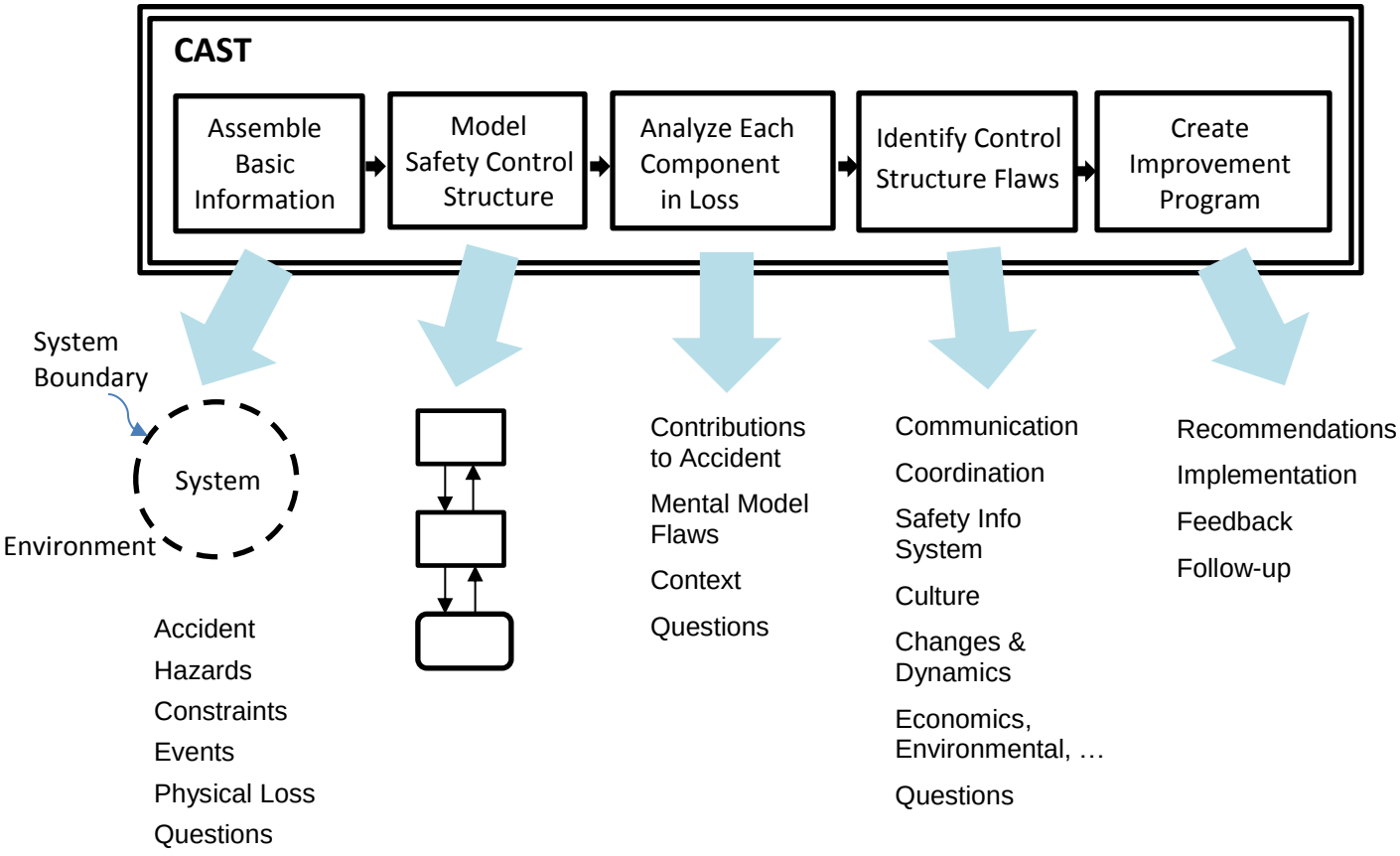
Chapter 4: Performing a CAST Analysis

Basic Components of CAST

CAST (Causal Analysis Based on Systems Theory) is a structured technique to analyze accident causality from a systems perspective.[14] CAST is an analysis method, not an investigation technique. But performing the CAST analysis as the investigation proceeds will assist in identifying what questions need to be answered and what information needs to be gathered during the investigation in order to create a comprehensive explanation as to why the loss occurred and to help formulate recommendations to prevent related accidents in the future.

Because the cause of an accident is defined in STAMP to be a safety control structure that did not prevent the loss, then the goal of the accident investigation is to identify why the safety control structure was unable to enforce the safety constraint that was violated and to determine what changes in the control structure are required to prevent a related loss in the future. In most cases, investigators will find that there was inadequate control provided at all levels of the safety control structure, not just the lower levels.

CAST has five parts:



[14] It is unfortunate that the same acronym is used for Commercial Aviation Safety Team. Both uses have existed for so long that there does not seem to be a simple solution. In this handbook, CAST is always used to mean Causal Analysis based on System Theory.

Basic Components of a CAST Analysis

1. *Collect the basic information to perform the analysis:*
   a. *Define the system involved and the boundary of the analysis,*
   b. *Describe the loss and hazardous state that led to it*
   c. *From the hazard, identify the system-level safety constraints required to prevent the hazard (the system safety requirements and constraints).*
   d. *Describe what happened (the events) without conclusions nor blame. Generate questions that need to be answered to explain why the events occurred.*
   e. *Analyze the physical loss in terms of the physical equipment and controls, the requirements on the physical design to prevent the hazard involved, the physical controls (emergency and safety equipment) included in the design to prevent this type of accident, failures and unsafe interactions leading to the hazard, missing or inadequate physical controls that might have prevented the accident, and any contextual factors that influenced the events.*

   The goal of rest of analysis is to identify the limitations of the safety control structure that allowed the loss and how to strengthen it in the future.
2. *Model the existing safety control structure for this type of hazard.*
3. *Examine the components of the control structure to determine why they were not effective in preventing the loss: Starting at the bottom of the control structure, show the role each component played in the accident and the explanation for their behavior (why they did what they did and why they thought it was the right thing to do at the time).*
4. *Identify flaws in the control structure as a whole (general systemic factors) that contributed to the loss. The systemic factors span the individual system control structure components.*
5. *Create recommendations for changes to the control structure to prevent a similar loss in the future. If appropriate, design a continuous improvement program for this hazard as part of your overall risk management program.*

These are not rigid steps or a straight-line process. Work on each of the parts may proceed throughout the investigation as deemed appropriate and practical, although the first two parts will provide the basic information for the later activities and probably need to be at least started before attempting the other parts. As more is learned during the investigation, analyses will be revisited and results changed or holes filled in.

Each step involves generating questions to answer later as more is learned. The questions will help the investigators determine what more needs to be learned to explain in depth why the loss occurred. The goal at the end of the investigation is to be able to answer all the questions or to determine that they are unanswerable. The answers to the questions will provide the “why’s” for the events.

A required format for recording the results of the analysis is not provided in this handbook. Different formats may be appropriate in different situations. Some examples are provided at the end of the chapter but you may find a better format for your purposes. In addition, some industries, such as aviation, have a required format and contents for the final investigation report, which may influence the format for the CAST analysis itself.

A running example analysis is used in this handbook to explain the CAST process. It is a real accident: an explosion of a chemical reactor and a fire on June 3, 2014 at the Shell Moerdijk plant in the Netherlands. The contents of the reactor were released into the wider environment, while sections of the reactor itself were blasted across 250 meters and other debris was later found 800 meters away.

The explosion could be heard 20 kilometers away. Two people working opposite the exploding reactor were hit by the pressure wave of the explosion and the hot and burning catalyst pellets that were flying around. A large, raging fire occurred, generating considerable amounts of smoke.

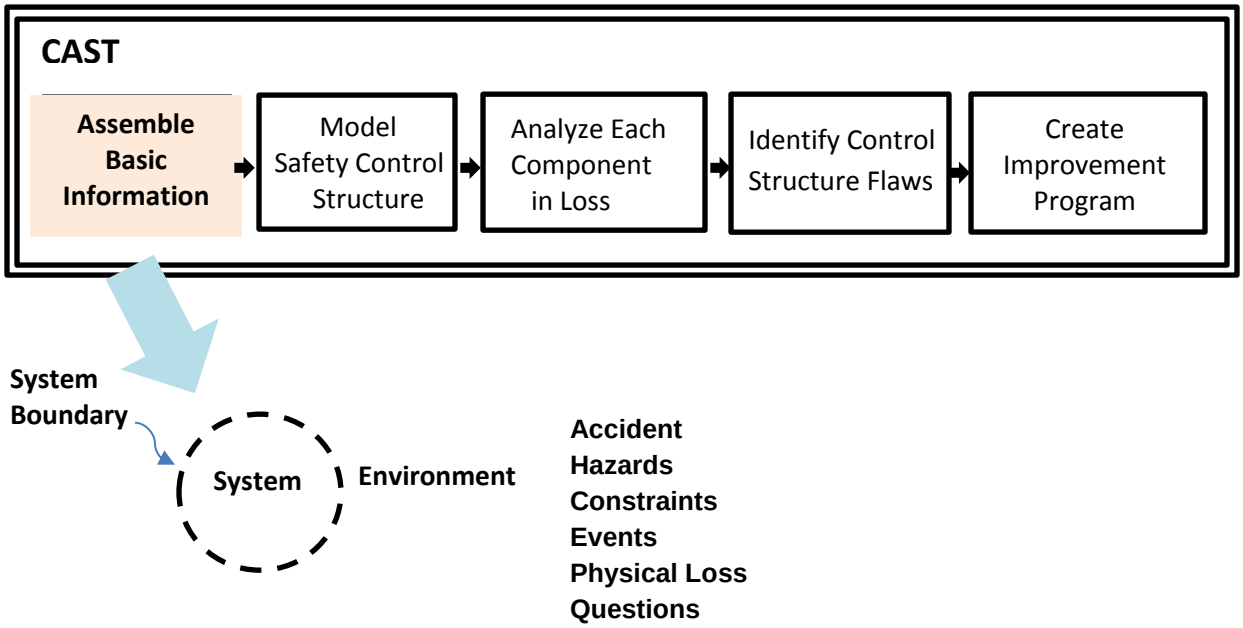
Figure 12: The Shell Moerdijk Explosion

Links to other online examples of real CAST analyses on a large variety of accidents, including the running example used here, is provided in Appendix A.

The complete CAST analysis for this accident is too large to include in this handbook but can be accessed online through the link provided in Appendix A. Technical information about the chemical process that goes beyond what is needed to understand the CAST example is provided in Appendix B, along with a summary of the full CAST analysis results.

The rest of this chapter describes how each of the CAST process steps is performed on the example accident. I recommend that you take an accident with which you are familiar and go through the CAST steps yourself on that accident as you read the explanation and the examples.

Assembling the Foundational Information



1. Collect the basic information to perform the analysis:
   a. Define the system involved and the boundary of the analysis,
   b. Describe the loss and hazardous state that led to it
   c. From the hazard, identify the system-level safety constraints required to prevent the hazard (the system safety requirements and constraints).
   d. Describe what happened (the events) without conclusions nor blame. Generate questions that need to be answered to explain why the events occurred.
   e. Analyze the physical loss in terms of the physical equipment and controls, the requirements on the physical design to prevent the hazard involved, the physical controls (emergency and safety equipment) included in the design to prevent this type of accident, failures and unsafe interactions leading to the hazard, missing or inadequate physical controls that might have prevented the accident, and any contextual factors that influenced the events.

The goal of rest of analysis is to identify the limitations of the safety control structure that allowed the loss and how to strengthen it in the future.

The first step is simply to gather basic information about what happened and to identify the goals for the analysis. The system hazard that occurred and the safety constraint violated are first identified. While seemingly simple and obvious, the hazard(s) and safety constraint(s) are important in identifying the controls included in the safety control structure in order to prevent this hazard and enforce the constraints. Starting from all constraints and controls is too inefficient.

We start by identifying the boundaries of the system of concern. In the Shell Moerdijk accident, the system analyzed is the chemical plant, its equipment, and the workers in the plant as well as the public in the area around the plant. The loss involved an explosion of Unit 4800 during startup after a maintenance stop. More details are included in Appendix B.

Next, the hazards that led to the loss and the constraints that must be satisfied in the design and operation of the system are identified.

System Hazard 1: Exposure of the public or workers to toxic chemicals.

Safety Constraints:

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

System Hazard 2: Explosion (uncontrolled release of energy) and/or fire.

Safety Constraints:

1. Chemicals must be under positive control at all times, i.e., runaway reactions must be prevented.
2. Warnings and other measures must be available to protect workers in the plant and to minimize losses to the outside community.
3. Means must be available, effective, and used to respond to explosions or fires inside or outside the plant.

In this case, there were two hazards that occurred. The constraints include the concerns of the investigation and the safety control structure to be considered that extend beyond the boundaries of the plant itself and, indeed, beyond the responsibilities of Shell. For example, responsibility for public (community) health is not normally the sole responsibility of the owners of the chemical plant itself, although they may by law be required to participate.

Deriving the safety constraints from the hazard is rather obvious, except perhaps for the inclusion of constraints to handle the case where the hazard is not avoided. In System Hazard 1 for the chemical plant (*Exposure of the public or workers to toxic chemicals*), the first safety constraint is simply a translation of the hazard to a goal statement, i.e., workers and the public must not be exposed to potentially harmful chemicals.

The second and the third are more easily missed. There is always a possibility that the safety constraint is not enforced. In that case, the hazard cannot be avoided, but it often can be mitigated and any potential harm reduced if the hazard occurs. That is the purpose of the second and third safety constraints, which require that the designers and controllers of the system and of the system's environment respond appropriately (1) to mitigate the impacts of the hazard as much as possible if the hazard does occur and (2) to minimize any potential losses if the hazard's impact cannot be totally mitigated.

Specifying the hazard itself is a bit trickier. In Chapter 1, a hazard is defined as something that has to be under the control of or within the boundaries of the system being designed. That argument is not repeated here. In engineering, designers and operators can only prevent something that they have control over. In addition, design and operations have to be performed considering the worst-case environment, not the expected or average case.

A common mistake is to state the hazard with respect to a system component and not as a statement about the system as a whole. Failure or unsafe behavior of a system component is not a system hazard—it is a cause of a hazard. Causes will be identified later in the CAST process. By starting at the system level and later generating the causes of the system hazards, you are much less likely to omit whole pieces of the puzzle in your causal analysis. It will also be easier to identify when causes are missing.

Here are some examples of proper system hazards and some that are not:

System hazard: The aircraft stalls and does not have adequate airspeed to provide lift.

Non-system-hazard: The engines do not provide enough propulsion to remain airborne.

Non-system- hazard: The pilots do not keep the angle-of-attack down to prevent or respond to a stall.

System hazard: The automobile violates minimum separation requirements from the car ahead

Non-system-hazard: The driver maneuvers the car in a way that violates minimum separation

Non-system-hazard: The automation does not slow the car adequately to avoid violating minimum separation from the car ahead

Non-system-hazard: Brake failure.

System hazard: Explosion and fire in a chemical plant

Non-system-hazard: Failure of the pressure release valve

Non-system-hazard: Over-pressurization of the reactor

Non-system-hazard: Operators not maintaining control over the reactor pressure

Non-system-hazard: Inappropriate reactor design for the chemical being produced.

Why are these limits on the specification of hazards being imposed? Consider the last example of an incorrect system-level hazard: "inappropriate reactor design for the chemical being produced." The problem is that it ignores the question of whether that chemical should have been produced at all or whether it should have been produced under the larger plant conditions that existed at the time. Instead, it focuses on design of the reactor and not on the operations of the other components of the plant, which may have contributed to the loss. It ignores management decisions that may have played a role. Instead, it immediately focuses the investigation down to the physical design level of part of the system, that is, the reactor design itself.

Remember, our goal is not just to find an explanation for the events but to identify the most comprehensive explanation and *all* contributions to the loss in order to maximize learning and to prevent as many future losses as possible. Focusing on the behavior of one component will lead to missing the contributions of other system components and the interactions among multiple components, like the car, the driver, the design of the interface between the car and the driver, etc. Rarely, if ever, is only one system component involved in a loss; focusing too narrowly leads to missing important information.

At this point, the events can be delineated if desired. Given the limited usefulness of the chain of events in investigating a loss, generating it is not required to complete a CAST analysis. It can, in fact, divert attention away from where it should be directed. Focusing on events alone does not provide the information necessary to determine why the events occurred, which is the goal of the CAST analysis.

While not required to start a CAST analysis, identifying the proximate events preceding the loss may sometimes be useful in starting the process of generating questions that need to be answered in the accident investigation and causal analysis. Table 1 shows the primary proximate events leading up to and following the explosion at Shell Moerdijk and some questions they raise that any accident analysis should answer. Once again, the goal is to identify ways to prevent such accidents in the future, not to find someone or something to blame.

Remember that the goal of listing the events is NOT to select one or several to identify as the cause of the loss. Instead the goal is to generate questions for the investigation that will be used in the overall causal analysis. Do not use blame-laden words such as the operators *failed* to … or "should have" in describing the events. These imply conclusions and blame. Simply describe what the hardware or operators did or did not do.

Table 1: Proximal Events Leading up to the Shell Moerdijk Loss

ID	Event	Example Questions Raised
1.	The plant had been shut down for a short, scheduled maintenance stop (called a pit stop) to replace the catalyst pellets and was being restarted at the time of the explosion	*Accidents usually occur after some type of change (planned or unplanned). The change may commonly involve a shutdown, a startup, or maintenance (including a workaround or temporary "fix"). Was there an MOC (Management of Change) policy for the plant and the company? If so, was it followed? If it was not followed, then why not? If it was followed, then why was it not effective?*
2.	One of the restart procedures is to warm up the reactors with ethylbenzene. During the warming (reheating) process, uncontrolled	*Why were the reactions unforeseen? Were they foreseeable? Were there precursors that might have been used to foresee the reactions? Did*

	energy was released and unforeseen chemical reactions occurred between the warming up liquid (ethylbenzene) and the catalyst pellets that were used.	*the operators detect these reactions before the explosion? If not, then why not? If they did, why did they not do anything about controlling them?*
3	The reactions caused gas formation and increased pressure in the reactors.	*Did the design account for the possibility of this increased pressure? If not, why not? Was this risk assessed at the design stage?*
4	An automatic protection system was triggered that was designed to prevent liquid from entering the exhaust gas system (flare). But preventing the liquids from entering the flare also prevented the gases in the system from being discharged, increasing pressure in the reactor.	*Did the operators notice this? Was it detectable? Why did they not respond? This seems like a predictable design flaw. Was the unsafe interaction between the two requirements (preventing liquid from entering the flare and the need to discharge gases to the flare) identified in the design or hazard analysis efforts? If so, why was it not handled in the design or in operational procedures? If it was not identified, why not?*
5	Continued warming up of the reactors caused more chemical reactions to occur between the ethylbenzene and the catalyst pellets, causing more gas formation and increasing pressure in the reactor.	*Why wasn't the increasing pressure detected and handled? If there were alerts, why did they not result in effective action to handle the increasing pressure? If there were automatic overpressurization control devices (e.g., relief valves), why were they not effective? If there were not automatic devices, then why not? Was it not feasible to provide them?*
6	The pressure rose so fast that it could no longer be controlled by the pressure relief devices, and the reactor exploded due to high pressure and the separation vessel collapsed and exploded.	*Was it not possible to provide more effective pressure relief? If it was possible, why was it not provided? Was this type of pressure increase anticipated? If it was anticipated, then why was it not handled in the design or operational procedures? If it was not anticipated, why not?*
7	The contents of the reactor and its associated separation vessel were released into the wider environment. Sections of the reactor were blasted across 250 meters while other debris was later found 800 meters away. The explosion could be heard 20 kilometers away.	*Was there any way to contain the contents within some controlled area (barrier), at least the catalyst pellets?*
8	Two people working opposite Unit 4800 at the time of the explosion were hit by the pressure wave of the explosion and the hot and burning catalyst pellets that were flying around.	*Why was the area around the reactor not isolated during a potentially hazardous operation? Why was there no protection against catalyst pellets flying around?*
9	A large, raging local fire occurred, generating considerable amounts of smoke.	

10 Community firefighting, healthcare, crisis management, and crisis communications were initiated.

Notice that the word "failed" does not appear anywhere in the events description (and will not appear anywhere in the CAST analysis unless a physical component failure occurred). Nor are hindsight bias statements made such as "the operators should have …." It is way too early to start making judgments and conclusions (which should be avoided even later). In addition, the questions identified in this early part of the analysis are very general. As more is learned, these questions will be refined and the answers will generate many more questions. At the end, the goal is to answer all the questions or to determine that they cannot be answered. The answers together will provide an in-depth understanding of why this accident occurred and why the controls and protection devices did not mitigate the effects of the events.

The example event chain provided here is far from "complete" (whatever that might mean because more events could always be added). In fact, their completeness will have little impact on the results of the CAST analysis. The questions that need to be answered will be generated later if not here. The event chain simply can provide a starting place if one is not obvious. Again, starting with an event chain is not strictly necessary when doing a CAST analysis.

SUGGESTED EXERCISE: Take an accident with which you are familiar or for which you have access to a detailed description of what happened. Write down the major events. The list need not be complete; this is only a starting point. Create questions associated with the events that need to be answered to understand why the events occurred. Your questions will again almost surely not be complete unless the accident is very simple. The questions you create simply form a starting point in your thinking. Many more will be created (and hopefully answered) as you go through the CAST process.

Understanding What Happened in the Controlled Process

Identifying "why" something occurred requires first knowing "what" occurred. Physical injury or losses necessarily involve a physical process while other types of losses (e.g., financial) may involve a non-physical process. In either case, the first step is to understand what happened in the controlled process. While CAST can be (and has been) applied to losses involving other types of processes, such as business processes or even criminal and legal processes, the examples in this chapter focus on physical processes. The next chapter provides examples of applying CAST to social systems.

