11 Analyzing Accidents and Incidents (CAST)

The causality model used in accident or incident analysis determines what we look for, how we go about looking for "facts," and what we see as relevant. In our experience using STAMP-based accident analysis, we find that even if we use only the information presented in an existing accident report, we come up with a very different view of the accident and its causes.

Most accident reports are written from the perspective of an event-based model. They almost always clearly describe the events and usually one or several of these events is chosen as the "root cause(s)." Sometimes "contributory causes" are identified. But the analysis of why those events occurred is usually incomplete: The analysis frequently stops after finding someone to blame—usually a human operator—and the opportunity to learn important lessons is lost.

An accident analysis technique should provide a framework or process to assist in understanding the entire accident process and identifying the most important systemic causal factors involved. This chapter describes an approach to accident analysis, based on STAMP, called CAST (Causal Analysis based on STAMP). CAST can be used to identify the questions that need to be answered to fully understand why the accident occurred. It provides the basis for maximizing learning from the events.

The use of CAST does not lead to identifying single causal factors or variables. Instead it provides the ability to examine the entire sociotechnical system design to identify the weaknesses in the existing safety control structure and to identify changes that will not simply eliminate symptoms but potentially all the causal factors, including the systemic ones.

One goal of CAST is to get away from assigning blame and instead to shift the focus to *why* the accident occurred and how to prevent similar losses in the future. To accomplish this goal, it is necessary to minimize hindsight bias and instead to determine why people behaved the way they did, given the information they had at the time.

An example of the results of an accident analysis using CAST is presented in chapter 5. Additional examples are in appendixes B and C. This chapter describes

the steps to go through in producing such an analysis. An accident at a fictional chemical plant called Citichem [174] is used to demonstrate the process.[1] The accident scenario was developed by Risk Management Pro to train accident investigators and describes a realistic accident process similar to many accidents that have occurred in chemical plants. While the loss involves release of a toxic chemical, the analysis serves as an example of how to do an accident or incident analysis for any industry.

An accident investigation process is not being specified here, but only a way to document and analyze the results of such a process. Accident investigation is a much larger topic that goes beyond the goals of this book. This chapter only considers how to analyze the data once it has been collected and organized. The accident analysis process described in this chapter does, however, contribute to determining what questions should be asked during the investigation. When attempting to apply STAMP-based analysis to existing accident reports, it often becomes apparent that crucial information was not obtained, or at least not included in the report, that is needed to fully understand why the loss occurred and how to prevent future occurrences.

11.1 The General Process of Applying STAMP to Accident Analysis

In STAMP, an accident is regarded as involving a complex process, not just individual events. Accident analysis in CAST then entails understanding the dynamic process that led to the loss. That accident process is documented by showing the sociotechnical safety control structure for the system involved and the safety constraints that were violated at each level of this control structure and why. The analysis results in multiple views of the accident, depending on the perspective and level from which the loss is being viewed.

Although the process is described in terms of steps or parts, no implication is being made that the analysis process is linear or that one step must be completed before the next one is started. The first three steps are the same ones that form the basis of all the STAMP-based techniques described so far.

1. Identify the system(s) and hazard(s) involved in the loss.
2. Identify the system safety constraints and system requirements associated with that hazard.
3. Document the safety control structure in place to control the hazard and enforce the safety constraints. This structure includes the roles and responsi-

1. Maggie Stringfellow and John Thomas, two MIT graduate students, contributed to the CAST analysis of the fictional accident used in this chapter.

bilities of each component in the structure as well as the controls provided or created to execute their responsibilities and the relevant feedback provided to them to help them do this. This structure may be completed in parallel with the later steps.

4. Determine the proximate events leading to the loss.
5. Analyze the loss at the physical system level. Identify the contribution of each of the following to the events: physical and operational controls, physical failures, dysfunctional interactions, communication and coordination flaws, and unhandled disturbances. Determine why the physical controls in place were ineffective in preventing the hazard.
6. Moving up the levels of the safety control structure, determine how and *why* each successive higher level allowed or contributed to the inadequate control at the current level. For each system safety constraint, either the responsibility for enforcing it was never assigned to a component in the safety control structure or a component or components did not exercise adequate control to ensure their assigned responsibilities (safety constraints) were enforced in the components below them. Any human decisions or flawed control actions need to be understood in terms of (at least): the information available to the decision maker as well as any required information that was *not* available, the behavior-shaping mechanisms (the context and influences on the decision-making process), the value structures underlying the decision, and any flaws in the process models of those making the decisions and why those flaws existed.
7. Examine overall coordination and communication contributors to the loss.
8. Determine the dynamics and changes in the system and the safety control structure relating to the loss and any weakening of the safety control structure over time.
9. Generate recommendations.

In general, the description of the role of each component in the control structure will include the following:

- Safety Requirements and Constraints
- Controls
- Context
  - Roles and responsibilities
  - Environmental and behavior-shaping factors
- Dysfunctional interactions, failures, and flawed decisions leading to erroneous control actions

- Reasons for the flawed control actions and dysfunctional interactions
  - Control algorithm flaws
  - Incorrect process or interface models.
  - Inadequate coordination or communication among multiple controllers
  - Reference channel flaws
  - Feedback flaws

The next sections detail the steps in the analysis process, using Citichem as a running example.

11.2 Creating the Proximal Event Chain

While the event chain does not provide the most important causality information, the basic events related to the loss do need to be identified so that the physical process involved in the loss can be understood.

For Citichem, the physical process events are relatively simple: A chemical reaction occurred in storage tanks 701 and 702 of the Citichem plant when the chemical contained in the tanks, K34, came in contact with water. K34 is made up of some extremely toxic and dangerous chemicals that react violently to water and thus need to be kept away from it. The runaway reaction led to the release of a toxic cloud of tetrachloric cyanide (TCC) gas, which is flammable, corrosive, and volatile. The TCC blew toward a nearby park and housing development, in a city called Oakbridge, killing more than four hundred people.

The direct events leading to the release and deaths are:

1. Rain gets into tank 701 (and presumably 702), both of which are in Unit 7 of the Citichem Oakbridge plant. Unit 7 was shut down at the time due to lowered demand for K34.
2. Unit 7 is restarted when a large order for K34 is received.
3. A small amount of water is found in tank 701 and an order is issued to make sure the tank is dry before startup.
4. T34 transfer is started at unit 7.
5. The level gauge transmitter in the 701 storage tank shows more than it should.
6. A request is sent to maintenance to put in a new level transmitter.
7. The level transmitter from tank 702 is moved to tank 701. (Tank 702 is used as a spare tank for overflow from tank 701 in case there is a problem.)
8. Pressure in Unit 7 reads as too high.

9. The backup cooling compressor is activated.
10. Tank 701 temperature exceeds 12 degrees Celsius.
11. A sample is run, an operator is sent to check tank pressure, and the plant manager is called.
12. Vibration is detected in tank 701.
13. The temperature and pressure in tank 701 continue to increase.
14. Water is found in the sample that was taken (see event 11).
15. Tank 701 is dumped into the spare tank 702
16. A runaway reaction occurs in tank 702.
17. The emergency relief valve jams and runoff is not diverted into the backup scrubber.
18. An uncontrolled gas release occurs.
19. An alarm sounds in the plant.
20. Nonessential personnel are ordered into units 2 and 3, which have positive pressure and filtered air.
21. People faint outside the plant fence.
22. Police evacuate a nearby school.
23. The engineering manager calls the local hospital, gives them the chemical name and a hotline phone number to learn more about the chemical.
24. The public road becomes jammed and emergency crews cannot get into the surrounding community.
25. Hospital personnel cannot keep up with steady stream of victims.
26. Emergency medical teams are airlifted in.

These events are presented as one list here, but separation into separate interacting component event chains may be useful sometimes in understanding what happened, as shown in the friendly fire event description in chapter 5.

The Citichem event chain here provides a superficial analysis of what happened. A deep understanding of why the events occurred requires much more information. Remember that the goal of a STAMP-based analysis is to determine why the events occurred—*not* who to blame for them—and to identify the changes that could prevent them and similar events in the future.

11.3 Defining the System(s) and Hazards Involved in the Loss

Citichem has two relevant physical processes being controlled: the physical plant and public health. Because separate and independent controllers were controlling

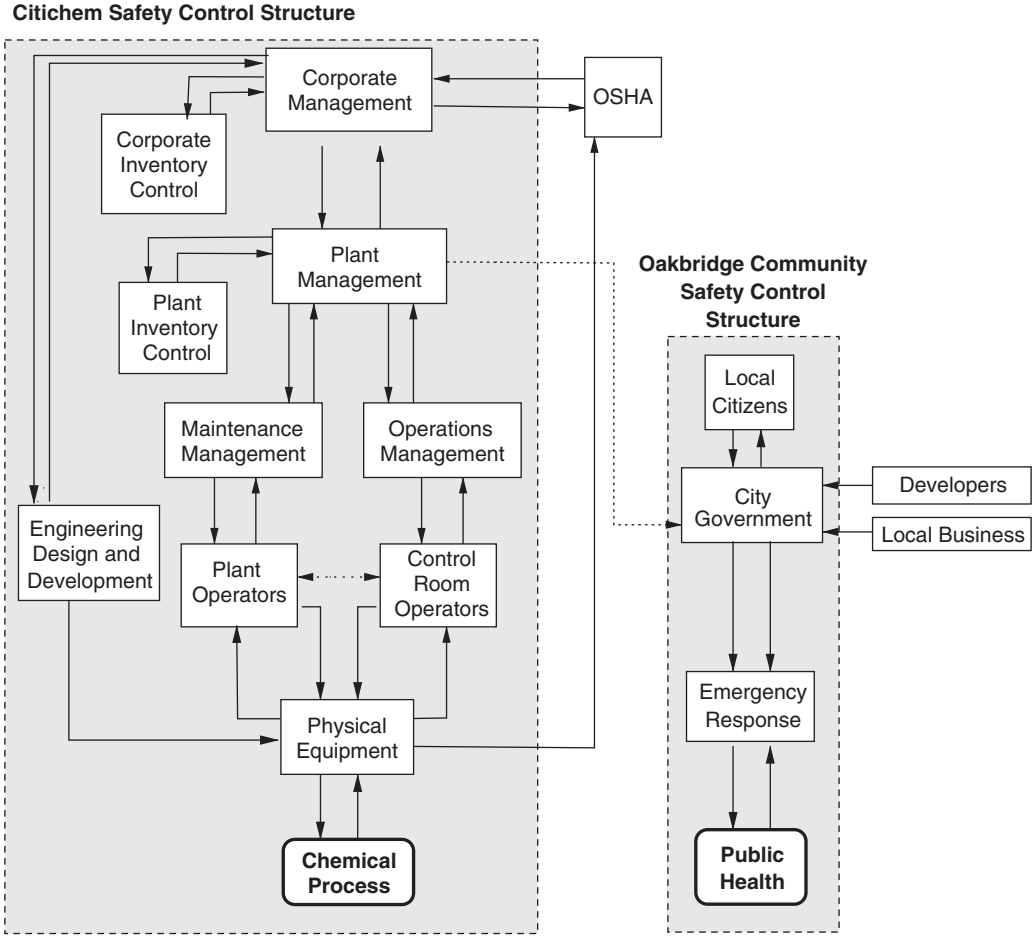

Figure 11.1
The two safety control structures most relevant to the Citichem accident analysis.

these two processes, it makes sense to consider them as two interacting but independent systems: (1) the chemical company, which controls the chemical process, and (2) the public political structure, which has responsibilities for public health. Figure 11.1 shows the major components of the two safety control structures and interactions between them. Only the major structures are shown in the figure; the details will be added throughout this chapter.[2] No information was provided

2. OSHA, the Occupational Safety and Health Administration, is part of a third larger governmental control structure, which has many other components. For simplicity, only OSHA is shown and considered in the example analysis.

about the design and engineering process for the Citichem plant in the accident description, so details about it are omitted. A more complete example of a development control structure and analysis of its role can be found in appendix B.

