CAST Analysis of the Shell Moerdijk Accident

Nancy G. Leveson

Massachusetts Institute of Technology

This analysis was created for a benchmarking exercise led by the E.U. Major Accident Hazards Bureau (MAHB), 2016–2017.

INTRODUCTION TO CAST

CAST (Causal Analysis based on Systems Theory) is an accident analysis technique using the STAMP (Systems-Theoretic Accident Model and Processes) accident causality model. Traditionally, accidents have been thought of as resulting from a chain of failure events, each event directly related to the event that precedes it in the chain. For example, water gets into a tank causing corrosion which leads to weakened metal. When the weakened metal is combined with a certain pressure in the tank, the tank may explode leading to injuries and deaths. A comprehensive critique of event chain models is beyond the scope of this document. A detailed discussion can be found in Leveson [2012]. The biggest problem with the chain-of-events model is what it omits.

STAMP extends this model of accident causation to include the chain-of-events model as one subcase but includes the causes of accidents that do not fit within this model, particularly those that occur in the complex sociotechnical systems common today. These causes (in addition to component failure) include system design errors, unintended and unplanned interactions among system components (none of which may have failed), flawed safety culture and human decision making, inadequate controls and oversight, and flawed organizational design. In STAMP, accidents are treated as complex processes rather than simply chains of failure events.

Most safety engineering techniques used today are based on reliability theory and focus on failures. They treat software, human, and organizational behavior as exhibiting random failures and assume individual errors are independent (which these methods do in order to make the mathematics feasible). This approach is much too simplistic to account for the safety culture flaws and poor decision making often involved in major losses. These losses are not the result of a simple summation of individual component (human or technical) failures. For example, in the Deepwater Horizon (DWH) accident, the blowout preventer (BOP) was recognized as critical and had redundant components to make it operate very reliably. What was not accounted for was decision making based on profitability and other social and time pressures that would result in inadequate maintenance of the BOP and decisions to put off replacing the BOP batteries. It also does not account for the common-mode failures of the redundancy in the BOP (i.e., design errors in the attempts to make the BOP very reliable), which resulted from inadequate engineering and underestimation of the risk for such failures. And, of course, the BOP inadequacies are only a tiny part of the problems that occurred in the DWH accident. The social and managerial deficiencies in DWH eclipse the engineering and maintenance flaws.

In contrast, STAMP is based on systems theory and focuses on control. Informally, *s*ystems theory has four basic concepts: hierarchy, emergence, communication, and control [Checkland 1981, Leveson 2012]

<u>Hierarchy</u>: A general model of complex systems can be expressed in terms of a hierarchy of levels of organization. An example of a hierarchical safety control structure is shown in Figure 1, which shows an example for a typical regulated industry in the U.S. Notice that the operating process (the focus of most hazard analysis) in the lower right of the figure makes up only a small part of the safety control structure. There are two basic hierarchical control structures shown in Figure 1—one for system development (on the left) and one for system operation (on the right)—with interactions between them. Each level of the structure contains controllers with responsibility for control of the behavior of the components at the level below as well as their interactions. Higher level controllers may provide overall safety policy, standards, and procedures (downward arrows), and get feedback (upward arrows) about their effect in various types of reports, including incident and accident reports. The feedback provides the ability to learn and to improve the effectiveness of the safety controls.

There is usually interaction between the control structures. Manufacturers must communicate to their customers the assumptions about the operational environment in which the original safety analysis was based, e.g., maintenance quality and procedures, as well as information about safe operating procedures. The operational environment, in turn, provides feedback to the manufacturer about the performance of the system during operations. Each component in the hierarchical safety control structure has responsibilities for enforcing safety constraints appropriate for that component, and together these responsibilities should result in enforcement of the overall system safety constraints.

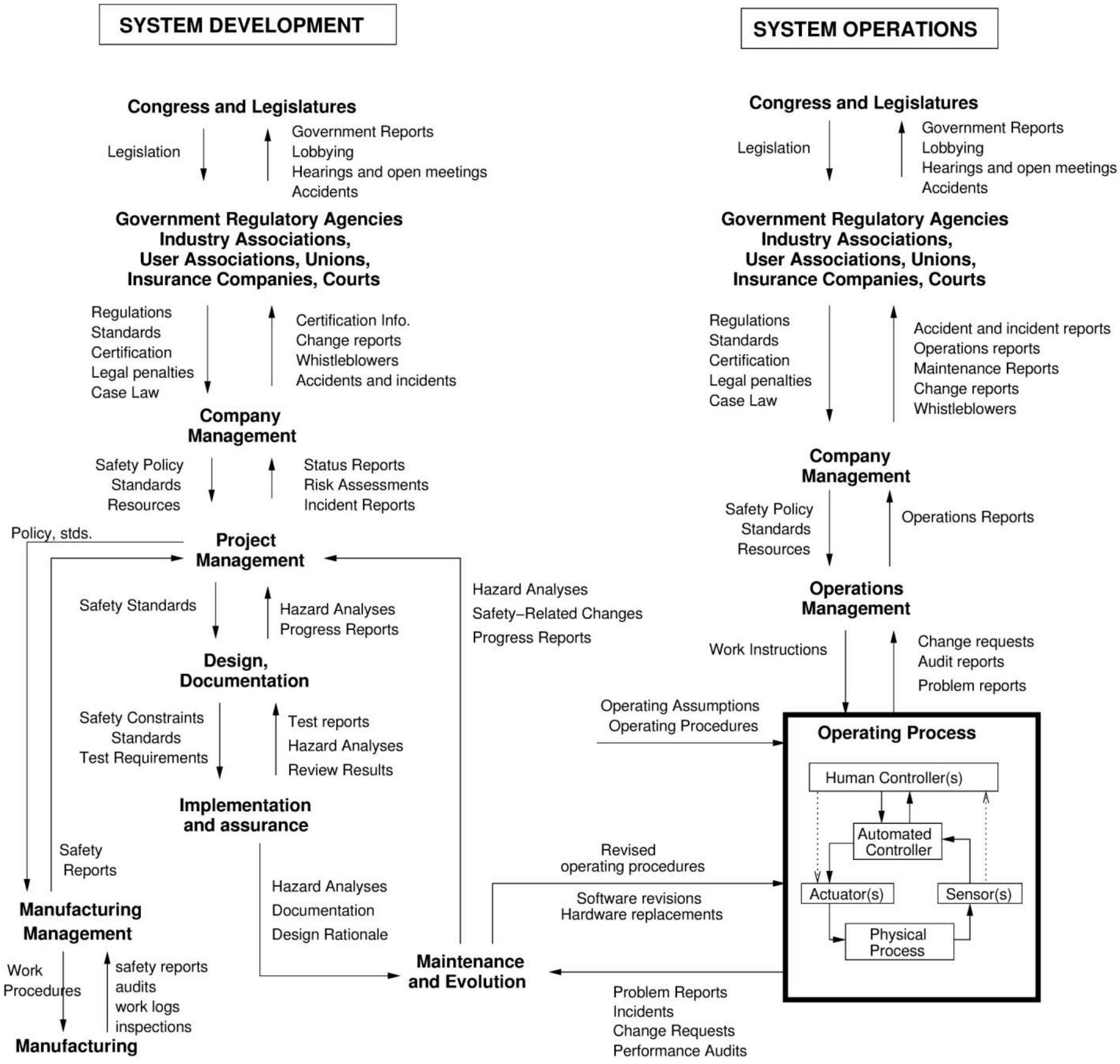

Figure 1. An Example Hierarchical Safety Control Structure

- Emergence: Each level of the hierarchy is characterized by having emergent properties. Emergent properties are not in the specific components at that level but instead *emerge* (arise) from the interactions among the components. For example, fire results when a source of combustion interacts with combustible material in the presence of oxygen. Safety and security are examples of emergent properties. A valve in a plant may be unsafe, for example, only when it interacts with other plant components in a particular way. Emergent properties associated with the behavior of components at one level in a hierarchy are related to constraints upon the degree of freedom of those components. One example constraint is that pressure in a chemical reactor must never be allowed to rise above a particular level and that communities near plants producing potentially toxic chemicals must have contingency plans in place to deal with an accidental release. Controls need to be created to ensure that the safety constraints are enforced.

- <u>Control</u>: Control involves the imposition of constraints upon the activity at a lower level of the hierarchy, i.e., at the interfaces between levels. The imposition of safety constraints on the behavior of the system components plays a fundamental role in a systems approach to safety. A physical example of a typical control for a chemical plant is a pressure relief valve. An organizational example is the safety engineering department creating standards for safe operation. Finally, a social control example is a regulator providing oversight and certification of plant activities and policies. Losses occur when the controls are not adequately designed or enforced, resulting in violation of the safety constraints.
- <u>Communication</u>: Control implies the need for communication between levels of the hierarchy and between the components at each level.

This type of model is similar to Rasmussen's model of sociotechnical control [Rasmussen 1997] except that he includes only the operational aspects of the system while treating engineering and manufacturing activities only as inputs to the model, and he ties his model to an event chain. See the AcciMap model of the Shell Moerdijk accident being produced independently for this benchmarking effort, which is based on Rasmussen's model.

Note that the use of the term "control" does not imply a rigid command and control structure. Behavior is controlled not only by engineered systems and direct management intervention, but also indirectly by policies, procedures, shared value systems, and other aspects of the organizational culture. All behavior is influenced and at least partially "controlled" by the social and organizational context in which the behavior occurs. Engineering (i.e., designing) this context can be an effective way to create and change a safety culture, i.e., the subset of organizational culture that reflects the general attitude about and approaches to safety by the participants in the organization or industry [Shein 1986]. Formal modeling and analysis of accidents/incidents must include these social and organizational factors and cannot be effective if it focuses only on the technical aspects of the system. As we have learned from major accidents in the oil and gas industry and most other industries, managerial and organizational factors are as important as technical factors in accident causation and prevention.