Explosions and fires are well-known hazards in chemical plants. There are usually a large number of protection systems, alarms, sensors, pressure relief valves, and so on. We start by examining the physical controls at the plant to determine why they did not control the explosion. At this point, a CAST analysis will not differ significantly from that done in most accident analysis except that in a CAST analysis, more than just physical failures are considered. For Shell Moerdijk, at the physical level, the CAST analysis would start by generating the following description of the physical controls:

Requirements for hazard mitigation:

Provide physical protection against hazards (protection for employees and others within the vicinity)

1. Protect against runaway reactions
2. Protect against inadvertent release of toxic chemicals or explosion
3. Provide feedback about the state of the safety-critical equipment and conditions
4. Provide indicators (alarms) of the existence of hazardous conditions
5. Convert released chemicals into a non-hazardous or less hazardous form
6. Contain inadvertently released toxic chemicals
7. Provide physical protection against human or environmental exposure after release

Controls:

The physical safety equipment (controls) in a chemical plant are usually designed as a series of barriers to satisfy the above hazard mitigation requirements. The Shell Moerdijk plant had the standard types of safety equipment installed. Not all of it worked as expected, however.

Emergency and safety equipment related to this accident were:

1. An automatic protection system to release gas to flare tower
2. Pressure relief devices in case of overpressurization
3. Alarms
4. Temperature sensors in the reactor

Next, we determine what happened. What physical failures and interactions led to the hazard?

Failures: None of the physical controls failed except for the final collapse of the reactor and separation vessel after pressure reached a critical level.

Unsafe Interactions: Accidents often result from interactions among the system components. In this case, the following unsafe (and mostly unexpected) interactions occurred:

1. The process to distribute the ethylbenzene over the catalyst pellets (wet them) resulted in dry zones. There were two main reasons for these dry zones:
   - The nitrogen flow was too low. To wet the catalyst properly, an adequate amount of ethylbenzene and nitrogen in the correct ratio must pass through the distribution plate. Because the flow of nitrogen was too low, the distribution plate did not operate properly. Later, due to this problem, along with other unintended interactions, the pressure increased eventually to the point where it exceeded the flow of nitrogen to the reactor. The nitrogen flow came to a standstill, resulting in a negative pressure differential.
   - The flow of ethylbenzene was unstable and at times too low. In addition to a sufficiently high nitrogen flow, a constant and sufficient flow of ethylbenzene is required in order to properly wet the pellets. The two reactors of Unit 4800 have different diameters, which means that reactor 1 requires an ethylbenzene flow of approximately 88 tons per hour while reactor 2 needs approximately 22 tons per hour. A constant flow of this volume was achieved in reactor 1. A constant flow of the correct volume was also initially achieved for reactor 2. However, once ethylbenzene began being heated, the flow became unstable. In the last hour before the explosion, this flow was virtually zero on two occasions. As a result, the ethylbenzene was not

evenly spread over the catalyst pellets, leading to the catalyst pellets not being adequately wetted and dry zones developing in reactor 2.

2. Energy released during the warming of the reactor led to unforeseen chemical reactions between the warming up liquid (ethylbenzene) and the catalyst pellets in the dry zones. As heating took place, the ethylbenzene began to react with one of the catalyst elements (barium chromate), generating heat. The ethylbenzene dissipated this heat in the areas that were sufficiently wetted. In the dry zones, however, this heat did not dissipate due to the lack of ethylbenzene. The result was that in the dry zones, the catalyst pellets heated up considerably, and there was localized development of very hot areas or "hotspots." The hotspots were not automatically detected due to the limited number of temperature sensors in the reactors.
3. Due to the rising temperature, the reaction in the hotspots kept accelerating, thereby producing even more heat. The localized temperature was now very high, which resulted in a chemical reaction between the ethylbenzene and another catalyst element (copper oxide). This reaction caused gases to be released. These follow-on reactions reinforced each other and could no longer be stopped: a runaway had developed. The rapidly rising temperature led to localized ethylbenzene evaporation.
4. Gas formation increased the pressure in the reactor. At the same time, the maximum liquid level in the second separation vessel was exceeded, causing the automatic protection system (used to release excess pressure) to shut down automatically in order to prevent liquids from entering the exhaust gas system (flare). As a result, the gases in the system could no longer be discharged. This automatic protection device to prevent liquids from entering the flare operated as designed, but had the unintended consequences of preventing the venting of the gas.
5. The buildup of gas caused the pressure to increase. Eventually, the pressure reached the point where the automatic pressure relief devices in place could not adequately release it. The pressure relief devices on the separation vessels were not designed for such rapid pressure increases, and eventually the collapse pressure of the reactors was reached. Reactor 2 collapsed and exploded, followed 20 seconds later by the explosion of the first separation vessel.
6. The contents of reactor and the separation vessel spread beyond the boundary of Unit 4800. A pressure wave and hot, burning catalyst pellets hit workers in the area causing injuries.
7. There are three remote-controlled containment valves. The explosions made these valves ineffective. The alternative was to use other limiting valves, but these valves cannot be remotely operated (they must be operated manually). Due to the intensity of the fire that had broken out and the risk of explosion, it was not possible for these to be operated immediately. An initial attempt was made around 02:30.

The above section shows why one does not need to start by listing the proximal events in isolation from the CAST analysis. The important events (failures and unsafe interactions) will be identified here as well as questions arising from these events.

After addressing what happened, we need to look at why it happened. Most of the reasons will be found in the later analyses, but physical design deficiencies and contextual factors are included here.

Missing or inadequate plant physical controls that might have prevented the accident:

1. There was an inadequate number of temperature sensors in the reactor to detect hot spots.
2. The plant was not fitted with pressure relief valves that would have prevented a runaway. Those that were installed were not designed for the rapid pressure increases that occurred.

Contextual Factors:

1. The plant was out of operation for a short, scheduled maintenance to replace the catalyst-causing granules.
2. Unexpected reactions occurred due to vulnerabilities related to the design, including the:
   - Potential for insufficient wetting (hot spots) due to design flaws.
   - Use of ethylbenzene and a design assumption that this substance is inert in the presence of the catalyst pellets.

Summary of the Role of the Physical Components in the Accident: None of the physical controls failed. The final physical collapse of the reactor and separation vessel occurred after pressure reached a critical level, which resulted from unexpected and unhandled chemical and physical interactions. Many of these unsafe interactions were a result of design flaws in the reactor or in the safety-related controls.

There are some things to be noted in this description. The description is restricted to the physical system. Operators, process control systems, etc. are not—and should not be—mentioned. The role they played will be considered later.

Also, remember that the accident model (STAMP) underlying CAST says that accidents result from lack of control, which may include control of failures. In this part of the analysis, an understanding is gained about why the physical controls were unsuccessful. Controls are used to enforce constraints on the behavior of the system components and the system as a whole and the identification of the inadequate controls will assist in refining the high-level system hazards and the safety constraints needed to prevent the hazards.

The original hazards and constraints were very general and apply to almost any chemical plant process. In fact, these could be identified for an industry as a whole and used for any accidents. Identifying the specific failures and unsafe interactions that occurred in the physical process will allow the general system hazard and safety constraints to be refined for this particular loss and therefore provide increased direction for the causal analysis.

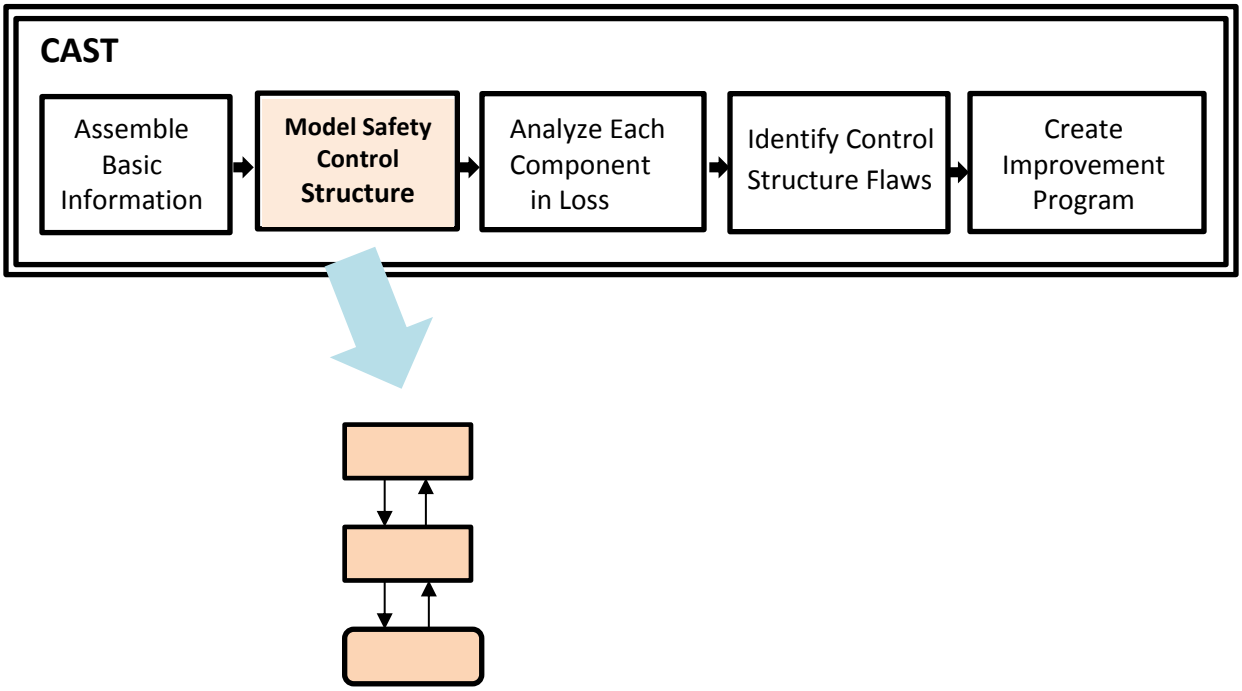
As an example, in the Shell Moerdijk case, the general constraint to keep chemicals under positive control can now be refined to identify the specific constraints that were violated and thus the specific goals for this accident analysis:

1. Chemicals must be under positive control at all times, i.e., runaway reactions must be prevented (see the general Safety Constraint 1 under System Hazard 2 on page 37).
   a. Distribution of ethylbenzene over the catalyst pellets must not result in dry spots during a reactor restart.
   b. Protection and warning systems must be created to react to the heat and pressure generated by unintended reactions related to dry spots if they nonetheless occur.

Constraints are theoretically enforced either through eliminating the related hazardous states from the physical system design, providing controls in the physical design to prevent or minimize the hazard, or providing operational controls. Usually, all are used as engineering design can almost never be perfect. So, the goal of the analysis now is to identify why the design flaws were introduced, i.e., why the attempts to enforce the constraints through physical design were ineffective and why the operational controls also were not successful.

To achieve this analysis goal, we start by looking at the safety control structure to identify its limitations in preventing the accident. Normally, both system development and system operations need to be included. Too often, accident analysis only focuses on operations and not system development and, therefore, only operational limitations are considered. Deficiencies in the way the system was developed are not always identified or fully understood.

Modeling the Safety Control Structure[15]



[15] A more common name for the safety control structure is the Safety Management System (SMS), although some standards for safety management systems are incomplete with respect to the safety control structure. The safety control structure includes functions and components not always in an SMS.

2. *Model the existing safety control structure for this type of hazard.*

The model of causality underlying CAST treats safety as a *control* problem, not a *failure* problem. The cause is always that the control structure and controls constructed to prevent the hazard were not effective in preventing the hazard. The goal is to determine why and how they might be improved.

Because CAST focuses on the controls and controllers and their role in the accident, modeling the control structure is necessary to start the analysis. There is no single or best way to accomplish this, assuming that a safety control structure for that system and the hazards identified in the previous step does not already exist. But there are some hints or heuristics that may help. The two most helpful are to (1) start with a very high-level, abstract control structure and then refine it later and (2) start by identifying the controls that exist for the hazard or hazards in general. These two activities may be done separately or the activities may be intertwined.

Usually, similar accidents have occurred previously, and controls have been created to prevent them. The major goal of the analysis in that case, as stated above, is to determine why they were not effective and how to improve them. Some of the controls will be common safety practices, while others may be special controls designed for unique situations. All the controls need not be identified at first. The questions generated as the analysis proceeds will identify more constraints and controls. The only mistake is to start too narrowly as this might cause you to miss important controls and controllers or system hazards. Important clues in identifying controls can usually be obtained from the original hazard analysis on the plant, assuming a hazard analysis was done that goes beyond simply identifying probabilities of component failures in order to assess the risk of the completed design.

If STPA was used for designing the system, there will be an explicit listing of the scenarios leading to an accident that were identified and the controls created during system development. If an STPA analysis for the system already exists, then it will provide a lot of information about what might have gone wrong. Theoretically, the STPA analysis should contain the scenario that occurred. If not, then there was a disconnect between the analysis during development and the operation of the system. One possibility is that the original STPA did not completely specify all the potential scenarios. Another is that the scenario that occurred was identified, but an effective control was not implemented. And, of course, the system and its environment may have changed over time after the system went into operation, negating the effectiveness of the designed controls and introducing new causal scenarios that were not analyzed originally.

If a control structure for the system does not already exist, most people find it helpful to start with a very abstract, high-level control structure that involves the general controls for this type of event. Figure 13 shows a preliminary, very high-level safety control structure for Shell Moerdijk. There are two physical processes being controlled: chemical production and public health.

The Shell Moerdijk plant has direct responsibility for control of the safety of the chemical process itself while state and local emergency management have the responsibility for preserving public health. The global Shell enterprise exerts control over the subsidiaries and Shell plants around the world. At this early point in the analysis, the type of control and responsibilities will be mostly unknown. These will need to be elaborated during the investigation. With respect to government oversight, there are local and Dutch oversight agencies and overarching EU controls. It is usually helpful to document the responsibilities (as understood so far) for each of these components with respect to the hazards involved. Again, the model will change as more information is accumulated during the investigation.

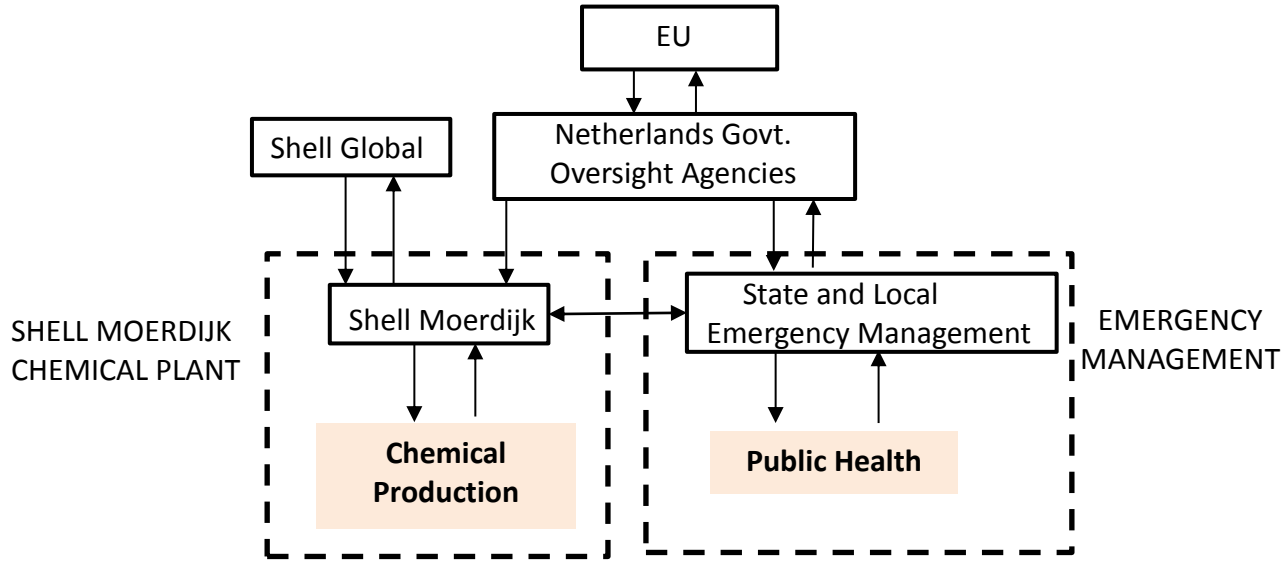


Figure 13: Very high-level safety control structure model for Shell Moerdijk.

In the process of creating the model, it may be helpful to first identify what types of controls exist both in general and in this particular system, for preventing the hazard. Once you have started the list of controls (you will probably add to it later), consider where responsibility for them exists in the physical design, human controllers, automation, or organization and social structure. For example, there will probably be physical controls (such as interlocks and relief valves), electronic controls (such as ground proximity warning systems on aircraft), electronic process control systems that monitor and adjust process parameters, human operators, equipment maintainers, management oversight, regulatory controls, and so on.

After the controls have been identified, modeling the hierarchy—to show what controls what—should be the only remaining challenge. Don't be surprised if you have some difficulty with this at first and end up making several changes. If you start with a high-level safety control structure, you should be able to place the controls in the structure as you discover them. As you proceed, more details can be added.

The control structure will probably also change as the investigation and understanding of the system develop. It may be helpful to make any changes first at the highest level that they are visible. Changes in the high-level control structure can lead to multiple changes at a lower level of abstraction. First making changes at a high-level will help to identify where extensive revisions in the control structure may be needed. For example, let's say you find late in the analysis process that maintenance was involved. Rather than try to add maintenance to the very detailed control structure developed by that time and include all the interactions it might have with other system components, it may be easier to go back to a high-level structure and add maintenance as a controller of the equipment and understand its relationship with other controllers. Once the overall role and place of maintenance in the system is modeled, more detailed control structures can be modified to include their relationships with maintenance controls.

Usually, the controls to prevent an accident are distributed around the control structure to the groups or system components best able to enforce the constraints and controls. Higher level components will have more general responsibilities, including the responsibility to oversee the operation of controls by the components below. For example, human operators may be responsible for adjusting physical parameters in the controlled process. Operations management may be responsible

for providing the training needed by the operators to perform their responsibility reliably and for hiring workers with appropriate backgrounds. Operations management probably will also be responsible for monitoring performance during operations to ensure that operators are performing adequately. Higher levels of management may ensure that training is taking place (but usually not the responsibility for specifying the details of that training) and that operations management is performing acceptably. The highest levels of corporate management and external regulatory oversight will be at yet a higher level of abstraction and detail. Together, the entire safety control structure should ensure that hazards are eliminated or controlled and safety constraints on the system behavior are enforced.

Once again, everything need not be identified at first in the causal analysis. Generating the questions and answering them as the analysis proceeds, will identify more controls and even constraints. Once several CAST analyses exist for a certain type of loss, the controls probably will have been identified in previous analyses. This step then becomes straightforward and simply involves finding unique controls for the particular loss involved. Why the controls were effective is part of the next step in the analysis. In this step, they are only listed.

Here is a demonstration of the refinement process for the Shell Moerdijk control structure, starting with the very high-level control structure in Figure 13. You need not generate a complete and final control structure at this point. Changes will likely be made and even structures added as the investigation proceeds. The goal is just to identify the controllers and their responsibilities to start the detailed CAST analysis.

Explosions and fires are well-known hazards in chemical plants, and controls are always included to prevent them. Controls will usually involve protection systems, alarms, sensors, pressure relief valves, and so on. Beyond the physical protection systems, there will usually be operators, process control systems, and safety management. Above them are various levels of management for these system components and for plant operations in general. A safety group usually exists that oversees both development and operations from a safety standpoint. This group may be responsible for various types of hazard analysis and risk assessment activities. Figure 14 includes the catalyst supplier (although it could be added later if the catalyst's role is not yet apparent) because the events point to a runaway reaction while the catalyst was being reheated. If it is not needed to explain the accident, then it can be removed later or it could be added later if omitted at this point. While the control structure can guide the analysis and make it easier to identify missing causal analysis, its major use is in the final report to help provide a coherent explanation of the accident, why it occurred, and what needs to be changed.