The analyst(s) also needs to identify the hazard(s) being avoided and the safety constraint(s) to be enforced. An accident or loss event for the combined chemical plant and public health structure can be defined as death, illness, or injury due to exposure to toxic chemicals.

The hazards being controlled by the two control structures are related but different. The public health structure hazard is *exposure of the public to toxic chemicals*. The system-level safety constraints for the public health control system are that:

1. The public must not be exposed to toxic chemicals.
2. Measures must be taken to reduce exposure if it occurs.
3. Means must be available, effective, and used to treat exposed individuals outside the plant.

The hazard for the chemical plant process is *uncontrolled release of toxic chemicals*. Accordingly, the system-level constraints are that:

1. Chemicals must be under positive control at all times.
2. Measures must be taken to reduce exposure if inadvertent release occurs.
3. Warnings and other measures must be available to protect workers in the plant and minimize losses to the outside community.
4. Means must be available, effective, and used to treat exposed individuals inside the plant.

Hazards and safety-constraints must be within the design space of those who developed the system and within the operational space of those who operate it. For example, the chemical plant designers cannot be responsible for those things outside the boundaries of the chemical plant over which they have no control, although they may have some influence over them. Control over the environment of a plant is usually the responsibility of the community and various levels of government. As another example, while the operators of the plant may cooperate with local officials in providing public health and emergency response facilities, responsibility for this function normally lies in the public domain. Similarly, while the community and local government may have some influence on the design of the chemical plant, the company engineers and managers control detailed design and operations.

Once the goals and constraints are determined, the controls in place to enforce them must be identified.

11.4 Documenting the Safety Control Structure

If STAMP has been used as the basis for previous safety activities, such as the original engineering process or the investigation and analysis of previous incidents and accidents, a model of the safety-control structure may already exist. If not, it must be created although it can be reused in the future. Chapters 12 and 13 provide information about the design of safety-control structures.

The components of the structure as well as each component's responsibility with respect to enforcing the system safety constraints must be identified. Determining what these are (or what they should be) can start from system safety requirements. The following are some example system safety requirements that might be appropriate for the Citichem chemical plant example:

1. Chemicals must be stored in their safest form.
2. The amount of toxic chemicals stored should be minimized.
3. Release of toxic chemicals and contamination of the environment must be prevented.
4. Safety devices must be operable and properly maintained at all times when potentially toxic chemicals are being processed or stored.
5. Safety equipment and emergency procedures (including warning devices) must be provided to reduce exposure in the event of an inadvertent chemical release.
6. Emergency procedures and equipment must be available and operable to treat exposed individuals.
7. All areas of the plant must be accessible to emergency personnel and equipment during emergencies. Delays in providing emergency treatment must be minimized.
8. Employees must be trained to
   a. Perform their jobs safely and understand proper use of safety equipment
   b. Understand their responsibilities with regards to safety and the hazards related to their job
   c. Respond appropriately in an emergency
9. Those responsible for safety in the surrounding community must be educated about potential hazards from the plant and provided with information about how to respond appropriately.

A similar list of safety-related requirements and responsibilities might be generated for the community safety control structure.

These general system requirements must be enforced somewhere in the safety control structure. As the accident analysis proceeds, they are used as the starting point for generating more specific constraints, such as constraints for the specific chemicals being handled. For example, requirement 4, when instantiated for TCC, might generate a requirement to prevent contact of the chemical with water. As the accident analysis proceeds, the identified responsibilities of the components can be mapped to the system safety requirements—the opposite of the forward tracing used in safety-guided design. If STPA was used in the design or analysis of the system, then the safety control structure documentation should already exist.

In some cases, general requirements and policies for an industry are established by the government or by professional associations. These can be used during an accident analysis to assist in comparing the actual safety control structure (both in the plant and in the community) at the time of the accidents with the standards or best practices of the industry and country. Accident analyses can in this way be made less arbitrary and more guidance provided to the analysts as to what should be considered to be inadequate controls.

The specific designed controls need not all be identified before the rest of the analysis starts. Additional controls will be identified as the analysts go through the next steps of the process, but a good start can usually be made early in the analysis process.

11.5 Analyzing the Physical Process

Analysis starts with the physical process, identifying the physical and operational controls and any potential physical failures, dysfunctional interactions and communication, or unhandled external disturbances that contributed to the events. The goal is to determine why the physical controls in place were ineffective in preventing the hazard. Most accident analyses do a good job of identifying the physical contributors to the events.

Figure 11.2 shows the requirements and controls at the Citichem physical plant level as well as failures and inadequate controls. The physical contextual factors contributing to the events are included.

The most likely reason for water getting into tanks 701 and 702 were inadequate controls provided to keep water out during a recent rainstorm (an unhandled external disturbance to the system in figure 4.8), but there is no way to determine that for sure.

Accident investigations, when the events and physical causes are not obvious, often make use of a hazard analysis technique, such as fault trees, to create scenarios to consider. STPA can be used for this purpose. Using control diagrams of the physical system, scenarios can be generated that could lead to the lack of enforcement

Physical Plant Safety Controls

Safety Requirements and Constraints Violated:

- Prevent runaway reactions
- Prevent inadvertent release of toxic chemicals or explosion
- Convert released chemicals into a nonhazardous of less hazardous form
- Provide indicators (alarms) of the existence of hazardous conditions
- Provide protection against human or environmental exposure after a release
- Provide emergency equipment to treat exposed individuals

Emergency and Safety Equipment (Controls): Partial list

- Air monitors
- Windsock to determine which way wind is blowing
- Automatic temperature controls to prevent overheating
- Pressure relief system to deal with excessive pressure
- Gauges and indicators to provide information about the state of the process
- Flares and scrubbers to burn off or neutralize released gas
- Positive pressure and filtered air in some units to protect employees
- Spare tank for runoff
- Emergency showers
- Eyewash fountain
- Protective equipment for employees
- Sirens

Failures and Inadequate Controls:

- Inadequate protection against water getting into tanks
- Inadequate monitoring of chemical process: Gauges were missing or inoperable
- Inadequate emergency relief system
  - Emergency relief valve jammed (could not send excess gas to scrubber)
  - Pop-up pressure relief valves in Units 7 and 9 were too small: Small amounts of corrosion in valves could prevent venting if non-gas material is present
  - Relief valve lines too small to relieve pressure fast enough: This is in effect a single point of failure for the emergency relief system

Physical Contextual Factors:

- The plant was built in a remote location 30 years ago so it would have a buffer area around it, but the city grew closer over the years
- The only access to the plant is a two-lane narrow road. There was a plan to widen the road in the future, but that never happened
- Approximately 24 different chemical products are manufactured at Oakbridge, most of which are toxic to humans and some very toxic
- The plant manufactures K34, which contains Tetra Chloric Cyanide (TCC). TCC is flammable, corrosive and volatile. It is extremely toxic and dangerous and reacts violently with water
- Unit 7 was previously used to manufacture pesticide, but production was moved to Mexico because it was cheaper to make there. At the time of the start of the accident proximal events, Unit 7 was shut down and was not being used. It was restarted to provide extra K34
- The plant operates 24 hours a day, with three different shifts
- The plant already was operating at capacity before the decision to increase production of K34

Figure 11.2
STAMP analysis at the Citichem physical plant level.

of the safety constraint(s) at the physical level. The safety design principles in chapter 9 can provide assistance in identifying design flaws.

As is common in the process industry, the physical plant safety equipment (controls) at Citichem were designed as a series of barriers to satisfy the system safety constraints identified earlier, that is, to protect against runaway reactions, protect against inadvertent release of toxic chemicals or an explosion (uncontrolled energy), convert any released chemicals into a non-hazardous or less hazardous form, provide protection against human or environmental exposure after release, and provide emergency equipment to treat exposed individuals. Citichem had the standard types of safety equipment installed, including gauges and other indicators of the physical system state. In addition, it had an emergency relief system and devices to minimize the danger from released chemicals such as a scrubber to reduce the toxicity of any released chemicals and a flare tower to burn off gas before it gets into the atmosphere.

A CAST accident analysis examines the controls to determine which ones did not work adequately and why. While there was a reasonable amount of physical safety controls provided at Citichem, much of this equipment was inadequate or not operational—a common finding after chemical plant accidents.

In particular, rainwater got into the tank, which implies the tanks were not adequately protected against rain despite the serious hazard created by the mixing of TCC with water. While the inadequate protection against rainwater should be investigated, no information was provided in the Citichem accident description. Did the hazard analysis process, which in the process industry often involves HAZOP, identify this hazard? If not, then the hazard analysis process used by the company needs to be examined to determine why an important factor was omitted. If it was not omitted, then the flaw lies in the translation of the hazard analysis results into protection against the hazard in the design and operations. Were controls to protect against water getting into the tank provided? If not, why not? If so, why were they ineffective?

Critical gauges and monitoring equipment were missing or inoperable at the time of the runaway reaction. As one important example, the plant at the time of the accident had no operational level indicator on tank 702 despite the fact that this equipment provided safety-critical information. One task for the accident analysis, then, is to determine whether the indicator was designated as safety-critical, which would (or should) trigger more controls at the higher levels, such as higher priority in maintenance activities. The inoperable level indicator also indicates a need to look at higher levels of the control structure that are responsible for providing and maintaining safety-critical equipment.

As a final example, the design of the emergency relief system was inadequate: The emergency relief valve jammed and excess gas could not be sent to the scrubber.

The pop-up relief valves in Unit 7 (and Unit 9) at the plant were too small to allow the venting of the gas if non-gas material was present. The relief valve lines were also too small to relieve the pressure fast enough, in effect providing a single point of failure for the emergency relief system. Why an inadequate design existed also needs to be examined in the higher-level control structure. What group was responsible for the design and why did a flawed design result? Or was the design originally adequate but conditions changed over time?

The physical contextual factors identified in figure 11.2 play a role in the accident causal analysis, such as the limited access to the plant, but their importance becomes obvious only at higher levels of the control structure.