For space reasons, Figure 1 emphasizes the high-level components of a safety control structure and not their detailed design. The detailed design of the operating process (lower right-hand box) can be quite complex, such as the detailed design of the physical chemical plant itself and the operations in the plant.

Figure 2 shows the basic form of the interactions between the levels of the control structure, where the controller imposes control actions on the controlled process. The standard requirements for effective management—assignment of responsibility, authority, and accountability—are part of the control structure design and specification.

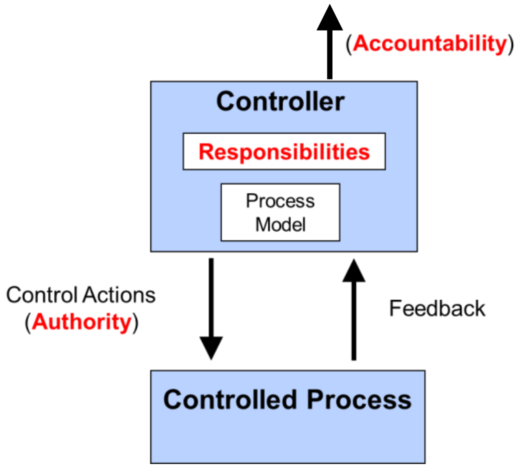

Figure 2. A Simple Feedback Control Loop showing the relationship to standard management concepts of responsibility, authority, and accountability

The controller uses information about the current state of the controlled process, usually derived at least partially from feedback. In STAMP, feedback information is incorporated into the controller's model of the controlled process, called the *process model* or, if the controller is a human, it may be called the *mental model*. Accidents often result when the controller's process model becomes inconsistent with the actual state of the process and the controller provides unsafe control as a result. For example, the controller thinks that catalyst has been added to the reactor when, in fact, it has not. Other examples are that the manager of a plant undergoing restart after a maintenance stop believes the operators have adequate training and expertise to perform the operation safely when they do not or an operator thinks that the pressure in a reactor is within a safe limit when it is in the danger zone.

The problems occur not just with inconsistency between the controller's process model and the state of the controlled process but also when different operators, all involved in the same general task—particularly under safety-critical or emergency conditions—are operating with different mental models of either (a) what the system is currently doing, or (b) what should be done to control it.

Process models are kept up to date through feedback or from information received externally. A common factor in accidents is that appropriate feedback or other information about the controlled process is incorrect, missing, or delayed.

There are four types of unsafe control actions:

- A provided control action leads to a hazard
- Not providing a necessary control action leads to a hazard
- A control action provided with wrong timing (early, late) or in the wrong order leads to a hazard
- A continuous control action provided for too long or too short a time leads to a hazard

These four types of unsafe control actions, along with the hierarchical safety control structure, can be used after an accident to generate the causal scenarios that led to it or to identify future potential accident scenarios so they can be eliminated or mitigated.

The use of the process model concept is a much better way to understand why humans or software may have done the wrong thing and how to prevent such events in the future than simply saying the human or software "failed," which only attaches a pejorative word without providing any insight about *why* the person or software did something dangerous.

CAST is a method for analyzing accidents with the STAMP causality model as its foundation. Hence, it assumes accidents are caused by a lack of effective enforcement of safety constraints on the system behavior to prevent hazardous states (conditions). CAST takes a "systems thinking" view of accidents using the following assumptions:

- Accidents are complex and do not have single or even several "root causes." A root cause is often defined as an event in the event chain whose removal would prevent the final undesirable consequence. In practice, the root cause is usually identified by going back in the event chain until some event can be labeled as the root cause. Rasmussen suggests that a practical explanation for why actions by operators actively involved in the dynamic flow of events are so often identified as the cause of an accident is the difficulty in continuing the backtracking "through" a human [Rasmussen 1990]. The concept of a root cause is seductive because it gives us an illusion of control. It often leads to a sophisticated "whack-a-mole" process that results in fixing symptoms but not the flaws that led to those symptoms. The result may be an organization or industry that is in continual fire-fighting mode.

  Major accident causes never consist of just a few limited factors: Almost always there is unsafe behavior by the operator, flawed management decision making, flaws in the physical design of the equipment as well as flaws in the engineering process used to design that equipment, safety culture problems, regulatory deficiencies (if the industry is regulated), and unsafe interactions among all these factors or components of the system. Some accident analysis techniques focus on one aspect, such as human factors, system component failures or failures of barriers. Instead, we need accident analysis techniques that allow us to consider *all* the factors that may be involved in a loss, including social, managerial, organizational, human, and technological and their interactions and relationships, including *indirect* relationships.

  In STAMP, the root cause of all accidents is the same: The design and/or operation of the safety control structure were inadequate to prevent the loss or near miss. The goal of accident analysis, then, is to identify the flaws in the safety control structure that allowed the events to occur and to learn how to strengthen the controls to prevent similar losses from occurring in the future.
- Blame is the enemy of safety [Leveson, 2012]. Blame is a matter for courts. Engineers and managers need to understand *why* something occurred, not *who* to blame. While punishing the person or people involved may be satisfying, it does not fix the reasons why they did what they did and does not prevent similar events in the future. Too often, an accident investigation stops after assigning blame and does not provide enough information to eliminate the basic social and technical factors involved. In addition, blame can be counterproductive. For example, it can lead to finger pointing and hiding important information during investigations.
- Human error is a symptom of a system that needs to be redesigned. Most accidents are blamed on the operators. Human behavior, however, is always influenced by the context in which it occurs. That context usually has physical, organizational, psychological, and social aspects that impact on the behavior. Trying to change behavior without changing the context in which it occurs is usually doomed to failure. Identifying the contextual aspects of human behavior involved in an accident is necessary to learn what to change to prevent such behavior in the future.
- Hindsight bias hinders learning from accidents. For the most part, humans are trying to do the right thing and do not purposely do something that will injure themselves or others. After an accident, it is easy to see where people went wrong, what they should have done or not done, to judge people for missing a piece of information that turned out to be critical, and to blame them for not foreseeing or preventing the consequences [Dekker 2006]. Before the event, such insight is difficult and, usually, impossible. The Clapham Junction railway accident in Britain concluded: "There is almost no human action or decision that cannot be made to look flawed and less than sensible in the misleading light of hindsight." [Hidden 1990] Saying that a person

did something wrong provides very little useful information about how to eliminate that behavior. The common phrases in accident reports like "he could have," "she should have," or "if he or she would have" all indicate instances of hindsight bias. To improve safety, it is necessary to start with the premise that except for a few sociopathic individuals, nobody purposely engages in behavior that they think will lead to an accident. For maximum learning from the loss, we need to get rid of hindsight bias in our accident reports and go beyond listing what people did wrong and ask *why it made sense to the person to do what they did* [Dekker 2006]. Factors that can influence behavior include conflicting goals (e.g., safety vs. efficiency), unwritten rules or norms, lack of information observability (information may be available but not observable for many reasons), productivity pressures, attentional demands, and organizational context. CAST attempts to eliminate hindsight bias as much as possible from accident analysis and identify why the unsafe (in retrospect) behavior occurred.

In summary, the goals of CAST are to

1. Provide a framework and process to assist in understanding the *entire* accident process and identifying the systemic factors
2. Get away from blame ("who") and shift the focus to "why" and how to prevent such occurrences in the future
3. Identify why people behaved the way they did, including the contextual factors that influenced their behavior
4. Minimize hindsight bias
5. Determine the weaknesses in the safety control structure that allowed the loss to occur.

The basic process involved in a CAST analysis involves first creating the safety control structure at the time of the loss:

1. Starting at the bottom of this structure (the physical process involving the loss), identify the failures and unsafe interactions involved in the loss events (e.g., explosion) as well as any physical controls that were designed to prevent the specific loss events that occurred. Why were they not effective?
2. Next, starting with the controller(s) immediately above the physical process and moving in turn upward in the control structure, identify
    a. The controller's responsibilities related to preventing the loss
    b. Their unsafe control actions or lack of actions
    c. Why they behaved unsafely
        i. Process model flaws
        ii. Contextual factors
3. Identify other factors that affected the behavior and interactions among the safety control structure components including
    a. Industry and organizational safety culture
    b. Safety information system
    c. Communication and coordination among controllers
    d. Dynamics and changes over time
4. Generate recommendations that will eliminate or reduce the unsafe behavior. These will often involve missing feedback.

The rest of this report provides an example of CAST applied to an explosion in a Shell chemical plant in the Netherlands.

CAST Analysis of the Accident

This CAST analysis example is based on the official accident report by the Dutch Safety Board [2015]. Unfortunately, a lot of important information needed for the CAST analysis could not be obtained after the completion of the investigation. Where this occurred, the questions that would have been prompted if CAST had been used during the investigation are instead inserted. One of the important tasks of an accident analysis method is to identify the relevant questions to be asked by the investigators.

1.1 Background [1]

On 3 June 2014, an explosion and fire occurred at the Shell Moerdijk plant in The Netherlands. Shell Moerdijk produces chemicals, such as ethylene and propylene, used to manufacture plastic products. Heat is first used to convert gasoil, naphtha, and LPG into a wide variety of chemicals. These chemicals are then used, among other things, as raw materials to produce other products at Shell Moerdijk, including those produced by the styrene monomer and propylene oxide (MSPO) plant involved in the accident.

Shell has two MSPO plants in Moerdijk: MSPO1 (commissioned in 1979) and MSPO2. The accident took place in the MSPO2 plant, which was designed in 1996 by the predecessor of what is now called Shell Projects and Technology,[2] the license-holder for the process. On the basis of a user agreement, Shell Moerdijk is responsible for the operation of the MSPO2 plant.

The MSPO plants produce styrene monomer and propylene oxide using ethylbenzene as the raw material. Styrene monomer is used for the production of polystyrene, a plastic that is used in a wide range of products such as polystyrene foam. Propylene oxide is used for the production of propylene glycol, which is used in food, cosmetics, medicines and other products.