Responsibility for design activities rests somewhere; in the case of Shell Moerdijk, local design groups develop plant designs (not shown in Figure 14 but assumed to be under the control of and part of plant management) which are overseen or reviewed by Shell Projects and Technology at the Global level. There is also always some type of safety management at the corporate or global level. Finally, executive management (at least at the Board of Directors level) almost always has some type of corporate responsibility and oversight of safety at the enterprise management level. Here is what the control structure might look like at this point:

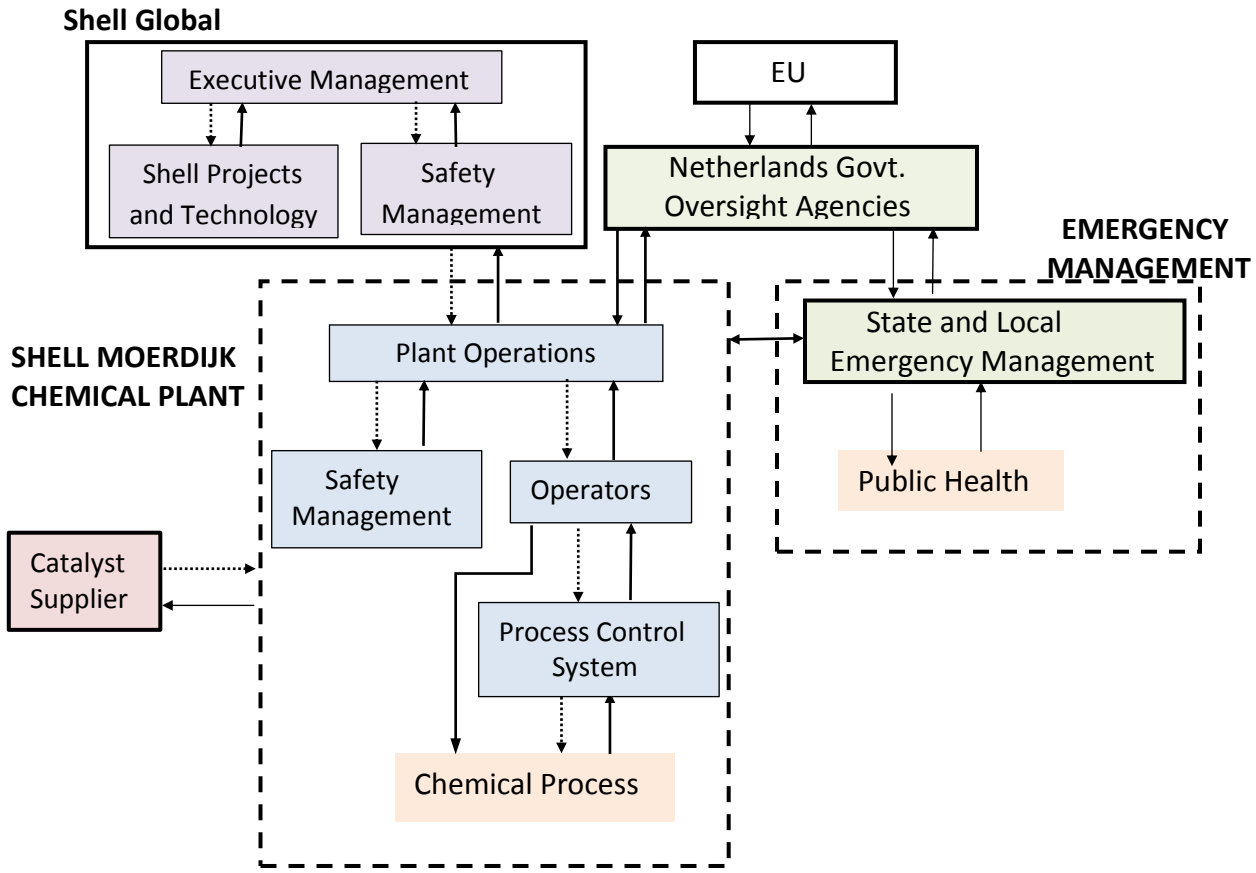


Figure 14: Shell Moerdijk safety control structure with more detail.

For readers who are familiar with STPA, which also starts with modeling the control structure, the model used in CAST need not be as detailed as that needed to perform STPA. In using CAST, most of the details will be filled in as the analysis proceeds. But the basic components should be identified at the beginning to help guide the analysis.

Once the basic components are identified, a specification of the responsibilities of each component can be started. For example, here are the responsibilities for the components included so far in the Shell Moerdijk safety control structure (Figure 14):

Process Control System safety-related responsibilities:

- Assist operators in controlling the plant during normal production and off-nominal operations (shut down, startup, maintenance, emergencies, etc.).
- Display relevant values, provide alerts, issue control actions on plant equipment.
- Control temperature, pressure, level, and flow to ensure that the process remains within the safe margins and does not end up in an alarm situation.

Operator Responsibilities:

General:

- Operate the plant in a way that does not lead to hazards
  - Monitor plant conditions and alarms
  - Control the process so that that it stays within safe boundaries of operation
  - Respond to unsafe conditions that occur.

Specific to this accident:

- Adjust gas and liquid flows as needed during startup.
- Make sure the Unit is not heated too quickly (in part to prevent damage to the catalyst pellets).

Plant Safety Management Relevant Responsibilities

- Identify plant hazards and ensure that they are eliminated, mitigated, or controlled.
- Either provide work instructions for safety-critical activities or review the work instructions provided by someone else for their safety implications.
- Ensure appropriately trained, skilled, and experienced people are assigned to high risk processes.
- Follow the Management of Change (MOC) procedures by doing a risk assessment for changes and implement risk controls based on the results.
- Provide for emergency treatment to exposed or injured individuals and ensure required medical equipment and personnel is available at all times. [*The injured personnel were treated effectively on the scene, so this aspect is not considered further.*]
- Perform audits of safety-critical activities or assist plant operations management in performing such audits [*It is not clear from the accident report who is responsible for audits, but there do appear to have been audits.*]

Operations Management relevant Safety-Related Responsibilities

- Establish safety policy for operations
- Ensure that Safety Management is fulfilling their responsibilities and providing realistic risk and hazard assessments.
- Use the results of the hazard and risk analyses provided by Safety Management in decision making about plant operations.

- Create a Shell Moerdijk Safety Management System consistent with the overall Shell Global Safety Management System and make sure it is both effective and being followed.

More specific operations management safety-related responsibilities include the following:

- Provide appropriate training for operators for nominal and off-nominal work activities.
- Follow MOC (Management of Change] procedures that require performing a risk assessment for changes or ensure that safety management is doing so. Use the risk assessment to provide oversight of the process and to design and implement risk controls in the plant and the operating procedures.
- Prepare (or at least review) the work instructions. Ensure they are safe and are being followed.
- Minimize number of personnel in the vicinity (at risk) during high-risk operations, such as a turnaround
- Keep records of incidents and lessons learned and ensure they are communicated and used by those that need to learn from them.
- Provide personnel assignments that are commensurate with the experience and training required for the activity.
- Provide a process control system that can assist operators in performing critical activities.
- Conduct audits. Establish leading indicators to be used in the audits (and in other feedback sources) or ensure that safety engineering is identifying appropriate leading indicators.

Shell Corporate Projects and Technology (Engineering) Safety-Related Responsibilities

- Create a safe design: Perform hazard analysis (or use the results of hazard analysis created by another group) and eliminate or mitigate the hazards in the design.
- Provide design, hazard, and operating information to the plant operators to assist those who are operating the plants in avoiding any hazardous scenarios that the designers were not able to eliminate or adequately mitigate in the design itself.
- Learn from the operation of their designs and improve the designs based on this feedback.

Shell Corporate Safety Management Relevant Responsibilities

- Safety of plant design, including conduct of hazard analysis on designs licensed to subsidiaries.
- Oversight of operational safety at the various Shell plants and facilities.
- Management of change procedures related to safety: creating them, making sure they are followed, and improving them using feedback from incidents.
- Communication among separate plants in different parts of the world about incidents, lessons learned, etc.
- Creating and updating a Shell-wide Safety Information System and ensuring the information is being communicated adequately both within Shell Corporate and globally and that it is complete and usable.

Executive-Level Corporate Management Responsibilities:

- Ensure that measures are taken to
  - Prevent major accidents from occurring and,
  - If accidents do occur, mitigating their consequences for humans and the environment
- Ensure the health and safety of the employees in relation to all aspects associated with the work (based on the Working Conditions Act and other regulations)
- Follow the government regulations in the countries where their plants are located.
- Create an effective safety management system and establish a strong safety culture policy. Ensure that the SMS and safety policies are being followed and they are effective.

Catalyst Manufacturer Safety-Related Responsibilities

- Provide information to customers necessary to evaluate the use of their catalyst in the reactor being designed and/or operated
- Alert customers when changes are made in the catalyst that could potentially affect the safety of its use.

Dutch Regulatory Authorities

All Dutch oversight safety and environmental authorities are grouped together here.

There are two main policies underlying this regulatory oversight:

1. Brzo: Companies must take all measures to prevent accidents and, if they occur, mitigate their consequences for humans and the environment. The company must implement this obligation by laying down policy assumptions in the Prevention Policy for Serious Accidents (PBZO), drawing up a safety report (VR), and organizing a safety management system.
2. Wabo: Regulators must check whether the company complies with regulations connected to the environmental permit, i.e., environmental safety.

General Relevant Safety-Related Responsibilities:

- Responsible for supervision and enforcement of Dutch laws to protect the environment and the public. Perform Brzo inspections focusing on process safety and Wabo inspections focusing on environmental safety.
- Responsible for enforcement of EU health and safety laws within the Netherlands.

More Specific Responsibilities:

- Identify shortcomings at companies they are responsible to oversee.
- Encourage companies to improve their safety-critical processes through supervision and enforcement. Identify shortcomings and persistently question companies to prompt them to investigate and detect deep-seated causes of incidents and accidents. Ensure that any shortcomings identified are corrected.
- Assess modifications made to plants, procedures, and processes (although they are not expected to perform the risk analyses for the companies).
- Pay greatest attention to safety-critical processes, including maintenance and reactor start-up

Emergency Services Responsibilities

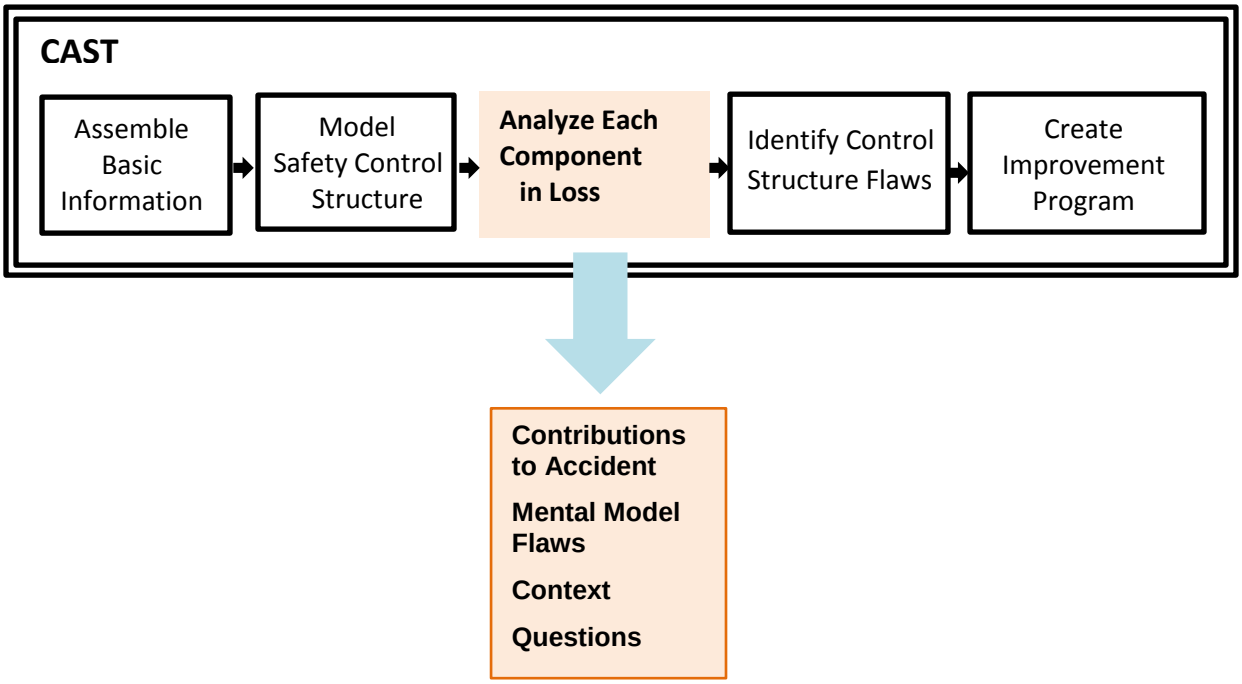
- Firefighting, crisis management, crisis communications including among other things:
  - Informing citizens of the incident,
  - Measuring substances released on a coordinated basis,
  - Operating a telephone advisory line,
  - Informing citizens about the results of the measurement of the substances released and the ensuing recommendations.

Again, the control structure model is not fixed but can and most likely will evolve and change as more is learned about the accident and about the responsibilities of each of the control structure components. The CAST analysis will essentially involve identifying whether the responsibilities were effectively implemented and, if not, why not and what changes might be made to prevent this type of accident in the future. Another potential conclusion might be that responsibilities are not adequately identified or

appropriately assigned and that the basic safety control structure needs to be redesigned. Most accident investigations will likely find both types of contributors to the loss.

How does the analyst identify the responsibilities? Most of these will be documented somewhere, either in company manuals or government documents. In addition, questioning the controllers about their own and other's responsibilities during the investigation will at least elicit what the controllers think they are. Confusion and inconsistencies here could be a clue as to why the accident occurred. One of the important characteristics of the U.S. Navy's SUBSAFE program, which has been spectacularly successful over its 50+ year existence, is that everyone in the program knows exactly what are their own responsibilities and also what everyone else's are. By continually reinforcing and auditing this knowledge about responsibilities, accidents are reduced.

Individual Component Analysis: Why were the Controls Ineffective?



3. *Examine the components of the control structure to determine why they were not effective in preventing the loss:*

   Starting at the bottom of the control structure, show the role each controller played in the accident and the explanation for its behavior: why each control component did what it did and why the controller thought it was the right thing to do at the time.

Once the basic control structure and controls are identified, the next step is to show why the control structure, i.e., the current controls, did not prevent the accident. There will be two parts to this process. The first, described in this section, looks at the individual controllers (which may be automated or human) and the role they played in the accident. The second, described in the next section, looks at the operation of the control structure as a whole and the interactions among the components. Remember, the goal is to identify flaws in the control structure: not to assign blame to individuals or individual components but to understand why it made sense for them to act the way they did.

Also, as started in the previous steps, the CAST process includes generating questions that need to be answered during the investigation so that at the end, a complete explanation for why the accident occurred can be provided. I find it most helpful to start at the bottom components in the control structure and work my way upward.

There are several parts in the CAST analysis of each controller:

- Component responsibilities related to the accident
- Contribution (actions, lack of actions, decisions) to the hazardous state: [16]

Why?

- Flaws in the mental/process model contributing to the actions:
- Contextual factors explaining the actions, decisions, and process model flaws:

The first two parts simply document the role the component played in the loss, if any. The component safety-related responsibilities were identified when modeling the safety control structure. Only those related to the loss need to be considered. The role or contribution (behavior related to the hazardous state) will be the responsibilities that were not fulfilled. For example, one responsibility of the operators during reheating of the reactor at Shell Moerdijk after a maintenance stop is to control the process so that it stays within safe boundaries of operation. In this case, they did not adjust the gas and liquid flows in a way that prevented the overheating of the catalyst pellets. Remember, no judgmental or hindsight words should be used like they "failed" to adjust the flows or they "should have" adjusted the flows. Simply describe what happened in a non-accusatory way. The behavior that contributed to the loss is described in a straightforward manner that simply says what the person or group did or did not do.

The "why" part of the analysis involves explaining why the component behaved in the way it did, i.e., the contextual and other factors that made the behavior seem correct to them at the time. For example, contextual factors might include incorrect information that the controller had at the time, inadequate training, pressures and incentives to act the way they did, misunderstanding about their role or about how the controlled components worked, etc. This "why" part of the analysis will also involve answering the questions previously raised about the behavior of this component. Answering the "why" questions for a component usually raises more questions, which may need to be answered in the analysis of the higher levels of the control structure. The goal is that at the end of the CAST analysis, all the questions raised are answered. In reality, there may be remaining questions that just cannot be answered definitively. These should, of course, be documented in the final conclusions. If the people involved understand that the goal of the accident investigation and causal analysis are not to find "guilty parties,"

[16] Although in STPA the term "unsafe control actions" is used without much complaint, the use there is about hypothetical actions and not things that actually have occurred. Using that term in CAST lends a tint of blame and judgment and should be avoided. We have used various terms such as "Control actions contributing to the hazard" or contributory control actions or simply "role or contribution of the controller to the hazardous state" to avoid common pejorative terminology.

they are more likely to provide candid answers. Enlist their help as part of an explanatory process to improve safety in the future. This kind of trust, of course, needs to be established over time.

Focus on understanding "why" the controllers acted the way they did. Most controllers are trying to do the right thing. If they had evil intent (were suicidal or homicidal), of course, that needs to be identified but such behavior is rare in accidents. Usually the controllers are trying to do a good job, and there is some reason that they didn't. For automated controllers, understanding will involve looking at the design and the designers of the automation and the assumptions they made about what type of behavior was required. Almost all software-related accidents involve incorrect assumptions about the behavior required to prevent the hazards, i.e., a flawed understanding of the requirements for safe operation.

Understanding the reasons for the behavior that occurred will provide the best guidance possible in creating effective recommendations. If the accident report identifies only what the controller did wrong, we learn almost nothing required to prevent the same behavior in the future beyond telling people "don't do that." As the controllers usually had a good reason for doing it at the time, this type of instruction is not helpful. Rules and procedures are never mindlessly obeyed under all circumstances. If the designers of the system intend for operators to thoughtlessly follow written directions, then those control responsibilities should be automated. Checklists are often provided as guidance, but we usually want people to make judgments about the appropriateness of the checklist at the time of the emergency. If they did not follow the checklist when they should have, then we need to understand why.

Humans are left in systems today to make cognitively complex decisions about what needs to be done. If they make the wrong decisions, the reasons why (e.g., they had incorrect information, they were misled by the process control system output, they were not given adequate support to make safe decisions, there was no or misleading feedback about the state of the component they were controlling) will provide the information needed to redesign the safety control structure and safety controls to assist controllers in making better decisions in the future.

The CAST process is designed to avoid hindsight bias as much as possible. After the accident or incident, the behavior will appear to be clearly wrong. That's obvious and doesn't need to be stated. What is useful is to understand why—*at that time*—it was not obviously wrong to the controller. Why not? What types of information did they need to make a better decision? Did they have it? Did they understand what that information meant at the time? Were there other competing pressures that made it difficult for them to absorb the information or to process it? The more fully the context can be identified, the more effective any resulting recommendations will be in reducing future losses. The context may be physical, psychological, informational, managerial, and situational, such as workload or productivity pressures, incentives/disincentives, etc.

The notation used to record the results of this analysis step is irrelevant as long as the information is recorded and easy to understand. Some suggestions for notations we have been used successfully are included at the end of this chapter.

In this handbook, only a few examples from the CAST analyses of the Shell Moerdijk are shown. A summary of the role played by all the components is provided in Appendix B. Links to the complete CAST analysis for Shell Moerdijk as well as many other real accidents are provided in Appendix A.

An automated process control system is a standard controller for plants. Therefore, it's a convenient place to start in understanding the Shell Moerdijk explosion. The safety-related responsibilities include:

Safety-Related Responsibilities of the Process Control System:

1. Assist operators in controlling the plant during normal production and off-nominal operations (shut down, startup, maintenance, emergencies, etc.).

2. Display relevant values, provide alerts, issue control actions on plant equipment.
3. Control temperature, pressure, level, and flow to ensure that the process remains within the safe margins and does not end up in an alarm situation.

To identify its role in the loss, we can start with determining whether these responsibilities were satisfied. In this case, the process control system contributed to the accident by:

Contribution to the hazardous state:

1. The process control system did not provide the assistance required by the operators to safely control the start-up process, including automatically controlling the heating rate and other important variables.
2. The process control system did not step in to stop the process when pressure and temperature increased precipitously.
3. The process control system did not issue an automatic reset after two high-high level alarms, so the gas discharge system remained closed.

As an example of the detailed "why" analysis, i.e., the contextual factors for number 2 (i.e., the process control system did not stop the process when pressure and temperature increased precipitously), consider:

Why? (Contextual Factors Affecting the Unsafe Control)	Questions Raised
There was no emergency stop button for Unit 4800. Without an emergency stop, there was no way to safely stop the operation of the unit quickly with a single press of a button. No reason was provided for this design "flaw" in the accident report but could have been answered at the time of the investigation. Emergency stop buttons are standard in safety-critical systems.	*Was this complacency, cost, or was there an engineering reason?*
The instrument-based safety devices were designed to respond to and prevent particular conditions, but not the ones that occurred. After this accident, a safety device was added to protect Unit 4800 from an excessively high temperature due to an unwanted chemical reaction with hydrogen.	*Why were these conditions omitted? Was a hazard analysis performed that could have identified them?*
There is a containment system, which is described as "one or more appliances of which any components remain permanently in open connection with each other and which is/are intended to contain one or more substances." The valves of the containment system, however, cannot be remotely operated and must be operated manually. Due to the intensity of the fire that night and the risk of additional explosions, it was not possible for these valves to be operated immediately and, in fact, were not operated until several hours later when the fire had been extinguished.	*The containment system design was not useful in this situation. Was this known beforehand? Was it impossible to design one that can be operated remotely?*

An important part of the understanding of why a controller behaved the way it did may arise from an incorrect process/mental model. The CAST analysis involves both identifying the flaws in this model and determining why they occurred.

Process Control System Process Model flaws: The Shell Moerdijk process control system, for the most part, had correct information about the state of the process. There was some missing information about temperature, however, resulting from an inadequate number of temperature sensors provided in the reactors.

When the component analysis has been completed and documented (details not included here), a summary can be made of the role of the component in the accident along with recommendations. Any open questions that are important in the causal analysis should also be documented.

Summary of the Role that the Process Control System Played in the Accident: The process control system was not designed to provide the necessary help to the operators during a start-up or to allow them to easily stop the process in an emergency. The reason for these design decisions rests primarily in incorrect assumptions by the designers about the impossibility of the scenario that occurred. Even after previous incidents at similar plants in which these assumptions were violated, the assumptions were not questioned and revisited (see the CAST analysis of the safety information system).

More generally, the process control system was configured only for the normal production phase. There were no special automated control circuits for the heating phase after a catalyst has been replaced, which is the phase in which the problems arose. In fact, this phase is commonly known to be the most accident prone, so the decision not to provide automated help to the human operators during this phase is quite strange, but no explanation is provided in the accident report.

Unanswered questions: Why was a decision made not to provide assistance to the operators during the restart phase of operations? Why was an emergency stop capability not designed into the system?