At this point of the analysis, several recommendations are reasonable: add protection against rainwater getting into the tanks, change the design of the valves and vent pipes in the emergency relief system, put a level indicator on Tank 702, and so on. Accident investigations often stop here with the physical process analysis or go one step higher to determine what the operators (the direct controllers of the physical process) did wrong.

The other physical process being controlled here, public health, must be examined in the same way. There were very few controls over public health instituted in Oakbridge, the community surrounding the plant, and the ones that did exist were inadequate. The public had no training in what to do in case of an emergency, the emergency response system was woefully inadequate, and unsafe development was allowed, such as the creation of a children's park right outside the walls of the plant. The reasons for these inadequacies, as well as the inadequacies of the controls on the physical plant process, are considered in the next section.

11.6 Analyzing the Higher Levels of the Safety Control Structure

While the physical control inadequacies are relatively easy to identify in the analysis and are usually handled well in any accident analysis, understanding why those physical failures or design inadequacies existed requires examining the higher levels of safety control: Fully understanding the behavior at any level of the sociotechnical safety control structure requires understanding how and why the control at the next higher level allowed or contributed to the inadequate control at the current level. Most accident reports include some of the higher-level factors, but usually incompletely and inconsistently, and they focus on finding someone or something to blame.

Each relevant component of the safety control structure, starting with the lowest physical controls and progressing upward to the social and political controls, needs to be examined. How are the components to be examined determined? Considering everything is not practical or cost effective. By starting at the bottom, the relevant

components to consider can be identified. At each level, the flawed behavior or inadequate controls are examined to determine why the behavior occurred and why the controls at higher levels were not effective at preventing that behavior. For example, in the STAMP-based analysis of an accident where an aircraft took off from the wrong runway during construction at the airport, it was discovered that the airport maps provided to the pilot were out of date [142]. That led to examining the procedures at the company that provided the maps and the FAA procedures for ensuring that maps are up-to-date.

Stopping after identifying inadequate control actions by the lower levels of the safety control structure is common in accident investigation. The result is that the cause is attributed to "operator error," which does not provide enough information to prevent accidents in the future. It also does not overcome the problems of hindsight bias. In hindsight, it is always possible to see that a different behavior would have been safer. But the information necessary to identify that safer behavior is usually only available after the fact. To improve safety, we need to understand the reasons people acted the way they did. Then we can determine if and how to change conditions so that better decisions can be made in the future.

The analyst should start from the assumption that most people have good intentions and do not purposely cause accidents. The goal then is to understand *why* people did not or could not act differently. People acted the way they did for very good reasons; we need to understand why the behavior of the people involved made sense to them at the time [51].

Identifying these reasons requires examining the context and behavior-shaping factors in the safety control structure that influenced that behavior. What contextual factors should be considered? Usually the important contextual and behavior-shaping factors become obvious in the process of explaining why people acted the way they did. Stringfellow has suggested a set of general factors to consider [195]:

- *History:* Experiences, education, cultural norms, behavioral patterns: how the historical context of a controller or organization may impact their ability to exercise adequate control.
- *Resources:* Staff, finances, time.
- *Tools and Interfaces:* Quality, availability, design, and accuracy of tools. Tools may include such things as risk assessments, checklists, and instruments as well as the design of interfaces such as displays, control levers, and automated tools.
- *Training:* Quality, frequency, and availability of formal and informal training.
- *Human Cognition Characteristics:* Person–task compatibility, individual tolerance of risk, control role, innate human limitations.

- *Pressures:* Time, schedule, resource, production, incentive, compensation, political. Pressures can include any positive or negative force that can influence behavior.
- *Safety Culture:* Values and expectations around such things as incident reporting, workarounds, and safety management procedures.
- *Communication:* How the communication techniques, form, styles, or content impacted behavior.
- *Human Physiology:* Intoxication, sleep deprivation, and the like.

We also need to look at the process models used in the decision making. What information did the decision makers have or did they need related to the inadequate control actions? What other information could they have had that would have changed their behavior? If the analysis determines that the person was truly incompetent (not usually the case), then the focus shifts to ask why an incompetent person was hired to do this job and why they were retained in their position. A useful method to assist in understanding human behavior is to show the process model of the human controller at each important event in which he or she participated, that is, what information they had about the controlled process when they made their decisions.

Let's follow some of the physical plant inadequacies up the safety control structure at Citichem. Three examples of STAMP-based analyses of the inadequate control at Citichem are shown in figure 11.3: a maintenance worker, the maintenance manager, and the operations manager.

During the investigation, it was discovered that a maintenance worker had found water in tank 701. He was told to check the Unit 7 tanks to ensure they were ready for the T34 production startup. Unit 7 had been shut down previously (see "Physical Plant Context"). The startup was scheduled for 10 days after the decision to produce additional K34 was made. The worker found a small amount of water in tank 701, reported it to the maintenance manager, and was told to make sure the tank was "bone dry." However, water was found in the sample taken from tank 701 right before the uncontrolled reaction. It is unknown (and probably unknowable) whether the worker did not get all the water out or more water entered later through the same path it entered previously or via a different path. We do know he was fatigued and working a fourteen-hour day, and he may not have had time to do the job properly. He also believed that the tank's residual water was from condensation, not rain. No independent check was made to determine whether all the water was removed.

Some potential recommendations from what has been described so far include establishing procedures for quality control and checking safety-critical activities. Any existence of a hazardous condition—such as finding water in a tank that is to

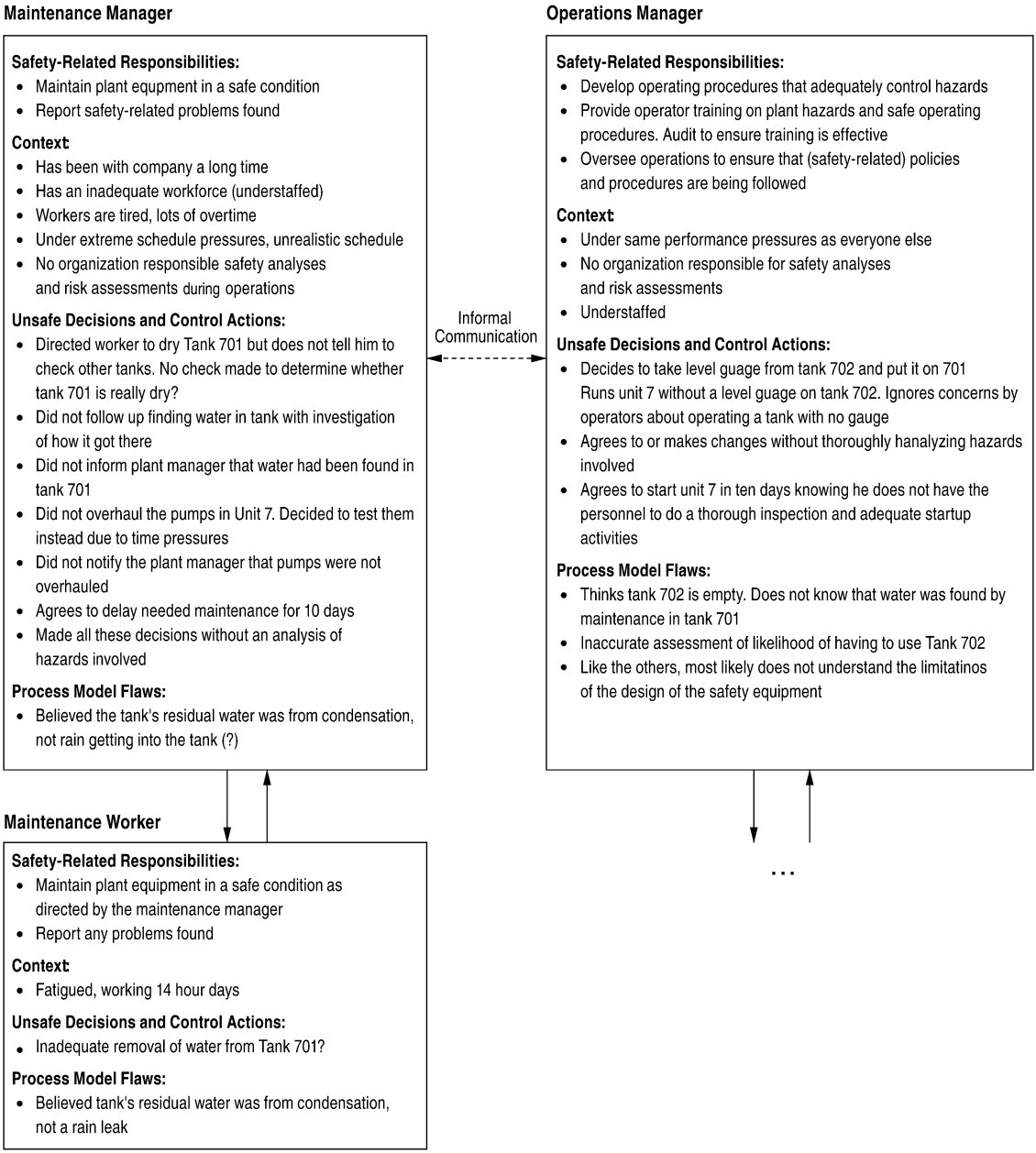

Figure 11.3
Middle-management-level analysis at Citichem.

be used to produce a chemical that is highly reactive to water—should trigger an in-depth investigation of why it occurred before any dangerous operations are started or restarted. In addition, procedures should be instituted to ensure that those performing safety-critical operations have the appropriate skills, knowledge, and physical resources, which, in this case, include adequate rest. Independent checks of critical activities also seem to be needed.

The maintenance worker was just following the orders of the maintenance manager, so the role of maintenance management in the safety-control structure also needs to be investigated. The runaway reaction was the result of TCC coming in contact with water. The operator who worked for the maintenance manager told him about finding water in tank 701 after the rain and was directed to remove it. The maintenance manager does not tell him to check the spare tank 702 for water and does not appear to have made any other attempts to perform that check. He apparently accepted the explanation of condensation as the source of the water and did not, therefore, investigate the leak further.

Why did the maintenance manager, a long-time employee who had always been safety conscious in the past, not investigate further? The maintenance manager was working under extreme time pressure and with inadequate staff to perform the jobs that were necessary. There was no reporting channel to someone with specified responsibility for investigating hazardous events, such as finding water in a tank used for a toxic chemical that should never contact water. Normally an investigation would not be the responsibility of the maintenance manager but would fall under the purview of the engineering or safety engineering staff. There did not appear to be anyone at Citichem with the responsibility to perform the type of investigation and risk analysis required to understand the reason for water being in the tank. Such events should be investigated thoroughly by a group with designated responsibility for process safety, which presumes, of course, such a group exists.

The maintenance manager did protest (to the plant manager) about the unsafe orders he was given and the inadequate time and resources he had to do his job adequately. At the same time, he did not tell the plant manager about some of the things that had occurred. For example, he did not inform the plant manager about finding water in tank 701. If the plant manager had known these things, he might have acted differently. There was no problem-reporting system in this plant for such information to be reliably communicated to decision makers: Communication relied on chance meetings and informal channels.

