan to protect the water system from agricultural runoff. Instead, the Ministry of the Environment was responsible for ensuring that the water systems could not be affected by such runoff.

The Ministry of the Environment (MOE) has primary responsibility for regulating and for enforcing legislation, regulations, and policies that apply to the construction and operation of municipal water systems. Guidelines and objectives are set by the MOE, based on Federal guidelines. They are enforceable through Certificates of Approval issued to public water utilities operators, under the Ontario Water Resources Act. The MOE also has legislative responsibility for building and maintaining water treatment plants and has responsibility for public water system inspections and drinking water surveillance, for setting standards for certification of water systems, and for continuing education requirements for operators to maintain competence as knowledge about water safety increases.

The Ministry of Health supervises local Health Units, in this case, the Bruce-Grey-Owen-Sound (BGOS) Department of Health, run by local Officers of Health in executing their role in protecting public health. The BGOS Medical Dept. of Health receives inputs from various sources, including hospitals, the local medical community, the Ministry of Health, and the Walkerton Public Utilities Commission, and in turn is responsible for issuing advisories and alerts if required to protect public health. Upon receiving adverse water quality reports from the government testing labs or the MOE, the local public health inspector in Walkerton would normally contact the WPUC to ensure that followup samples were taken and chlorine residuals maintained.

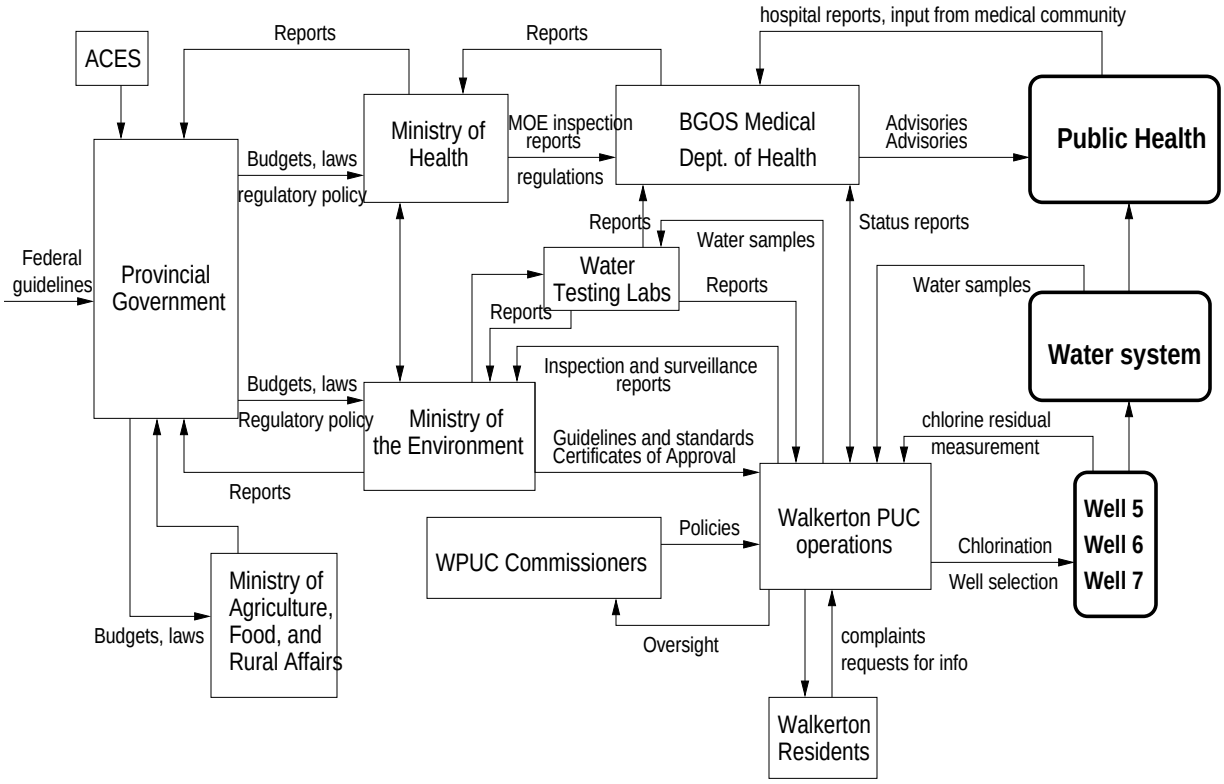
The public water system in Walkerton is run by the Walkerton Public Utilities Commission (WPUC), which operates the wells and is responsible for chlorination and for measurement of

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 compromised.

WPUC Operations Management

- Monitor operations to ensure that sample taking and reporting 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 5: The Basic Water Safety Control Structure. The hierarchical control structure is drawn here using the more common control notation from left to right rather than top to bottom as in Figure 2. 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.

chlorine residuals. Oversight of the WPUC is provided by elected WPUC Commissioners. The Commissioners are responsible for establishing and controlling the policies under which the PUC operates, while the general manager (Stan Koebel) and staff are responsible for administering these policies in operating the water facility. Although theoretically also responsible for the public water system, the municipality left the operation of the water system to the WPUC.

Together, the safety constraints enforced by all of these system control components must be adequate to enforce the overall system safety constraints. Figure 5 shows the overall theoretical water safety control structure in Ontario and the safety-related requirements and constraints for each system component.

Each component of the socio-technical public water safety system plays a role in enforcing the overall system safety constraint. Understanding the accident requires understanding the role in the accident scenario played by each level of the system's hierarchical control structure by not adequately enforcing its part of the safety constraint. The inadequate control (in terms of enforcing the safety constraints) exhibited by each component in the Walkerton accident is described in Sections 4.1, through 4.5. For each component, the contribution to the accident is described in terms of the four conditions required for adequate control, i.e., the goal (safety requirements and constraints), the actions (inadequate control actions and control algorithms), the process or mental models, and feedback. At each level of control, the context in which the behaviors took place is also considered. It is not possible to understand human behavior without knowing the context in which it occurs and the behavior-shaping factors in the environment.

This first level of analysis provides a view of the limitations of the static control structure at the time of the accident. But systems are not static—they adapt and change over time. In STAMP, a system is treated as a dynamic process that is continually adapting to achieve its ends and to react to changes in itself and its environment. The original system design must not only enforce the system safety constraints, but the system must continue to enforce the constraints as changes occur. The analysis of accidents, therefore, requires understanding not only the flaws in the static control structure that allowed the safety constraints to be violated but also the changes to the safety control structure over time (the *structural dynamics*) and the dynamic processes behind these changes (the *behavioral dynamics*). Section 4.6 analyzes the structural dynamics of the Walkerton accident while Section 4.7 shows the behavioral dynamics.

4.1 The Physical Process View of the Accident

As in many *system accidents*, there were no physical failures involved. If, as in Figure 6, we draw the boundary of the physical system around the wells, the public water system, and public health, then one can describe the "cause" of the accident at the physical system level as the inability of the physical design to enforce the physical safety constraint in the face of an environmental disturbance, i.e., the unusually heavy rains that resulted in the transport of contaminants from the fields to the water supply. The safety constraint being enforced at this level is that water must be free from unacceptable levels of contaminants.

Well 5 was a very shallow well: all of its water was drawn from an area between 5m and 8m below the surface. More significantly, the water was drawn from an area of bedrock, and the shallowness of the soil overburden above the bedrock along with the fractured and porous nature of the bedrock itself made it possible for surface bacteria to make its way to Well 5.