Recommendations: The operators' knowledge and skill are most challenged during off-nominal phases, and most accidents occur during such phases and after changes are made or occur. The process control system should be redesigned to assist operators in all safety-critical, off-nominal operations (not just this restart scenario). For manual operations, the goal should be for the process control system to provide all necessary assistance to the operators in decision making and taking action and to reduce attention and time pressures (see the section on the operators).

The rest of this section shows examples from the Shell Moerdijk CAST analysis for different types of controllers. The process control system analysis provides an example of an automated controller. The other controllers for the Shell Moerdijk Chemical Plant were people or groups of people. Details, again, are omitted here for space reasons.

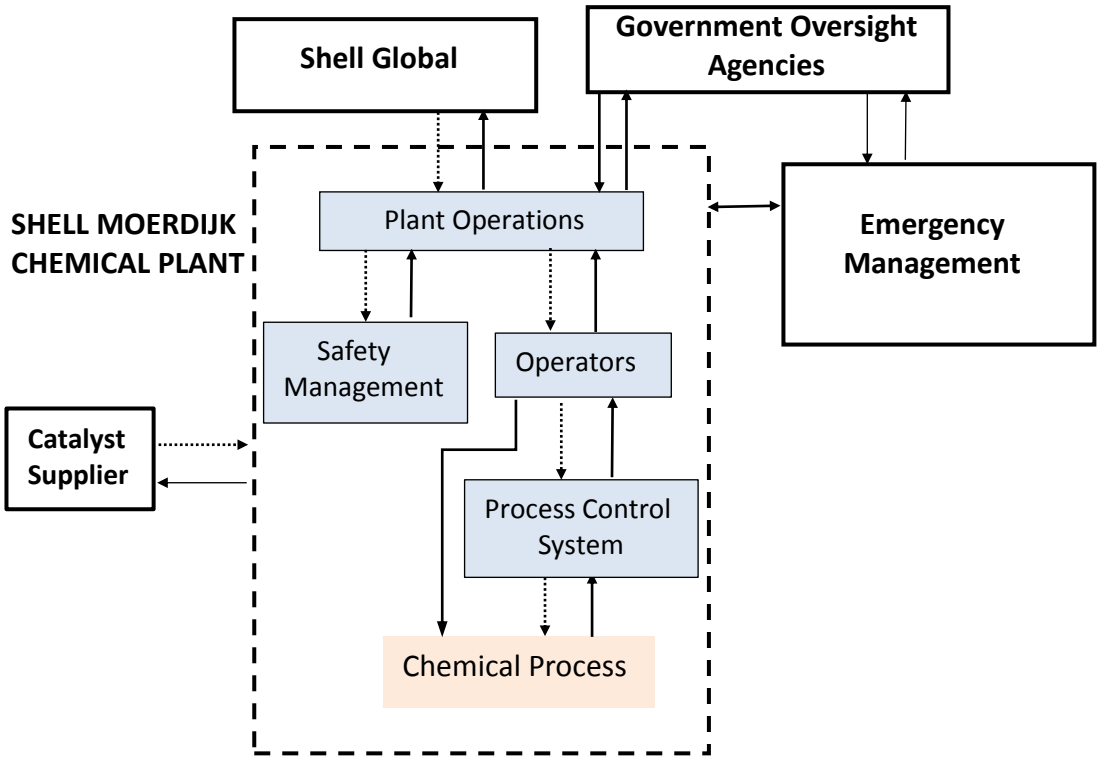


Figure 15: Shell Moerdijk Chemical Plant Safety Control Structure.

Operators

The operators' actions clearly contributed to the explosions. For example, they manually added additional warmth to the ethylbenzene at a time when heat was increasing precipitously; they did not notice and respond to hot spots and negative pressure differential; they did not respond appropriately to alarms; they left the gas discharge system closed when the gas was increasing; they did not stabilize, slow down, and stop the process when pre-set limits were exceeded (which is a fundamental principle in operator training at Shell); etc.

Given all these things that in hindsight the operators did wrong, they appear to have major responsibility for the loss. In fact, listing these actions is where many (most?) accident causal analyses and accident reports stop and the operators are deemed to be the major cause of the loss. While it is possible that everyone working the turnaround that day was negligent and irresponsible, it is more likely that they were trying to do their best. Without understanding *why* they made bad decisions, i.e. why the decisions seemed correct to them at the time, we cannot do much about preventing similar flawed decision making in the future. Many of the answers lie in higher levels of the control structure, but some of the operators' actions can be understood by looking at their process models and the context in which they were making decisions.

The relevant general safety-responsibilities assigned to the operators:

- Operate the plan in a way that does not lead to hazards
  - Monitor plant conditions and alarms
  - Control the process such that it stays within safe boundaries of operation
  - Respond to unsafe conditions that occur

And specific to this incident: • Adjust gas and liquid flows as needed during startup • Make sure the Unit is not heated too quickly (in part to prevent damage to the catalyst pellets)

None of these responsibilities were fulfilled. Examples of operator behavior that contributed to the hazardous state include:

- The operators did not stabilize or halt process before the explosion when critical process boundaries were exceeded.
- Heating was started (around 21:00) while the situation was still unstable and after only 45 minutes of wetting. Proper wetting had probably not been achieved by that time.
- The operators manually added additional warmth to the ethylbenzene at a time when heat was increasing precipitously.
- The operators did not notice and respond to hot spots. They also did not notice and respond to the related negative pressure differential.
- The operators did not properly adjust nitrogen flow. The lower (than required) nitrogen flow was one of the causes of the accident.
- The operators did not respond to alarms.

Looking only at these behaviors, the behavior of the operators seems egregious. This is where most accident reports stop. But the picture looks very different when the contextual factors and process model flaws are considered. Because of space reasons, only a few examples of these are provided below. The reader is referred to the full analysis in the CAST report for the more detailed analysis.

Why? (Contextual Factors Affecting the Unsafe Control)	Questions Raised
The operators were not provided with the information they needed to make correct decisions. The process control system provided almost no support (feedback). Throughout the accident report, there are many actions by the operator that are noted to require intense attention and deep understanding of the process dynamics.	*Why? Was any human factors analysis done when the decision was made to have the operators manually control startup to ensure that they were capable of doing this reliably? And without process control system support?*
Adjusting gas and liquid flows was known to be difficult, partly because of weaknesses in the design of the central pump. In addition, the job analysis does not provide clear instructions about how the filling and circulation has to be done. The only clear instruction was that the central pump not be allowed to run “dry” or it would break.	
Safety during the heating and wetting of the reactors was dependent on the knowledge and skill of the operators and production team leader on duty at the time. Shell Moerdijk’s written policies required that the starting and stopping of the reactors had to be done by experienced operators using the work instructions provided for this purpose. However, while the personnel performing this maintenance stop were experienced staff and were trained for working on this unit	

during regular production, a catalyst change only occurs once every three or four years and this was their first experience with restarting the reactor. At the same time, they were not provided with support from the process control system for this startup.	
The accident report says that the start-up procedures had been followed correctly by the operators. The problem, then, must have been in the procedures themselves. In fact, the work instructions used by the operators were incorrect and incomplete. The work instructions did not follow the format provided by Shell for such instructions and omitted much of the required information such as critical conditions and required steps to be taken by the operators. Nitrogen flow was not considered critical, for example, and was not included in the work instructions although it turned out to be critical after the fact.	*Why were incorrect and incomplete work instructions provided to the operators?*
The startup procedures were produced by the operators. There does not seem to have been any expert review by engineers and safety personnel. The accident report provides no explanation for *w*hy operators are writing their own work instructions for safety-critical operations without at least expert review by engineers and safety personnel.	*The report does not answer the obvious questions here: Were the work instructions produced by the operators performing the startup (who had no experience)? If it was other operators, did they have the experience and knowledge to create the work instructions? Who reviews these work instructions? Were they reviewed by anyone? (The answer to this question appears to be no).*
There is a design book, created by Shell Global Projects and Technology, that contains detailed information about the design and operation of the reactor. The Design Book was not used in creating the work instructions for the startup because, the accident report says, the book was too detailed and "intricately presented" and was not understandable by the operators charged with drawing up the work instructions.	*There are many obvious questions raised here.*

Why? (Process Model Flaws)	Questions Raised
There was a lot of hindsight bias in the accident report describing what the operators "should have" done, but the conditions that occurred were all consistent with their expectations (process model) given the conditions during previous maintenance stops. The operators considered fluctuations in pressure to be normal during restarts (process model flaw). The pressure had fluctuated continually since the beginning of the restart. Such	*Why were the expectations (their mental models of process behavior) not correct in this instance?*

fluctuations had occurred during previous restarts and that was what they expected. In hindsight, of course, these expectations turned out to be wrong. Given the situation, the number of alarms that sounded and their frequency was not out of the ordinary, without knowing *after the fact* that the process was indeed not in an ordinary state.	
The accident report says that the ability to make an assessment to intervene in special situations requires knowledge of, experience with, and thorough preparation for such special situations. The operators must fully grasp what caused the unit to exceed limits in order to assess risk. The operator did not have the required knowledge or expertise. . In fact, even the corporate safety engineers did not know that the conditions that occurred here could result in a hazardous state. If the designers did not believe such scenarios were possible, why would the operators? In fact, nobody at Shell thought that a scenario involving a fast and high-pressure buildup was possible.	*Why did the designers and corporate safety engineers believe that such scenarios were impossible?*

In summary, the actions of the operators look much less clearly negligent when the reasons why the operators behaved the way they did is the focus of the investigation rather than a focus on what the operators did that turned out to be wrong. The operators, in fact, acted appropriately or at least understandably given the context, the incorrect work instructions (which they followed), and their lack of training and required skill and knowledge in performing the work. In addition, they were provided with almost no assistance from the process control system. As many of the tasks they needed to do required intense attention, precision, mental effort, deep understanding of process dynamics, and frequent adjustments to a continually fluctuating process, such assistance would have been invaluable.

The designers of the plant did not recognize or understand the risks (see the appropriate sections of the CAST analysis) so the risks might not have been communicated thoroughly to the operators. Management seemed to rely on operators seeing something strange and stopping the process, but did not provide the information and training to ensure it was possible for operators to do this. Such a policy provides a convenient excuse to blame the operators after an accident, but it does not help the operators to carry out their responsibilities.

Generating recommendations will be covered later, but some obvious ones from this part of the analysis are that the operators must have the appropriate skills and expertise to perform their assigned activities, and there must be someone overseeing operations who is assigned the responsibility for implementing this requirement. Other possible recommendations include the need for a human factors study during the job analysis to ensure that the operators are provided with information and a work situation that allows them to make appropriate decisions under stressful conditions, better automated assistance during all phases of operation, training for activities that are known to be hazardous such as startup, and finally improved work instructions together with a better process for producing them.

This analysis, as usual, raises a lot of additional questions that need to be answered in order to understand what happened and make recommendations to prevent such occurrences in the future. These will be summarized in the rest of the section of the handbook (with the details omitted) so that readers have a fuller picture of the CAST process and the results that can be obtained from it.

So far, we have looked at the physical process, the automated process control system, and the plant operators. We now briefly look at the role that the CAST analysis identifies that each of the other controllers played in the loss, working our way up the safety control structure. Once again, detailed CAST analyses for each controller is not included in this handbook but can be found elsewhere.

Plant Safety Management

The plant safety department usually provides oversight of operational safety and provides information to plant operations management to ensure that operational decisions are made with safety in mind. Examples of the detailed analyses are included here, but we have found that too much detail discourages reading of the report. A useful compromise is to include the detail but also include a summary of the role in the component in the accident that summarizes the important points of the detailed analysis.

Relevant Responsibilities of Plant Safety Management

- Identify plant hazards and ensure that they are eliminated, mitigated, or controlled.
- Either provide work instructions for safety-critical activities or review the work instructions provided by someone else for their safety implications.
- Ensure appropriately trained, skilled, and experienced people are assigned to high risk processes.
- Follow the Management of Change (MOC) procedures by doing a risk assessment for changes and implement risk controls based on the results.
- Provide for emergency treatment to exposed or injured individuals and ensure required medical equipment and personnel is available at all times. [*The injured personnel were treated effectively on the scene so this aspect is not considered further.*]
- Perform audits of safety-critical activities or assist plant operations management in performing such audits [*It is not clear from the accident report who is responsible for audits but there do appear to have been audits.*]

Process Model Flaws of the plant safety managers

- Regarded ethylbenzene as a safe substance in this process.
- Considered the start-up process not to be high risk.
- Thought that the Operators and the Production Team Leader could manage and control the start-up manually based on their knowledge and experience.
- There were so sure that they understood the risks that even incidents at other similar plants did not trigger any doubts about their assumptions. Alternatively, they may not have been made aware of the previous incidents.

A Few Example Contextual/Process Model Factors (more included in summary below):

- Over time, understanding of the most appropriate procedures relating to Unit 4800 changed. Some of the procedures were not considered critical to safety. So, these procedures were not included (or were no longer included) in the amended work instructions.
- Safety assessment procedures complied with government requirements.
- Hazard assessment focused on processes that were considered higher risk and primarily assessed the effects of substances on the environment and not on safety.

Summary of the Role that Shell Moerdijk Safety Management Played in the Accident:

- The safety analysis methods used were either not appropriate, not applied or were applied incorrectly. However, the methods used complied with the Shell requirements and satisfied the Dutch legal and regulatory requirements. They were also standard in the petrochemical industry. Safety management did not consider certain relevant information nor investigate how ethylbenzene reacting with the catalyst could cause an explosion. Safety management at Shell Moerdijk, as is common in many places, seems to have been largely ineffectual, with lots of activity, but much of it directed to minimal compliance with government regulation. A partial explanation for their behavior is that everyone believed that a reaction between ethylbenzene and the catalyst was impossible and that the start-up process was low risk.
- Although Shell's safety management system includes requirements for dealing with changes, the Management of Change (MOC) procedures were not followed nor implemented effectively. Risks resulting from changes made to the plant, the catalyst, the processes, and the procedures were not identified and managed. Not following MOC procedures has been implicated in a very large number of accidents in all industries.
- A new catalyst was selected for use at Shell Moerdijk, but an assumption was made that the properties of the new catalyst were the same as those of the previous catalyst. The altered composition of the new catalyst was stated in the safety information sheet provided by the manufacturer, but safety engineering did not notice this change.
- Procedure changes (heating rate and nitrogen flow) were instituted without a risk assessment. These procedures were not included in the amended operator work instructions. Other plant and production changes were not systematically examined for their safety effects on the basis of a risk analysis in all cases. Only a few failure scenarios were examined, but this fulfilled both Shell Global and Dutch law. There were never any safety studies that focused on the circulation and heating of the unit involved in the accident. Safety was based on studies done in 1977 that had shown the catalyst (as it then existed) was inert in the presence of ethylbenzene. This assumption was never reassessed even though the composition of the catalyst changed over time and similar incidents occurred at other Shell installations. There were no requirements by either Shell Global or the Netherlands law to do so.
- The number of leaks was used as the primary leading indicator of process safety, which clearly has nothing to do with this accident. Because the number of leaks had been greatly reduced in recent years, decision makers assumed safety was improving. The use of this leading indicator is common in the petrochemical industry and was accepted by the Dutch regulatory authorities.
- Similar incidents occurred at Shell Nanhai and at Shell Moerdijk after initial startup in 1999. No explosion occurred at Nanhai because of special factors. These events did not trigger a response in terms of reassessing risk or procedures or the assumptions that a runaway was impossible. Recommendations following the Nanhai incident were not used to reduce risk. *Why? There is no information in the accident report about why the Nanhai incident recommendations were not implemented.*
- Safety engineering did not provide proper oversight of the generation of work instruction, which allowed unsafe work instructions to be provided to the operators. The work instructions did not follow the format provided by Shell for such instructions. They also omitted much of the required information such as critical conditions and required steps to be taken by the operators.

Recommendations:

While the problems specific to the explosions on 3 June 2014 should be fixed, there were a lot of weaknesses in the Shell Moerdijk safety management practices identified in the official Dutch Safety Agency accident report and in the CAST analysis. These need to be improved.

- Safety management at Shell Moerdijk needs to be made more effective. Safety engineering needs to be more than just going through the motions and minimally complying with standards.
- All work instructions should be reviewed for safety by knowledgeable people using information from the hazard analysis. [In this case, the hazard analysis was flawed too, but that is a different problem to fix.]
- MOC procedures must be enforced and followed. When changes occur, assumptions of the past need to be re-evaluated.
- Hazard analysis and risk assessment methods need to be improved.
- More inclusive and relevant leading indicators of risk need to be established.
- Procedures for incorporating and using lessons learned need to be established or improved.

Operations Management

Relevant Safety-Related Responsibilities

- Establish safety policy for operations.
- Ensure that Safety Management is fulfilling their responsibilities and providing realistic risk and hazard assessments.
- Use the results of the hazard and risk analyses provided by Safety Management in decision making about plant operations.
- Create a Shell Moerdijk Safety Management System consistent with the overall Shell Global Safety Management System, ensuring it is both effective and being followed.

More specific safety-related responsibilities include the following:

- Provide appropriate training for operators for nominal and off-nominal work activities.
- Follow MOC (Management of Change] procedures that require performing a risk assessment for changes or ensure that safety management is doing so. Use the risk assessment to provide oversight of the process and to design and implement risk controls in the plant and the operating procedures.
- Prepare (or at least review) the work instructions. Ensure they are safe and are being followed.
- Minimize the number of personnel in the vicinity (at risk) during high-risk operations, such as during a turnaround.
- Keep records of incidents and lessons learned and ensure they are communicated and used by those that need to learn from them.
- Provide personnel assignments that are commensurate with the experience and training required for the activity.
- Provide a process control system that can assist operators in performing critical activities.
- Conduct audits. Establish leading indicators to be used in the audits (and in other feedback sources) or ensure that safety engineering is identifying appropriate leading indicators.

Process Model Flaws of operations management personnel

- Regarded ethylbenzene as a safe substance (an inert medium) under all process conditions. Therefore, they did not consider the heating phase to be risky.
- Thought the personnel involved in the turnaround had appropriate training and experience.
- Did they not know about similar incidents at other Shell installations with the same design or did they not think they were relevant to Unit 4800?
- In general, they had an inaccurate view of the risk that existed in the plant.
- Inadequate feedback leading to these flaws:
  - The heating phase did not appear in the report provided by plant safety management.
  - Plant safety management did not provide correct risk assessments to operations management.

Contextual Factors: (omitted, see complete analysis; also included in summary below)

Summary of the Role of Operations Management in the Accident:

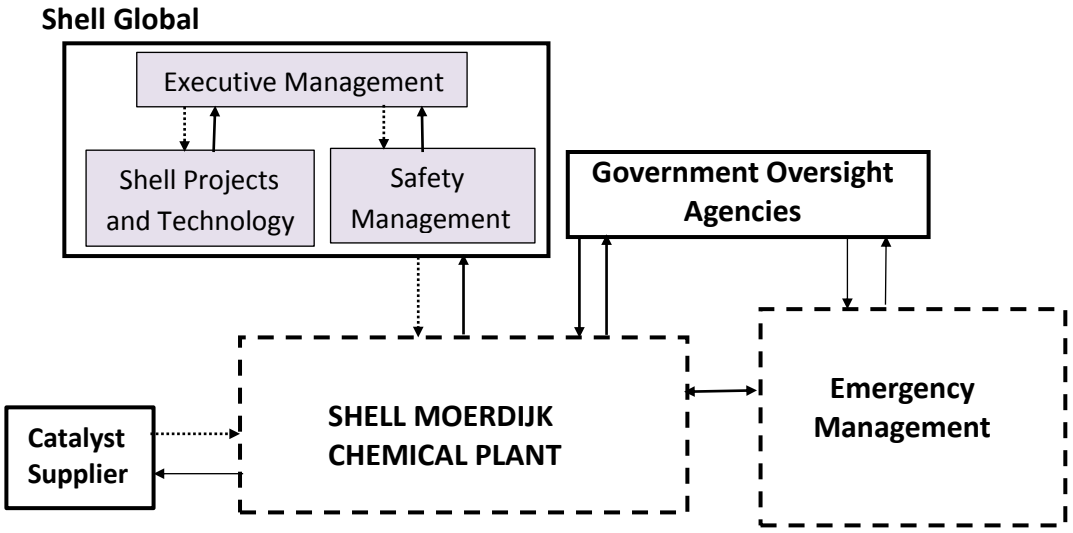
- Operations management did not identify the flaws in the risk analyses performed or the procedures used for these risk analyses. The risk analyses complied with the minimal requirements of the Dutch regulatory authorities and apparently with the Shell requirements.
- Changes over time were not subjected to assessment in accordance with the MOC procedures.
- Work instructions were created by the operators without safety engineering oversight. They did not comply with the required Shell format for such work instructions and did not include important criteria for the job such as heating rate. Nitrogen flow, an important factor in the accident, was ignored in the work instructions.
- A decision was made to configure the process control system to control the plant during the normal production phase but not during non-production and maintenance phases. They did not think these activities were high risk and thought that manual operation would suffice. The reasons for this decision are not in the accident report.
- Two employees from different contractors were allowed to work in the adjacent unit during the start-up, probably because they did not believe that phase was dangerous.
- Operations management did not assign operators to the start-up that had the qualifications required in the Safety Report. No reason is given in the accident report as to why this happened.
- Operations management did not ensure that lessons learned from similar plants and at Shell Moerdijk in 1999 were incorporated in the design and operation of Unit 4800.
- The Safety Management System at Shell Moerdijk did not prevent unsafe situations from being overlooked or internal procedures from not being followed. There is no information in the accident report about who created the SMS or who was responsible for ensuring that it was working properly.
- Internal Shell Moerdijk audits did not show any of these shortcomings. Not enough information is provided to determine why they were ineffective.
- Shell Moerdijk has a Business Management System in which safety management is integrated. No details are provided, but in general this is a poor practice and has been a factor in major petrochemical company accidents such as Deepwater Horizon. Decision making needs to occur with full information about all the factors that must be considered and not lost by integrating risk information in a nontransparent way.