Worldwide, Shell has three more plants in which styrene monomer and propylene oxide are produced by means of a process that is virtually the same as at the MSPO2 plant. Two plants are located in Singapore, at a site called Seraya, and one plant is in Nanhai, China.

In general terms, styrene monomer and propylene oxide are produced as follows (Figure 2[3]): Ethylbenzene reacts with oxygen whereby it is converted into ethylbenzene hydroperoxide. The ethylbenzene hydroperoxide then reacts with propylene with the help of a catalyst[4] and is converted into propylene oxide and methylphenylcarbinol and methylphenyl ketone. The methylphenyl ketone is a by-product of this reaction. In the last step, the methylphenylcarbinol is converted into styrene monomer. The by-product methylphenyl ketone is also converted into methylphenylcarbinol in a separate process step with the help of a different catalyst. It was in this final step of the process that the accident occurred.

The explosion was in the hydrogenation Unit (4800) of the MSPO2 plant. In the reactors of Unit 4800, hydrogen is used along with a catalyst to convert methylphenyl ketone into methylphenylcarbinol. This conversion, using hydrogen, is known as hydrogenation. The reaction with hydrogen in Unit 4800 releases heat, which is dissipated by allowing liquid ethylbenzene to flow along the catalyst in the reactors. The process is called "exothermic hydrogenation reaction." It requires a pressure increase in the reactor. Because hydrogen is very flammable when combined with the increased pressure, fire can

[1] Most of this section is taken directly from the Dutch Safety Board's Accident Investigation Report.

[2] Because I do not know the name of the predecessor organization, it will be referred to by the current name, Shell Projects and Technology, in this analysis.

[3] I know very little about chemical engineering so I made up a notation for the figure that made sense to me. There is probably a standard notation used by chemical engineers.

[4] A catalyst is a substance that influences the rate of a specific chemical reaction.

occur in the event of a leak. This hazard places important safety requirements on the design and operation of the Unit.

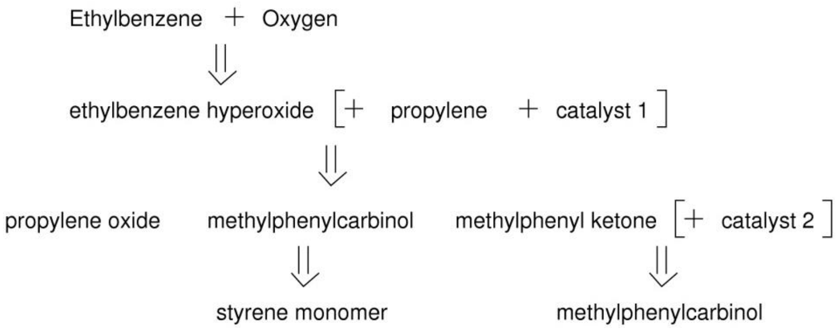

Figure 2. The chemical processing involved in the accident

In general terms, Unit 4800 consists of two reactors, two separation vessels, a combined installation with which a liquid can be heated or cooled, and an installation for condensing the gas flow. The various parts of the Unit 4800 installation are interconnected by pipes and one central pump. See Figure 3.

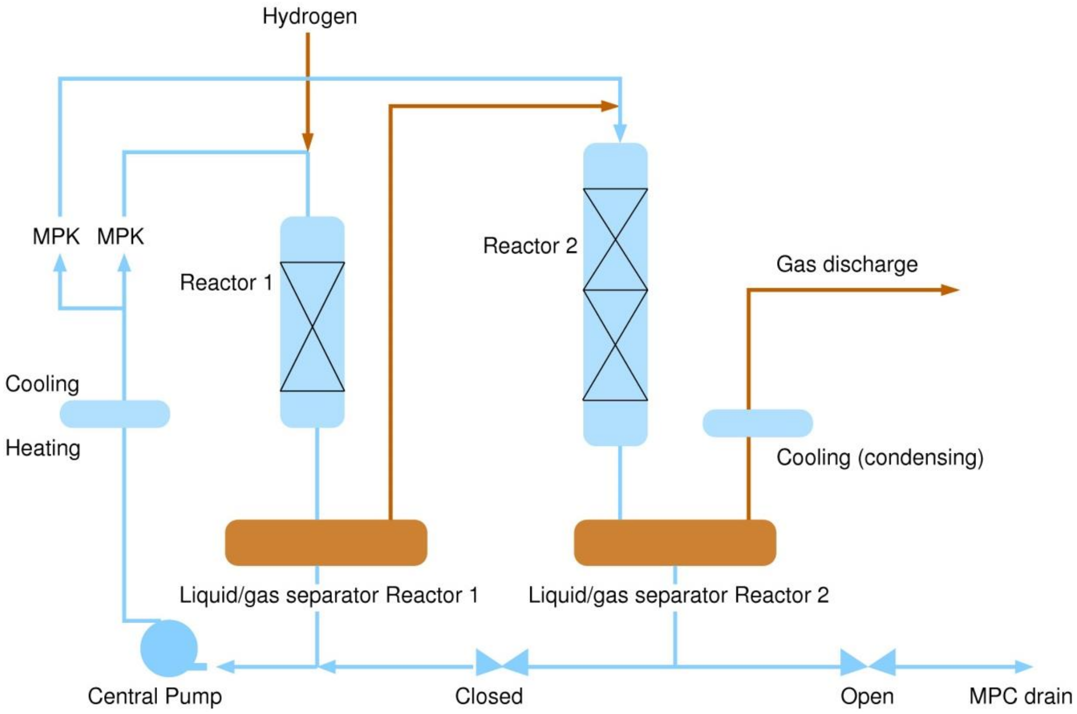

Figure 3. Unit 4800 during normal production [taken from DSB report]

Liquids and gases from the reactor are separated from each other in the separation vessels. The gases from the first separation vessel go to reactor 2, and the gases from the second separation vessel go to the flare (combustion). In order for the separation vessel to function properly, it is important to achieve the correct ratio of gas and liquid. Various safety devices are used to achieve this goal.

The reactors contain a catalyst. The catalyst is used to accelerate the reaction between the substances being used in the reactors. In Unit 4800, the catalyst is in the form of cylindrical catalyst pellets. These are composed of different elements, including copper, chromium and barium. After a number of years of production, the effects of the catalyst decline and it has to be replaced. The catalyst pellets are replaced during a brief maintenance stop. The replacement of the pellets was uneventful in this case.

After the catalyst pellets have been replaced, Unit 4800 has to be restarted. This restart involves several steps: (1) release the oxygen from the Unit and then test for leaks; (2) flush the Unit with ethylbenzene to remove contamination; (3) fill the Unit with clean ethylbenzene and start circulating the ethylbenzene (called the *circulation phase*); (4) heat up the Unit (the *reheating phase*); and (5) reduce the catalyst using hydrogen (the *reduction phase*).

Circulating the ethylbenzene and heating the Unit (Steps 3 and 4) are necessary in order to wet the catalyst pellets and to raise the Unit temperature to a level that facilitates the reduction of the catalyst. The accident occurred during the reheating phase (Step 4).

Thoroughly wetting the catalyst pellets in a trickle-bed reactor[5] is critical. Wetting involves fully soaking the catalyst with ethylbenzene and keeping the pellets continuously wet. If there are localized dry zones, the heat released from a reaction cannot dissipate. The result can be an undesirable rise in the temperature of the reactors. To ensure the catalyst pellets are wet down thoroughly, enough ethylbenzene and nitrogen must be allowed to flow through the reactors and the ethylbenzene must be well distributed. These requirements are achieved by feeding ethylbenzene (liquid) and nitrogen (gas) in the correct ratios through a distribution plate in the reactors, creating a “shower effect” that distributes the liquid optimally across the catalyst pellets.

Catalyst reduction (the fifth step in restarting the reactor) can begin once the plant is at the correct temperature and hot ethylbenzene has been circulated through it for at least 6 hours. Unit 4800 never reached this step on the evening of the accident due to explosions and fire during the heating phase.

1.2 ESTABLISHING THE FUNDAMENTALS FOR THE ANALYSIS

A CAST analysis starts with identification of the hazards that lead to the loss, and the constraints that must be satisfied in the design and operation of the system to prevent those hazards. Hazards in System Safety Engineering (upon which CAST is based) are defined somewhat differently than in many fields. Hazards are defined as states of the system that, when combined with worst case environmental conditions, lead to accidents[6] or losses.

The potential accidents or losses is define very broadly in STAMP and can include any undesirable consequences, such as human death or injury, damage to physical equipment, loss of mission or production, or even damage to reputation.

The system, in this case, is the chemical plant and equipment as well as worker and public health and safety related to chemical plants in the Netherlands.

System Hazard 1: Exposure of 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

[5] Trickle-bed reactors (used in Unit 4800) have “open” columns filled with catalyst in which a gas and a liquid flow together in the same direction under the influence of gravity,

[6] The term “incident” is defined so differently in different fields that it will be avoided here.

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 time (runaway reactions must be prevented)
2. Warnings and other measures must be available to protect workers in the plant and 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.

After the hazards and safety constraints are identified, the safety control structure at the time of the accident can be modeled, showing the controls in place to enforce the constraints. The goal of the safety control structure is to enforce the identified safety constraints on system operation. A major goal of the analysis is to identify why the safety control structure was not able to prevent the adverse events. Then recommendations can be created to strengthen the current controls.

I do not know the details of the safety control structure beyond the information included in the accident report. If this analysis were being done at the time of the accident, the safety control structure could have easily been identified. In this case, I am limited to the information in the official accident report. Some basic organizational structures in process plants will be assumed in this benchmarking exercise.

Figure 4 shows the hierarchical safety control structure at a very high level of abstraction. There were two major subsystems involved: (1) Shell Moerdijk (shown in the dotted box on the left) and the state and community emergency management system (the dotted box on the right). These two subsystems have above them the Dutch regulatory authorities that control the safety of the operation of Shell Moerdijk and other chemical plants in The Netherlands and the state and local emergency management. Shell Global oversees Shell Moerdijk and other Shell subsidiaries.