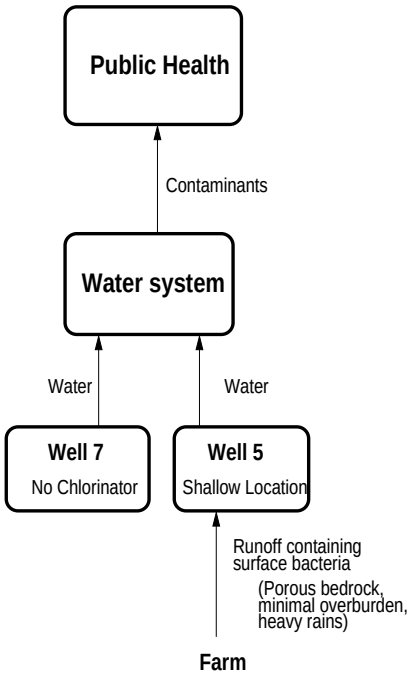


Figure 6: The Physical Components of the Water Safety Control Structure.

4.2 The First Level Operations

Besides the physical system analysis, most hazard analysis techniques and accident investigations consider the immediate operators of the system. Figure 7 shows the results of a STAMP analysis of the flaws by the lower operations levels at Walkerton that were involved in the accident.

The safety requirements and constraints on the operators of the local water system were that (1) they must apply adequate doses of chlorine to kill bacteria and (2) they must measure chlorine residuals. Stan Koebel, the WPUC Manager, and Frank Koebel, its foreman, were not qualified to hold their positions within the WPUC. Before 1993, there were no mandatory certification requirements and after 1993 they were certified through a grandfathering process based solely on experience. Mr. Koebel knew how to operate the water system mechanically, but he lacked knowledge about the health risks associated with a failure to properly operate the system and of the importance of following the requirements for treatment and monitoring of the water quality. The inquiry report stated that many improper operating practices had been going on for years before Stan Koebel became manager: He simply left them in place. These practices, some of which went back 20 years, included misstating the locations at which samples for microbial testing were taken, operating wells without chlorination, making false entries in daily operating sheets, not measuring chlorine residuals daily, not adequately chlorinating the water, and submitting false annual reports to the MOE.

The operators of the Walkerton water system did not intentionally put the public at risk. Stan Koebel and the other WPUC employees believed the untreated water was safe and often drank it themselves at the well sites. Local residents also pressed the WPUC to decrease the amount of chlorine used because they objected to the taste of chlorinated water.

A second first-level control component was the Local Health Units, in this case, the Bruce-Grey-

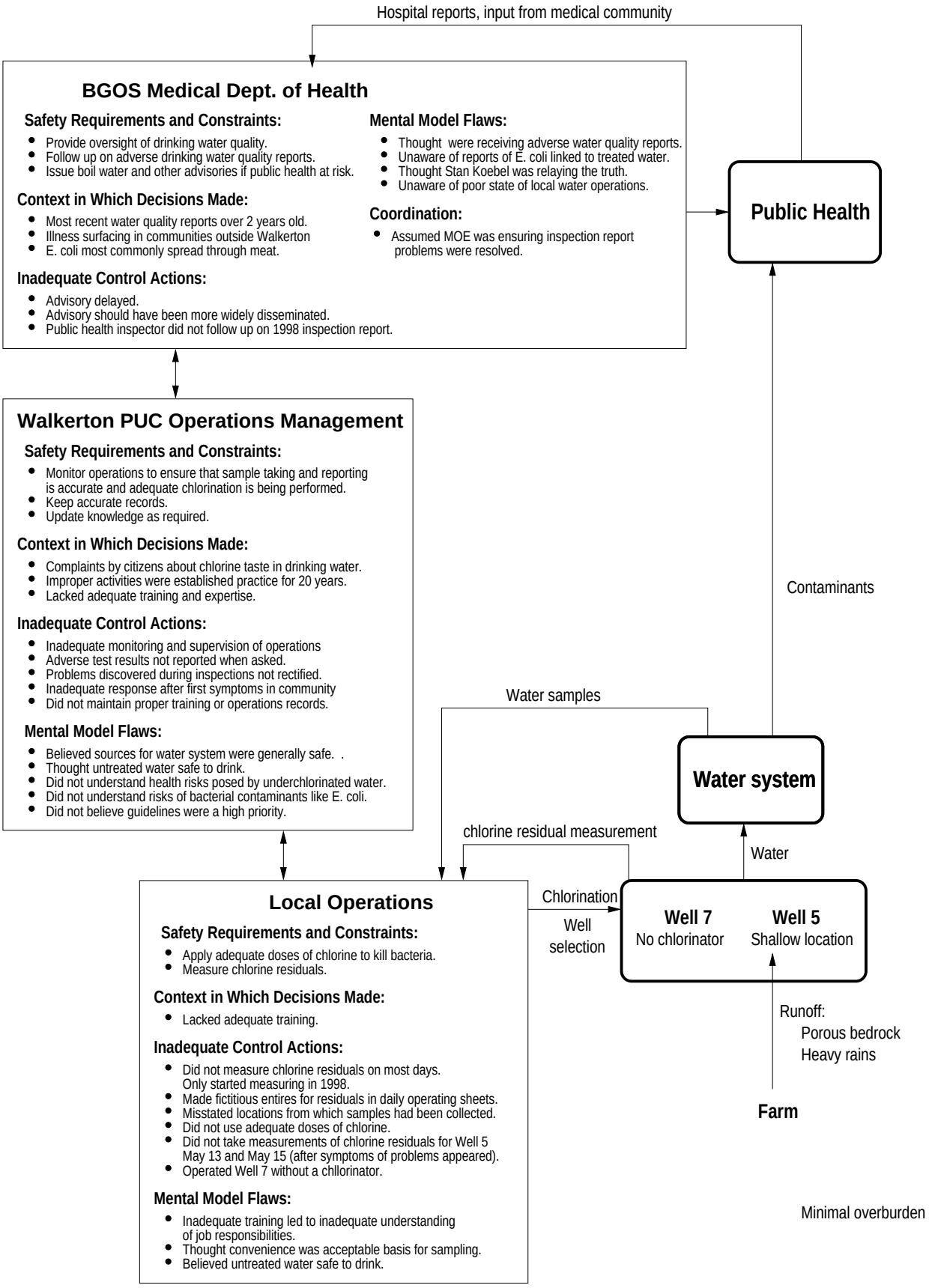


Figure 7: The Physical and Operational Components of the Water Safety Control Structure.

Owen-Sound (BGOS) Department of Health. Local Health Units are supervised by the Ministry of Health and run by local Officers of Health to execute their role in protecting public health. The BGOS Medical Dept. of Health receives inputs (feedback) from various sources, including hospitals, the local medical community, the Ministry of Health, and the WPUC, and in turn is responsible for issuing advisories and alerts if required to protect public health. While the local Health Unit did issue a boil water advisory on local radio when they finally decided that the water system might be involved, this means of notifying the public was not very effective—other more effective means could have been employed. One reason for the delay was simply that evidence was not strong that the water system was the source of the contamination. E. coli is not often spread by meat, thus its common reference as the "hamburger disease." In addition, some reported cases of illness came from people who did not live in the Walkerton water district. Finally, the local health inspector had no reason to believe that there were problems with the way the Walkerton water system was operated.

An important event related to the accident occurred in 1996, when the government water testing laboratories were privatized. Previously, water samples were sent to government laboratories for testing. These labs then shared the results with the appropriate government agencies as well as the local operators. Upon receiving adverse water quality reports from the government testing labs or the MOE, the local public health inspector in Walkerton would contact the WPUC to ensure that followup samples were taken and chlorine residuals maintained.

After water testing laboratory services for municipalities were assumed by the private sector in 1996, the MOH Health Unit for the Walkerton area sought assurances from the MOE's local office that the Health Unit would continue to be notified of all adverse water quality results relating to community water systems. It received that assurance, both in correspondence and at a meeting, but it did not receive adverse water test reports and, therefore, without feedback about any problems in the water system, the local public health authorities assumed everything was fine.

In fact, there *were* warnings of problems. Between January and April of 2000 (the months just prior to the May E. Coli outbreak), the lab that tested Walkerton's water repeatedly detected coliform bacteria—an indication that surface water was getting into the water supply. The lab notified the MOE on five separate occasions. The MOE in turn phoned the WPUC, was assured the problems were being fixed, and let it go at that. The MOE did not inform the local Walkerton Medical Office of Health, however, as by law it was required to do.