Recommendations:

- Establish and ensure proper MOC procedures are followed. If changes occur, retest assumptions that could be affected by those changes. This implies that these assumptions must be recorded, leading indicators established for identifying when they may no longer be correct, and a process established for testing and responding to changes that might affect these assumptions.
- A thorough review of the Shell Moerdijk SMS should be done with emphasis on why it was unable to prevent this accident. Major factors in this accident are related to basic activities that should have been controlled by the SMS.
- Update procedures to eliminate the causes of the accident such as lack of control and supervision of the work instruction creation and oversight processes, inadequate hazard analysis and risk assessment procedures, assignment of operators to perform the turnaround who did not have the required skills and expertise, inadequate use of lessons learned from the past, and audit procedures that did not identify the shortcomings before the accident.
- Improve the process control system to provide appropriate assistance to operators performing functions that are outside of normal production.

Shell Global (Corporate)

Three basic functions are included here: Engineering design (Shell Projects and Technology), corporate safety management, and executive-level corporate management, including the Board of Directors. The exact distribution of the safety responsibilities in the Shell Global management structure was not included in the accident report, so they may be distributed throughout the Shell Global management structure differently than assumed here. The bottom line is that they need to be somewhere.



Shell Projects and Technology (Engineering)

Plant design was done at the corporate level and the technology licensed to the facilities.

Safety-Related Responsibilities

- Create a safe design: Perform hazard analysis (or use the results of hazard analysis created by another group) and eliminate or mitigate the hazards in the design.
- Provide design, hazard, and operating information to the plant operators to help those who are operating the plants avoid any hazardous scenarios that the designers were not able to eliminate or adequately mitigate in the design itself.
- Learn from the operation of their designs and improve the designs based on this feedback.

Summary of the Role of Shell Projects and Technology:

The design data provided to the licensees was not usable by those creating work instructions at the plants. The design had safety-critical design flaws that were not found in hazard analyses during the initial design phase. These flaws were not fixed after receiving information about related incidents in other Shell plants. One example was an overpressure incident that occurred due to an inadequate number of temperature sensors and pressure relief valves unable to handle the excessive pressure that occurred. Unsafe and incomplete work instructions were approved by Shell Projects and Technology for the Unit 4800 turnaround at Shell Moerdijk.

Unanswered Questions:

Without more information about the operations at Shell Corporate, which was not included in the accident report, it is difficult to determine exactly why the unsafe control occurred. More questions than answers arise from the CAST analysis, such as *Why were the design flaws introduced and how did they get through the design process? What type of hazard analysis is performed by Shell Projects and Technology or by other groups? Why were identified design flaws not fixed after the incidents at Shell Moerdijk in 1999 and Nanhai in 2011? What other types of feedback is provided about the safety of their designs during operations in the Shell plants? What information about the safety aspects (hazards) of the plant design are passed from Shell Projects and Technology to the licensees of their designs? What information is included in the design book? Is the design data provided sufficient for the licensees to create safe work instructions if engineers are writing the work instructions instead of operators and did they not know who was going to be performing this task? Why did they approve unsafe work instructions that did not even follow the required Shell format? What information is provided in the Design Book about start-up and the hazards of start-up? What types of hazard analyses are performed during the design process? What is the process for ensuring safety when changes are made? How are safety-related assumptions recorded and what triggers a re-analysis of these assumptions? What feedback do the designers get about the operation of their designs?*

Recommendations:

Fix the design features contributing to accident. Determine how these flaws got through the design process and improve both the design and the design review processes. Fix the design book so that is understandable by those who are writing the work instructions and includes all the information needed to safely operate installations of the licensed technology. Fix the work instruction review process by Shell Projects and Technology to ensure the instructions are complete and safe. Review and improve the hazard analysis process used by Shell Projects and Technology.

Corporate Safety Management

There is no mention in the accident report about a Shell corporate safety program or about any of its potential contributions to the accident. In the CAST analysis, I took the information about what happened at the local Shell Moerdijk level and projected what would normally be the responsibility at the corporate level of a well-designed SMS to control the flawed safety activities. There must have been someone with ultimate responsibility for safety at the corporate level, but it is unclear where the activities associated with that management role resided within the corporate structure or even whether these activities occurred.

Relevant Responsibilities

- Ensuring the safety of the plant design, including the conduct of hazard analysis on designs licensed to subsidiaries.
- Oversight of operational safety at the various Shell plants and facilities.
- Management of change procedures related to safety: creating them, making sure they are followed, and improving them using feedback from incidents.
- Ensuring communication among separate plants in different parts of the world about incidents, lessons learned, etc.
- Creating and updating a Shell-wide Safety Information System and ensuring the information is being communicated adequately both within Shell Corporate and globally and that it is complete and usable.

Summary of the Role of Corporate Safety Management: There appears to have been a flawed view of the state of risk and the effectiveness of the safety management system in local Shell plants. The flawed process model is most likely related to inadequate feedback (including audits and leading indicators). The accident report says that Shell uses the outdated HEMP and bow tie model. There is little information about what other hazard analyses and risk assessments are used at the corporate level. Presumably HAZOP is also practiced (as in most of the process industry), but that is not mentioned in the report. Bow tie, which is about 60 years old and dates back to the late 60s, uses a simple chain-of-events model and is too simplistic to capture the hazards and risks in today's complex systems, including chemical plants. Once again, many questions are raised from the CAST analysis that need to be answered to understand the role of corporate level safety management in the accident and thereby to provide more effective safety management in the future.

Recommendations: Improve Shell safety audits. Review all risk assessment and hazard analysis processes and, in general, improve their approach to safety with respect to both safety analysis and safety management. Shell is not alone among the large oil companies in needing to update their methods. The petrochemical industry has too many accidents and incidents that are avoidable.

More specifically, the accident report says that Shell should "evaluate how risk analyses are performed and make changes. This should include procedures and policies about re-evaluation of earlier presumptions and assumptions. Conduct new risk analyses, put adequate measures in place, and ensure that the team that performs these analyses has sufficient critical ability. Pay particular attention to assumptions based on risks that had previously been ruled out."

Evaluate and improve the corporate safety management system. Improve procedures for learning from process safety-related incidents. Create better feedback mechanisms, including audits and leading indicators, and procedures for learning from incidents.

Executive-Level Corporate Management

Responsibilities:

- Take all measures necessary to
  - Prevent major accidents from occurring and,
  - If accidents do occur, mitigate their consequences for humans and the environment
- Ensure the health and safety of the employees in relation to all aspects associated with the work (based on the Working Conditions Act and other regulations)
- Follow the government regulations in the countries where their plants are located.
- Create an effective safety management system and establish a strong safety culture policy. Ensure that the SMS and safety policies are being followed and they are effective.

Process Model Flaws

Leaders clearly had misunderstandings about the state of safety being practiced in Shell corporate and the local installations and the effectiveness of their defined procedures.

Contextual Factors (omitted, see full analysis):

Summary of the Role of Executive-Level Management:

Corporate management is responsible to ensure that an effective safety management system is created. Typical policies of an effective safety management system were violated at both Shell Corporate and Shell Moerdijk. The group overseeing safety at the Shell corporate level was clearly not effective. There is nothing included in the accident report about the assigned safety-related responsibilities for corporate management.

There is also nothing included in the accident report about context that might explain why standard executive-level responsibilities for safety were not effectively carried out. There seems to be a safety culture problem at Shell. (See later analysis of the safety culture and high-level safety policy at Shell.) What is the culture of the chemical industry in terms of corporate management oversight of the safety of global installations?

The accident report notes that the Safety Management System was integrated with the Business Management System at Shell Moerdijk. Was this also true at the corporate level? This is a very poor practice (and was a factor in the Deepwater Horizon accident). Safety risk assessments need to be kept separate from business risk assessments so that information is not hidden from high-level decision-makers.

Recommendations: Review the SMS design and determine why it did not prevent obvious violations of policy such as shortcomings in safety studies, management of change procedures, learning from accidents, not following regulations (e.g., having experienced operators and following the format for work instructions). Determine why audits were not effective in finding such obvious procedural noncompliance. While it is possible that this was the first time such lapses have occurred, it is highly unlikely. Strengthen audit procedures, including identifying better leading indicators of increasing risk than simply the number of leaks and create other forms of feedback to identify when the safety management system is drifting off course and risk is increasing. Establish better feedback channels to ensure that management of change procedures and corporate safety policy are being followed.

Catalyst Supplier

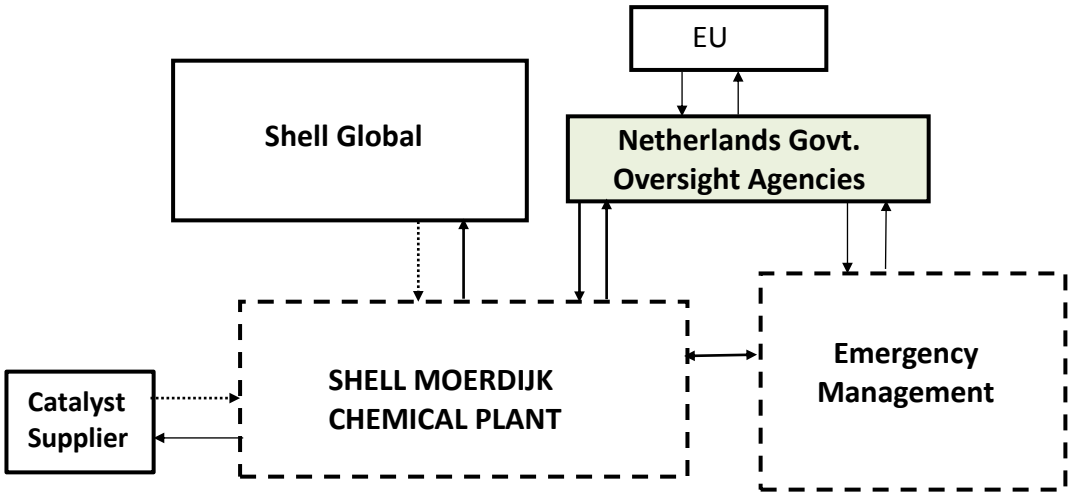
Safety-Related Responsibilities

- Provide information to customers that is needed to evaluate the use of their catalyst in the reactor being designed and/or operated
- Alert customers when changes are made in the catalyst that could potentially affect the safety of its use.

Summary of the Role of the Catalyst Manufacturer in the Accident: The changes made in the catalyst were not pointed out to Shell, but they were included in a new safety information sheet. While the catalyst manufacturer cannot determine the impact of their changes on a customer, the manufacturer should provide some clear alert that changes have been made and what they are so the customers are made aware of them.

Recommendations: Change contractual relationships between Shell and its suppliers to ensure that potentially critical changes are communicated appropriately. Make changes within information sheets so they are clear and obvious.

Dutch Regulatory Authorities



All Dutch oversight safety and environmental authorities are grouped together here. There are two main policies:

1. Brzo: Companies must take all measures to prevent accidents and, if they occur, mitigate their consequences for humans and the environment. The company must implement this obligation

by laying down policy assumptions in the Prevention Policy for Serious Accidents (PBZO), drawing up a safety report (VR), and organizing a safety management system.

2. Wabo: Regulators must check whether the company complies with regulations connected to the environmental permit, i.e., environmental safety.

General Relevant Safety-Related Responsibilities

- Responsible for supervision and enforcement of Dutch laws to protect the environment and the public. Perform Brzo inspections focusing on process safety and Wabo inspections focusing on environmental safety.
- Responsible for enforcement of EU health and safety laws within the Netherlands.

More Specific Responsibilities:

- Identify shortcomings at companies they are responsible to oversee.
- Encourage companies to improve their safety-critical processes through supervision and enforcement. Identify shortcomings and require companies to investigate and detect deep-seated causes of incidents and accidents. Ensure that any shortcomings identified are corrected.
- Assess modifications made to plants, procedures, and processes (although they are not expected to perform the risk analyses for the companies).
- Pay greatest attention to safety-critical processes, including maintenance and reactor start-up.

Process Model Flaws

The accident report said "Regulators had a positive view of the Shell Moerdijk safety management system. A number of shortcomings at Shell Moerdijk did not alter this view."

Contextual Factors (omitted, see full analysis and summary below)

Summary:

At least partly because of limited resources, the government authorities do "system-related supervision," effectively a form of performance-based regulation where responsibility is placed on the operator of high-risk activities to identify their own shortcomings. Regulators check both the design and operation of the safety management system and perform annual inspections to ensure they are operating as designed. Regulators only ensure that companies have the right documented procedures and spot check that they are being used.

They did not notice or did not react to Shell not acting in accordance with its own SMS. As just some examples: Changes and upgrades to the plant were not consistently subjected to risk analyses (violating the Shell SMS requirements), but this deficiency was not noted by the regulators nor required to be fixed. Changes were not adequately evaluated for safety. Requirements for expertise and training in performing startups were not enforced.

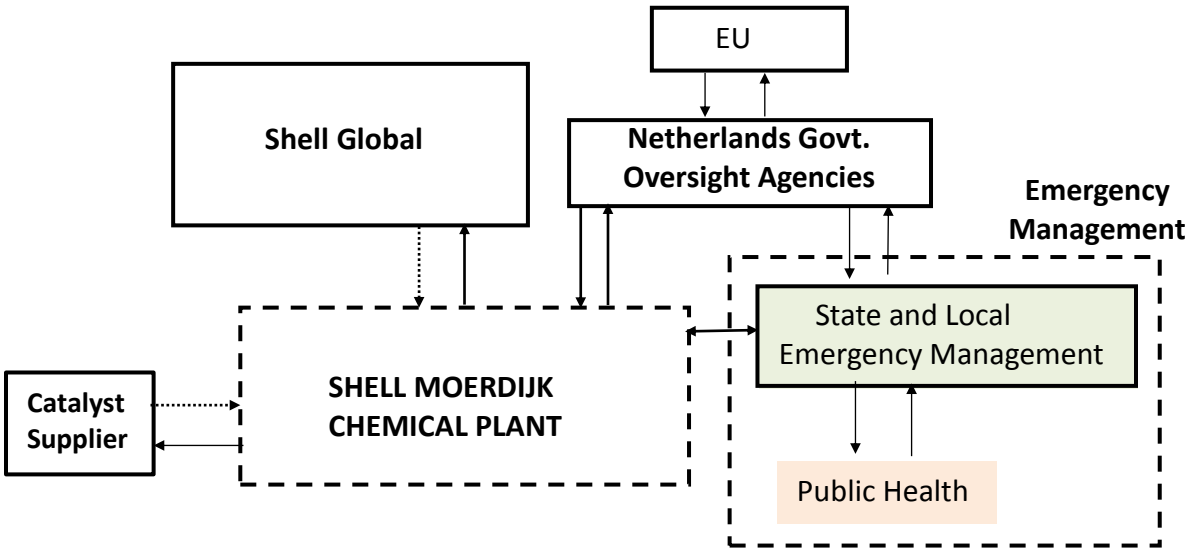
The accident report implies that regulators gave Shell Moerdijk a pass on behavior that might have instead been labeled violations. Plant scenario deficiencies should have been considered a violation but were not. Scenarios were not up to date or were incomplete. Working under limited resources and time is difficult under any supervision model, but system-level supervision has major limitations in ensuring public safety. The accident investigation showed many flaws in Shell Moerdijk operations

safety management as defined and as implemented. *What is wrong with the supervision model that the regulators did not detect the deficiencies?*

Recommendations:

Better supervision of the highest risk activities is needed, including turnarounds. Regulators need to oversee and ensure that strict procedures are being used for the most dangerous activities and that the safety management system is operating effectively and following its own rules. Operating under limited resources does not preclude doing something effective, it simply requires a more intelligent selection of activities that are performed. There is a need for better evaluation procedures and oversight of safety management system effectiveness. The regulators should rethink system-level supervision to ensure that what they are doing is effective in preventing accidents like the Shell Moerdijk explosion.

Emergency Services



Responsibilities

- Firefighting [collaborative fire brigades did this effectively in this case], crisis management, crisis communications including among other things:
  - Informing citizens of the incident
  - Measuring substances released on a coordinated basis
  - Operating a telephone advisory line
  - Informing citizens about the results of the measurement of the substances released and the ensuing recommendations.

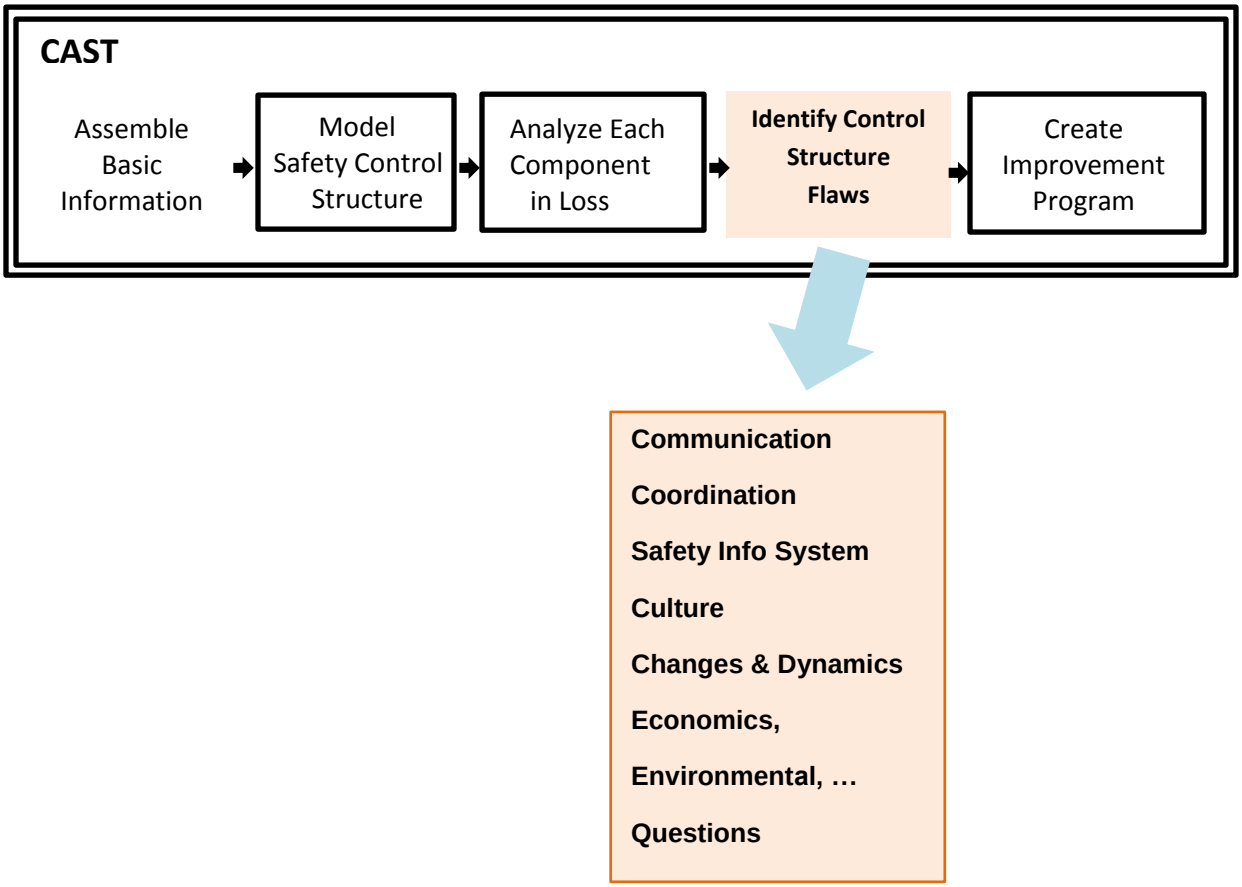
Summary of the Role of Emergency Services in the Accident:
Emergency services were mostly very effective in carrying out their responsibilities, but some deficiencies, particularly in communication, were uncovered in the accident response. For example, many people used WhatsApp instead of the National Crisis Management System designed for use in these conditions. It did not lead to loss of life because of the nature of the accident in this case, but under other circumstances it could have.

Recommendations: What was learned from this case should be used to improve the National Crisis Management System, including why many people used WhatsApp instead, and how the official system can incorporate those features.

Even for system components that did not cause a loss, as in this instance, accidents create an opportunity to look closely at the actual operation of our systems in times of stress and provide a learning opportunity that should not be wasted. As demonstrated in the example, most of the components may have contributed to the accident in some way or did not operate exactly as planned. When looking only at what the operators did or did not do, it appears that they were the primary contributors to the loss. Usually, as in this case, the actions of the operators will be found to be understandable when the reason for their behavior is examined.

This section described and provided examples of individual component analysis in CAST. Examining the individual controllers in the control structure is not enough, however. It is necessary to also examine the operation of the control structure as a whole.

Analyzing the Control Structure as a Whole



4. *Identify flaws in the control structure as a whole by investigating the general systemic factors that contributed to the loss. The systemic factors span the individual system control structure components.*

The CAST analysis process described so far focuses on individual system components and their control over other components. It examines why each of the controllers was unable to enforce the controls and constraints assigned to it.

In contrast, this part of CAST looks at the control structure as a whole and the systemic factors that led to the ineffectiveness of the designed controls. It is perhaps the least structured part of the analysis, but guidance is provided in this section of the handbook on what to look for and how to explain the role it played when you find it.

The systemic analysis focuses on factors that affect the behavior and interactions of all the components working together within the safety control structure to prevent hazardous system states. By looking at the system as a whole, rather than individual components, we can identify causal factors that impact how the various safety control structure components interact. These systemic factors provide another way to understand why the individual components may not fulfill their individual safety responsibilities and why together their behavior did not satisfy the system safety constraints. That is, safety control structures are usually created so that one component's misbehavior cannot alone lead to an accident. The systemic causal factors, however, can negatively impact the behavior of many or even all of the components and defeat these efforts.