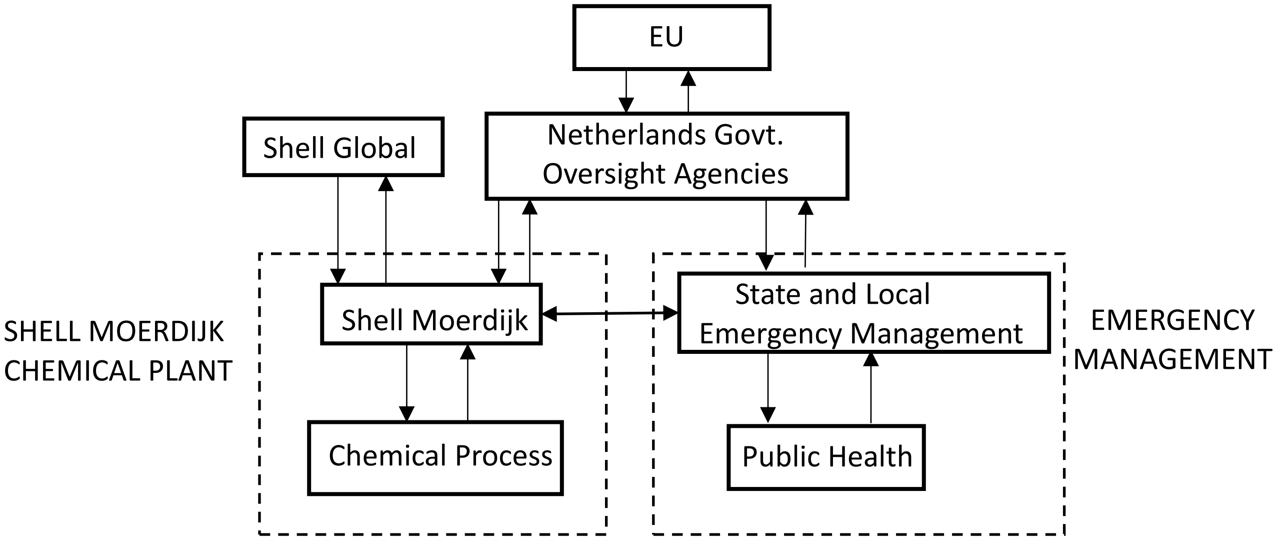
EU
Shell Global
Netherlands Govt. Oversight Agencies
SHELL MOERDIJK CHEMICAL PLANT
Shell Moerdijk
Chemical Process
State and Local Emergency Management
Public Health
EMERGENCY MANAGEMENT

Figure 4. The High-Level Safety Control Structure

As stated earlier, the goal of a CAST analysis is not to place blame or to identify so-called root causes but to understand why the accident occurred. The "root cause" of all accidents, using the STAMP causality model, is that the safety control structure was not able to prevent the adverse events. After all, that is the goal of the safety control structure (or, as it is sometimes called, the safety management system). The goal of the analysis, then, is to understand the weaknesses in this structure so that it can be strengthened.

The CAST analysis process examines each of the components of the safety control structure at the time of the loss and determines how they may have contributed to the events. The process does not stop after a "root cause" is identified but continues until all contributors are understood. Only then can maximum learning occur and changes to strengthen the entire safety control structure be identified. In the events at Shell Moerdijk, as in almost all major accidents, nearly every part of the safety control structure contributed to the events and can be improved.

The safety control structure consists of the controls that have been implemented to prevent hazards. To understand why the accident (the events) occurred using systems thinking and treating safety as a control problem, it is necessary to determine why the controls created to prevent it were unsuccessful and what changes are necessary to provide more effective control over safety.

Figure 5 shows a more detailed version of the safety control structure using the information in the accident report, the author's knowledge of the process industry in general, and the Shell public website. It almost surely does not match the structure within Shell, but it is adequate for this benchmarking exercise.

Each component in a safety control structure has particular responsibilities with respect to safety. For the purpose of this CAST demonstration, responsibilities have been inferred that seemed reasonable but may not match the actual Shell organization. If the CAST analysis had been done as part of the investigation, the responsibilities and control structure could have been determined.

An accident analysis using CAST involves determining whether these responsibilities were carried out and, if not, why not. If the safety control structure used for the analysis does not exactly match that existing at the time of the accident, it will have little impact on the analysis as those responsibilities should be assigned to someone. The goal is not to determine blame but to identify weaknesses in the safety control structure and the changes that need to be made to prevent future losses.

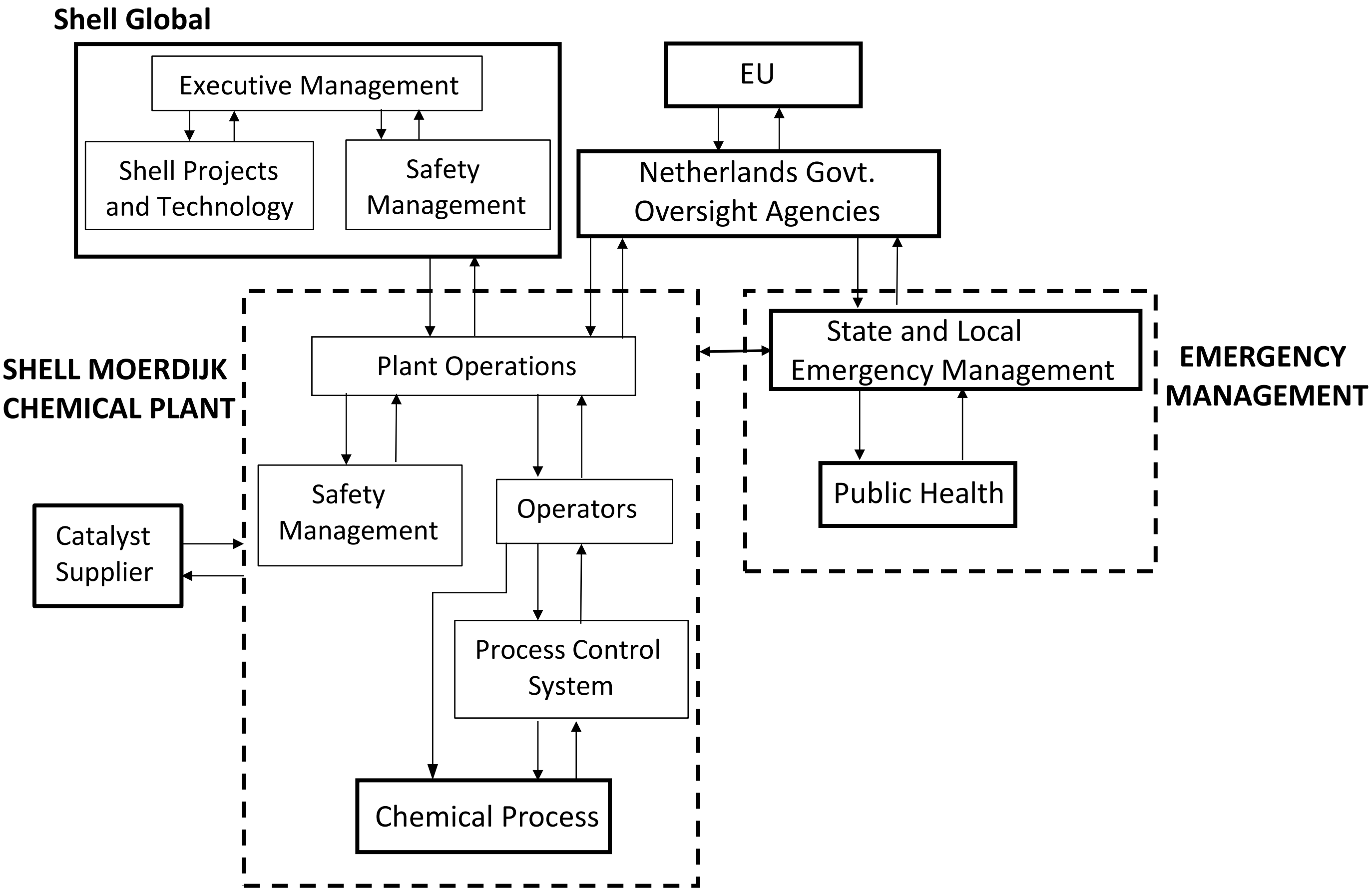

Figure 5. The Assumed Detailed Safety Control Structure for Shell Moerdijk

1.3 Events Involved in the Loss

Focusing on the events only does not provide the information necessary to identify *why* the events occurred, which should be the goal of the accident analysis. Identifying the proximate events preceding the loss is, however, a useful starting place for the analysis. The events can be used to identify questions that need to be answered in the accident investigation and causal analysis. Table 1 shows the primary proximate events leading to and following the explosion and some questions they raise that any accident analysis should answer.

Table 1: Proximal Events Leading to the Loss

ID	Event	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	*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/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 energy was released and unforeseen chemical reactions occurred between the warming up liquid (ethylbenzene) and the catalyst pellets that were used.	*Why were the reactions unforeseen? Were they foreseeable? Were there precursors that might have been used to foresee the reactions? Did 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.	
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 infeasible 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?
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 not isolated during a potentially hazardous operation?* *Why was there no protection against catalyst pellets flying around?*
	A large, raging local fire occurred, generating considerable amounts of smoke	
	Community firefighting, healthcare, crisis management, and crisis communications were initiated.	

After the control structure has been constructed and the events leading to the accident identified, CAST involves examining the role each controller played in the events, starting with the lowest physical plant safety controls at the bottom of the safety control structure and working upward to the social and political controls. At each step, the goal is to look at the higher levels to determine why the unsafe control at the current level occurred. Only the controls related to the specific events are examined, although general safety-related responsibilities are included here. Where the specific information needed for a complete analysis of this particular accident could not be located, questions are inserted (in italics) in the analysis results that would have been asked during a CAST-driven investigation and included in the final report. CAST helps investigators to identify what information needs to be gathered and the questions to ask those involved.