The WPUC changed water testing laboratories in May 2000. The new laboratory, A&L Canada Laboratories East, was unaware of any notification guidelines. In fact, they considered test results to be confidential and thus improper to send to anyone but the client (in this case, the WPUC manager Stan Koebel).

In 1998, the BGOS Health Unit did receive a report on an MOE inspection of the Walkerton water system that showed some serious problems did exist. When the local Walkerton public health inspector read the report, he filed it, assuming that the MOE would ensure that the problems identified were properly addressed. Note the coordination problems here in an area of overlapping control. Both the MOE and the local public health inspector should have followed up on the 1998 inspection report, but there was no written protocol instructing the public health inspector on how to respond to adverse water quality or water system inspection reports. The MOE also lacked such protocols. Once again, the local public health authorities received no feedback that indicated water system operations were problematic.

Looking only at the physical system and local operations, it appears that the accident was simply the result of incompetent water system operators, who initially lied to protect their jobs (but who were unaware of the potentially fatal consequences of their lies) made worse by an inadequate response by the local Health Unit. If the goal is to find someone to blame, this conclusion is

reasonable. If, however, the goal is to understand why the accident occurred in order to make effective changes (beyond simply firing the Koebel brothers) in order to prevent repetitions in the future or to learn how to prevent accidents in other situations, then a more complete study of the larger water safety control structure within which the local operations is embedded is necessary.

4.3 Municipal Government

Figure 8 summarizes the flaws in the municipal water system control structure that allowed the dysfunctional interactions and thus the accident to occur.

Operating conditions on the public water system should theoretically have been imposed by the municipality, the Walkerton Public Utilities Commissioners, and the manager of the WPUC. The municipality left the operation of the water system to the WPUC. The WPUC Commissioners, who were elected, became over the years more focused on the finances of the PUC than the operations. They had little or no training or knowledge of water system operations or even water quality itself. Without such knowledge and with their focus on financial issues, they gave all responsibility for operations to the manager of the WPUC (Stan Koebel) and provided no other operational oversight.

The WPUC Commissioners received a copy of the 1998 inspection report but did nothing beyond asking for an explanation from Stan Koebel and accepting his word that he would correct the deficient practices. They never followed up to make sure he did. The mayor of Walkerton and the municipality also received the report but they assumed the WPUC would take care of the problems.

4.4 The Provincial Regulatory Agencies (Ministries)

The Ministry of the Environment (MOE) has primary responsibility for regulating and for enforcing legislation, regulations, and policies that apply to the construction and operation of municipal water systems. Guidelines and objectives are set by the MOE, based on Federal guidelines. They are enforceable through Certificates of Approval issued to public water utilities operators, under the Ontario Water Resources Act.

Walkerton Well 5 was built in 1978 and issued a Certificate of Approval by the MOE in 1979. Despite potential problems—the groundwater supplying the well was recognized as being vulnerable to surface contamination—no explicit operating conditions were imposed at the time.

Although the original Certificate of Approval for Well 5 did not include any special operating conditions, over time MOE practices changed. By 1992, the MOE had developed a set of model operating conditions for water treatment and monitoring that were routinely attached to new Certificates of Approval for municipal water systems. There was no effort, however, to determine whether such conditions should be attached to existing certificates, such as the one for Well 5.

The Provincial water quality guidelines were amended in 1994 to require the continuous monitoring of chlorine residuals and turbidity for wells supplied by a groundwater source that was under the direct influence of surface water (as was Walkerton's Well 5). Automatic monitoring and shutoff valves would have mitigated the operational problems at Walkerton and prevented the deaths and illness associated with the E. coli contamination in May 2000 if the requirement had been enforced in existing wells. However, at the time, there was no program or policy to review existing wells to determine whether they met the requirements for continuous monitoring. In addition, MOE inspectors were not directed to notify well operators (like the Koebel brothers) of the new requirement nor to assess during inspections if a well required continuous monitoring.

Stan and Frank Koebel lacked the training and expertise to identify the vulnerability of Well 5 themselves and to understand the resulting need for continuous chlorine residual and turbidity

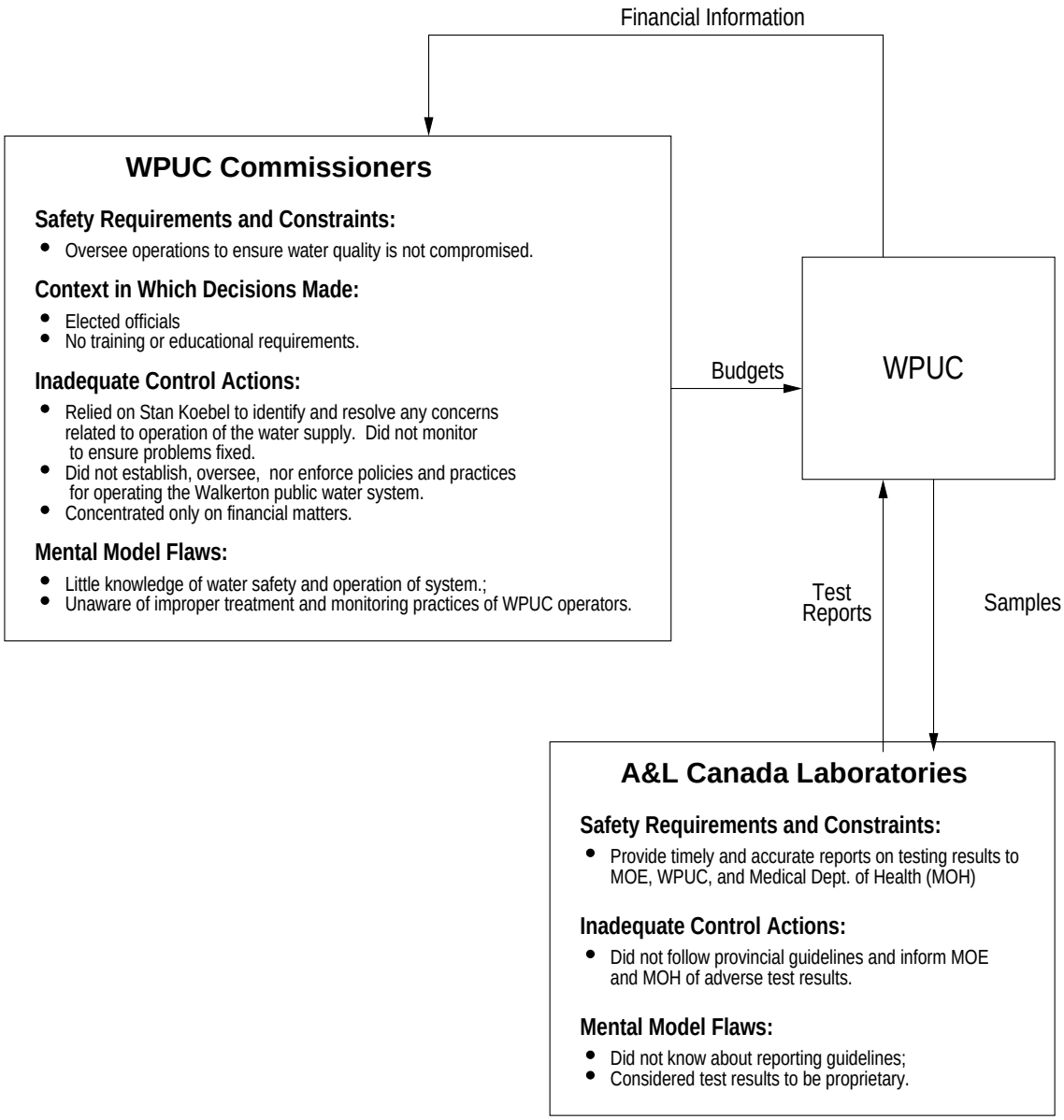


Figure 8: The Municipal Control Structure and Its Contribution to the Accident.