This is the truly unique part of a systems approach to accident analysis that is omitted from event-based models, such as the Swiss Cheese or domino models. There are causal factors that can prevent all the barriers from operating correctly and simultaneously cause "holes" in all the protections and cheese slices that were created to prevent accidents. Getting away from focusing on a few causal factors or explaining accidents in terms of the behavior of one or several components provides a larger view of causality that can be used to identify very powerful prevention measures.

The following are some of the systemic factors that might be considered. This list is not comprehensive, but simply a starting point.

- Communication and coordination
- The safety information system
- Safety culture
- Design of the safety management system
- Changes and dynamics over time: in the system and in the environment
- Internal and external economic and related factors in the system environment not covered previously in the analysis. Some of these may be generated while considering changes over time.

Communication and Coordination

Many of the factors that lead to losses involve inadequate communication and coordination among components of the safety control structure. Lack of coordination and communication can lead to inconsistent actions, missing actions, and so on.

An example can be found in the collision of two aircraft in 2002 over Überlingen, a town in southern Germany in 2003. A poorly planned maintenance activity resulted in almost all the communication links in the air traffic control tower being temporarily broken. Some of the outages were known ahead, others resulted from an error during the maintenance. Planning for the loss of communication would have helped. For example, the air traffic controller on duty did not know that his aural and visual alerts about a potential collision would be inoperable during the maintenance. Contingency actions could have been taken to cope with the maintenance activity if it had been planned and management of change procedures used. The communication outage eliminated all the built-in redundancy that was designed to prevent such collisions.

Drawing the communication links as intended and what was operational during the accident can provide an important visual explanation. Figure 16 shows the communication channels that were designed into the system. Figure 17 shows those that were working at the time of the collision. This type of diagram is a powerful tool for understanding and communicating about what happened and why. The phone lines were out so that a controller at another site who saw the collision about to happen, could not get through to give a warning. When the air traffic controller who was controlling the two aircraft at the time of the collision became overloaded due to an unforeseen emergency landing, there was no way for him to contact another air traffic control facility to help him with his overload.

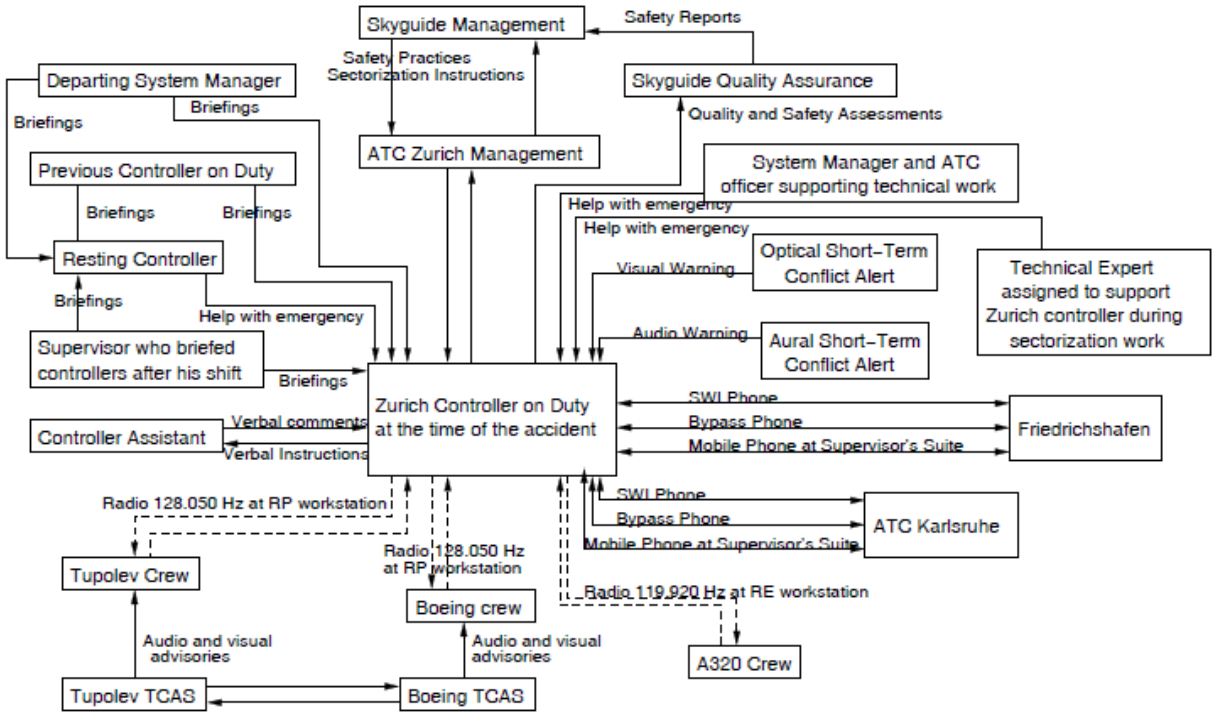


Figure 16: Communications links theoretically in place in the Überlingen accident

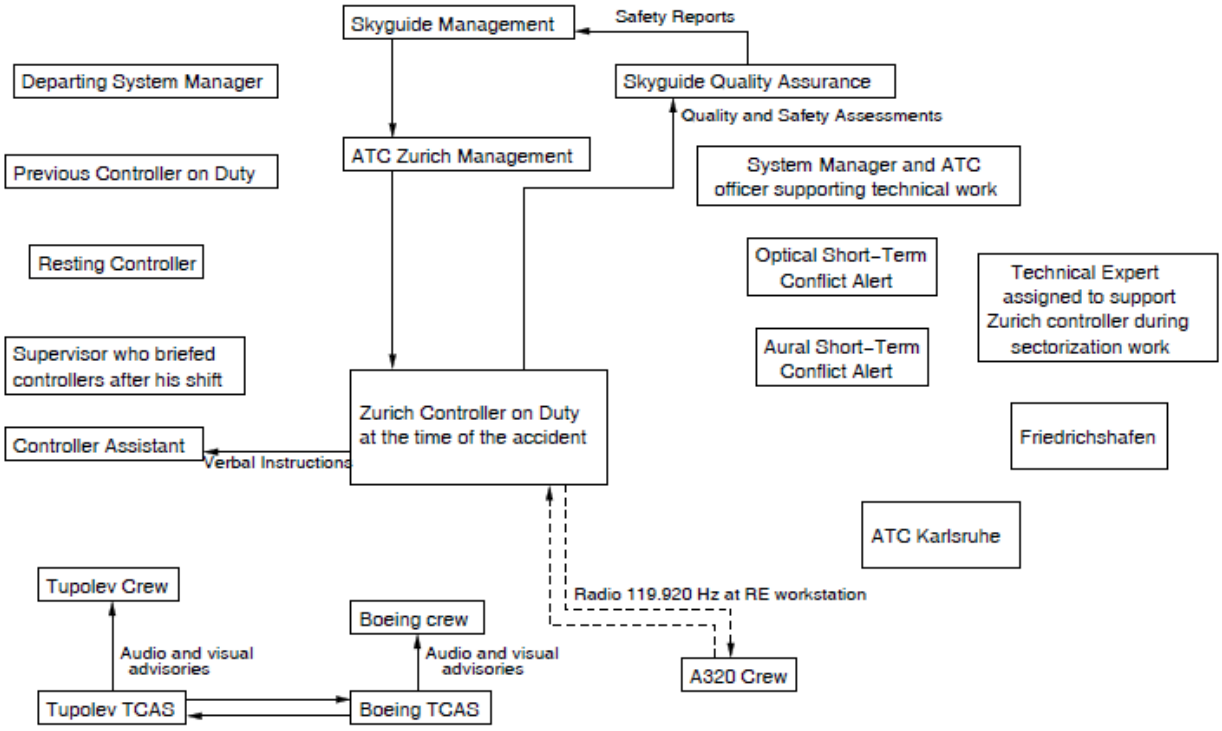


Figure 17: The operational communication links at the time of the accident

The communication and coordination problems in this case were confined to the time of the accident. But they can exist for a long time before. Sometimes, one controller assumes that another is handling a responsibility while the other one thinks the first is. As an example, in a Canadian water contamination incident, both the Ministry of the Environment (MOE) and the Ministry of Health (MOH) were responsible for performing some of the same oversight duties: the local MOH facility assumed that the MOE was performing this function and cut back on their own activities, but the MOE's budget had been cut, and follow-ups were not done. A common finding after an accident is that each of the responsible groups may assume another controller is performing the needed oversight when there are overlapping responsibilities. Alternatively, the two controllers may have non-overlapping responsibilities but they may provide indirectly conflicting commands.

Inadequate feedback in the safety control structure is one important type of communication that is often found to contribute to poor decision making. Other types of communication are, of course, also important. In the Shell Moerdijk accident, there were instances of ineffective communication between Shell Global Projects and Technology and Shell Moerdijk and between groups within Shell Moerdijk itself. In addition, the change to the catalyst by the manufacturer was not communicated to Shell. Did the required communication channels exist at the time of the accident? Were they fully operational or were there inhibitors to the transmission of required information?

In a friendly fire accident analyzed in Chapter 5 of *Engineering a Safer World*,[17] potential ambiguity in the responsibility for tracking friendly aircraft had been eliminated by partitioning the tracking responsibility between two different controllers. This partitioning broke down over time due to factors such as unofficial attempts to increase efficiency, with the result that neither was tracking the aircraft

[17] Nancy Leveson, *Engineering a Safer World*, MIT Press, 2012, Chapter 5.

that was shot down on the day of the loss. No performance auditing had been done to ensure that the assumed and designed behavior of the safety control structure components was actually occurring.

After an accident, all communication links should be examined to ensure that the design allowed for the transmission of critical information. Even if the design was adequate, were the transmission channels working properly? If not, the reasons for the inadequate communication must be determined. Sometimes a communication channel involves a person who has conflicting goals with the communication of the information. In some cases, the communication links may simply have failed. In others, they may be purposely down for maintenance purposes, as in the Überlingen accident. Occasionally, communication and coordination links may have been available, but the controller did not know about them. In the friendly fire example, the links degraded and became inactive over time.

Analyzing communication requires first understanding and modeling the critical communication channels. The control structure below, created by Captain Paul Nelson in his CAST analysis of a wrong runway takeoff accident at Lexington Airport, shows dotted lines where the communication channels never existed (some involving feedback channels that were never included in the design) or were inoperable for various reasons at the time of the accident. Simply drawing the safety control structure and finding missing feedback channels in the design is a strong clue that there is a problem with the control structure design. All control loops should have feedback channels for proper decision making to occur.

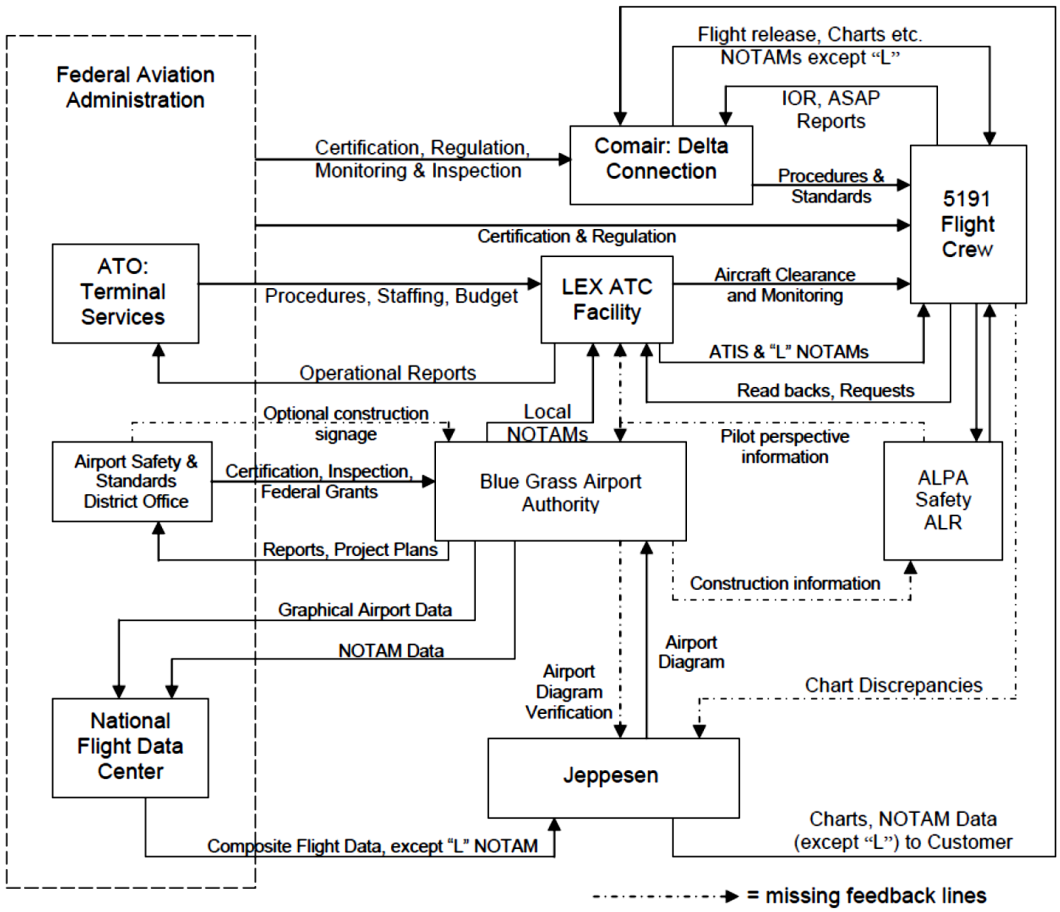


Figure 18: The Lexington ComAir wrong runway accident safety control structure. The control is drawn left to right instead of top to bottom. Dotted lines represent missing feedback and communication that contributed to the loss [Paul Nelson, A STAMP Analysis of the LEX Comair 5191

Accident, Master's Thesis, Lund University, June 2008. A link to this thesis is provided in Appendix A.]

Another common type of communication breakdown, described earlier, can occur in the problem-reporting channels. In many accidents, the investigators find that the problems were identified in time to prevent the loss, but the required problem-reporting channels were not used, often because they were unusable.

Safety information system

In a study of the safety information systems of various companies, Kjellan found that the quality of the safety information system was the second most important factor in discriminating between companies with high and low accident rates [Kjellan 1982].[18] Uses for a safety information system include storing and passing on information about hazards, detecting trends and deviations that portend an accident, evaluating the effectiveness of safety controls and standards, comparing models and risk assessments with actual behavior, identifying and controlling hazards to improve designs and standards, etc. Accident investigations should include an examination of the organization's safety information system (SIS).

The Shell Moerdijk accident report does not provide any information about the Shell or Shell Moerdijk SIS, but it does describe many instances of deficiencies that could have been prevented with a well-designed SIS, such as not learning from incidents and previous maintenance stops, not identifying flaws in previous hazard and risk assessments when contrary evidence arose, etc. The accident report also notes that important information was lost between the design of the unit and the ultimate operations management of the unit. The report says that "A discrepancy therefore occurred between the available information during the design phase and the operations management that was ultimately conducted." A well-designed safety information system should be able to prevent these types of problems.

Just having a safety information system does not guarantee that it will be useful or used. Data may be distorted by the way it is collected. Common problems are filtering, suppression, and unreliability. Data collected in accident and incident reports tend to focus on proximal events and actors, and not on the systemic factors involved such as management problems or organizational deficiencies. Limited categories of conditions may be identified, especially when checklists are used. It is difficult to obtain comparable data from multiple sources in an unbiased and systematic manner.

Data collection tends to be more useful for events that are similar to those that have occurred in the past than for events in new types of systems where past experience about hazards and causal factors is more limited. Software errors and computer problems are often omitted or inadequately described in incident reports because of lack of knowledge, lack of accepted and consistent categorizations for such errors, or simply discounting them as a causal factor. CAST can be used to encourage the inclusion of systemic factors in safety information systems.

Some common deficiencies include not recording the information necessary to detect trends, changes and other precursors to an accident; to evaluate the effectiveness of the controls used to prevent accidents; to compare risk assessments of those in the industry with actual behavior; and to learn from events and improve their safety management practices.

Simply collecting the information, of course, is not enough. Problems may arise from the difficulty in consolidating a large mass of data into a form useful for learning. While with digital technology today it

[18] The highest-ranking factor was top-level management concern about safety. Urban Kjellan, An evaluation of safety information systems at six medium-sized and large firms, *Journal of Occupational Accidents*, 3:273-288, 1982.

is easy to design large scale data collection channels, finding the time and manpower to analyze all the data that results may be difficult or impractical. As a result, the safety information system may contain only summary statistical data that can be easily processed by a computer but not the information about trends and changes over time that is needed to learn from events before major losses occur. Airlines today are particularly suffering from this type of data overload due to large-scale automated information collection.

Another deficiency of many safety information systems lies in the retrieval and dissemination mechanisms. Information—which is not the same as data—may not be presented in a form that people can learn from, apply to their daily operations, and use throughout the system life cycle. Updating may not occur in a timely manner: Accidents have resulted from changes during operations or due to insufficient updates to the hazard analyses when engineering modifications were made. The information may not be tailored to the needs and cognitive styles of the users or not integrated into the environment in which safety-related decisions are made and therefore may be hard to use.

The safety information system must also exist within a safety management system that can use and benefit from the information provided. Simply having information stored in a safety information system does not mean that companies have the structures and processes needed to benefit from it.

When conducting an accident investigation, the safety information system and any possible impact on the events needs to be examined. Was the information needed to prevent the loss not collected or stored? Was it lost in the collection or analysis process? Was it available and easily retrieved in the daily activities of controllers?

Design of the safety management system

The safety management system (SMS) is theoretically the same as the safety control structure used in CAST analyses. The more general term "safety control structure" is used here as some industries define an SMS that excludes important controls necessary to prevent accidents.

There is no single correct design for the safety control structure: Alternative safety control structures can be effective with responsibilities distributed in different ways. The culture of the industry and the organization will play a role in what is practical and effective. There are some general design principles, however, that are necessary for any safety control structure to be effective,[19] and these can be used to evaluate an organization's safety management system after an accident. In general, the necessary safety constraints on organizational behavior should be reflected in the design of the safety control structure: Is the assignment of responsibility, authority, and accountability for safety to the controllers adequate to prevent hazards and accidents? A list of general responsibilities for management, development and operations that need to be assigned is included in Appendix D.

The accident investigation should evaluate the official design of the safety control structure as well as how it actually operated at the time of the loss. Were performance or other types of audits used to ensure that it was working effectively? Previous minor incidents may be clues that something is amiss and should have been used to identify problems before a major loss. Were near-miss and incident reporting systems used to identify flaws in the operation of the safety control structure or simply to assign blame to operators?

Clues will be available during the investigation that will provide guidance on where to look. For example, the Shell Moerdijk official accident report, which did not document or evaluate Shell's safety management system, notes that unsafe situations were overlooked, internal procedures were not properly followed, lessons were not learned from previous incidents, incorrect assumptions about basic

[19] See Leveson, *Engineering a Safer World, 2012* and Chapter 7 (Designing and Effective Safety Management System) in Leveson and Thomas, *STPA Handbook*, 2018.

chemical reactions were not re-evaluated after evidence surfaced that they were incorrect, changes were not managed and controlled, inadequate hazard analysis and risk assessment procedures were used, recommendations from previous incidents and accidents were never implemented, and oversight of critical activities was missing. Were responsibilities assigned for performing and overseeing these activities? What types of audits or inspections were used to identify these types of poor practices? Why were they not identified and corrected before the accident?

Oversight of a company's safety management system (SMS) usually lies in the responsibilities of government or professional regulatory agencies or organizations. At Shell Moerdijk, for example, the Dutch Regulatory Authorities have the responsibility to check whether the company has a safety management system in place, whether the systems and procedures incorporated in that system are appropriate, and whether the company actually applies these systems and procedures. They did not notice or did not react to Shell not acting in accordance with its own SMS. As just some examples, changes and upgrades to the plant were not consistently subjected to risk analyses, which violated the Shell SMS requirements, but this deficiency was not noted by the regulators nor required to be fixed. Changes were not adequately evaluated for safety. Requirements for expertise and training in performing startups were not enforced.

In fact, the regulators were unanimous in their positive appraisal of the Shell Moerdijk SMS. Government inspections and supervision are partly determined by the judged quality of the SMS, so oversight activities were limited for Shell Moerdijk. The Dutch Regulatory Authorities did not have adequate resources (a common problem) and thus allocated them based on perceived risk. They only perform "system-oriented supervision," that is, if the right systems are in place, then the authorities do not look further at the actual activities in the plant. The official accident report notes, however, that even under this type of limited supervision, it was possible for the inspectors to observe that changes and upgrades to the plant were not consistently subjected to risk analyses and that the safety management system did not indeed function well.

In the Shell Moerdijk accident, there had been two previous incidents involving the same catalyst, neither of which seemed to generate concerns or questions about the design of the plant, the risk assessments that were performed, or the creation of the start-up work instructions. The information about the incidents may not have been effectively stored by Shell (and thus stemmed from a deficiency in the safety information system), but more likely it simply was not used due to deficiencies in the operation of the company's safety management system. Asking appropriate questions during the investigation could have identified the source of these problems.

Safety culture

Acceptable safety information systems and safety management system structures can both be defeated by safety culture problems. In fact, the safety culture in an organization or industry impacts the behavior of every component in the safety control structure.

Edgar Shein, considered to be the "father of organizational culture," defined safety culture as "*the values and assumptions in the industry and/or organization used to make safety-related decisions*"[20] Figure 19 shows Shein's three levels of organizational culture and, more specifically, safety culture.