1.4 The Role of the Physical Design of the Plant (Plant Equipment) in the Loss

The analysis of the physical controls does not differ significantly from that done in most accident analysis except that more than failures are considered.

Controls: The physical safety equipment (controls) in a chemical plant are usually designed as a series of barriers to protect against runaway reactions; protect against inadvertent release of toxic chemicals or an explosion (uncontrolled energy); convert any released chemicals into a non-hazardous or less hazardous form; provide protection against human or environmental exposure after release; and treat exposed individuals. The Shell Moerdijk plant had the standard types of safety equipment installed. Not all of it worked as expected, however.

Requirements: 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

Emergency and Safety Equipment (Controls) related to this accident:

- Automatic protection system to release gas to flare tower
- Pressure relief devices in case of overpressurization
- Alarms
- Temperature sensors in reactor

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

- There was an inadequate number of temperature sensors in the reactor to detect hot spots.
- 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.

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:

- 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 and ratio of ethylbenzene and nitrogen 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.

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.

Contextual Factors:

- The plant was out of operation for a short, scheduled maintenance to replace the catalyst-causing granules.
- Unexpected reactions occurred due to vulnerabilities related to the design, including:
  - potential for insufficient wetting
  - use of ethylbenzene and an assumption that this substance is inert

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 after pressure reached a critical level 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.

Recommendations: The physical design limitations and inadequate physical controls need to be fixed. (The potential detailed fixes are not included here; they need to be determined by a qualified chemical engineer.)

The above analysis is useful in terms of learning about flaws in the design of the physical equipment and how to eliminate them to prevent the same occurrence in the future. It does not, however, fully explain why the accident occurred and what needs to be changed (beyond this specific design) in the design process, in the assumptions used in the design process, and in operations to prevent a wide variety of accidents in the future and not just a repetition of these specific events. Many questions are raised from this analysis, such as: Why did the design flaws get through the design and review process? Were they there from the beginning or did they result from changes over time? Were there any precursor events that might have been used to identify the design flaws before an accident occurred? Why did the operators not notice the increasing pressure before the runaway occurred and prevent the explosion? And so on.

To answer these questions, it is necessary to look at the higher-level components of the safety control structure that were meant to prevent and control unsafe conditions in the physical plant.

1.5 PROCESS CONTROL SYSTEM

It is assumed in the ensuing analysis that Shell Moerdijk got the basic design of the plant from Shell Projects and Technology, but that the design of the process control system was local. If this assumption is incorrect, it will not change the final recommendations, but simply where in the overall safety control structure the poor decision-making (in hindsight) occurred.

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.

Unsafe Control Actions (UCAs):

UCA: 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.

Process Model Flaws: It appears that the process control system, for the most part, had the correct information to assist the operators in controlling the start-up. There was some missing information about temperature that was the result of inadequate numbers of temperature sensors.

Why? (Factors Affecting the Unsafe Control)	Questions Raised
The process control system was configured for the normal production phase. In an automatic control circuit, the control system regulates and checks that the set value is achieved and stabilized, without intervention by an operator. For example, at a set heating rate, both	*Why was this decision made? Who made it? What was the rationale?*

the required temperature and the time required for heating are checked by the process control system and the values are coordinated together. However, there were no special automated control circuits for the heating phase after a catalyst has been replaced, which was the phase in which the problems arose. Even for procedures that were known to be difficult to manage (such as heating) or required “intense attention” by the operators, no assistance was provided. The accident report does not provide any reason why the process control system was configured only for a normal production phase.	
After a Unit stops, in the pit stop period, most of the controls are set on manual. This decision was justified as giving the Panel Operator more flexibility. However, because the filling, circulating, and heating phases during the preparatory phase for reducing are not included in the design, this flexibility can be dangerous and lead to operator errors.	*Who made the decision? With what rationale? What analysis and review was done to justify this decision?*
The temperature in the reactors is measured using temperature elements that do not allow the temperature throughout the volume of the reactor to be measured. As a result, measurements may be delayed and/or areas in the reactor may be hotter/colder than temperatures registered by the temperature element. The aim of circulating is therefore to ensure that the catalyst bed is wetted and heated homogeneously. The different temperature controls were sometimes operated manually by the Panel Operator and sometimes automatically by the system. This design also meant the Panel Operator had to be extremely attentive.	*Because there are two possible controllers, is there potential for confusion over who is actually in control at any particular time?*

UCA: There was no automatic reset after two high-high level alarms so the gas discharge system remained closed.

Why? (Factors Affecting the Unsafe Control)	Questions Raised
There were two high-high level alerts that night. The PLC (Programmable Logic Controller) is supposed to intervene after such an alert. When the PLC intervenes, the relevant process installation is shut down entirely or partially or steps are taken to ensure a safe condition. The PLC intervened with a reset after the first high-high level alert that night. There was no reset in the second instance, however, and the gas discharge system (the flare installation) remained closed, which made it possible for pressure to build up to a dangerous level. The accident report says that “it is unclear to the Safety Board why there was no actual reset after the second high-high level alarm.” Not having any additional information, I cannot speculate about why. But given that the engineers could find no physical reason, the software needs to be examined closely.	

UCA: The process control system did not step in to stop the process when pressure and temperature increased precipitously.

Why? (Factors Affecting the Unsafe Control)	Questions Raised
A safety margin was built into the collapse pressure, which is at least 3 times higher than the design pressure. The vessel was actually able to withstand an even higher pressure. None of this prevented the pressure from the chemical reaction from exceeding the collapse pressure of the two affected vessels. But the incorrect designed safety margin may have created complacency in the Process Control system designers and reduced the need in their minds to provide ways to stop rapidly increasing temperature and pressure. They appear to have assumed that such a pressure/temperature increase was not possible.	
The designers did not anticipate a scenario whereby a fast and high pressure build-up was possible. This assumption affected the configuration of the instrumentation safety devices. For example, it was estimated that any pressure/temperature build-up (a few bar and a maximum temperature of approximately 74 ° C) due to a runaway would not actually be high enough to reach the pre-set pressure on the pressure relief valve and to operate this valve. The programmed Emergency Depressuring System (EDP) was therefore configured in such a way that during an unwanted pressure build-up, the pressure in Unit 4800 would be relieved within a half hour. During this pressure relief, the pressure in the Unit would drop to 50% of the design pressure. The Panel Operator also had to activate this instrument-based pressure relief manually. On 3 June 2014, this instrument-based pressure relief was not activated. According to the accident report, if the Panel Operator had activated this valve, it would most likely not have made any difference, however, in terms of the explosion.	*I am not completely sure why activating the valve would have made no difference, but it is probably because the very high rate of the pressure build-up did not provide enough time between exceeding the set point and the explosion for the EDP to work.*
The installed independent pressure relief valves were specifically intended to accommodate the pressure that could build up if the hydrogen feed valve did not open. In that case, the pressure in the hydrogen system could cause a pressure build-up in the Unit 4800. The blow-off capacity of this pressure relief was insufficient to provide for the scenario that occurred that night.	
In a previous incident at another Shell plant (Nanhai) with the same design, a runaway was observed that resulted in a temperature many hundreds of degrees Celsius higher as well as a higher pressure than was previously estimated. Nobody felt this was a reason to reconsider the runaway scenario and the associated instrument-based safety devices (see higher level system control and design components).	

UCA: There was no emergency stop button for Unit 4800.

Why? (Factors Affecting the Unsafe Control)	Questions Raised

Without an emergency stop, there was way to safely stop operation of the Unit 4800 quickly with a single press of a button.	*I could not find a reason in the accident report for the omission of an emergency stop button for Unit 4800. Was this complacency, cost, or an engineering reason? Emergency stop buttons are standard for safety-critical systems.*
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?*
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 it impossible to design one that can be operated remotely?*

Summary of the Role of the Process Control System in the Accident: The process control system was not configured 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.

Recommendations: The operators' knowledge and skill is 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 to provide all necessary assistance to the operators in decision making and taking action and to reduce attention and time pressures (see the next Section).

1.6 Operators (including Control Panel Operator and Production Team Leader)

The operators' actions 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 accident causal analyses and accident reports stop and the operators are blamed for the accident. 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.

To understand the operators' actions, a time line of relevant actions is useful.

20:15	Panel operator started circulating ethylbenzene through the Unit.
20.56	When the ethylbenzene flow through the Unit had been stable for approximately 45 minutes, the Panel Operator decided to begin heating the Unit
21:00	Ethylbenzene flow to Reactor 2 starts to be unstable. Operator notices temperature increasing too slowly
21.28	Operator increases heating
22:16	Gas discharge system shuts off automatically. Fluctuations had occurred from start-up (20:15) to the occurrence of this safety device actuation.
------	Increasing pressure
22:48	Temperature alarm sounds
22:48:26	Explosions

Process Model Flaws: Operator decisions are based on their mental model of the state of the controlled system (in this case, the reactor) and its expected behavior. Mental models are created by past experience in operating the process, by training, and by feedback about the current state of the controlled process. At least a partial understanding of why the operators acted the way they did is gained by looking at their mental models at the time of their unsafe control actions.

Contextual Factors: Human behavior is always affected by the context in which it occurs. To understand why a person behaved the way they did, it is necessary to identify the contextual factors that affected their behavior.

Relevant Safety-Related Responsibilities:

General:

- Operate the plant 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.

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).