Ministry of the Environment

Safety Requirements and Constraints:

- Ensure those in charge of water supplies are competent to carry out their responsibilities.
- Perform inspections and enforce compliance if problems found.
- Perform hazard analyses to provide information about where vulnerabilities are and monitor them.
- Perform continual risk evaluation of 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 so that dysfunctional paths cannot prevent reporting.
- Enforce legislation, regulations, and policies applying to construction and operation of municipal water systems.
- Establish certification and training requirements for water system operators.

Context in Which Decisions Made:

- Critical information about history of known vulnerable water sources not easily accessible.
- Budget cuts and staff reductions

Inadequate Control Actions:

- No legally enforceable measures taken to ensure that concerns identified in inspections are addressed. Weak response to repeated violations uncovered in periodic inspections.
- Relied on voluntary compliance with regulations and guidelines.
- No systematic review of existing certificates of approval to determine if conditions should be added for continuous monitoring.
- Did not retroactively apply new approvals program to older facilities when procedures changed in 1992.
- Did not require continuous monitoring of existing facilities when ODWO amended in 1994.
- MOE inspectors not directed to assess existing wells during inspections.
- MOE inspectors not provided with criteria for determining whether a given well was at risk. Not directed to examine daily operating sheets.
- Inadequate inspections and improperly structured and administered inspection program..
- Approval of Well 5 without attaching operating conditions or special monitoring or inspection requirements.
- No followup on inspection reports noting serious deficiencies.
- Did not inform Walkerton Medical Officer of Health about adverse test results in January to April 2000 as required to do.
- Private labs not informed about reporting guidelines.
- No certification or training requirements for grandfathered operators.
- No enforcement of continuing training requirements.
- Inadequate training of MOE personnel.

Mental Model Flaws:

- Incorrect model of state of compliance with water quality regulations and guidelines.
- Several local MOE personnel did not know E. coli could be fatal.

Feedback:

- Did not monitor effects of privatization on reporting of adverse test results.
- Inadequate feedback about state of water quality and water test results.

Coordination:

- Neither MOE nor MOH took responsibility for enacting notification legislation.

Ministry of Health

Safety Requirements and Constraints:

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

Inadequate Control Actions:

- No written protocol provided to local public health inspector on how to respond to adverse water quality or inspection reports.

Coordination:

- Neither MOE nor MOH took responsibility for enacting notification legislation.

Figure 9: The Role of the Ministries in the Accident.

monitors. After the introduction of mandatory certification in 1993, the Koebel brothers were certified on the basis of experience even though they did not meet the certification requirements. The new rules also required 40 hours of training a year for each certified operator. Stan and Frank Koebel did not take the required amount of training, and the training they did take did not adequately address drinking water safety. The MOE did not enforce the training requirements and did not focus the training on drinking water safety.

The Koebel brothers and the Walkerton commissioners were not the only ones with inadequate training and knowledge of drinking water safety. Evidence at the Inquiry showed that several environmental officers in the MOE's local office were unaware that E. coli was potentially lethal and their mental models were also incorrect with respect to other matters essential to water safety.

At the time of the privatization of the government water testing laboratories in 1996, the MOE sent a guidance document to those municipalities that requested it. The document strongly recommended that a municipality include in any contract with a private lab a clause specifying that the laboratory directly notify the MOE and the local Medical Officer of Health about adverse test results. There is no evidence that the Walkerton PUC either requested or received this document. The MOE had no mechanism for informing private laboratories of the existing guidelines for reporting adverse results to the MOE and the MOH.

In 1997, the Minister of Health took the unusual step of writing to the Minister of the Environment requesting that legislation be amended to ensure that the proper authorities would be notified of adverse water test results. The Minister of the Environment declined to propose legislation, indicating that the existing guidelines dealt with the issue. On several occasions, officials in the MOH and the MOE expressed concerns about failures to report adverse test results to local Medical Officers of Health in accordance with the protocol. But the anti-regulatory culture and the existence of the Red Tape Commission discouraged any proposals to make notification legally binding on the operators or municipal water systems and private labs.

Another important impact of the 1996 law was a reduction in the MOE water system inspection program. The cutbacks at the MOE negatively impacted the number of inspections, although the inspection program had other deficiencies as well.

The MOE inspected the Walkerton water system in 1991, 1995, and 1998. At the time of the inspections, problems existed relating to water safety. Inspectors identified some of them, but unfortunately two of the most significant problems—the vulnerability of Well 5 to surface contamination and the improper chlorination and monitoring practices of the PUC—were not detected. Information about the vulnerability of Well 5 was available in MOE files, but inspectors were not directed to look at relevant information about the security of water sources and the archived information was not easy to find. Information about the second problem, improper chlorination and monitoring practices of the WPUC, was there to be seen in the operating records maintained by the WPUC. The Walkerton Inquiry report concludes that a proper examination of the daily operating sheets would have disclosed the problem. However, the inspectors were not instructed to carry out a thorough review of operating records.

The 1998 inspection report did show there had been problems with the water supply for years: detection of E. coli in treated water with increasing frequency, chlorine residuals in treated water at less than the required 0.5 mg/L, non-compliance with minimum bacteriological sampling requirements, and not maintaining proper training records.

The MOE outlined improvements that should be made, but desperately short of inspection staff and faced with small water systems across the province that were not meeting standards, it never scheduled a follow-up inspection to see if the improvements were in fact being carried out. The Walkerton Inquiry report suggests that the use of guidelines rather than regulations had an impact here. The report states that had the Walkerton PUC been found to be in non-compliance with a

legally enforceable regulation, as opposed to a guideline, it is more likely that the MOE would have taken stronger measures to ensure compliance—such as the use of further inspections, the issuance of a Director's Order (which would have required the WPUC to comply with the requirements for treatment and monitoring), or enforcement proceedings. The lack of any followup or enforcement efforts may have led the Koebel brothers to believe the recommendations were not very important, even to the MOE.

Many adverse water quality reports were received from Walkerton between 1995 and 1998. During the mid to late 1990s, there were clear indications that the water quality was deteriorating. In 1996, for example, hundreds of people in Collingswood (a town near Walkerton), became ill after cryptosporidium (a parasite linked to animal feces) contaminated the drinking water. Nobody died, but it should have acted as a warning that the water safety control structure had degraded. Between January and April of 2000 (the months just prior to the May E. coli outbreak), the lab that tested Walkerton's water repeatedly detected coliform bacteria—an indication that surface water was getting into the water supply. The lab notified the MOE on five separate occasions. The MOE in turn phoned the WPUC, was assured the problems were being fixed, and let it go at that. The MOE failed to inform the Medical Officer of Health, as by law it was required to do.

Looking at the role of this hierarchical level in the Ontario water quality control system provides greater understanding of the reasons for the Walkerton accident and suggests more corrective actions that might be taken to prevent future accidents. But examining the control flaws at this level is not enough to understand completely the actions or lack of actions of the MOE. A larger view of the Provincial government role in the tragedy is necessary.

4.5 The Provincial Government

The last component in the Ontario water quality control structure is the Provincial government. Figure 10 summarizes its role in the accident.

All of the weaknesses in the water system operations at Walkerton (and other municipalities) might have been mitigated if the source of contamination of the water had been controlled. A weakness in the basic Ontario water control structure was the lack of a government watershed and land use policy for agricultural activities that can impact drinking water sources. In fact, at a meeting of the Walkerton town council in November 1978 (when Well 5 was constructed), MOE representatives suggested land use controls for the area around Well 5, but the municipality did not have the legal means to enforce such land use regulations because the government of Ontario had not provided the legal basis for such controls.