Lots of recommendations for changes could be generated from this part of the analysis, such as providing rigorous procedures for hazard analysis when a hazardous condition is detected and training and assigning personnel to do such an analysis. Better communication channels are also indicated, particularly problem reporting channels.

The operations manager (figure 11.3) also played a role in the accident process. He too was under extreme pressure to get Unit 7 operational. He was unaware that the maintenance group had found water in tank 701 and thought 702 was empty. During the effort to get Unit 7 online, the level indicator on tank 701 was found to be not working. When it was determined that there were no spare level indicators at the plant and that delivery would require two weeks, he ordered the level indicator on 702 to be temporarily placed on tank 701—tank 702 was only used for overflow in case of an emergency, and he assessed the risk of such an emergency as low. This flawed decision clearly needs to be carefully analyzed. What types of risk and safety analyses were performed at Citichem? What training was provided on the hazards? What policies were in place with respect to disabling safety-critical equipment? Additional analysis also seems warranted for the inventory control procedures at the plant and determining why safety-critical replacement parts were out of stock.

Clearly, safety margins were reduced at Citichem when operations continued despite serious failures of safety devices. Nobody noticed the degradation in safety. Any change of the sort that occurred here—startup of operations in a previously shut down unit and temporary removal of safety-critical equipment—should have triggered a hazard analysis and a management of change (MOC) process. Lots of accidents in the chemical industry (and others) involve unsafe workarounds. The causal analysis so far should trigger additional investigation to determine whether adequate management of change and control of work procedures had been provided but not enforced or were not provided at all. The first step in such an analysis is to determine who was responsible (if anyone) for creating such procedures and who was responsible for ensuring they were followed. The goal again is not to find someone to blame but simply to identify the flaws in the process for running Citichem so they can be fixed.

At this point, it appears that decision making by higher-level management (above the maintenance and operations manager) and management controls were inadequate at Citichem. Figures 11.4 and 11.5 show example STAMP-based analysis results for the Citichem plant manager and Citichem corporate management. The plant manager made many unsafe decisions and issued unsafe control actions that directly contributed to the accident or did not initiate control actions necessary for safety (as shown in figure 11.4). At the same time, it is clear that he was under extreme pressure to increase production and was missing information necessary to make better decisions. An appropriate safety control structure at the plant had not been established leading to unsafe operational practices and inaccurate risk assessment by most of the managers, especially those higher in the control structure. Some of the lower level employees tried to warn against the high-risk practices, but appropriate communication channels had not been established to express these concerns.

Citichem Oakbridge Plant Manager

Safety-Related Responsibilities:

- Ensure safe operation of the plant
  - Establish a safety organization and ensure it has adequate resources, appropriate expertise, and communication channels to all parts of the plant
  - Seek and use appropriate inputs from the safety organization when making safety-critical decisions
  - Establish appropriate responsibilitiy, accountability, and authority for safety-related decision making and activities at all plant management levels
  - Provide oversight to ensure compliance with company safety policies and standards at the plant
  - Create and oversee communication channels for safety-related information
- Ensure appropriate emergency preparedness and response within the plant
- Ensure that adequate emergency preparedness information is provided to the community

Context:

- Under pressure to manufacture a large amount of K34 in a short time to satisfy company sales orders. If unsuccessful, corporate could close the plant and move operations to Mexico. The need for a turnaround (major maintenance) on Unit 9 increases the pressure even more
- The plant is already stretched to capacity. The additional resources needed for increased production are not available and no budget to add more employees so must increase production without additional workers
- Highly skilled and very experienced (has been working for company for over 20 years). He has strong ties to the community and wants to ensure that Oakbridge remains a key revenue source for Citichem corporate so the employees can keep their jobs
- The Citichem Oakbridge plant as had very few acidents in the past 30 years
- The plant passes several OSHA inspections every year

Unsafe Decisions and Control Actions:

- Agrees to produce extra K34 without the resources to do it safely
- Initiates start up of Unit 7 under unsafe conditions (all safety-related equipment is not operational, and pumps are not overhauled)
- Delayed in responding to new information about inadequacy of emergency relief system design
- Does not use safety analysis information when making safety-related decisions. No management of change policies to evaluate hazards involved before changes are made
- Established inadequate inventory control policies and procedures to ensure safety-related equipment in stock at all times
- Has not set up and enforced a policy for thorough incident/accident investigation
- Has not established appropriate communication channels within the plant for safety-related information, including a problem-reporting system
- Did not warn community about dangers of development next to the plant
- Did not make sure community has information necessary for emergency preparedness activities and the handling of chemical emergencies

Process Model Flaws:

- Inaccurate risk assessment. Believes the “risks are acceptable, considering the benefits.” Does not tie the recent incidents to decreasing safety margins
- Incorrectly believed the pumps had been overhauled
- Did not know that water had been found in Tank 701
- Does not know about lack of working indicator on Tank 702 and lack of spare parts

Figure 11.4
Citichem plant management analysis.

Citichem Corporate Management

Safety-Related Responsibilities:

- Ensure that Citichem plants are operated safely and that adequate equipment and resources are provided to accomplish this goal
- Ensure that communication with communities surrounding the plants is adequate and information exchanged to reduce risk of injury for those explosed to chemicals should a release or other hazardous event occur
- Provide leadership on safety issues, including the creation and enforcement of a company safety policy

Context:

- Price competition has increased. The British recently cut their K34 prices
- Chemical plants are cheaper to operate in Mexico (and many other countries) than in the U.S
- Production at Oakbridge has been increased in the past without an incident despite warnings of decreased safety margins

Unsafe Decisions and Control Actions:

- Long-term planning of production goals and creation of sales targets was performed with inadequate regard for safety. There was no hazard or risk analysis of increasing the production of K34 at Oakbridge given the current resources there
- Inadequate allocation of resources to Oakbridge for increased production and unrealistic schedule
- Ignored feedback from Oakbridge Plant Manager that increasing production without increasing resources would require cutting safety margins to inadequate levels
- Inadequate oversight and enforcement of maintenance schedules and other plant operations related to safety
- Inadequate inventory control policies for safety-critical components and parts
- Implemented a policy of not disclosing what chemicals are used and the products they make to surrounding communities because of business competition reasons (which hindered community emergency response)
- Did not require in-depth analysis of incidents and accidents

Process Model Flaws:

- Inaccurate assessment of risk of increased production
- Belief that the only way to eliminate the risks was to eliminate the industry — that risk cannot be reduced without reducing profits or productivity
- Belief that recent incidents were not indicative of true high risk in the system and resulted simply from the employees own errors and negligence

Figure 11.5
Corporate-level Citichem management analysis.

Safety controls were almost nonexistent at the corporate management level. The upper levels of management provided inadequate leadership, oversight and management of safety. There was either no adequate company safety policy or it was not followed, either of which would lead to further causal analysis. A proper process safety management system clearly did not exist at Citichem. Management was under great competitive pressures, which may have led to ignoring corporate safety controls or adequate controls may never have been established. Everyone had very flawed mental models of the risks of increasing production without taking the proper precautions. The recommendations should include consideration of what kinds of changes might be made to provide better information about risks to management decision makers and about the state of plant operations with respect to safety.

Like any major accident, when analyzed thoroughly, the process leading to the loss is complex and multi-faceted. A complete analysis of this accident is not needed here. But a look at some of the factors involved in the plant's environment, including the control of public health, is instructive.

Figure 11.6 shows the STAMP-based analysis of the Oakbridge city emergency-response system. Planning was totally inadequate or out of date. The fire department did not have the proper equipment and training for a chemical emergency, the hospital also did not have adequate emergency resources or a backup plan, and the evacuation plan was ten years out of date and inadequate for the current level of population.

Understanding why these inadequate controls existed requires understanding the context and process model flaws. For example, the police chief had asked for resources to update equipment and plans, but the city had turned him down. Plans had been made to widen the road to Oakbridge so that emergency equipment could be brought in, but those plans were never implemented and the planners never went back to their plans to see if they were realistic for the current conditions. Citichem had a policy against disclosing what chemicals they produce and use, justifying this policy by the need for secrecy from their competitors, making it impossible for the hospital to stockpile the supplies and provide the training required for emergencies, all of which contributed to the fatalities in the accident. The government had no disclosure laws requiring chemical companies to provide such information to emergency responders.

Clear recommendations for changes result from this analysis, for example, updating evacuation plans and making changes to the planning process. But again, stopping at this level does not help to identify systemic changes that could improve community safety: The analysts should work their way up the control structure to understand the entire accident process. For example, why was an inadequate emergency response system allowed to exist?

Oakbridge Emergency Response

Safety-Related Responsibilities:

General: Provide appropriate emergency response such as fire fighting, evacuation, medical intervention

- *Fire Chief:*
  - Ensure there is adequate fire fighting equipment and emergency planning in case of a serious incident
  - Effectively communicate emergency needs to city council, mayor, and city manager (city government)
  - Learn about potential safety hazards posed by the plant (including the chemicals being manufactured and stored there)
  - Coordinate with medical facilities and other emergency responders
- *Fire Brigade:* Ensure there is adequate emergency equipment and training inside and outside the plant and drill those outside the boundaries of the plant
- *Doctors and Hospital (and other medical facilities in the area):*
  - Learn what chemicals and other dangerous products at Citichem could affect the health of the population surrounding the plant
  - Obtain adequate supplies and the information necessary to respond in an emergency as well as plan for obtaining additional human resources if required
  - Coordinate with other emergency responders (e.g., the fire department)
  - Conduct regular drills to assess and improve planning for emergency response

Context:

- Evacuation plan for city is 10 years out of date and hopelessly inadequate for the current population The police chief has asked for money several times to fund a study to update the plans, but each time is is turned down by the city
- The city government does not rank emergency preparedness as a high priority
- Citichem has a policy against disclosing what chemicals are used and the products they make. The state has no disclosure law to force them to provide this information
- Citichem is better equipped to fight chemical spills, has better equipment than they do, and knows more than the fire brigade about chemical spills
- The fire chief prefers that Citichem handle its own problems. This preference reinforces the lack of preparedness
- Plans to widen the road to Oakbridge were never implemented

Unsafe Decisions and Control Actions:

- Unless Citichem requests assistance (which they never have), the fire brigade stays "outside the fence." The fire brigade made no attempt to learn about potential Citichem hazards nor to ensure that adequate emergency equipment, training, and resources were available within Citichem
- Just about everyone outside Citichem made inadequate preparation for emergencies
- The hospital did not obtain adequate resources for an emergency and made no backup plan

Process Model Flaws:

- Hospital knows nothing about the health hazards of the plant
- Fire brigade does not know what chemicals are being used at the plant
- Everyone believed risk from the plant was low

Figure 11.6
STAMP analysis of the Oakbridge emergency response system.

The analysis in figure 11.7 helps to answer this question. For example, the members of the city government had inadequate knowledge of the hazards associated with the plant, and they did not try to obtain more information about them or about the impact of increased development close to the plant. At the same time, they turned down requests for the funding to upgrade the emergency response system as the population increased as well as attempts by city employees to provide emergency response pamphlets for the citizens and set up appropriate communication channels.