Unsafe Control Actions

The following are contextual factors affecting all the unsafe control actions:

Why? (Context)	Questions Raised
Safety during the heating and wetting of the reactors was dependent on the knowledge and skill of the Panel Operator and the Production Team Leader on duty. Shell Moerdijk's safety report (dated 2000) stated that the starting and stopping of the plants had to be undertaken by experienced operators using the work instructions that are present for this purpose. The Operator and Production Team Leader performing this maintenance stop were experienced staff on Unit 4800, and were educated and trained for working at the MSPO2 plant during regular production. However, only once every three to four years is Unit 4800 started up after a catalyst change. This was the first time that the Panel Operator and Production Team Leader had experienced a startup of Unit 4800 after a catalyst change. Therefore, in this incident, both the Panel Operator and Production Team Leader involved were lacking the specific experience required to safely start up Unit 4800.	*Why were they assigned to this task? Given that the safety of the startup was known to be dependent on the knowledge and experience of the operators (as stated in the 2000 Safety Report), who made the decision to let operators inexperienced in a reactor start-up control the start-up? More important than who is "why" This question is not answered in the report. Were they the only ones available or the most experienced available or was the person making the decision unaware of the safety report requirements or unaware of the experience levels of the operators assigned or …? The answers to these questions will help to formulate effective recommendations for changes to prevent future accidents.*
Without the appropriate knowledge and experience needed to adjust gas and liquid flows during startup, support from the process control system was needed. However, the process control system was configured for production, not start-up, and therefore did not provide the assistance they needed. The accident report says "It was assumed that the Operators and the Production Team Leader could manage and control the start-up manually based on their knowledge and experience." Adjusting gas and liquid flows was also difficult because of the Unit 4800 design having a single central pump. Because the central pump has considerable pump capacity compared to the capacity of the separation vessels, work has to performed with the shut-offs and valves almost closed, which had a negative impact on stability of the gas and liquid flows during circulation and filling. 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.	*Who made this assumption? On what was it based?*
The accident report says that Shell (*who in Shell?*) stated 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 (see	*It is unclear from the report whether the operators who produced the work instructions were those performing the start-up during the accident or this task was done by other operators. If it was other operators, did they have the*

Section 1.7). The operators produced the work instructions.	*experience and knowledge to create the work instructions? Who reviews these work instructions? Were they reviewed by anyone? Why are operators writing their own work instructions?*
After a Unit stops, in the pit stop period, most of the controls are set on manual. This is justified as giving the Panel Operator more flexibility. However, because the filling, circulating, and heating phases during the preparatory phase for reducing are not included in the design, this flexibility can be dangerous and lead to operator errors. • In an automatic control circuit, the control system regulates and checks that the set value is achieved and stabilized, without further interference from an operator. For example, at a set heating rate, both the required temperature and the time required for heating are checked by the process control system and the values are coordinated together. Without such an automated control system, manual control by the Panel Operator and the Production Team Leader was required during the wetting and heating of the reactors. The manual filling, circulating, and heating phases require a great deal of focus, precision, and experience on the part of the Panel Operator. • The accident report says that “The controls to be used for filling, circulation, and heating are linked by software (in the process control system), such that the temperature control of the liquid flows has an impact on their volumes. In addition, the level measurement of the separation vessel of reactor 1 is linked to the liquid flow to reactor 2. Moreover, the pipes for the ethylbenzene flows to the reactors are interconnected, as a result of which they can have a negative influence on each other. Coordinating the different flows with each other is necessary in order to prevent oscillations (swings) in the control system. This coordination activity is mentally challenging and requires intense operator attention and deep understanding of the process dynamics.”	*The accident report does not provide any reason why the process control system was configured only for a normal production phase. Why did the process control system designers make this decision? Was the major concern and goal for the process control system to optimize productivity while safety was not a high priority? Was there a lack of resources? Was there a human factors oriented hazard analysis done that considered the risks involved in operators controlling a critical process requiring focus and precision without automated assistance?* *Computers can perform much more complex control procedures than can be performed manually by a human. Indeed, this is one reason that computers are used. But manual control of such systems may be very error prone. Was any human factors analysis done when a decision was made to have the operators manually control start-up to ensure that they were capable of doing this reliably? The accident report notes many actions by the operator that required intense attention.* *Were the reactions out of view because of the lack of sensors and*

• The report says that “Reactions caused by warming up actions were out of view of panel operator and the production team leader.” There is no further explanation.	*feedback? Or was it not on the main screen and had to be called up specially? If the problem was not simply a matter of a lack of sensor feedback because there were not enough sensors, then a human factors analysis of the interface with which the operators were interacting is required to understand the impact of this contextual factor on the operators’ behavior. Was any human factors analysis done on the control interface, either before or after the accident? Nothing is noted in the accident report.*

<u>Specific Unsafe Control Actions</u>:

UCA: The operators did not stabilize or halt process before the explosion when critical process boundaries were exceeded.

Why? (Context)	Questions Raised
The accident report says that the fundamental principle in the training is that, among other things, if pre-set limits are exceeded, the situation is abnormal. In an abnormal situation, an operator must “Stabilize, Slowdown, and Stop” the process.	
Shell Moerdijk has an “Ensure Safe Production” (ESP) policy that, given the limitations of the safety procedures and work instructions, gives the staff a degree of professional freedom to intervene on the basis of their knowledge and experience. The ESP training provides insights that give operators points of reference for interpreting this professional freedom. The main purpose of ESP is to ensure that operational limits are known and that operators always operate within those limits. Operators take part in training courses every three years, where a fundamental principle is taught that if pre-set limits are exceeded, the situation is abnormal and the operators must stabilize, slowdown, or stop the process. In ESP, in the event that process limits and non-controlled process conditions are exceeded (such as considerably fluctuating levels in the separation vessels, heating rate nitrogen and ethylbenzene input flows and pressure differences), the Panel Operator can decide either independently or in consultation with the Production Team Leader, to slow down an ongoing process and, ultimately, to even stop it. A decision to stop a process requires knowing that critical conditions have been exceeded. Critical process boundaries were not included in the work instructions or, in some cases, what was included was	*Did these operators take the ESP training?* *Is plant start-up included in this training?* *What are the contextual pressures on the operators with respect to a decision to slow down or stop a process?*

incorrect. The accident report says that important information was lost between the unit designers and the ultimate managers (and the operators) of the unit. The operators (like everyone else) accordingly treated the heating phase as a non-hazardous process step and, therefore, did not identify any critical process conditions for the work instructions. Risk control procedures provide for the possibility to waive the obligation to intervene in special situations, such as a startup phase, on condition that the non-intervention will not result in a potentially unsafe situation. In order to be able to assess whether an unsafe situation could result, the operator(s) needs to have a full understanding of the cause of and reasons for operating outside the limits. The ability to make such an assessment and knowing when to intervene requires knowledge of, experience with, and thorough preparation for such special situations. The operators did not have this knowledge or expertise. As will be seen, even the corporate safety engineers did not know that the conditions that occurred here could result in an unsafe state. The Panel Operator and Production Team Leader did not realize that the situation was dangerous and therefore did not decide to intervene in accordance with ESP policy. They did not have a comprehensive view of all the signs they were getting. They interpreted the signs as though they resulted from the setting and stabilization of the circulation flow and normal system dynamics. They did not have a comprehensive view of the consequences of their actions in relation to the combination of high-pressure alarms, the liquid level alarm in the separation vessels, low ethylbenzene flows, and a high pressure differential. In exceptional cases, for instance during start-up or shut-down, several critical limits or standard levels remain in the alarm mode for some time. The ESP approach does not dictate any immediate changes when this occurs, unless some danger could arise. The Operator must fully grasp what caused the Unit to exceed the limits in order to assess this risk. Such situations, which form an exception within the ESP approach (i.e., immediate intervention in case of alarm is not required), place more stringent requirements on the preparation, instructions, and experience of the Operators on duty. They must fully understand the process and be provided with the information necessary to make this decision.[7]	

[7] Many companies have policies that require operators to intervene when something goes wrong but do not specify specific conditions under which to do this or do not provide the information necessary to make this decision. Such policies are used to place blame on the operators after an accident but do little to improve safety.

The process control system did not have an emergency stop button. Operators were only able to respond to specific conditions using the instrument-based safety devices. While there is no emergency stop button for Unit 4800, the Operator does has the option to shut down the Unit 4800 partially or completely via the ESD trip switch, which is independent from the automatic trips (instrument-based safety devices). The automatic trip did not occur (see Section 1.5 for why) and the manual ESD trip switches were not used that night. There is no explanation that I could find in the accident report about why they were not used although one can guess.	*If the designers did not believe such a scenario was possible, why would the operators? In fact, as will be seen, nobody at Shell thought it was possible.*
The designers did not envision a scenario whereby a fast and high pressure build-up was possible. If the designers did not believe such a scenario existed, why would the operators? In fact, as will be seen, nobody at Shell thought such a scenario was possible.	

UCA: The operators did not manually activate the instrument-based (automated) pressure relief valve.

Why? (Context)	Questions Raised
Pressure rose sharply within the space of two minutes. At about 22:47, the pressure rose from 7 bar (normal) to more than the collapse pressure of the reactors, which the report says was at least 93 bar. Alarms indicating the temperature in the reactors had exceeded the set alarm limits sounded 23 seconds before the explosion. 20 seconds later, a second explosion occurred when reactor 2's separation vessel collapsed.	*Did they expect the automated system to react?* *In human factors, it is known that people cannot be expected to react immediately when confronted by unusual information. They will first try to figure out what is going on first. If there is no time for the operators to do this, then the shutdown should be automatic.*
The operators considered fluctuations in pressure to be normal during restarts (process model flaw). Such fluctuations had occurred during previous restarts and that was what they expected. The pressure had fluctuated continually since the beginning of the start-up.	

UCA: 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.

Why? (Context)	Questions Raised
The accident report says that to achieve proper wetting, the circulation of ethylbenzene must continue for at least 6 hours before hydrogen can be used. However, given the assumption that ethylbenzene does not react with the catalyst, it is possible to start heating earlier. Everyone, including the unit designers, believed the assumption that ethylbenzene does not react with the catalyst.	
The instruction about waiting 6 hours was not included in the work instructions.	

UCA: The operators manually added additional warmth to the ethylbenzene at a time when heat was increasing precipitously.