[20] Edgar Shein, *Organizational Culture and Leadership*, San Francisco: Jossey Bass, 2004

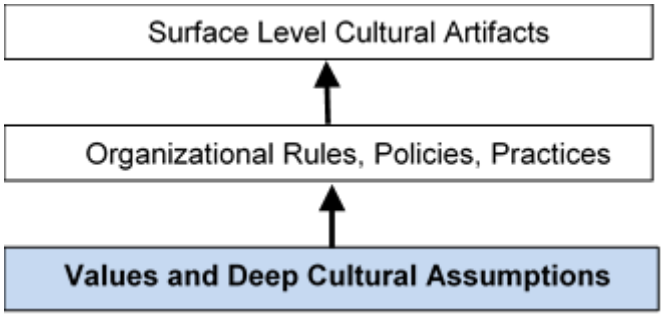


Figure 19: Shein's model of organizational culture

The essence of culture is the lowest-level set of values and deep cultural assumptions that underlie decision-making and the higher-level cultural artifacts in an organization or industry. The middle and top levels are not the culture; they merely reflect the organizational culture.

There is always a safety culture. The important question is how the existing safety culture impacts accident rates. Some aspects of safety culture that you might look for when investigating an accident are:

- Culture of Risk Acceptance: This culture is based on the assumptions that accidents are inevitable and that nothing much can be done to prevent them beyond exhorting everyone to be careful. Accidents are considered to be the price of productivity. Often this assumption is accompanied by the belief that everyone should be responsible for safety—their own and others—and that accidents result from a lack of responsible behavior on the part of individuals. The belief is prevalent that if only everyone would act responsibly and safely, accidents would be reduced or even eliminated.
- Culture of Denial: In a culture of denial, risk assessment is often unrealistically low, with credible risks and warnings being dismissed without appropriate investigation: Management only wants to hear good news so that is what they are told. The focus is on showing the system is acceptably safe, not on identifying the ways it might be unsafe. The use of "safety cases" rather than hazard analyses, is common.
- Culture of Compliance: The focus here is on complying with government regulations. The underlying cultural belief is that complying with regulations will lead to acceptable results. Because regulatory agencies tend to focus on certifying that a final product or service is safe, assurance of the safety of completed or existing designs is emphasized rather than building safety into the design during development. Often extensive "safety case" arguments are produced for managers or regulators with little or no impact on the actual product or product design effort. In addition, the bulk of the safety efforts may involve complying with standards and the requests of regulators instead of proactively taking steps to improve safety because it is a basic value in the organization. Even if employees fix immediately what is found to be lacking by government inspectors, did they aggressively search for problems internally without being prompted by a regulatory agency?
- Paperwork Culture: This culture rests on the belief that producing lots of documentation and analysis paperwork leads to safe products and services. Piles of paper analyses are produced but they have little real impact on design and operations. The bulk of the safety-related paperwork may be produced by a group that is independent from and has little interaction with those who

are designing and operating the products, implementing the processes, or providing the services. The paperwork sits in files, assuring everyone that the system is safe.

- Culture of "Swagger": Safety is for sissies. Real men thrive on risk. The problem here with respect to preventing accidents is, of course, obvious.

The safety culture in any organization is set by the top management. A sincere commitment by management to safety is often cited as the most important factor in achieving it. Employees need to feel that they will be supported if they exhibit a reasonable concern for safety in their work and if they put safety ahead of other goals such as schedule and cost. Often, concern for safety is merely lip-service and sloganeering. Employees take their cues from actions, not from empty words.

Analysis of the safety culture during an accident investigation should start with an evaluation of the company's documented safety philosophy and safety policy. If these do not exist, then there clearly is a problem. After a serious safety problem was found in a medical device, I was asked by the company to come in and investigate what happened. I had told them previously that they needed a written safety policy, but they had never produced one. After the safety problems in their products, I asked why and was told that it should have been obvious to the employees that the devices they were designing and selling were safety-critical and therefore a policy was not needed. At the same time, there were lots of written policies and rules about other product properties. In addition, they said that their lawyers had advised them not to create a safety policy because it was an admission that their product was potentially hazardous. The hazardous nature of the product was obvious and the lack of a safety policy would not have fooled anyone into thinking that there were no hazards associated with it. It simply made the company look negligent. Shortly after the adverse events that I was consulted about, the company went bankrupt and ceased to exist.

The safety philosophy is a short, written statement of the relationship that management desires between safety and other organizational goals. Some examples of general principles that might be part of the Safety Philosophy statement:

1. All injuries and accidents are preventable.
2. Safety and productivity go hand in hand. Improving safety management leads to improving other quality and performance factors. Maximum business performance requires safety.
3. Safety has to be built into a product or the design of a service. Adding it later will be less effective and more expensive. After-the-fact assurance cannot guarantee a safe design where safety is not already present. It is better to build safety in than try to ensure it after the fact.
4. The goal of accident/incident causality analysis is to determine why the loss (or near loss) occurred so that appropriate changes can be made rather than to find someone or something to blame.
5. Incidents and accidents are an important window into systems that are not operating safely and should trigger comprehensive causal analysis and improvement actions.
6. Safety information must be surfaced without fear. Safety analysis will be conducted without blame.
7. Safety commitment, openness and honesty is valued and rewarded in the organization
8. Effective communication and the sharing of information is essential to preventing losses.

While these principles look deceptively simple, they actually take quite a bit of thought to create and are often not the principles actually guiding a company's decision making. More explanation behind them can be found in the STPA Handbook, Chapter 7.

The safety philosophy establishes the principles upon which the more extensive safety policies and standards are built and assessed and provides a succinct statement of how management wants employees to make safety-related decisions and to act.

Of course, simply having a written philosophy does not mean that there has been buy-in by management and other employees. Do the managers actually implement the philosophy in their daily practices? Is there any process for ensuring that the philosophy is adopted and the principles practiced? How are the principles communicated to the employees? A written statement of the safety philosophy and more detailed policy statements and standards is a start, but it is not enough. Employees quickly identify when the written policy differs from the actual behavior of management. Do employees believe those at the top of the organization are sincerely committed to safety and are not just sloganeering and going through the motions? Asking some simple questions can identify when a deficient safety culture contributes to accidents.

While accident investigations sometimes use elaborate employee surveys to understand the existing safety culture, I have never found them useful. Writing down in a survey what one thinks they should say or believe does not mean that they actually think or act in that manner. I find that observing actual behavior is much more enlightening. Safety culture is best evaluated by studying management and employee behavior directly. How people behave is a much better indicator of their internal value system than what they answer on surveys.

How is commitment demonstrated? It is shown by setting priorities and following through on them; by personal involvement (e.g., top management chairing groups where safety decisions are made or at least getting personally involved); by setting up appropriate organizational structures; by appointing designated, high-ranking leaders to safety-related responsibilities and providing adequate resources for them to be effective; by assigning the best employees to safety-related activities and rewarding them for their efforts; and by responding to initiatives by others. It is also communicated by minimizing blame. Leaders need to demonstrate that their highest priority is to fix the systemic factors leading to losses and not just to find someone on which to pin blame (usually someone at the lowest levels in the organization) and then moving on when incidents or accidents occur. Finally, the incentive structure in the organization should be designed to encourage the behavior desired. Again, asking some questions about these factors during an accident investigation can provide insight into the contribution of the safety culture to the events. Does management value safety enough to use it as an important criterion when making decisions about promotions and raises?

Changes and Dynamics over Time: In the System and in the Environment

Accidents usually occur after some type of change. The changes may be in the physical process, the operating procedures, individual behavior, the safety activities or processes, the management process, oversight practices (both internal and external), or in the environment in which the system exists and with which it must interact.

Changes may be planned or unplanned. Both types of changes need to be controlled and can lead to accidents if they are not.

If the changes are planned, a strong and well-designed management of change policy that is enforced and followed should be in place. In many accidents, management of change (MOC) procedures existed, but they were neither effective nor enforced. Examples in the Shell Moerdijk explosion include the switch to a new catalyst without testing it and assuming that previous catalyst properties still held and the removal of parts of the work instructions for Unit 4800 (again without assessment) because they were not considered critical. Critical requirements regarding nitrogen flow were removed during periodic updates of the work instructions in an attempt to limit their content to information that was

believed essential and to focus on what was incorrectly thought to be the most important from a safety and operational view. Other information was omitted from the work instructions because, over time, understanding of the most appropriate procedures related to Unit 4800 changed.

Changes impacting risk may also be unplanned. There needs to be a way to detect unplanned changes that affect safety and to prevent them from occurring. Detection may be accomplished by using leading indicators and safety-focused audits. There may also be periodic planned re-evaluation of assumptions underlying the original safety-related design features and management procedures. At Shell Moerdijk, the leading indicators (such as number of leaks) were inadequate and too narrow, audits did not seem to be effective, and assumptions about the properties of ethylbenzene established in 1977 were never revisited.

Changes may occur slowly over time, as occurred at Shell Moerdijk with the work instructions for Unit 4800. As the work instructions were amended before each turnaround, important information was omitted—in some cases intentionally and in others unintentionally. Examples include the nitrogen flow requirements mentioned above and the required heating rate for the reactor. Changes do not appear to have been reviewed by experts, but if they were, then the review process was flawed.

Changes may be known and planned in one system component but appear as unplanned and unknown changes to another component of the system. The change in composition of the catalyst was known by the catalyst manufacturer but not by Shell Moerdijk. Clearly communication is an important factor here.

Leading indicators are commonly used in some industries to identify when the system is migrating toward a state of higher risk. At Shell Moerdijk, as well as most chemical plants, leading indicators used may be common throughout the whole industry, in this case number of leaks. Their selection seems to be predicated primarily on ease of collection and lack of having any alternatives for creating more effective ones.

I have created a new approach to identifying leading indicators that I called "assumption-based leading indicators."[21] Briefly the idea is that certain assumptions are made during system development that are used to design safety into a system. When, over time, those assumptions no longer hold, then the organization is likely to migrate to a state of higher risk. Leading indicators, then, can be identified by checking the original safety-related assumptions during operations to make sure that they are still true. Systems will always change and evolve over time, as will the environment in which the system operates. Because changes are necessary and inevitable, processes must be created to ensure that safety is not degrading. This new approach to leading indicators is being evaluated by Diogo Castilho, a Ph.D. candidate at MIT, on airline operations.[22]

Changes may evolve slowly over time and their impact may not be obvious. In a CAST analysis of crash of a cargo aircraft while landing at Birmingham Airport, one factor implicated in the inadequate operation of the safety control structure as a whole was an increase in night cargo operations at airports. Is there as much weight placed on cargo aircraft safety as passenger aircraft. Is more concern shown for daylight operations than for operations in the early darkness, which may be complicated by fatigue? We found that historical assumptions about airport operations may need to be revisited in the light of changes to airline operations and traffic.

Informal (and even formal) risk assessment may change as time passes without a loss. The actual risk has probably not decreased, but our perception of it does. That leads to a change in priorities and in the

[21] Nancy Leveson, (2015), A systems approach to risk management through leading safety indicators, *Reliability Engineering and System Safety*, 136: 17-34, April.

[22] Diogo Silva Castilho, *A Systems-Based Model and Processes for Integrated Safety Management Systems*, Ph.D. Dissertation, Aeronautics and Astronautics, MIT, expected September 2019.

resolution of conflicting goals. Indeed, the Space Shuttle losses can be partly explained in this way, particularly the Columbia accident. Unfortunately, a strange dynamic can arise where success at preventing accidents can actually lead to behavior and decision making that paradoxically increases risk. A circular dynamic occurs where safety efforts are successfully employed, the feeling grows that accidents cannot occur, which leads 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 and so on.

The complacency factor is so common that safety control structures need to include ways to deal with it. SUBSAFE, the U.S. nuclear submarine safety program puts major emphasis on fighting this tendency and has been particularly successful in accomplishing this goal. Identifying the migration to states of higher risk is an important part of any accident investigation. Understanding the reason for this migration during an accident causal analysis in which unrealistic risk perception is involved can help to identify ways to design the safety control structure to prevent it or detect it when it occurs.

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 better information controllers have, the more accurate will be their process models and therefore their decisions. Accident analysis should involve a careful investigation of the accuracy of risk perception in the mental models of those controlling safety.

Internal and external economic and related factors

Systemic factors contributing to accidents often involve both internal and external economic conditions such as external market competition or declining profits. Market conditions may lead to management reducing the safety margins and ignoring established safety practices. Usually, there are precursors signaling the increasing risks associated with these changes, but too often these precursors are not recognized.

Another common factor is reduction in the physical separation between people and dangerous processes. Hazardous facilities are usually 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 may be more readily available near heavy industrial plants, as was the case at Bhopal. The lure of providing jobs and economic development may encourage government officials to downplay risks and not rigorously enforce their safety control and emergency response requirements.

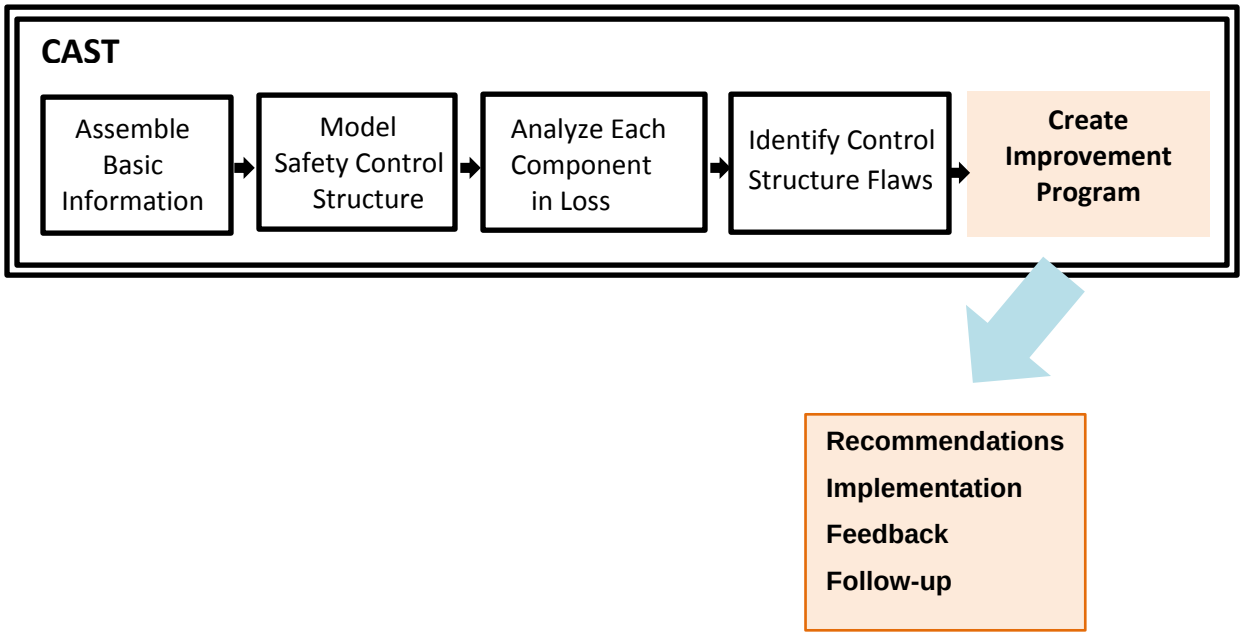
Over time, the land available for building may only be available near dangerous parts of the plant, as happened at the Texas City refinery where trailers were built to house employee offices next to the ISOM tower that exploded in 2005. With increasing population, local emergency facilities, such as firefighting and medical resources, may lag behind the increasing requirements due to constraints on resources and other competing priorities.

These factors may relate to the system environment not covered previously in the analysis of the individual controllers or even other general systemic factors, particularly changes and dynamics over time. How was individual controller behavior affected by these factors? Obvious factors are financial and competition concerns as well as new products and markets. Some non-obvious factors might be fatigue and duty cycles, distraction by contract negotiations, poor morale on the part of the work force due to a variety of factors, pressures to increase productivity beyond a reasonable level, etc.

Sometimes processes are automated and the standard safety controls implemented by humans are not implemented in the automated processes. There is often a naïve belief that software is always safe because it doesn't "fail" or that computers are more reliable than humans and therefore will improve

safety. Unfortunately, introducing automated systems introduces other changes into the system, often some that were not previously present. Complacency rises and new causes of accidents are introduced that are not controlled by the existing safety control structure.

Generating Recommendations and Changes to the Safety Control Structure



5. *Create recommendations for changes to the control structure to prevent a similar loss in the future. If appropriate, design a continuous improvement program for this hazard as part of your overall risk management program.*

Generating Recommendations

Once the other parts of the analysis are completed, generating recommendations should be straightforward. The biggest complaint about CAST we hear is that it generates too many recommendations. This complaint is only justified if the goal of the accident investigation is to make as few recommendations as possible. Accident investigation has had the goal of identifying "root causes" or "probable causes" for so long that it may be a cultural shock to start looking at more causal factors that generate more recommendations.

One of the objections raised to including a large number of recommendations is that responding to them is overwhelming. This is simply a logistical problem and not one that should be solved by learning less from each accident. There is no reason that recommendations cannot be prioritized according to specified criteria. There is also no implication that all the recommendations must be implemented immediately. Some recommendations will be relatively straightforward to implement immediately while others may take longer. Some may require such extensive changes that implementing them will take a great deal of effort and resources. Examples of the latter include establishing a new oversight agency or changing regulations and laws. Difficulty of implementation is not an excuse to omit a recommendation from the accident report, but it may be a good reason to categorize it as a longer-term goal rather than an immediate fix.

Taking steps to "jury-rig" short-term solutions should not be an excuse for endlessly delaying comprehensive and effective solutions.

Establishing a Structure for Continual Improvement

Sometimes recommendations are made but never implemented. Not only must there be some way to ensure recommendations are followed, there must also be feedback to ensure that they are effective in terms of achieving the goals and strengthening the safety control structure.

Essentially there are three requirements:

1. Assigning responsibility for implementing the recommendations
2. Checking that they have been implemented
3. Establishing a feedback system to determine whether they were effective in strengthening the controls.

The third requirement implies the need to collect evidence about the effectiveness of the recommended changes. Such feedback can come from audits and inspections and from the analysis of later incidents to determine whether previous recommendations were successful. Such an activity is a critical component of any safety management system, but it is often omitted.

Subsequent accidents or losses, particularly if they are analyzed using CAST, provide a rich source of information to understand why previous recommendations were not effective and what else is needed. Was the original causal analysis flawed? Were assumptions about the potential effectiveness of particular improvements incorrect? Did other changes occur that thwarted the attempt to strengthen the safety control structure? Did the planned changes result in unforeseen consequences?

The goal here is to ensure that your organization is continually learning and improving its risk management efforts so that the potential for losses is reduced over time.

Suggestions for Formatting the CAST Results

In STAMP, losses involve complex processes, not just a simple chain of events or even combination of event chains. The interactions among the events and causal factors are often intricate and subtle or indirect. In the end, it may be infeasible to list them as separate factors but only to understand the relationships among them. As a result, the format for presenting CAST results should emphasize the relationships among the various causal factors rather than a simple list, although lists are often difficult to avoid.

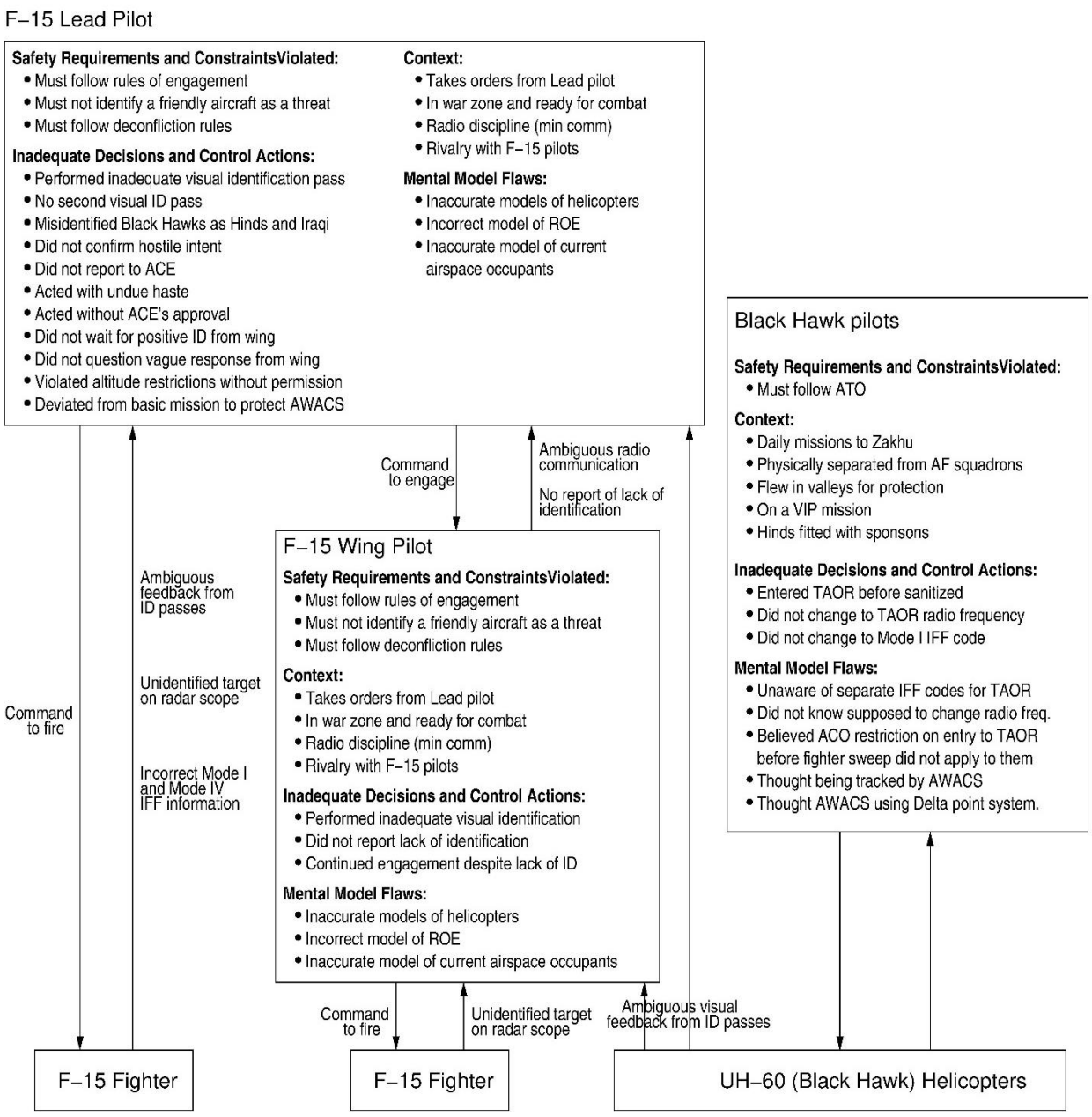
Tools for storing and organizing the results of a CAST analysis could easily be created, with extensive use of hyperlinks to show the relationships between various factors and behaviors and the location of answers to generated questions throughout the CAST analysis. More difficult, however, is coming up with a satisfactory standard notation for the presentation of the CAST results.