At the same time as the increase in factory farms was overwhelming the ability of the natural filtration process to prevent the contamination of the local water systems, the spreading of manure had been granted a long-standing exemption from EPA requirements. Annual reports of the Environment Commissioner of Ontario for the four years before the Walkerton accident included recommendations that the government create a groundwater strategy. A Health Canada study stated that the cattle counties of Southwestern Ontario, where Walkerton is located, are high-risk areas for E. coli infections. The report pointed out the direct link between cattle density and E. coli infection, and showed that 32 percent of the wells in rural Ontario showed fecal contamination. Dr. Murray McQuigge, the Medical Officer of Health for the BGOS Health Unit (and the man who handled the Walkerton E. coli outbreak) warned in a memo to local authorities that "poor nutrient management on farms is leading to a degradation of the quality of ground water, streams, and lakes." Nothing was done in response.

With the election of a conservative provincial government in 1995, a bias against environmental regulation and red tape led to the elimination of many of the government controls over drinking

Provincial Government

Safety Requirements and Constraints:

- Establish regulatory bodies and codes of responsibilities, authority, and accountability for the province.
- 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 plan is in place.
- Enact legislation to protect water quality.

Context in Which Decisions Made:

- Anti−regulatory culture.
- Efforts to reduce red tape.

Inadequate Control Actions:

- No risk assessment or risk management plan created to determine extent of known risks, whether risks should be assumed, and if assumed, whether they could be managed.
- Privatized laboratory testing of drinking water without requiring labs to notify MOE and health authorities of adverse test results. (Privatizing without establishing adequate governmental oversight)
- Relied on guidelines rather than legally enforceable regulations.
- No regulatory requirements for agricultural activities that create impacts on drinking water sources.
- Spreading of manure exempted from EPA requirements for Certificates of Approval
- Water Sewage Services Improvement Act ended provincial Drinking Water Surveillance program
- No accreditation of water testing labs (no criteria established to govern quality of testing personnel, no provisions for licensing, inspection, or auditing by government).
- Disbanded ACES.
- Ignored warnings about deteriorating water quality.
- No law to legislate requirements for drinking water standards, reporting requirements, and infrastructure funding.
- Environmental controls systematically removed or negated.

Feedback:

- No monitoring or feedback channels established to evaluate impact of changes

Figure 10: The Role of the Provincial Government in the Accident.

water quality. A Red Tape Commission was established by the provincial government to minimize reporting and other requirements on government and private industry. At the same time, the government disbanded groups like the Advisory Committee on Environmental Standards (ACES), which reviewed ministry standards, including those related to water quality. At the time of the Walkerton contamination, there was no opportunity for stakeholder or public review of the Ontario clean water controls.

Budget and staff reductions by the conservative government took a major toll on environmental programs and agencies (although budget reductions had started before the election of the new provincial government). The MOE budget was reduced by 42% and 900 of the 2400 staff responsible for monitoring, testing, inspection, and enforcement of environmental regulations were laid off. The official Walkerton Inquiry report concludes that the reductions were not based on an assessment of the requirements to carry out the MOE's statutory requirements nor on any risk assessment of the potential impact on the environment or, in particular, on water quality. After the reductions, the Provincial Ombudsman issued a report saying that cutbacks had been so damaging that the government was no longer capable of providing the services that it was mandated to provide. The report was ignored.

In 1996, the Water Sewage Services Improvement Act was passed, which shut down the government water testing laboratories, downloaded control of provincially owned water and sewage plants to the municipalities, eliminated funding for municipal water utilities, and ended the provincial Drinking Water Surveillance Program, under which the MOE had monitored drinking water across the province.

The Provincial water quality guidelines directed testing labs to report any indications of unsafe water quality to the MOE and to the local Medical Officer Of Health. The latter would then decide whether to issue a boil water advisory. When government labs conducted all of the routine drinking water tests for municipal water systems throughout the province, it was acceptable to keep the notification protocol in the form of a guideline rather than a legally enforceable law or regulation. However, the privatization of water testing and the exit of government labs from this duty in 1996 made the use of guidelines ineffective in ensuring necessary reporting would occur. At the time, private environmental labs were not regulated by the government. No criteria were established to govern the quality of testing or the qualifications or experience of private lab personnel, and no provisions were made for licensing, inspection, or auditing of private labs by the government. In addition, the government did not implement any program to monitor the effect of privatization on the notification procedures followed whenever adverse test results were found.

In 1997, the Minister of Health took the unusual step of writing to the Minister of the Environment requesting that legislation be amended to ensure that the proper authorities would be notified of adverse water test results. The Minister of the Environment declined to propose legislation, indicating that the Provincial water quality guidelines dealt with the issue. On several occasions, officials in the MOH and the MOE expressed concerns about failures to report adverse test results to local Medical Officers of Health in accordance with the protocol. But the anti-regulatory culture and the existence of the Red Tape Commission discouraged any proposals to make notification legally binding on the operators or on municipal water systems and private labs.

A final important change in the safety control structure involved the drinking water surveillance program in which the MOE monitored drinking water across the province. In 1996, the Provincial government dropped E. coli testing from its Drinking Water Surveillance Program. The next year, the Drinking Water Surveillance Program was shut down entirely. At the same time, the provincial government directed MOE staff not to enforce dozens of environmental laws and regulations still on the books. Farm operators, in particular, were to be treated with understanding if they were discovered to be in violation of livestock and waste-water regulations. By June, 1998, the Walkerton

town council was concerned enough about the situation to send a letter directly to the Premier (Mike Harris), appealing for the province to resume testing of municipal water. There was no reply.

MOE officials warned the government that closing the water testing program would endanger public health. Their concerns were dismissed. In 1997, senior MOE officials drafted another memo that the government *did* heed [7]. This memo warned that cutbacks had impaired the Ministry's ability to enforce environmental regulations to the point that the Ministry could be exposed to lawsuits for negligence if and when an environmental accident occurred. In response, the Provincial government called a meeting of the Ministry staff to discuss how to protect itself from liability, and it passed a Bill ("The Environmental Approvals Improvement Act") which, among other things, prohibited legal action against the government by anyone adversely affected by the Environment Minister's failure to apply environmental regulations and guidelines.

Many other groups warned senior government officials, ministers, and the Cabinet of the danger of what it was doing, such as reducing inspections and not making the notification guidelines into regulations. The warnings were ignored. Environmental groups prepared briefs. The Provincial Auditor, in his annual reports, criticized the MOE for deficient monitoring of groundwater resources and for failing to audit small water plants across the province. The International Joint Commission expressed its concerns about Ontario's neglect of water quality issues, and the Environmental Commissioner of Ontario warned that the government was compromising environmental protection, pointing specifically to the testing of drinking water as an area of concern.

In January 2000 (three months before the Walkerton accident), staff at the MOE's Water Policy Branch submitted a report to the Provincial government warning that "Not monitoring drinking water quality is a serious concern for the Ministry in view of its mandate to protect public health." The report stated that a number of smaller municipalities were not up to the job of monitoring the quality of their drinking water. It further warned that because of the privatization of the testing labs, there was no longer a mechanism to ensure that the MOE and the local Medical Officer of Health were informed if problems were detected in local water systems. The Provincial government ignored the report.

The warnings were not limited to groups or individuals. Many adverse water quality reports had been received from Walkerton between 1995 and 1998. During the mid to late 1990s, there were clear indications that the water quality was deteriorating. In 1996, for example, hundreds of people in Collingswood (a town near Walkerton), became ill after cryptosporidium (a parasite linked to animal feces) contaminated the drinking water. Nobody died, but it should have acted as a warning that the water safety control structure had degraded.

The Walkerton Inquiry report notes that the decisions to remove the water safety controls in Ontario or to reduce their enforcement were taken without an assessment of the risks or the preparation of a risk management plan. The report says there was evidence that those at the most senior levels of government who were responsible for the decisions considered the risks to be manageable, but there was no evidence that the specific risks were properly assessed or addressed.