Why did they make what in retrospect look like such bad decisions? With inadequate knowledge about the risks, the benefits of increased development were ranked above the dangers from the plant in the priorities used by the city managers. A misunderstanding about the dangers involved in the chemical processing at the plant contributed also to the lack of planning and approval for emergency-preparedness activities.

The city government officials were subjected to pressures from local developers and local businesses that would benefit financially from increased development. The developer sold homes before the development was approved in order to increase pressure on the city council. He also campaigned against a proposed emergency response pamphlet for local residents because he was afraid it would reduce his sales. The city government was subjected to additional pressure from local businessmen who wanted more development in order to increase their business and profits. The residents did not provide opposing pressure to counteract the business influences and trusted that government would protect them: No community organizations existed to provide oversight of the local government safety controls and to ensure that government was adequately considering their health and safety needs (figure 11.8).

The city manager had the right instincts and concern for public safety, but she lacked the freedom to make decisions on her own and the clout to influence the mayor or city council. She was also subject to external pressures to back down on her demands and no structure to assist her in resisting those pressures.

In general, there are few requirements for serving on city councils. In the United States, they are often made up primarily of those with conflicts of interest, such as real estate agents and developers. Mayors of small communities are often not paid a full salary and must therefore have other sources of income, and city council members are likely to be paid even less, if at all.

If community-level management is unable to provide adequate controls, controls might be enforced by higher levels of government. A full analysis of this accident would consider what controls existed at the state and federal levels and why they were not effective in preventing the accident.

Oakbridge City Government

Safety-Related Responsibilities:

- Ensure that emergency preparedness planning is adequate and in place and provide necessary resources
- Ensure public safety. Approve only development that does not degrade public safety below acceptable levels

Context:

- Under pressure to create a hospitable environment for investment and development. Need support of business community and people who work at the plant and live in the community to be elected and to perform their duties
- Believe the plant is safe based on the fact that it has been there for 30 years and there have been no worse consequences than "bad smells." The plant passes several OSHA inspections every year
- The city manager worked for 18 years to get to where she is and does not want to lose her position Although she sees many problems, she feels she has no ability to change the system
- Oakbridge can use the extra tax base from additional development. Development brings jobs, more opportunities, increased tax revenues, better schools, better housing, and benefits for the local business community
- There was very little turnout for the public hearing on new development by the plant
- There is lots of pressure from developers and local businessmen to allow development

Unsafe Decisions and Control Actions:

- City council turned down funding for an emergency response pamphlet and never produced one
- City government did not ensure that adequate emergency preparedness was in place. The City Council turned down funding to update the emergency evacuation plan
- Allowed development without having an adequately sized road in place for emergency access. Argued road would be widened the next year, but then never ensured that that happened
- Allowed erosion of the physical safety buffer. Approved a children's park near the plant fence
- Ranked development and increasing the tax base over ensuring public safety
- Did not attempt to get a proper risk assessment of the increased development. Instead they took the Citichem plant manager's word that the risks were acceptable with respect to the benefits (jobs, revenues, etc.)
- The expressed concerns by the city manager were not heeded or considered adequately. Attempts by the city manager to get insight into the potential hazards and to set up formal communications between the plant and the city were thwarted

Process Model Flaws:

- Believed risk from plant was less than it really was. Assumed past perceived safety guarantees future safety
- Believed the two-lane, narrow road was not an issue because of plans to widen to four lanes "next year"

Figure 11.7
STAMP analysis of the Oakbridge city government's role in the accident.

Oakbridge Residents (Local Citizens)

Safety-Related Responsibilities:
- Ensure that elected officials are adequately executing their responsibilities with repect to public safety
- Inform themselves about potential community hazards, protection mechanisms, and emergency preparedness when moving into communities near chemical or other plants
- Understand what to do in case of an emergency

Context:
- People want to live near where they work
- Usually cheaper to live in communities near industrial plants (especially smelly ones)
- No information is available to the public about the hazards of the plant and there is often no way for them to obtain this information without the assistance of government and public disclosure laws
- Development brings jobs, more opportunities, better schools, better housing

Unsafe Decisions and Control Actions:
- Did not show up for hearings on the new development or display interest in any other way
- Did not ask about hazards or risks associated with the plant before or after moning to Oakbridge or about the state of emergency preparedness

Process Model Flaws:
- Do not know about or understand the hazards of the plant
- Do not know about the lack of emergency preparedness in their community
- Assume elected officials and local government are adequately looking out for their safety

Figure 11.8
Analysis of the role of the Oakbridge residents.

11.7 A Few Words about Hindsight Bias and Examples

One of the most common mistakes in accident analyses is the use of hindsight bias. Words such as "could have" or "should have" in accident reports are judgments that are almost always the result of such bias [50]. It is not the role of the accident analyst to render judgment in terms of what people did or did *not* do (although that needs to be recorded) but to understand *why* they acted the way they did.

Although hindsight bias is usually applied to the operators in an accident report, because most accident reports focus on the operators, it theoretically could be applied to people at any level of the organization: "The plant manager should have known …"

The biggest problem with hindsight bias in accident reports is not that it is unfair (which it usually is), but that an opportunity to learn from the accident and prevent future occurrences is lost. It is always possible to identify a better decision in retrospect—or there would not have been a loss or near miss—but it may have been difficult or impossible to identify that the decision was flawed at the time it had to be made. To improve safety and to reduce errors, we need to understand why

the decision made sense to the person at the time and redesign the system to help people make better decisions.

Accident investigation should start with the assumption that most people have good intentions and do not purposely cause accidents. The goal of the investigation, then, is to understand why they did the wrong thing in that particular situation. In particular, what were the contextual or systemic factors and flaws in the safety control structure that influenced their behavior? Often, the person had an inaccurate view of the state of the process and, given that view, did what appeared to be the right thing at the time but turned out to be wrong with respect to the actual state. The solution then is to redesign the system so that the controller has better information on which to make decisions.

As an example, consider a real accident report on a chemical overflow from a tank, which injured several workers in the vicinity [118]. The control room operator issued an instruction to open a valve to start the flow of liquid into the tank. The flow meter did not indicate a flow, so the control room operator asked an outside operator to check the manual valves near the tank to see if they were closed. The control room operator believed that the valves were normally left in an open position to facilitate conducting the operation remotely. The tank level at this time was 7.2 feet.

The outside operator checked and found the manual valves at the tank open. The outside operator also saw no indication of flow on the flow meter and made an effort to visually verify that there was no flow. He then began to open and close the valves manually to try to fix the problem. He reported to the control room operator that he heard a clunk that may have cleared an obstruction, and the control room operator tried opening the valve remotely again. Both operators still saw no flow on the flow meter. The outside operator at this time got a call to deal with a problem in a different part of the plant and left. He did not make another attempt to visually verify if there was flow. The control room operator left the valve in the closed position. In retrospect, it appears that the tank level at this time was approximately 7.7 feet.

Twelve minutes later, the high-level alarm on the tank sounded in the control room. The control room operator acknowledged the alarm and turned it off. In retrospect, it appears that the tank level at this time was approximately 8.5 feet, although there was no indication of the actual level on the control board. The control room operator got an alarm about an important condition in another part of the plant and turned his attention to dealing with that alarm. A few minutes later, the tank overflowed.

The accident report concluded, "The available evidence should have been sufficient to give the control room operator a clear indication that [the tank] was indeed filling and required immediate attention." This statement is a classic example of hindsight bias—note the use of the words "should have …" The report does not

identify what that evidence was. In fact, the majority of the evidence that both operators had at this time was that the tank was *not* filling.

To overcome hindsight bias, it is useful to examine exactly what evidence the operators had at time of each decision in the sequence of events. One way to do this is to draw the operator's process model and the values of each of the relevant variables in it. In this case, both operators thought the control valve was closed—the control room operator had closed it and the control panel indicated that it was closed, the flow meter showed no flow, and the outside operator had visually checked and there was no flow. The situation is complicated by the occurrence of other alarms that the operators had to attend to at the same time.

Why did the control board show the control valve was closed when it must have actually been open? It turns out that there is no way for the control room operator to get confirmation that the valve has actually closed after he commands it closed. The valve was not equipped with a valve stem position monitor, so the control room operator only knows that a signal has gone to the valve for it to close but not whether it has actually done so. The operators in many accidents, including Three Mile Island, have been confused about the actual position of valves due to similar designs.

An additional complication is that while there is an alarm in the tank that should sound when the liquid level reaches 7.5 feet, that alarm was not working at the time, and the operator did not know it was not working. So the operator had extra reason to believe the liquid level had not risen above 7.5 feet, given that he believed there was no flow into the tank and the 7.5-foot alarm had not sounded. The level transmitter (which provided the information to the 7.5-foot alarm) had been operating erratically for a year and a half, but a work order had not been written to repair it until the month before. It had supposedly been fixed two weeks earlier, but it clearly was not working at the time of the spill.

The investigators, in retrospect knowing that there indeed had to have been some flow, suggested that the control room operator "could have" called up trend data on the control board and detected the flow. But this suggestion is classic hindsight bias. The control room operator had no reason to perform this extra check and was busy taking care of critical alarms in other parts of the plant. Dekker notes the distinction between *data availability*, which is what can be shown to have been physically available somewhere in the situation, and *data observability*, which is what was observable given the features of the interface and the multiple interleaving tasks, goals, interests, and knowledge of the people looking at it [51]. The trend data were available to the control room operator, but they were not observable without taking special actions that did not seem necessary at the time.

While that explains why the operator did not know the tank was filling, it does not fully explain why he did not respond to the high-level alarm. The operator said that he thought the liquid was "tickling" the sensor and triggering a false alarm. The

accident report concludes that the operator should have had sufficient evidence the tank was indeed filling and responded to the alarm. Not included in the official accident report was the fact that nuisance alarms were relatively common in this unit: they occurred for this alarm about once a month and were caused by sampling errors or other routine activities. This alarm had never previously signaled a serious problem. Given that all the observable evidence showed the tank was not filling and that the operator needed to respond to a serious alarm in another part of the plant at the time, the operator not responding immediately to the alarm does not seem unreasonable.

An additional alarm was involved in the sequence of events. This alarm was at the tank and denoted that a gas from the liquid in the tank was detected in the air outside the tank. The outside operator went to investigate. Both operators are faulted in the report for waiting thirty minutes to sound the evacuation horn after this alarm went off. The official report says:

> Interviews with operations personnel did not produce a clear reason why the response to the [gas] alarm took 31 minutes. The only explanation was that there was not a sense of urgency since, in their experience, previous [gas] alarms were attributed to minor releases that did not require a unit evacuation.

This statement is puzzling, because the statement itself provides a clear explanation for the behavior, that is, the previous experience. In addition, the alarm maxed out at 25 ppm, which is much lower than the actual amount in the air, but the control room operator had no way of knowing what the actual amount was. In addition, there are no established criteria in any written procedure for what level of this gas or what alarms constitute an emergency condition that should trigger sounding the evacuation alarm. Also, none of the alarms were designated as critical alarms, which the accident report does concede might have "elicited a higher degree of attention amongst the competing priorities" of the control room operator. Finally, there was no written procedure for responding to an alarm for this gas. The "standard response" was for an outside operator to conduct a field assessment of the situation, which he did.