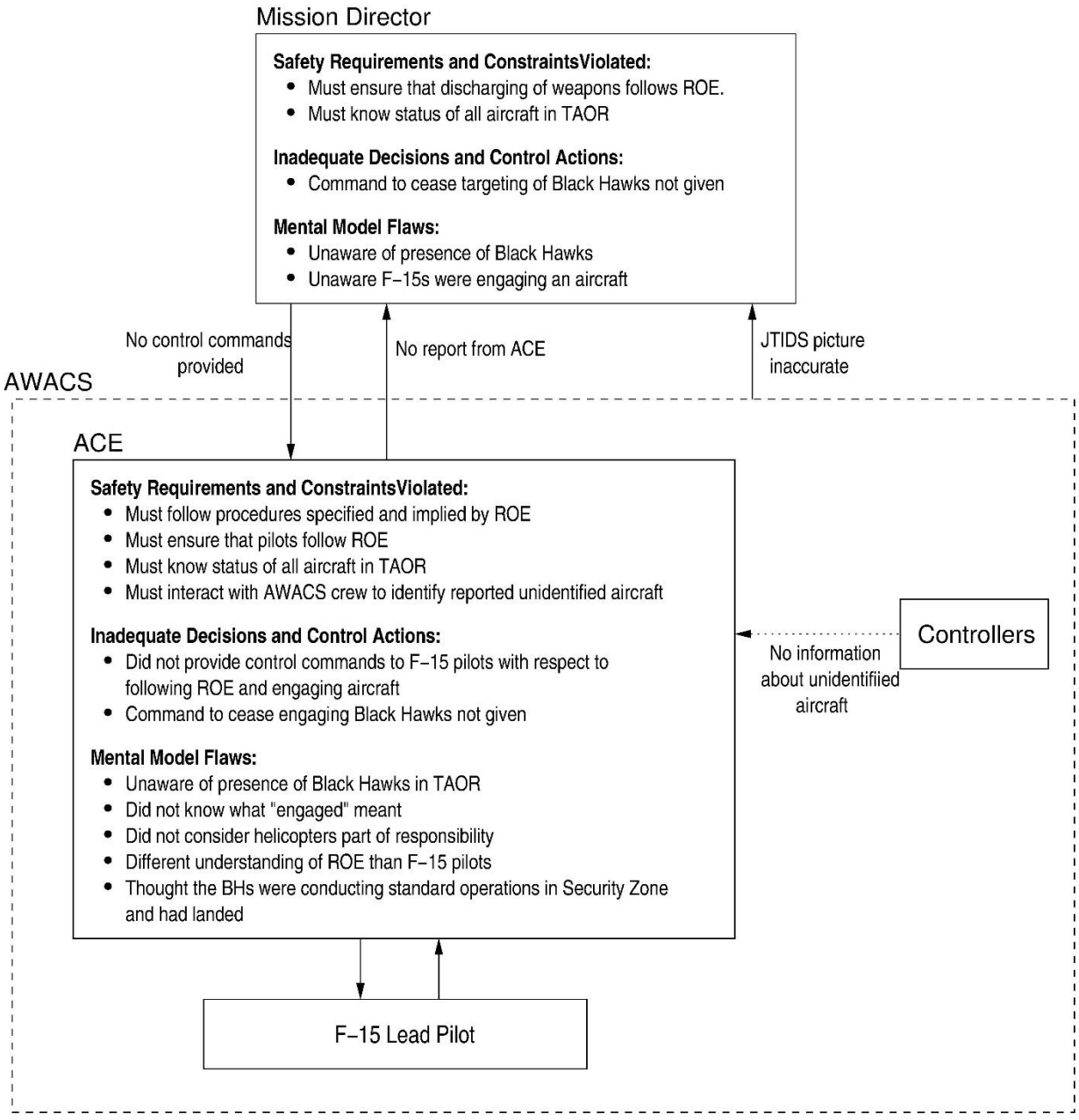
The goal is, of course, to provide the reader with an understanding of all the causal factors involved and how they all relate to each other. Different notations have had advantages in different accident analyses, with none that we have found working best for all of them.

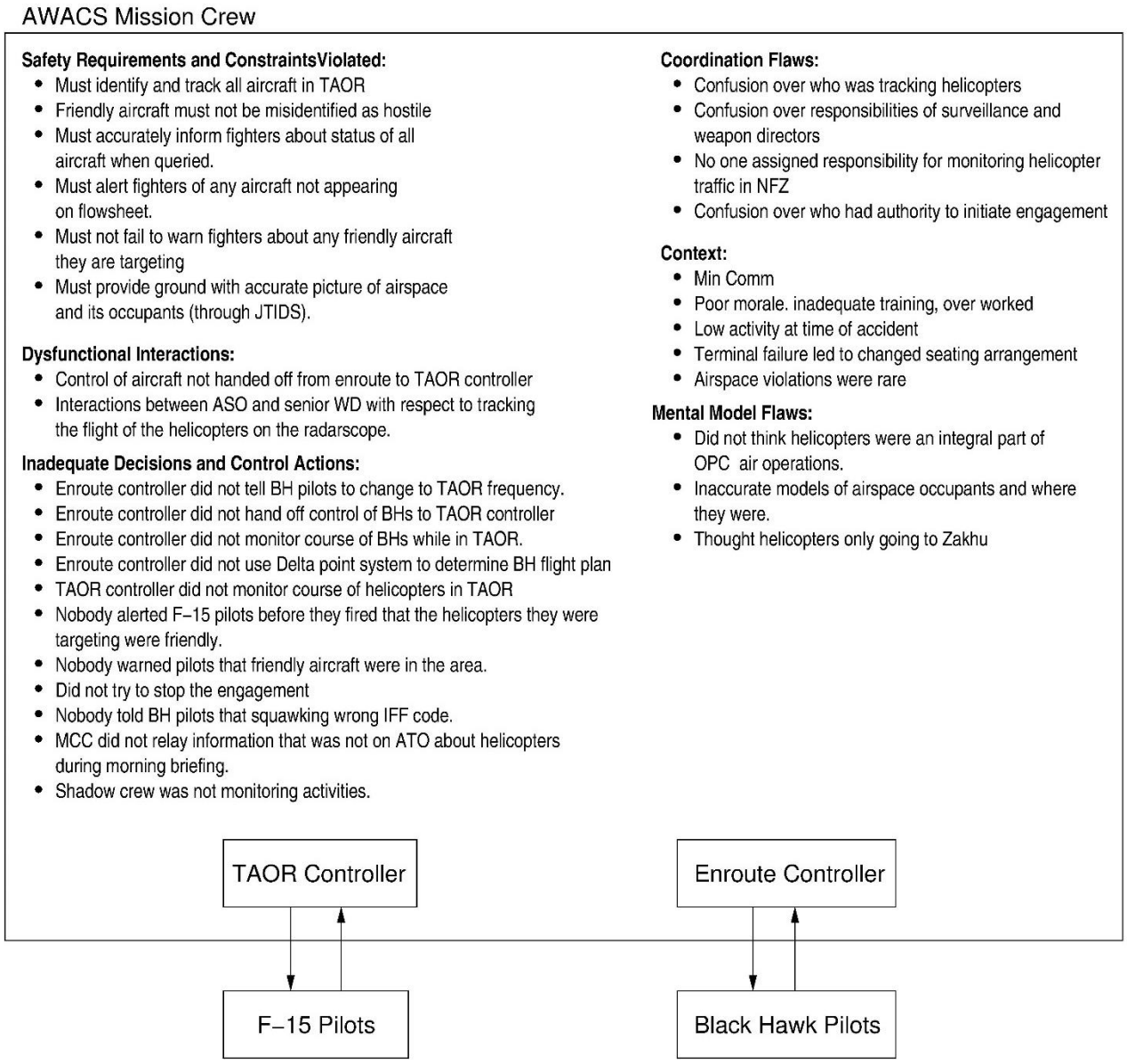
As a result, documenting all the details of the analysis can use various types of notation, but readability and comprehensibility are important in a final summary of the causes of the accident. While all the details may not be necessary, there needs to be a way to present critical conclusions and argument. Trying to fit this all on a page (as with AcciMap analyses) leads to oversimplification and omission of important information. On the other hand, spreading the information over too many pages may lead to information overload and missing the bigger picture. I present here only a couple of examples that I have used and leave it for others to come up with better ideas.

For the Shell Moerdijk accident, I used the following format: a colored safety control structure with a table using colors as links to the summary analyses of the components as can be seen in Appendix B.

Alternatively, I have tried to insert the most important summary information in the control structure itself. Several figures from my analysis of a friendly fire accident where a U.S. F-15 shot down a U.S. Black Hawk helicopter over the Iraqi No-Fly-Zone are included here. The first shows the actions and analysis for the pilots, i.e., the F-15 lead pilot, the F-15 wing pilot, and the Black Hawk pilots. The second shows the analysis of the director of the ACE (the Airborne Command Element) up in the AWACS aircraft, who was commanding traffic in the area. The Mission Director was on the ground and overseeing the activities of the ACE. The third figure shows the analysis of the AWACS crew. Each of these figures is described in much more detail with accompanying text in the actual CAST analysis report. The notation does, however, allow an overview of the analysis. The additional text in the full CAST report should provide important but more detailed information.


F–15 Lead Pilot
Safety Requirements and ConstraintsViolated:
• Must follow rules of engagement
• Must not identify a friendly aircraft as a threat
• Must follow deconfliction rules
Inadequate Decisions and Control Actions:
• Performed inadequate visual identification pass
• No second visual ID pass
• Misidentified Black Hawks as Hinds and Iraqi
• Did not confirm hostile intent
• Did not report to ACE
• Acted with undue haste
• Acted without ACE's approval
• Did not wait for positive ID from wing
• Did not question vague response from wing
• Violated altitude restrictions without permission
• Deviated from basic mission to protect AWACS
Context:
• Takes orders from Lead pilot
• In war zone and ready for combat
• Radio discipline (min comm)
• Rivalry with F–15 pilots
Mental Model Flaws:
• Inaccurate models of helicopters
• Incorrect model of ROE
• Inaccurate model of current airspace occupants
Black Hawk pilots
Safety Requirements and ConstraintsViolated:
• Must follow ATO
Context:
• Daily missions to Zakhu
• Physically separated from AF squadrons
• Flew in valleys for protection
• On a VIP mission
• Hinds fitted with sponsons
Inadequate Decisions and Control Actions:
• Entered TAOR before sanitized
• Did not change to TAOR radio frequency
• Did not change to Mode I IFF code
Mental Model Flaws:
• Unaware of separate IFF codes for TAOR
• Did not know supposed to change radio freq.
• Believed ACO restriction on entry to TAOR before fighter sweep did not apply to them
• Thought being tracked by AWACS
• Thought AWACS using Delta point system.
Command to engage
Ambiguous radio communication
No report of lack of identification
F–15 Wing Pilot
Safety Requirements and ConstraintsViolated:
• Must follow rules of engagement
• Must not identify a friendly aircraft as a threat
• Must follow deconfliction rules
Context:
• Takes orders from Lead pilot
• In war zone and ready for combat
• Radio discipline (min comm)
• Rivalry with F–15 pilots
Inadequate Decisions and Control Actions:
• Performed inadequate visual identification
• Did not report lack of identification
• Continued engagement despite lack of ID
Mental Model Flaws:
• Inaccurate models of helicopters
• Incorrect model of ROE
• Inaccurate model of current airspace occupants
Ambiguous feedback from ID passes
Unidentified target on radar scope
Incorrect Mode I and Mode IV IFF information
Command to fire
Command to fire
Unidentified target on radar scope
Ambiguous visual feedback from ID passes
F–15 Fighter
F–15 Fighter
UH–60 (Black Hawk) Helicopters


Mission Director
Safety Requirements and ConstraintsViolated:
• Must ensure that discharging of weapons follows ROE.
• Must know status of all aircraft in TAOR
Inadequate Decisions and Control Actions:
• Command to cease targeting of Black Hawks not given
Mental Model Flaws:
• Unaware of presence of Black Hawks
• Unaware F–15s were engaging an aircraft
No control commands provided
No report from ACE
JTIDS picture inaccurate
AWACS
ACE
Safety Requirements and ConstraintsViolated:
• Must follow procedures specified and implied by ROE
• Must ensure that pilots follow ROE
• Must know status of all aircraft in TAOR
• Must interact with AWACS crew to identify reported unidentified aircraft
Inadequate Decisions and Control Actions:
• Did not provide control commands to F–15 pilots with respect to following ROE and engaging aircraft
• Command to cease engaging Black Hawks not given
Mental Model Flaws:
• Unaware of presence of Black Hawks in TAOR
• Did not know what "engaged" meant
• Did not consider helicopters part of responsibility
• Different understanding of ROE than F–15 pilots
• Thought the BHs were conducting standard operations in Security Zone and had landed
Controllers
No information about unidentifiied aircraft
F–15 Lead Pilot



Systemic factors can often be described effectively with figures. The communication losses in the Überlingen accident was shown using two figures (Figure 16 and 17): one showed the designed communication links and the other showed the links actually operable at the time of the accident. Missing and flawed feedback was shown in Figure 18 for the ComAir Lexington crash. Figures can also be an effective way to show important changes over time in the control structure. Figure 20 shows the original designed control structure involved in an E. coli contamination of a water supply in Walkerton Canada. The details are not important here. Figure 21 shows the control structure as it existed at the time of the accident. The greyed-out structures in Figure 21 show the parts of the control structure that were eliminated over time with the blue structures depicting additions.

System Hazard: Public is exposed to E. coli or other health–related contaminants through drinking water.
System Safety Constraints: The safety control structure must prevent exposure of the public to contaminated water.
(1) Water quality must not be compromised.
(2) Public health measures must reduce risk of exposure if water quality is compromised (e.g., notification and procedures to follow)

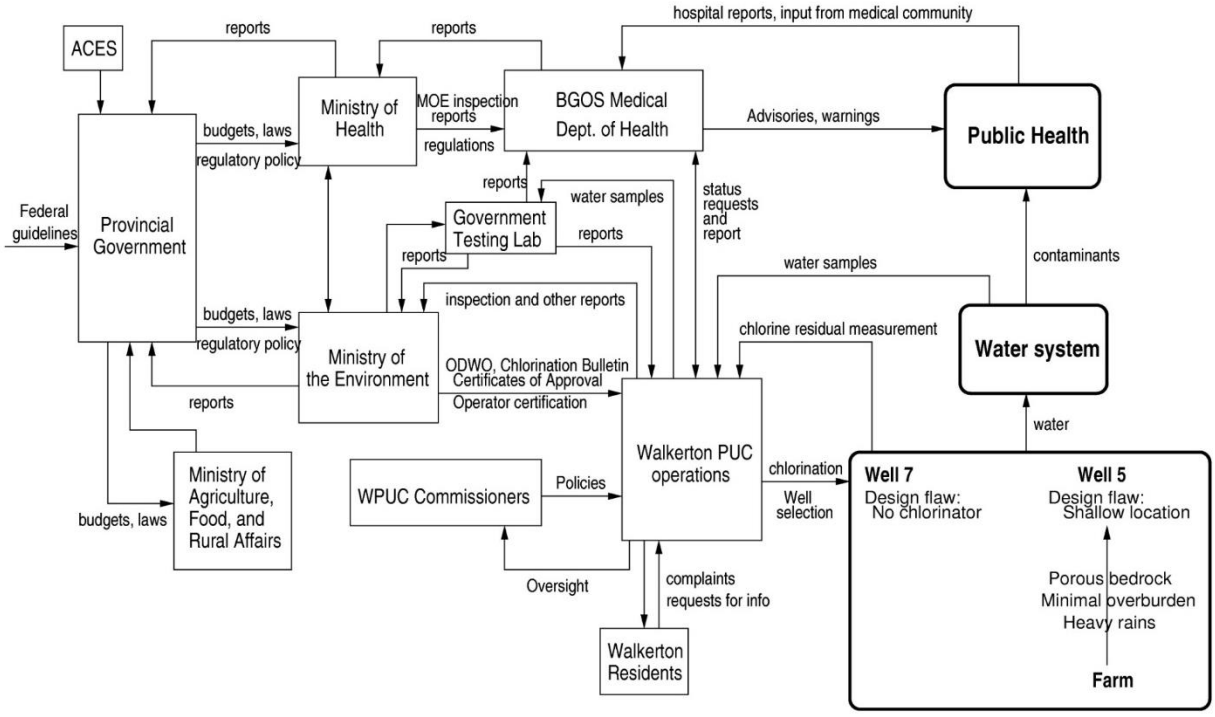


Figure 20: The original, designed control structure to control water quality in Ontario, Canada.

In this water contamination accident, a conservative government had been elected and decided to privatize the government water testing lab. This change would have been OK if the private labs had been required to inform the government about the results of their water testing. However, there was also an effort to reduce what was considered to be red tape and excessive reporting by private companies, so the private testing labs only reported their results directly to the operators overseeing water supply operations in Walkerton, who did not understand that water could be contaminated with E. coli. Figure 21 shows the resulting loss of all feedback about the behavior of the Walkerton operations by the Ministry of the Environment. By shading out the parts of the control structure that had disappeared, the problem is clearly depicted. While the Medical Dept. of Health might have been able to detect the problems, they assumed that the Ministry of the Environment was providing oversight and did not intervene. The blue parts of the control structure show the additions over time. Like any accident, the explanation is quite complicated. For one thing, although operator certification was instituted (which would have required additional education for the Walkerton operators), they were grandfathered out of new education and certification requirements.

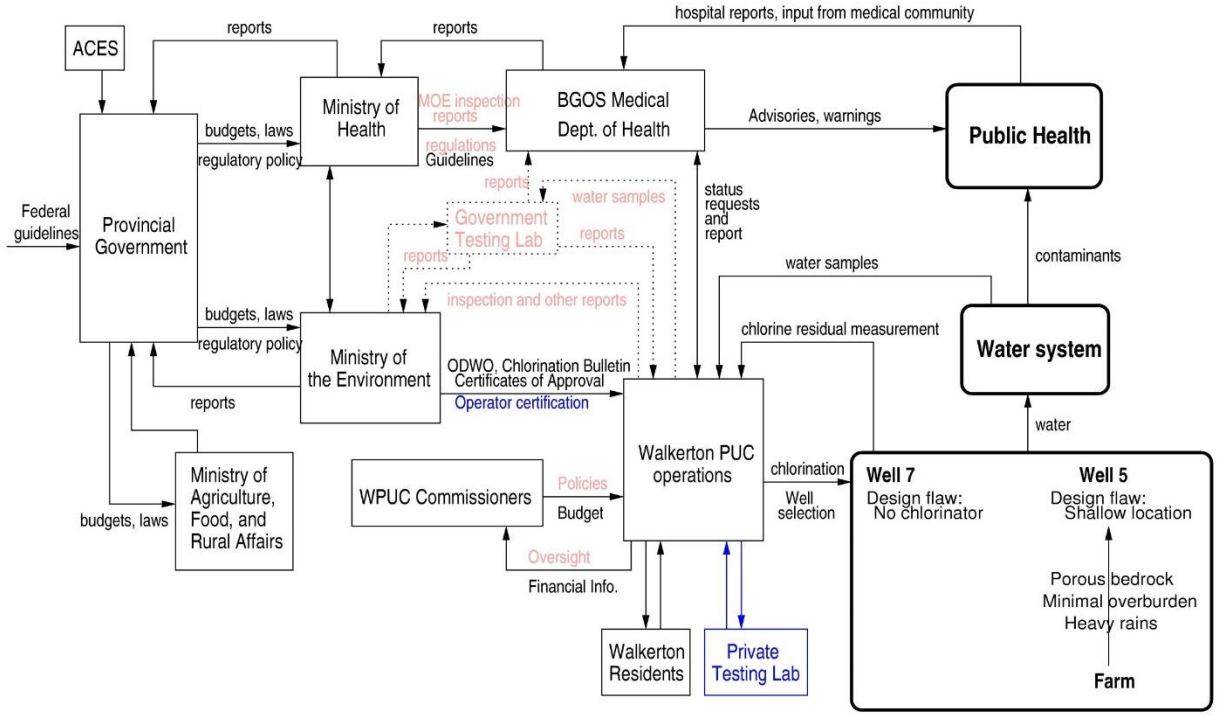


Figure 21: The control structure that existed at the time of the water contamination events.