Why? (Context)	Questions Raised
Shell Projects and Technology design data specified that heating had to be performed at 30°C per hour. The Panel Operator, Production Team Leader, and Process Engineer agreed on a rate of 50°C per hour. At 21:00, the Panel Operator observed that the temperature in the Unit was rising too slowly. At 21:30, he intervened by applying more heat to the ethylbenzene. The temperature then rose so fast that the ultimate heating rate was greater than the agreed upon rate. While the design data stated that heating had to be performed at 30° C per hour, this requirement was not recorded in the work instructions for the heating phase. Not being told about the requirement, the Panel Operator, Production Team Leader, and Process Engineer agreed on the rate of 50°C per hour.	
The Panel Operator did not intervene when the temperature rose so fast that the heating rate was greater than the agreed upon rate. The reason given in the accident report is that the Panel Operator was not concerned by the temperature developing in this way. It was not expected to create any problems for the unit.	
The agreed upon rate of 50° C was neither controlled automatically nor was it monitored by the system. To achieve the required heating rate, the Panel Operator had to continually adjust the temperature of the ethylbenzene manually. This task was complex.	
The operators thought the reactors were not warming up fast enough (a process model flaw) so they increased the heat. Measurement data on the panel's screens showed fluctuations	*A human factors analysis is required here, but the graphs shown in the accident report (a mapping of temperatures over time) appear difficult for*

when the warming-up procedure started. Temperatures were shown but not the rate of the increase in the temperature.	*an operator to determine the actual rate of increase. There was a lot of instability in the graphs, which the operators expected from previous start-ups.*
Controlling steam supply to the heat exchanger requires a degree of attentiveness on the part of the operators. It makes a difference whether the steam valve can be fully opened (low-pressure steam) or whether it can only be opened partly, to create the same conditions (medium-pressure steam). Furthermore, it is unclear what heat energy is supplied in the latter case. This is evident the second time that the steam valve was opened further: at this point much more heat energy was supplied.	*Several things seem to require a lot of attentiveness on the part of the operators. What kind of human factors job analysis was done on the total start-up requirements?*
The temperature in the reactors is measured using temperature elements that do not allow the temperature throughout the volume of the reactor to be measured. As a result, measurements may be delayed and areas in the reactor may be hotter/colder than temperatures registered by the temperature elements. The aim of circulating is therefore to ensure that the catalyst bed is wetted and heated homogeneously. The different temperature controls were sometimes operated manually by the Panel Operator and sometimes automatically by the system. This method also meant the Panel Operator had to be extremely attentive.	*Was confusion created in the mind of the operator by having the automation operate the temperature controls at the same time as the operator was doing this?*

UCA: The operators did not notice and respond to hot spots. They also did not notice and respond to the related negative pressure differential [8]

Why? (Context)	Questions Raised
Hotspots are not automatically detected due to the limited number of temperature sensors in the reactors. Without appropriate feedback from such sensors, the Panel Operator often does not notice the development of hotspots, as was the situation in this case.	*Why are there a limited number of temperature sensors in the reactors? Is this a physical limitation or a design choice based on some rationale?*
Because the pressure in the reactor exceeded the pressure of the nitrogen flow to the reactor, the nitrogen flow came to a standstill. This	*Why did the operator not notice this? There are so many reasons*

[8] Normally the difference in pressure between the top and the bottom of the catalyst bed is low (20-50 millibar). The accident report says that a significantly higher pressure difference (positive or negative) or a sudden change in the pressure difference can be indicative of contamination or blockage or other malfunctions that can have a negative impact on the effect of the catalyst.

resulted in a negative pressure difference that was not noticed by the Operator. The supplier of the catalyst recommended that the pressure difference be kept low across the reactors.	*that it is difficult to speculate about the answer to this question.* *Was this in the work instructions?*

UCA: The operators did not properly adjust nitrogen flow. The lower (than required) nitrogen flow was one of the causes of the accident.

Why? (Context)	Questions Raised
When the distribution plate was designed, it was calculated that a nitrogen flow of 475 kilograms per hour was required to enable adequate wetting. However, Shell Moerdijk engineers assumed that, in principle, the Operators needed to be able to adjust the nitrogen flow during the heating phases at their own discretion in order to be able to adjust other processes. The nitrogen flow was not considered critical and was not included in the work instructions.	

UCA: The operators did not respond to alarms.

.

Why? (Context)	Questions Raised
For the duration of the Panel Operator's shift, alarms occurred regularly, including the liquid level alarm in the separation vessel.	*Was there alarm overload? Was there a distinction between a critical alarm and a non-critical one?*
The conditions under which the alarms occurred were all consistent with the expectations of the Panel Operator and the Production Team Leader for this heating phase. Previous maintenance stops had shown that, in the manual control mode, the gas and liquid flows as well as the liquid levels were sometimes unstable. Therefore the instability and deviations that occurred were in line with the operators' expectations.	
The liquid level was regularly above the set limit and in the "abnormal" process zone. The unit was in a start-up phase and a stable situation had not yet been reached. In this situation, the number of alarms and the frequency thereof were not out of the ordinary.	

Despite the previous experience showing that liquid levels and liquid flows were difficult to stabilize manually, no automated assistance was provided.	

UCA: The Panel Operator did not reopen the connection to the gas discharge system after the liquid level in the Reactor 2 separation vessel rose so high that the connection to the gas charge system was closed (by an automated safety device) to prevent liquids from entering the flare tower.[9]

Why? (Context)	Questions Raised
No explanation is provided in the report as to why nobody noticed that the gas discharge system was left closed after this protection system automatically was triggered. It had triggered earlier in the start-up and had been manually reopened. Twenty three seconds before the reactor collapsed due to overpressure was the first time the Panel Operator noticed that alarm signals indicating that the pressure in the gas discharge system was too high.	*Why did nobody notice this time but they had earlier? What kind of indication is there that the safety device had triggered? The report shows a message that is provided (in a long string of messages) but there is no indication as to whether there is an audible alarm or whether attention might have been directed elsewhere at the time. To determine why the operator did not respond, it is necessary to look at the design of the interface, the other activities the operator was performing, and the potential for distraction. We know that the operators were very busy. Detailed information about the control room interface design was not included in the accident report. Again, a human factors analysis would be helpful here.*

<u>Summary of the Role of the Operators in the Accident</u>: The operators 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, while 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.

The designers of the plant did not recognize the risks (see the later sections of this analysis) so the risks might not have been communicated thoroughly. 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 result in providing adequate assistance to the operators to carry out their responsibilities.

[9] The gas discharge system is that part of the plant that discharges excess gases from the separation vessels via a safety valve and burns them. The purpose of the automatic closure of the gas discharge system is to prevent flammable liquids from being supplied to the flare (a hazard)

Recommendations: The operators must have the appropriate skills and expertise to perform their assigned activities, and there must be someone overseeing operations assigned the responsibility for enforcing this requirement. A human factors study during the job analysis is needed 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 should be provided in all phases of operation, training should be provided for activities that are known to be hazardous like startup, and work instructions as well as the process for producing them need to be improved.

1.7 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.

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.*]

Unsafe Control Actions

UCA: Created work instructions that were unsafe or did not adequately review the work instructions that were created and used. [This CAST analysis, in the absence of detailed information about the safety management system at Shell Moerdijk and Shell Global, assumes that performing job analyses and creating safe work instructions was the responsibility of Plant Operations Management (Section 1.7), but any reasonable safety management system would assign responsibility to safety management for reviewing these work instructions to ensure they adequately controlled safety.]

Why? (Context)	Questions Raised
The operators created the work instructions, using a job analysis and instructions from previous maintenance stops.	*What kind of review was performed on the work instructions the operators created?*
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.	*The omission of required parts of the work instructions should have been easily identified in any review. Was a review not done? Was it standard*

	practice to omit required information?

UCA: Did not identify and manage potential risks resulting from changes made to the plant, the catalyst, the processes, and the procedures. Did not reassess risks when changes were made. [*It is not clear from the report whether some of these changes were made by Shell Projects and Technology or Shell Moerdijk. I am assuming most were made by Shell Moerdijk.*]

Why? (Context)	Questions Raised
Accidents often occur after changes, both planned and unplanned. In a chemical plant, the process of starting up after a maintenance stop is particularly hazardous. Nobody seemed to be aware of the risks involved in this start-up.	
Dutch Government regulations require that petrochemical plants in the Netherlands have a safety management system with appropriate procedures for dealing with changes and those procedures must be applied consistently. Shell Moerdijk has such a procedure, the goal of which is to ensure that changes to plants, procedures, or organizations are only made once it is clear what will change, the risks of this change are known, the change has been assessed and approved, and the change has then been recorded. These goals were not achieved for changes that occurred in the Shell Moerdijk MSPO2.	*The details of the Shell Moerdijk Management of Change process are not included in the public accident report. The goals listed (from the report) do not specify that the changes must be safe, only that the risks are known and approved. Is this simply an omission from the accident report?*

- **Catalyst change**: A new catalyst was selected for the reactor and tested between 1999 and 2000 [*Was this done by Shell Moerdijk or by Shell Projects and Technology? This analysis is assuming Shell Moerdijk. Otherwise, just move this unsafe control action upward in the control structure.]* Using a new catalyst led to a higher risk of a reaction occurring with ethylbenzene, but this higher risk was not recognized.