While there is training information provided about the hazards of the particular gas that escaped, this information was not incorporated in standard operating or emergency procedures. The operators were apparently on their own to decide if an emergency existed and then were chastised for not responding (in hindsight) correctly. If there is a potential for operators to make poor decisions in safety-critical situations, then they need to be provided with the criteria to make such a decision. Expecting operators under stress and perhaps with limited information about the current system state and inadequate training to make such critical decisions based on their own judgment is unrealistic. It simply ensures that operators will be blamed when their decisions turn out, in hindsight, to be wrong.

One of the actions the operators were criticized for was trying to fix the problem rather than calling in emergency personnel immediately after the gas alarm sounded. In fact, this response is the *normal* one for humans (see chapter 9 and [115], as well as the following discussion): if it is not the desirable response, then procedures and training must be used to ensure that a different response is elicited. The accident report states that the safety policy for this company is:

> At units, any employee shall assess the situation and determine what level of evacuation and what equipment shutdown is necessary to ensure the safety of all personnel, mitigate the environmental impact and potential for equipment/property damage. When in doubt, evacuate.

There are two problems with such a policy.

The first problem is that evacuation responsibilities (or emergency procedures more generally) do not seem to be assigned to anyone but can be initiated by all employees. While this may seem like a good idea, it has a serious drawback because one consequence of such a lack of assigned control responsibility is that everyone may think that someone else will take the initiative—and the blame if the alarm is a false one. Although everyone should report problems and even sound an emergency alert when necessary, there must be someone who has the actual responsibility, authority, and accountability to do so. There should also be backup procedures for others to step in when that person does not execute his or her responsibility acceptably.

The second problem with this safety policy is that unless the procedures clearly say to execute emergency procedures, humans are very likely to try to diagnose the situation first. The same problem pops up in many accident reports—humans who are overwhelmed with information that they cannot digest quickly or do not understand, will first try to understand what is going on before sounding an alarm [115]. If management wants employees to sound alarms expeditiously and consistently, then the safety policy needs to specify exactly when alarms are required, not leave it up to personnel to "evaluate the situation" when they are probably confused and unsure as to what is going on (as in this case) and under pressure to make quick decisions under stressful situations. How many people, instead of dialing 911 immediately, try to put out a small kitchen fire themselves? That it often works simply reinforces the tendency to act in the same way during the next emergency. And it avoids the embarrassment of the firemen arriving for a non-emergency. As it turns out, the evacuation alert had been delayed in the past in this same plant, but nobody had investigated why that occurred.

The accident report concludes with a recommendation that "operator duty to respond to alarms needs to be reinforced with the work force." This recommendation is inadequate because it ignores *why* the operators did not respond to the alarms. More useful recommendations might have included designing more accurate

and more observable feedback about the actual position of the control valve (rather than just the commanded position), about the state of flow into the tank, about the level of the liquid in the tank, and so on. The recommendation also ignores the ambiguous state of the company policy on responding to alarms.

Because the official report focused only on the role of the operators in the accident and did not even examine that in depth, a chance to detect flaws in the design and operation of the plant that could lead to future accidents was lost. To prevent future accidents, the report needed to explain such things as why the HAZOP performed on the unit did not identify any of the alarms in this unit as critical. Is there some deficiency in HAZOP or in the way it is being performed in this company? Why were there no procedures in place, or why were the ones in place ineffective, to respond to the emergency? Either the hazard was not identified, the company does not have a policy to create procedures for dealing with hazards, or it was an oversight and there was no procedure in place to check that there is a response for all identified hazards.

The report does recommend that a risk assessed procedure for filling this tank be created that defines critical operational parameters such as the sequence of steps required to initiate the filling process, the associated process control parameters, the safe level at which the tank is considered full, the sequence of steps necessary to conclude and secure the tank-filling process, and appropriate response to alarms. It does not say anything, however, about performing the same task for other processes in the plant. Either this tank and its safety-critical process are the only ones missing such procedures or the company is playing a sophisticated game of Whack-a-Mole (see chapter 13), in which only symptoms of the real problems are removed with each set of events investigated.

The official accident report concludes that the control room operator "did not demonstrate an awareness of risks associated with overflowing the tank and potential to generate high concentrations of [gas] if the [liquid in the tank] was spilled." No further investigation of why this was true was included in the report. Was there a deficiency in the training procedures about the hazards associated with his job responsibilities? Even if the explanation is that this particular operator is simply incompetent (probably not true) and although exposed to potentially effective training did not profit from it, then the question becomes why such an operator was allowed to continue in that job and why the evaluation of his training outcomes did not detect this deficiency. It seemed that the outside operator also had a poor understanding of the risks from this gas so there is clearly evidence that a systemic problem exists. An audit should have been performed to determine if a spill in this tank is the only hazard that is not understood and if these two operators are the only ones who are confused. Is this unit simply a poorly designed and managed one in the plant or do similar deficiencies exist in other units?

Other important causal factors and questions also were not addressed in the report such as why the level transmitter was not working so soon after it was supposedly fixed, why safety orders were so delayed (the average age of a safety-related work order in this plant was three months), why critical processes were allowed to operate with non-functioning or erratically functioning safety-related equipment, whether the plant management knew this was happening, and so on.

Hindsight bias and focusing only on the operator's role in accidents prevents us from fully learning from accidents and making significant progress in improving safety.

11.8 Coordination and Communication

The analysis so far has looked at each component separately. But coordination and communication between controllers are important sources of unsafe behavior.

Whenever a component has two or more controllers, coordination should be examined carefully. Each controller may have different responsibilities, but the control actions provided may conflict. The controllers may also control the same aspects of the controlled component's behavior, leading to confusion about who is responsible for providing control at any time. In the Walkerton *E. coli* water supply contamination example provided in appendix C, three control components were responsible for following up on inspection reports and ensuring the required changes were made: the Walkerton Public Utility Commission (WPUC), the Ministry of the Environment (MOE), and the Ministry of Health (MOH). The WPUC commissioners had no expertise in running a water utility and simply left the changes to the manager. The MOE and MOH both were responsible for performing the same oversight: The local MOH facility assumed that the MOE was performing this function, but the MOE's budget had been cut, and follow-ups were not done. In this case, each of the three responsible groups assumed the other two controllers were providing the needed oversight, a common finding after an accident.

A different type of coordination problem occurred in an aircraft collision near Überlingen, Germany, in 2002 [28, 212]. The two controllers—the automated onboard TCAS system and the ground air traffic controller—provided uncoordinated control instructions that conflicted and actually caused a collision. The loss would have been prevented if both pilots had followed their TCAS alerts or both had followed the ground ATC instructions.

In the friendly fire accident analyzed in chapter 5, the responsibility of the AWACS controllers had officially been disambiguated by assigning one to control aircraft within the no-fly zone and the other to monitor and control aircraft outside it. This partitioning of control broke down over time, however, with the result that neither controlled the Black Hawk helicopter on that fateful day. No performance

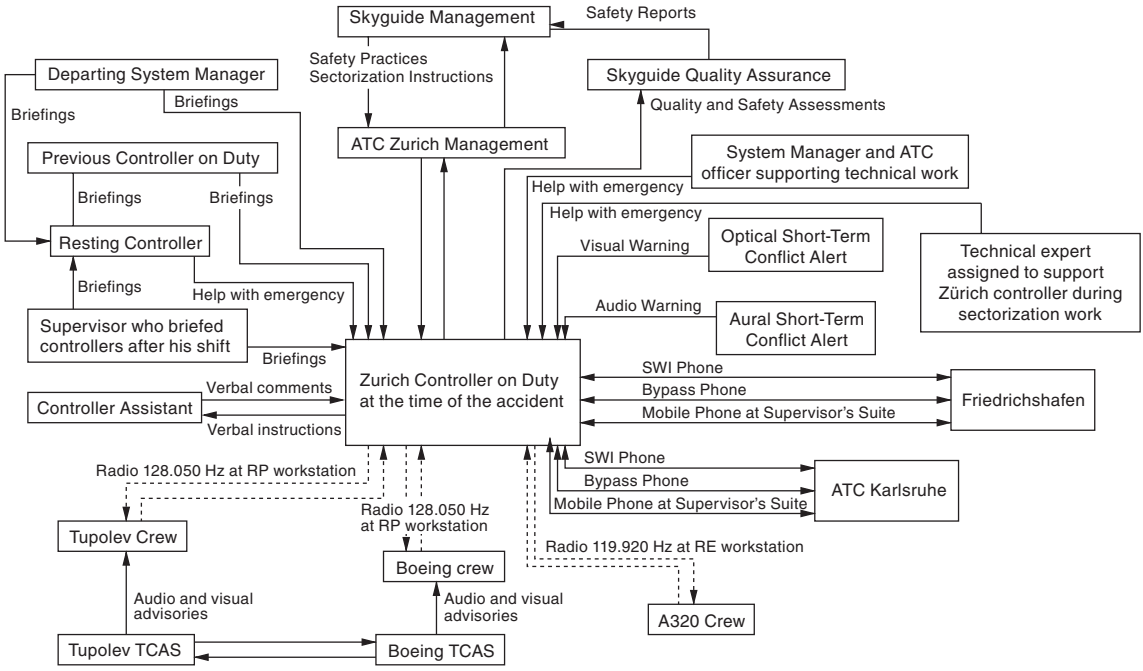

Figure 11.9
The communication links theoretically in place at the time of the Überlingen aircraft collision (adapted from [212]).

auditing occurred to ensure that the assumed and designed behavior of the safety control structure components was actually occurring.

Communication, both feedback and exchange of information, is also critical. All communication links should be examined to ensure they worked properly and, if they did not, the reasons for the inadequate communication must be determined. The Überlingen collision, between a Russian Tupolev aircraft and a DHL Boeing aircraft, provides a useful example. Wong used STAMP to analyze this accident and demonstrated how the communications breakdown on the night of the accident played an important role [212]. Figure 11.9 shows the components surrounding the controller at the Air Traffic Control Center in Zürich that was controlling both aircraft at the time and the feedback loops and communication links between the components. Dashed lines represent partial communication channels that are not available all the time. For example, only partial communication is available between the controller and multiple aircraft because only one party can transmit at one time when they are sharing a single radio frequency. In addition, the controller cannot directly receive information about TCAS advisories—the Pilot Not Flying (PNF) is

supposed to report TCAS advisories to the controller over the radio. Finally, communicating all the time with all the aircraft requires the presence of two controllers at two different consoles, but only one controller was present at the time.

Nearly all the communication links were broken or ineffective at the time of the accident (see figure 11.10). A variety of conditions contributed to the lost links.