Up to this point, the Walkerton accident has been viewed in terms of inadequate control and enforcement of safety constraints. But systems are not static. The next two sections describe the dynamic aspects of the accident.

4.6 Understanding the Structural Dynamics of Accidents

Most hazard analysis and other safety engineering techniques treat systems and their environments as a static design. But systems are never static: They are continually adapting and changing to achieve their ends and to react to changes within themselves, in their goals, and in their environment. The original design must not only enforce appropriate constraints on behavior to ensure

safe operation, but it must continue to operate safely as changes and adaptations occur over time. Accidents in a systems-theoretic framework are viewed as the result of flawed processes and control structures that evolve over time. This assumption explains the observation by Rasmussen quoted in Section 2.4 that accidents in complex systems frequently involve a migration of the system toward a state where a small deviation (in the physical system, human operator behavior, or the environment) can lead to a catastrophe.

Humans and organizations can adapt and still maintain a low level of risk as long as the adaptations do not involve degradation in the control structure enforcing the system safety constraints. If this degradation does occur, however, the system moves toward states of increasing risk until an accident is triggered. The key here is that adaptation is not a random process. Instead, it is an optimization process, and therefore should be predictable and potentially controllable.

For an accident model to handle system adaptation over time, it must consider the processes involved in accidents and not simply events and conditions: Processes control a sequence of events and describe system and human behavior as it changes and adapts over time rather than considering individual events and human actions. To talk about *the cause* or *causes* of an accident makes no sense in this view of accidents. As Rasmusssen argues, deterministic, causal models are inadequate to explain the organizational and social factors in highly adaptive socio-technical systems. Instead, accident causation must be viewed as a complex *process* involving the entire socio-technical system including legislators, government agencies, industry associations and insurance companies, company management, technical and engineering personnel, operations, etc.

The public water safety control structure in Ontario started out with some weaknesses, which were mitigated by the presence of other controls. In some cases, the control over hazards was improved over time, for example, by the introduction of operator certification requirements and by requirements added in 1994 for continuous monitoring or chlorine residuals and turbidity in wells directly influenced by surface water. While these improvements were helpful for new wells, the lack of a policy to apply them to the existing wells and existing operators left serious weaknesses in the overall public health structure.

At the same time, other actions, such as the reduction in inspections and the elimination of the surveillance program reduced the feedback to the MOE and the MOH about the state of the system components. The water testing laboratory privatization by itself did not degrade safety, it was the way the privatization was implemented, i.e., without mandatory requirements for the private testing labs to inform the government agencies about adverse test results and without informing the private labs about the guidelines for this notification. Without regulations or oversight or enforcement of safe operating conditions, and with inadequate mental models of the safety requirements, operating practices have a tendency to change over time in order to optimize a variety of goals that conflict with safety, in this case, cutting budgets, reducing government, and reducing red tape.

An example of asynchronous evolution of the control structure is the assumption by the municipal government (Mayor and City Council) that the WPUC Commissioners were providing appropriate oversight of the public water system operations. This assumption was true for the early operations. But the elected Commissioners over time became more interested in budgets and less expert in water system operation until they were not able to provide the necessary oversight. The municipal government, not understanding the changes, did not make an appropriate response to counter their effects.

Changes may also involve the environment. The lack of a Provincial watershed protection plan was compensated for by the Ministry of the Environment ensuring that the water systems could not be affected by such runoff. The original Walkerton design satisfied this safety constraint. But factory farms and farming operations increased dramatically and the production of animal waste overwhelmed the existing design safeguards. The environment had changed, but the existing

controls were not revisited to determine whether they were still adequate. The system safety control structure had not changed in response to the changes in the environment, allowing an unusual but possible event (in this case, unusually heavy rain) to lead to a tragedy.

All of these changes in the Ontario water safety control structure over time led to the modified control structure shown in Figure 11. Dotted lines represent communication, control or feedback channels that still existed but had become ineffective. One thing to notice in comparing the original structure at the top and the one at the bottom is the disappearance of many of the feedback loops.

4.7 Modeling the Behavioral Dynamics of the Walkerton Accident

.

As discussed in the previous section, the system's defenses or safety controls may degrade over time due to changes in the behavior of the components of the safety control loop. The reasons for the migration of the system toward a state of higher risk will be system specific and can be quite complex. In contrast to the usually simple and direct relationships represented in event-chain accident models, most accidents in complex systems involve relationships between events and human actions that are highly non-linear, involving multiple feedback loops. The analysis or prevention of these accidents requires an understanding not only of the static structure of the system and of the changes to this structure over time (the *structural dynamics*), but also the dynamics behind these changes (the *behavioral dynamics*).

The previous section presented an approach to describing and analyzing the static safety control structure and how to use that to describe the changes to that structure that occur over time. This section presents a way to model and understand the dynamic processes *behind* the changes to the static control structure and *why* it changed, potentially leading to ineffective controls and unsafe or hazardous states.

The approach proposed uses the modeling techniques of *system dynamics*. The field of system dynamics, created at MIT in the 1950's by Jay Forrester, is designed to help decision makers learn about the structure and dynamics of complex systems, to design high leverage policies for sustained improvement, and to catalyze successful implementation and change. Drawing on engineering control theory and the modern theory of nonlinear dynamical systems, system dynamics involves the development of formal models and simulators to capture complex dynamics and to create an environment for organizational learning and policy design. While system dynamics has been primarily used to model business systems, it has been applied to the analysis of a mining accident [6].

System dynamics modeling is particularly relevant when analyzing system accidents. The world is dynamic, evolving, and interconnected, but we tend to make decisions using mental models that are static, narrow, and reductionist [19]. Thus decisions that might appear to have no effect on safety—or even appear to be beneficial—may in fact degrade safety and increase risk. Using system dynamics, one can, for example, understand and predict instances of policy resistance or the tendency for well-intentioned interventions to be defeated by the response of the system to the intervention itself.

Figure 12 shows a system dynamics model for the Walkerton accident. The basic structures in the model are variables, stocks (represented by rectangles), and flows (double arrows into and out of stocks). Lines with arrows between the structures represent causality links, with a positive polarity meaning that a change in the original variable leads to a change in the same direction in the target variable. Similarly, a negative polarity means that a change in the original variable leads to a change in the opposite direction of the target variable. Double lines across a link represent a delay. Delays introduce the potential for instabilities in the system.