The first reason for the dysfunctional communication was unsafe practices such as inadequate briefings given to the two controllers scheduled to work the night shift, the second controller being in the break room (which was not officially allowed but was known and tolerated by management during times of low traffic), and the reluctance of the controller's assistant to speak up with ideas to assist in the situation due to feeling that he would be overstepping his bounds. The inadequate briefings were due to a lack of information as well as each party believing they were not responsible for conveying specific information, a result of poorly defined roles and responsibilities.

More links were broken due to maintenance work that was being done in the control room to reorganize the physical sectors. This work led to unavailability of the direct phone line used to communicate with adjacent ATC centers (including ATC Karlsruhe, which saw the impending collision and tried to call ATC Zurich) and the loss of an optical short-term conflict alert (STCA) on the console. The aural short-term conflict alert was theoretically working, but nobody in the control room heard it.

Unusual situations led to the loss of additional links. These include the failure of the bypass telephone system from adjacent ATC centers and the appearance of a delayed A320 aircraft landing at Friedrichshafen. To communicate with all three aircraft, the controller had to alternate between two consoles, changing all the aircraft–controller communication channels to partial links.

Finally, some links were unused because the controller did not realize they were available. These include possible help from the other staff present in the control room (but working on the resectorization) and a third telephone system that the controller did not know about. In addition, the link between the crew of the Tupolev aircraft and its TCAS unit was broken due to the crew ignoring the TCAS advisory.

Figure 11.10 shows the remaining links after all these losses. At the time of the accident, there were no complete feedback loops left in the system and the few remaining connections were partial ones. The exception was the connection between the TCAS units of the two aircraft, which were still communicating with each other. The TCAS unit can only provide information to the crew, however, so this remaining loop was unable to exert any control over the aircraft.

Another common type of communication failure is in the problem-reporting channels. In a large number of accidents, the investigators find that the problems were identified in time to prevent the loss but that the required problem-reporting

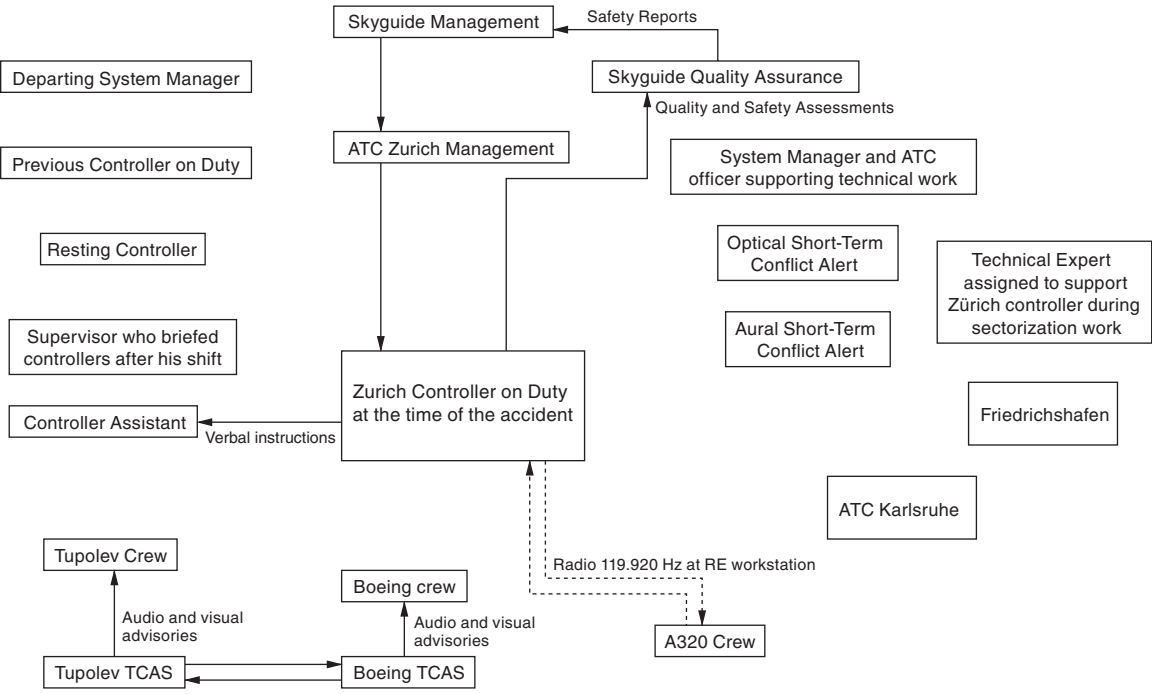

Figure 11.10
The actual state of the communication links and control loops at the time of the accident (adapted from [212]). Compare this figure with the designed communication links shown in figure 11.9.

channels were not used. Recommendations in the ensuing accident reports usually involve training people to use the reporting channels—based on an assumption that the lack of use reflected poor training—or attempting to enforce their use by reiterating the requirement that all problems be reported. These investigations, however, usually stop short of finding out why the reporting channels were not used. Often an examination and a few questions reveal that the formal reporting channels are difficult or awkward and time-consuming to use. Redesign of a poorly designed system will be more effective in ensuring future use than simply telling people they have to use a poorly designed system. Unless design changes are made, over time the poorly designed communication channels will again become underused.

At Citichem, all problems were reported orally to the control room operator, who was supposed to report them to someone above him. One conduit for information, of course, leads to a very fragile reporting system. At the same time, there were few formal communication and feedback channels established—communication was informal and ad hoc, both within Citichem and between Citichem and the local government.

11.9 Dynamics and Migration to a High-Risk State

As noted previously, most major accidents result from a migration of the system toward reduced safety margins over time. In the Citichem example, pressure from commercial competition was one cause of this degradation in safety. It is, of course, a very common one. Operational safety practices at Citichem had been better in the past, but the current market conditions led management to cut the safety margins and ignore established safety practices. Usually there are precursors signaling the increasing risks associated with these changes in the form of minor incidents and accidents, but in this case, as in so many others, these precursors were not recognized. Ironically, the death of the Citichem maintenance manager in an accident led the management to make changes in the way they were operating, but it was too late to prevent the toxic chemical release.

The corporate leaders pressured the Citichem plant manager to operate at higher levels of risk by threatening to move operations to Mexico, leaving the current workers without jobs. Without any way of maintaining an accurate model of the risk in current operations, the plant manager allowed the plant to move to a state of higher and higher risk.

Another change over time that affected safety in this system was the physical change in the separation of the population from the plant. Usually hazardous facilities are originally placed far from population centers, but the population shifts after the facility is created. People want to live near where they work and do not like long commutes. Land and housing may be cheaper near smelly, polluting plants. In third world countries, utilities (such as power and water) and transportation facilities may be more readily available near heavy industrial plants, as was the case at Bhopal.

At Citichem, an important change over time was the obsolescence of the emergency preparations as the population increased. Roads, hospital facilities, firefighting equipment, and other emergency resources became inadequate. Not only were there insufficient resources to handle the changes in population density and location, but financial and other pressures militated against those wanting to update the emergency resources and plans.

Considering the Oakbridge community dynamics, the city of Oakbridge contributed to the accident through the erosion of the safety controls due to the normal pressures facing any city government. Without any history of accidents, or risk assessments indicating otherwise, the plant was deemed safe, and officials allowed developers to build on previously restricted land. A contributing factor was the desire to increase city finances and business relationships that would assist in reelection of the city officials. The city moved toward a state where casualties would be massive when an accident did occur.

The goal of understanding the dynamics is to redesign the system and the safety control structure to make them more conducive to system safety. For example, behavior is influenced by recent accidents or incidents: As safety efforts are successfully employed, the feeling grows that accidents cannot occur, leading to reduction in the safety efforts, an accident, and then increased controls for a while until the system drifts back to an unsafe state and complacency again increases . . .

This complacency factor is so common that any system safety effort must include ways to deal with it. SUBSAFE, the U.S. nuclear submarine safety program, has been particularly successful at accomplishing this goal. The SUBSAFE program is described in chapter 14.

One way to combat this erosion of safety is to provide ways to maintain accurate risk assessments in the process models of the system controllers. The more and better information controllers have, the more accurate will be their process models and therefore their decisions.

In the Citichem example, the dynamics of the city migration toward higher risk might be improved by doing better hazard analyses, increasing communication between the city and the plant (e.g., learning about incidents that are occurring), and the formation of community citizen groups to provide counterbalancing pressures on city officials to maintain the emergency response system and the other public safety measures.

Finally, understanding the reason for such migration provides an opportunity to design the safety control structure to prevent it or to detect it when it occurs. Thorough investigation of incidents using CAST and the insight it provides can be used to redesign the system or to establish operational controls to stop the migration toward increasing risk before an accident occurs.

11.10 Generating Recommendations from the CAST Analysis

The goal of an accident analysis should not be just to address symptoms, to assign blame, or to determine which group or groups are more responsible than others.

Blame is difficult to eliminate, but, as discussed in section 2.7, blame is antithetical to improving safety. It hinders accident and incident investigations and the reporting of errors before a loss occurs, and it hinders finding the most important factors that need to be changed to prevent accidents in the future. Often, blame is assigned to the least politically powerful in the control hierarchy or to those people or physical components physically and operationally closest to the actual loss events. Understanding why inadequate control was provided and why it made sense for the controllers to act in the way they did helps to diffuse what seems to be a natural desire to assign blame for events. In addition, looking at how the entire safety control structure was flawed and conceptualizing accidents as complex

processes rather than the result of independent events should reduce the finger pointing and arguments about others being more to blame that often arises when system components other than the operators are identified as being part of the accident process. "More to blame" is not a relevant concept in a systems approach to accident analysis and should be resisted and avoided. Each component in a system works together to obtain the results, and no part is more important than another.

The goal of the accident analysis should instead be to determine how to change or reengineer the entire safety-control structure in the most cost-effective and practical way to prevent similar accident processes in the future. Once the STAMP analysis has been completed, generating recommendations is relatively simple and follows directly from the analysis results.

One consequence of the completeness of a STAMP analysis is that many possible recommendations may result—in some cases, too many to be practical to include in the final accident report. A determination of the relative importance of the potential recommendations may be required in terms of having the greatest impact on the largest number of potential future accidents. There is no algorithm for identifying these recommendations, nor can there be. Political and situational factors will always be involved in such decisions. Understanding the entire accident process and the overall safety control structure should help with this identification, however.

Some sample recommendations for the Citichem example are shown throughout the chapter. A more complete list of the recommendations that might result from a STAMP-based Citichem accident analysis follows. The list is divided into four parts: physical equipment and design, corporate management, plant operations and management, and government and community.

Physical Equipment and Design

1. Add protection against rainwater getting into tanks.
2. Consider measures for preventing and detecting corrosion.
3. Change the design of the valves and vent pipes to respond to the two-phase flow problem (which was responsible for the valves and pipes being jammed).
4. Etc. (the rest of the physical plant factors are omitted)

Corporate Management

1. Establish a corporate safety policy that specifies:
   a. Responsibility, authority, accountability of everyone with respect to safety
   b. Criteria for evaluating decisions and for designing and implementing safety controls.

2. Establish a corporate process safety organization to provide oversight that is responsible for:
   a. Enforcing the safety policy
   b. Advising corporate management on safety-related decisions
   c. Performing risk analyses and overseeing safety in operations including performing audits and setting reporting requirements (to keep corporate process models accurate). A safety working group at the corporate level should be considered.
   d. Setting minimum requirements for safety engineering and operations at plants and overseeing the implementation of these requirements as well as management of change requirements for evaluating all changes for their impact on safety.
   e. Providing a conduit for safety-related information from below (a formal safety reporting system) as well as an independent feedback channel about process safety concerns by employees.
   f. Setting minimum physical and operational standards (including functioning equipment and backups) for operations involving dangerous chemicals.
   g. Establishing incident/accident investigation standards and ensuring recommendations are adequately implemented.
   h. Creating and maintaining a corporate process safety information system.
3. Improve process safety communication channels both within the corporate level as well as information and feedback channels from Citichem plants to corporate management.
4. Ensure that appropriate communication and coordination is occurring between the Citichem plants and the local communities in which they reside.
5. Strengthen or create an inventory control system for safety-critical parts at the corporate level. Ensure that safety-related equipment is in stock at all times.

Citichem Oakbridge Plant Management and Operations

1. Create a safety policy for the plant. Derive it from the corporate safety policy and make sure everyone understands it. Include minimum requirements for operations: for example, safety devices must be operational, and production should be shut down if they are not.
2. Establish a plant process safety organization and assign responsibility, authority, and accountability for this organization. Include a process safety manager whose primary responsibility is process safety. The responsibilities of this organization should include at least the following:
   a. Perform hazard and risk analysis.

b. Advise plant management on safety-related decisions.
c. Create and maintain a plant process safety information system.
d. Perform or organize process safety audits and inspections using hazard analysis results as the preconditions for operations and maintenance.
e. Investigate hazardous conditions, incidents, and accidents.
f. Establish leading indicators of risk.
g. Collect data to ensure process safety policies and procedures are being followed.

3. Ensure that everyone has appropriate training in process safety and the specific hazards associated with plant operations.
4. Regularize and improve communication channels. Create the operational feedback channels from controlled components to controllers necessary to maintain accurate process models to assist in safety-related decision making. If the channels exist but are not used, then the reason why they are unused should be determined and appropriate changes made.
5. Establish a formal problem reporting system along with channels for problem reporting that include management and rank and file workers. Avoid communication channels with a single point of failure for safety-related messages. Decisions on whether management is informed about hazardous operational events should be proceduralized. Any operational conditions found to exist that involve hazards should be reported and thoroughly investigated by those responsible for system safety.
6. Consider establishing employee safety committees with union representation (if there are unions at the plant). Consider also setting up a plant process safety working group.
7. Require that all changes affecting safety equipment be approved by the plant manager or by his or her designated representative for safety. Any outage of safety-critical equipment must be reported immediately.
8. Establish procedures for quality control and checking of safety-critical activities and follow-up investigation of safety excursions (hazardous conditions).
9. Ensure that those performing safety-critical operations have appropriate skills and physical resources (including adequate rest).
10. Improve inventory control procedures for safety-critical parts at the Oakbridge plant.
11. Review procedures for turnarounds, maintenance, changes, operations, etc. that involve potential hazards and ensure that these are being followed. Create an MOC procedure that includes hazard analysis on all planned changes.

12. Enforce maintenance schedules. If delays are unavoidable, a safety analysis should be performed to understand the risks involved.
13. Establish incident/accident investigation standards and ensure that they are being followed and recommendations are implemented.
14. Create a periodic audit system on the safety of operations and the state of the plant. Audit scope might be defined by such information as the hazard analysis, identified leading indicators of risk, and past incident/accident investigations.
15. Establish communication channels with the surrounding community and provide appropriate information for better decision making by community leaders and information to emergency responders and the medical establishment. Coordinate with the surrounding community to provide information and assistance in establishing effective emergency preparedness and response measures. These measures should include a warning siren or other notification of an emergency and citizen information about what to do in the case of an emergency.

Government and Community

1. Set policy with respect to safety and ensure that the policy is enforced.
2. Establish communication channels with hazardous industry in the community.
3. Establish and monitor information channels about the risks in the community. Collect and disseminate information on hazards, the measures citizens can take to protect themselves, and what to do in case of an emergency.
4. Encourage citizens to take responsibility for their own safety and to encourage local, state, and federal government to do the things necessary to protect them.
5. Encourage the establishment of a community safety committee and/or a safety ombudsman office that is not elected but represents the public in safety-related decision making.
6. Ensure that safety controls are in place before approving new development in hazardous areas, and if not (e.g., inadequate roads, communication channels, emergency response facilities), then perhaps make developers pay for them. Consider requiring developers to provide an analysis of the impact of new development on the safety of the community. Hire outside consultants to evaluate these impact analyses if such expertise is not available locally.
7. Establish an emergency preparedness plan and re-evaluate it periodically to determine if it is up to date. Include procedures for coordination among emergency responders.

8. Plan temporary measures for additional manpower in emergencies.
9. Acquire adequate equipment.
10. Provide drills and ensure alerting and communication channels exist and are operational.
11. Train emergency responders.
12. Ensure that transportation and other facilities exist for an emergency.
13. Set up formal communications between emergency responders (hospital staff, police, firefighters, Citichem). Establish emergency plans and means to periodically update them.

One thing to note from this example is that many of the recommendations are simply good safety management practices. While this particular example involved a system that was devoid of the standard safety practices common to most industries, many accident investigations conclude that standard safety management practices were not observed. This fact points to a great opportunity to prevent accidents simply by establishing standard safety controls using the techniques described in this book. While we want to learn as much as possible from each loss, preventing the losses in the first place is a much better strategy than waiting to learn from our mistakes.

These recommendations and those resulting from other thoroughly investigated accidents also provide an excellent resource to assist in generating the system safety requirements and constraints for similar types of systems and in designing improved safety control structures.

Just investigating the incident or accident is, of course, not enough. Recommendations must be implemented to be useful. Responsibility must be assigned for ensuring that changes are actually made. In addition, feedback channels should be established to determine whether the recommendations and changes were successful in reducing risk.

11.11 Experimental Comparisons of CAST with Traditional Accident Analysis

Although CAST is new, several evaluations have been done, mostly aviation-related.

Robert Arnold, in a master's thesis for Lund University, conducted a qualitative comparison of SOAM and STAMP in an Air Traffic Management (ATM) occurrence investigation. SOAM (Systemic Occurrence Analysis Methodology) is used by Eurocontrol to analyze ATM incidents. In Arnold's experiment, an incident was investigated using SOAM and STAMP and the usefulness of each in identifying systemic countermeasures was compared. The results showed that SOAM is a useful heuristic and a powerful communication device, but that it is weak with respect to

emergent phenomena and nonlinear interactions. SOAM directs the investigator to consider the context in which the events occur, the barriers that failed, and the organizational factors involved, but not the processes that created them or how the entire system can migrate toward the boundaries of safe operation. In contrast, the author concludes,

> STAMP directs the investigator more deeply into the mechanism of the interactions between system components, and how systems adapt over time. STAMP helps identify the controls and constraints necessary to prevent undesirable interactions between system components. STAMP also directs the investigation through a structured analysis of the upper levels of the system's control structure, which helps to identify high level systemic countermeasures. The global ATM system is undergoing a period of rapid technological and political change. . . . The ATM is moving from centralized human controlled systems to semi-automated distributed decision making. . . . Detailed new systemic models like STAMP are now necessary to prevent undesirable interactions between normally functioning system components and to understand changes over time in increasingly complex ATM systems.

Paul Nelson, in another Lund University master's thesis, used STAMP and CAST to analyze the crash of Comair 5191 at Lexington, Kentucky, on August 27, 2006, when the pilots took off from the wrong runway [142]. The accident, of course, has been thoroughly investigated by the NTSB. Nelson concludes that the NTSB report narrowly targeted causes and potential solutions. No recommendations were put forth to correct the underlying safety control structure, which fostered process model inconsistencies, inadequate and dysfunctional control actions, and unenforced safety constraints. The CAST analysis, on the other hand, uncovered these useful levers for eliminating future loss.

Stringfellow compared the use of STAMP, augmented with guidewords for organizational and human error analysis, with the use of HFACS (Human Factors Analysis and Classification System) on the crash of a Predator-B unmanned aircraft near Nogales, Arizona [195]. HFACS, based on the Swiss Cheese Model (event-chain model), is an error-classification list that can be used to label types of errors, problems, or poor decisions made by humans and organizations [186]. Once again, although the analysis of the unmanned vehicle based on STAMP found all the factors found in the published analysis of the accident using HFACS [31, 195], the STAMP-based analysis identified additional factors, particularly those at higher levels of the safety control structure, for example, problems in the FAA's COA[3] approval process. Stringfellow concludes:

3. The COA or Certificate of Operation allows an air vehicle that does not nominally meet FAA safety standards access to the National Airspace System. The COA application process includes measures to mitigate risks, such as sectioning off the airspace to be used by the unmanned aircraft and preventing other aircraft from entering the space.

> The organizational influences listed in HFACS . . . do not go far enough for engineers to create recommendations to address organizational problems. . . . Many of the factors cited in Swiss Cheese-based methods don't point to solutions; many are just another label for human error in disguise [195, p. 154].

In general, most accident analyses do a good job in describing *what* happened, but not *why*.

11.12 Summary

In this chapter, the process for performing accident analysis using STAMP as the basis is described and illustrated using a chemical plant accident as an example. Stopping the analysis at the lower levels of the safety-control structure, in this case at the physical controls and the plant operators, provides a distorted and incomplete view of the causative factors in the loss. Both a better understanding of why the accident occurred and how to prevent future ones are enhanced with a more complete analysis. As the entire accident process becomes better understood, individual mistakes and actions assume a much less important role in comparison to the role played by the environment and context in which their decisions and control actions take place. What may look like an error or even negligence by the low-level operators and controllers may appear much more reasonable given the full picture. In addition, changes at the lower levels of the safety-control structure often have much less ability to impact the causal factors in major accidents than those at higher levels.

At all levels, focusing on assessing blame for the accident does not provide the information necessary to prevent future accidents. Accidents are complex processes, and understanding the entire process is necessary to provide recommendations that are going to be effective in preventing a large number of accidents and not just preventing the symptoms implicit in a particular set of events. There is too much repetition of the same causes of accidents in most industries. We need to improve our ability to learn from the past.

Improving accident investigation may require training accident investigators in systems thinking and in the types of environmental and behavior shaping factors to consider during an analysis, some of which are discussed in later chapters. Tools to assist in the analysis, particularly graphical representations that illustrate interactions and causality, will help. But often the limitations of accident reports do not stem from the sincere efforts of the investigators but from political and other pressures to limit the causal factors identified to those at the lower levels of the management or political hierarchy. Combating these pressures is beyond the scope of this book. Removing blame from the process will help somewhat. Management also has to be educated to understand that safety pays and, in the longer term, costs less than the losses that result from weak safety programs and incomplete accident investigations.