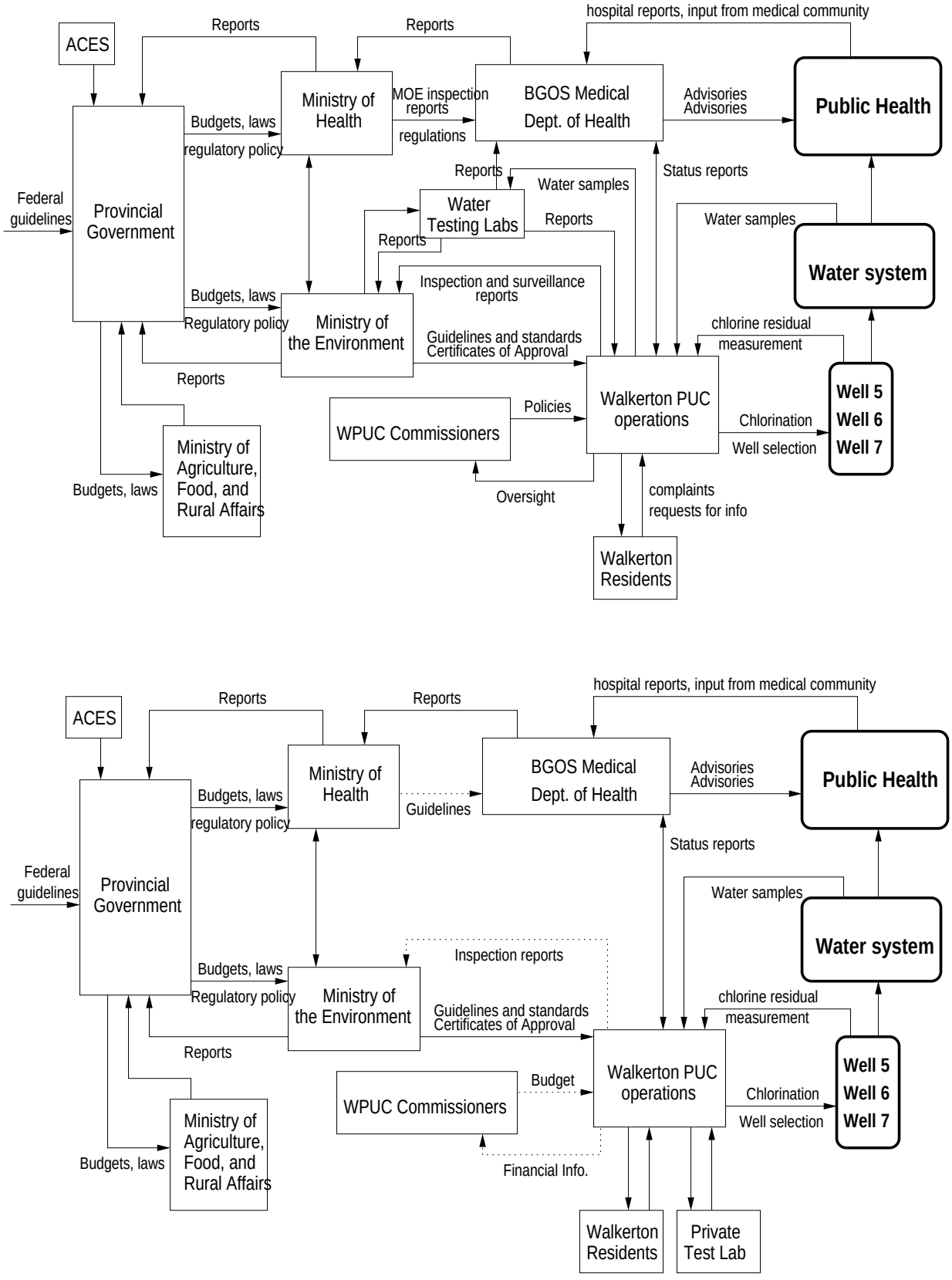


Figure 11: The Theoretical water safety control structure (top) and the structure existing at the time of the accident (bottom). Note the elimination of many feedback loops.

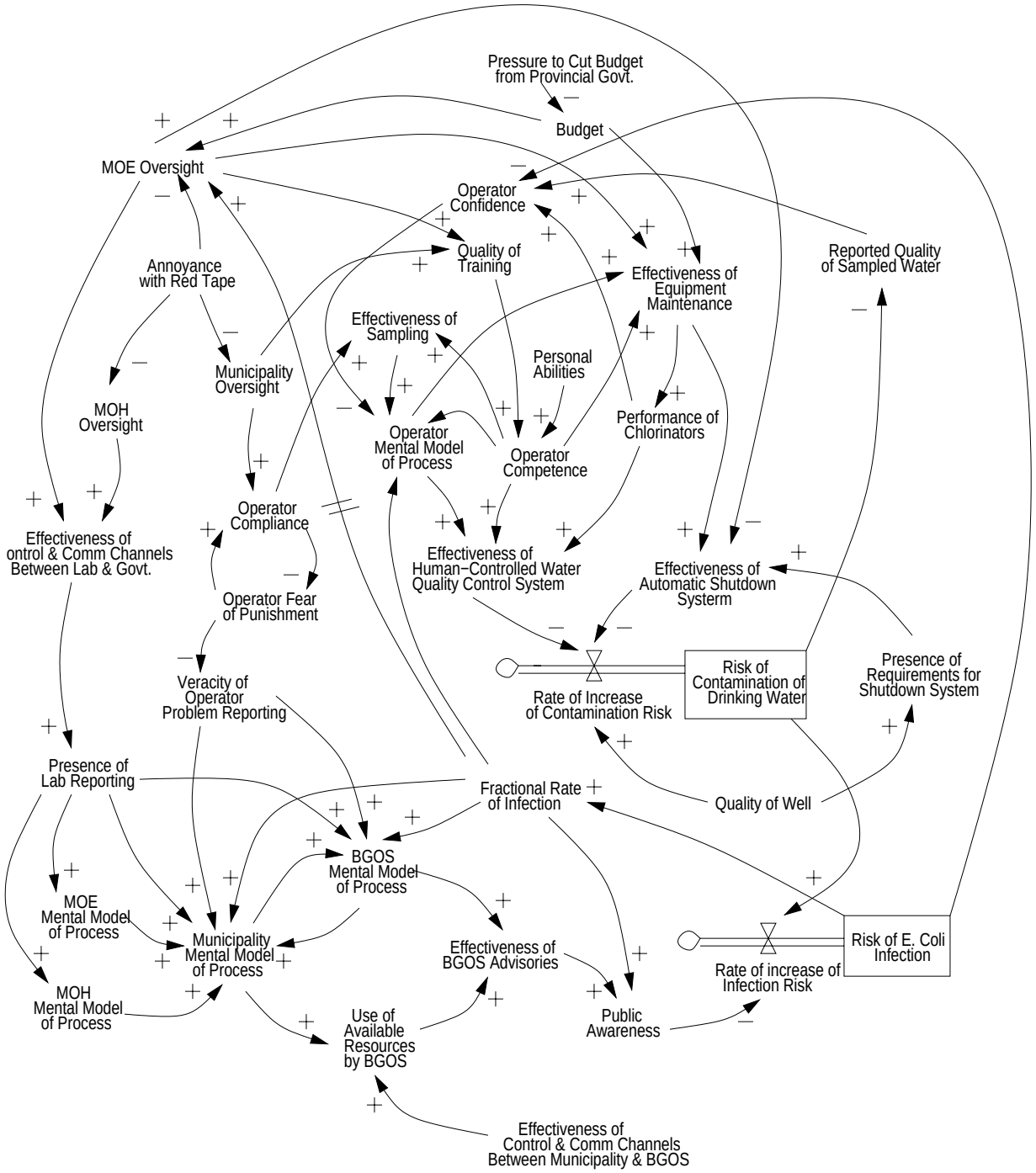


Figure 12: A Systems Dynamics Model for the Walkerton Water Contamination Accident

Modeling the entire systems' dynamics is usually impractical. The challenge is to choose relevant subsystems and model them appropriately for the intended purpose. STAMP provides the guidance for determining what to model when the goal is risk management. In the example provided, we focused primarily on the organizational factors, excluding the physical processes allowing the mixing of manure with the source water. Depending on the scope or purpose of the model, different processes could be added or removed.

According to systems dynamics theory, all the behavioral dynamics of the system, despite their complexity, arise from two types of feedback loops [19]: positive (reinforcing) and negative (balancing). In system dynamics terms, degradation over time of the safety control structure, as represented by reinforcing loops, would lead inevitably to an accident, but there are balancing loops, such as regulation and oversight, that control those changes. In Ontario, as feedback and monitoring controls were reduced, the mental model of the central government leaders and the ministries responsible for water quality about the current state of the water system became increasingly divorced from reality. A belief that the water quality controls were in better shape than they actually were led to disregarding warnings and continued reduction in what were regarded as unnecessary regulation and red tape.

Accidents occur when the balancing loops do not adequately overcome the influences degrading the safety controls. Understanding why this degradation occurred (why risk increased) is an important part of understanding why the accident occurred and learning how to prevent repetitions in the future, i.e. how to set up more effective safety control structures. It is also an important part of identifying when the socio-technical system is moving toward a state of unacceptable risk.

Our Walkerton model includes a number of exogenous variables (pressure to cut budgets, attempts by a conservative government to reduce business and government red tape, etc.) that act as levers on the behaviors of the system. When these variables are changed without any consideration of the dynamics of the system, the effectiveness of the safety control structure can deteriorate progressively, with few if any visible signs. For instance, the attempts to reduce red tape decreased the oversight of the ministries and municipalities. This decrease in oversight in turn had a negative effect on the control and communication channels between the government and the laboratories performing water quality analyses. Eventually, the laboratories stopped reporting the results of the tests. Because of this lack of reporting, the Walkerton municipality was much slower to realize that the water was contaminated, leading to a delay in the mobilization of the resources needed to deal with the contamination, and the effectiveness of the advisories issued was thus greatly diminished, increasing the risk of infection in the population.

Accident investigations often end with blame being assigned to particular individuals, often influenced by legal or political factors. The system dynamics models, on the other hand, can show how the attitude and behavior of individuals is greatly affected by the system structure and how and why such behavior may change over time. For instance, operator competence depends on the quality of training, which increases with government oversight but may decrease over time without such oversight due to competing pressures. An operator's fear of punishment, which in this case led Stan Koebel to lie about the adverse water quality test reports, is balanced by compliance with existing rules and regulations. This compliance, in turn, is directly influenced by the extent of government oversight and by the government's response to similar behavior in the past.

5 Using a Systems Theoretic Approach to Safety

To summarize, a systems-theoretic view of accidents such as STAMP focuses particular attention on the role of constraints in safety management. Accidents are seen as resulting from inadequate

control or enforcement of constraints on safety-related behavior at each level of the system development and system operations control structures. Accidents can be understood, therefore, in terms of why the controls that were in place did not prevent or detect maladaptive changes, that is, by identifying the safety constraints that were violated at each level of the control structure as well as why the controls designed to enforce them were inadequate or, if they were potentially adequate, why the system was unable to exert appropriate control over their enforcement. The process leading to an accident (loss event) is described in terms of an adaptive feedback function that fails to maintain safety as performance changes over time to meet a complex set of goals and values. Adaptation is critical in understanding accidents, and the adaptive feedback mechanism inherent in the model allows a STAMP analysis to incorporate adaptation as a fundamental system property.

The components included in the accident or safety analysis will obviously influence the causal factors considered. In the Walkerton accident, considering only the technical process and the immediate operators of the system, which are often the focus of accident investigation and prevention, provides only a limited view of the causal factors. If assigning blame in an accident investigation is the goal, then examining these two levels is usually enough to find someone that can be assigned responsibility for the accident. When designing safer systems is the goal rather than identifying who to punish, the emphasis needs to shift from *cause* (in terms of events or errors), which has a limiting, blame orientation, to understanding accidents in terms of *reasons*, i.e., why the events and errors occurred.

The use of a systems-theoretic accident model like STAMP does not lead to identifying single causal factors or variables. Instead it provides the ability to examine the entire socio-technical system design to understand the role each component plays in ensuring the safety constraints. This information can be used in an incident or accident investigation to identify the flaws in an existing structure and identify changes that will not simply eliminate symptoms but the root causes of accidents or incidents. It can also be used in a proactive way during system design, development, and operation to identify the flaws in the physical and social system design and safety controls that could lead to an accident, to design the physical and social system and controls to reduce the likelihood of an accident, to establish metrics for detecting when the safety control structure is degrading and risk is becoming unacceptably high, and to assist in decision-making about changes in the system to determine whether they will increase risk. These are the basic elements of a risk management plan, and thus STAMP provides a foundation for designing and implementing effective risk management. An important factor noted in the Walkerton accident report was the failure of the Provincial government to perform risk assessment or develop a risk management plan for provincial water quality control.

Each time one of the authors of this paper has presented this system-theoretic analysis of the Walkerton accident to an audience, one or two members of the audience (usually employees of government regulatory agencies or accident investigation authorities) have objected and declared that the government actions were irrelevant and the accident cause was simply the actions of the Koebel brothers. Indeed, government representatives argued this point of view to the Walkerton accident investigators, although the author of the official Walkerton Inquiry report did not accept the viewpoint. Instead, the Inquiry report included recommendations to establish regulatory requirements for agricultural activities with potential impacts on drinking water sources, to update standards and technology, to improve current practices in setting standards, to establish legally enforceable regulations rather than guidelines, to require mandatory training for all water system operators and require grandfathered operators to pass certification examinations within two years, to develop a curriculum for operator training and mandatory training requirements specifically emphasizing water quality and safety issues, to adopt a province-wide drinking water policy and a

Safe Drinking Water Act, to strictly enforce drinking water regulations, and to commit sufficient resources (financial and otherwise) to enable the MOE to play their role effectively. To date, most of these recommendations have not been implemented, but in May 2003 (exactly three years after the accident), the Koebel brothers were arrested for their part in the events. Water contamination incidents continue to occur in small towns in Ontario.

References

[1] Russell L. Ackoff. Towards a system of systems concepts. *Management Science*, 17(11):661–671, July 1971.

[2] Ashby, W.R., 1956. *An Introduction to Cybernetics*. Chapman and Hall, London.

[3] Bertalanffy, L. *General Systems Theory: Foundations, Development, and Applications*. G. Braziller, New York, 1969.

[4] Peter Checkland. *Systems Thinking, Systems Practice*. John Wiley & Sons, New York, 1981.

[5] R.C. Conant and W.R. Ashby. Every good regulator of a system must be a model of that system. *International Journal of System Science*, 1, ppg. 89-97, 1970.

[6] David L. Cooke. A system dynamics analysis of the Westray mine disaster. *System Dynamics Review*, Vol. 19, Issue 2, pages 139-166.

[7] Ulli Diemer. Contamination: The Poisonous Legacy of Ontario's Environment Cutbacks. *Canada Dimension Magazine*, July-August, 2000.

[8] Jacques Leplat. Occupational accident research and systems approach. In Jens Rasmussen, Keith Duncan, and Jacques Leplat, editors, *New Technology and Human Error*, pages 181–191, John Wiley & Sons, New York, 1987.

[9] Nancy G. Leveson. *Safeware: System Safety and Computers*. Addison-Wesley, 1995.

[10] Nancy Leveson. The Analysis of a Friendly Fire Accident using a System Model of Accidents. *International Conference of the System Safety Society*, Denver 2002.

[11] Nancy Leveson. A New Approach to Hazard Analysis for Complex Systems. *Int. Conference of the System Safety Society*, Ottawa, August 2003.

[12] Nancy G. Leveson. A New Accident Model for Engineering Safer Systems. *Safety Science*, Vol. 42, No. 4, Elsevier, April 2004, pp. 237-270.

[13] J.L. Lions. Ariane 501 Failure: Report by the Inquiry Board. 19 July, 1996.

[14] NASA/ESA Investigation Board. SOHO Mission Interruption. 31 August 1998

[15] Dennis R. O'Connor. Report of the Walkerton Inquiry. Ontario Ministry of the Attorney General, 2002.

[16] Simon Ramo. The systems approach. In Ralph F. Miles Jr., editor, *Systems Concepts: Lectures on Contemporary Approaches to Systems*, pages 13–32, John F. Wiley & Sons, New York, 1973.

[17] Jens Rasmussen. Risk Management in a Dynamic Society: A Modelling Problem. *Safety Science*, vol. 27, No. 2/3, Elsevier Science Ltd., 1997, pages 183-213.

[18] Jens Rasmussen and Inge Svedung. *Proactive Risk Management in a Dynamic Society*, Swedish Rescue Services Agency, 2000.

[19] John D. Sterman. *Business Dynamics*. McGraw-Hill, 2000.

[20] Dennis M. Woo and Kim J. Vicente. Sociotechnical systems, risk management, and public health: comparing the North Battleford and Walkerton outbreaks. *Reliability Engineering and System Safety*, Vol. 80, Issue 3, June 2003, pages 253-269.