Why? (Context)	Questions Raised
During the 1999-2000 tests, the conditions during start-up were not considered, and the conditions that were considered deviated greatly from the plant conditions. In addition, the tests focused mainly on assessing the normal production phase, not start-up.	
In 2011, the manufacturer of the selected new catalyst implemented changes in its production process, resulting in the catalyst containing considerably more hexavalent Chromium compounds. The changes were contained in a Safety Information Sheet provided by the manufacturer, but they did not explicit report this change. Safety engineering did not identify the increased potential for a chemical reaction between ethylbenzene and the new catalyst.	
In 2014, Shell Moerdijk performed a risk screening for the new catalyst in the MSP02 plant. In this risk screening, Shell Moerdijk	

assumed that the properties of the new catalyst were the same as those of the previous catalyst. The report says that "The persons performing this risk screening reached this conclusion [of low or no risk] based on their knowledge and experience." It is not clear what this means. The company did not carry out any laboratory tests for the new catalyst, and the methodology used in the risk screening was not appropriate for testing complex substances, such as a catalyst. The altered composition of the new catalyst was stated in the safety information sheet provided with the product, but safety engineering at Shell Moerdijk (and/or Shell Projects and Engineering?) did not notice this change.	

- **Procedure changes** (heating rate, nitrogen flow) were instituted without a risk assessment.

Why? (Context)	Questions Raised
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. These changes were not assessed for new risks in accordance with the Shell Management of Change (MOC) procedure.	*Why were the MOC procedures not followed? Why did management not know they were not being followed?*
Some of the changes that were not assessed for safety in Unit 4800 were those implicated in the accident, such as heating rate and nitrogen flow.	

- **MSP02 plant and production changes** were not systematically examined for their safety effects and replacements were not systematically examined on the basis of a risk analysis in all cases.

Why? (Context)	Questions Raised
Unknown. There are, of course, a lot of potential reasons. Improvement in practices requires identifying these reasons.	*Why were the MOC procedures not followed and changes not systematically examined on the basis of a risk assessment?*

UCA: Shell Moerdijk did not identify the risks involved in opting for a trickle-bed reactor and its associated design choices. In particular, the risk of a reaction between ethylbenzene and the catalyst was not identified as well as other risks associated with Unit 4800.

Why? (Context)	Questions Raised
The methodology used in the relevant safety studies was not always appropriate or applied correctly. There were three types of studies done and reports produced in the period between the design of the MSPO2 plant and 2011: a Desk Safety Review (1997), an Integrated Safety Report (2000), and a Reactive Hazard Assessment (2011).	

Desk Safety Review (1997): For new designs, the Shell subsidiary selects the most appropriate risk evaluation method, based on an "initial assessment" of Shell Projects and Technology. The relevant division then selects the method. The division may choose a different method, provided it substantiates its deviation from the Shell norm. Among other things, this Desk Safety Review examined various failure scenarios for Unit 4800. However, it only looked at failure scenarios for the production and reduction phases, not for the heating phase (which was when the accident occurred). There were never *any* safety studies that specifically focused on the circulation and heating of Unit 4800 in the MSPO2 plant because it was considered to be low risk. Studies done in 1977 had shown that the catalyst (as it existed then) was inert in the presence of ethylbenzene. This assumption was never reassessed even though the composition of the catalyst changed over time and incidents occurred within Shell reactors that should have prompted a re-examination of that assumption (see below). Accordingly, ethylbenzene explosion was not included in the quantitative risk analysis of the Desk Safety Review because they considered it highly unlikely although they were aware that the impact would be huge.	*Shell Moerdijk licensed the trickle-bed reactor design from Shell Projects and Technology. Were the risks identified there and communicated to Shell Moerdijk? What kind of initial assessment was done by Shell Projects and Technology?*
Integrated Safety Report (2000): An Integrated Safety Report was required for companies with major risks by European Legislation (Seveso II Directive) and its implementation in the Netherlands by Brzo legislation (see Section 1.11.1). The Integrated Safety Report describes both internal and external safety, covering environmental requirements and the requirements of the fire brigade, in addition to those related to working conditions. The Integrated Safety Report only describes (in summary) "the biggest" risks in the form of event scenarios. The safety report must include plant scenarios for each plant, such as the MSPO2 plant. In order to prepare these plant scenarios, safety engineers at Shell Moerdijk used HEMP (Hazard and Effect Management)[10] for each plant and for each containment system (such as Unit 4800). Unit 4800 was considered low risk. Other containment systems[11] were	*Why HEMP? The techniques involved (like Bow Tie) are 50 years old and the underlying accident that assumes accidents are caused by chains of failure events is*

[10] The Hazards and Effects Management Process (HEMP) is an analysis technique that reviews identified hazards and uses a Risk Assessment Matrix to rank the risks based on consequence and likelihood. The hazards and identified risk rankings of high, medium or low are documented in a Hazard Register. The hazards identified as being high risk are modeled using the bow ties. Bow tie models combine a fault tree analysis with an event tree analysis. While the name "HEMP" is relatively new, the techniques involved are at least 50 years old.

[11] A containment system consists of one or more appliances in which the components are permanently in open connection with each other and is intended to contain one or more substances which, in the event of an

higher risk and were therefore included. There is no mention of an ethylbenzene-related explosion in this Safety Report. Dozens of quantitative risk analyses were conducted for MSPO2, but Unit 4800 was not included.	*not true for today's more complex systems and new technology.*
In principle, the Integrated Safety Report could have subjected thousands of scenarios to a risk assessment, but Shell Moerdijk only analyzed 10 scenarios as required by the law.[12] As with the Desk Safety Review, none of these scenarios included Ethylbenzene, Unit 4800, or a reactor explosion: Again, although the impact would be huge, the likelihood was considered to be very low.	*How were the 10 scenarios determined to be the biggest risks?*
Examining only a few scenarios out of potentially thousands cannot provide much evidence for safety and can lead to a perfunctory and useless exercise performed on the risks that are already well understood and controlled and thus unlikely to lead to an accident. By definition, accidents occur when the assumptions underlying the design and the safety analysis about the risks involved are wrong. In this case, there was strong evidence that the assumptions about Ethylbenzene being low risk had been invalidated at other Shell plants. However, the report says that engineers and managers at Shell Moerdijk considered an ethylbenzene-related explosion in Unit 4800 to be literally unimaginable. This belief was confirmed in interviews by the accident investigators. Ethylbenzene had been determined to be a safe substance under all conditions since 1977 and nobody had investigated nor questioned the validity of this belief since that time.	
The Integrated Safety Report included a requirement that only experienced operators were to start up and shut down the plants, using the work instructions provided for this purpose. Either "experienced" was not defined appropriately or Shell Moerdijk management did not enforce this rule. And the work instructions were incorrect and unsafe.	*How was this requirement enforced?*
The accident report says that because Unit 4800 was no longer included in the risks analyses from 2001 onward, safety management thought the Unit was relatively safe. This impression was not disputed either internally or externally.	

(imminent) major accident, can be closed in a short period of time. Unit 4800 is a containment system; MSPO2 is a plant that is constructed from a number of containment systems.

[12] The law requires companies to prepare 10 scenarios per plant (such as MSPO2). For these scenarios, the company must select the hazards with the greatest risks and the nature of the risks must be varied.

A Reactive Hazard Assessment[13] was performed by safety engineering at Shell Moerdijk from 2010-2011 that included Unit 4800. Attention, however, was focused on other processes that were considered higher risk, and process conditions in the reactor were not considered. The assessment was primarily focused on assessing the effects of substances on the environment and not on safety. Unit 4800 was included, but most of the attention was on other processes in the MSPO2 plant that were considered higher risk. The process conditions in the reactor were not taken into account. In addition, Reactive Hazard Assessment is not appropriate for testing complex substances, such as a catalyst. To use it for these substances, assumptions have to be made, which resulted in regarding ethylbenzene only as a flammable substance with no consideration that it could react with substances present during start-up. No laboratory testing was performed, and the question about whether ethylbenzene can react with the catalyst was not raised in the study. Shell Moerdijk guidelines require the use of all relevant information sources to conduct this study, and current data about the catalyst, the Safety Information Sheet, and specialist literature (such as a chemical hazards handbook) were used. The accident report says that the question of whether ethylbenzene can react with the catalyst was not raised in the study, despite mention in the Safety Information Sheet that ethylbenzene reacts strongly with oxygen, which is in the catalyst. The specialist literature used in the study also included known reactions between numerous hydrocarbons and the chrome oxide contained in the catalyst. The long-standing belief that ethylbenzene was inert in the presence of this catalyst blinded the analysts to any evidence that it might not be.	

UCA: Did not establish appropriate indicators of process safety.

Why? (Context)	Questions Raised
At Shell Moerdijk, as is true for many chemical plants and companies, number of leaks (a sign of loss of primary containment) is used as the most important indicator of process safety. The number of leaks has been greatly reduced in recent years, from which decision makers assumed safety was increasing. The resulting complacency may have contributed to the inadequate responses to signs and signals about the	*Is this the only indicator that they use? What else do they use to provide an estimate of process safety and update*

[13] A reactive hazard assessment is described in the accident report as an analysis approach derived from an Environmental Protection Agency method. It is intended for identifying the effects of substances on the environment.

risk of a runaway reaction and their exclusion of an ethylbenzene-related explosion in the hazard analyses and risk assessments.	*their mental model of current risk?*

UCA: Inadequate learning from incidents: After accidents in similar plants around the world, relevant signs and conditions involved in these events were not incorporated into new risk analyses or procedures (including work instructions) for MSPO2.

Why? (Context)	Questions Raised
In a previous incident at another Shell plant (Nanhai in 2010) with the same design as MSPO2, a runaway was observed during the heating phase that resulted in a temperature many hundreds of degrees Celsius higher than the design temperature of the Moerdijk reactors as well as a higher pressure than was previously estimated. This event did not trigger a response in terms reassessing risk or procedures or the assumptions that such a runaway was impossible. In the Nanhai events, as in the Shell Moerdijk accident, the gas discharge system was closed, thus stopping the flow of nitrogen. No explosion resulted at Nanhai because of special factors: • The central pump failed, and as a result ethylbenzene was no longer able to flow out of the reactors and could collect in the separation vessels. • The gas discharge system to the flare was opened early enough to prevent a dangerous build-up of pressure • The ability to feed nitrogen into both reactors made it possible to mitigate the high temperature • Heating was only started after six hours of circulation, to help ensure adequate wetting. This information could have been used to make improvements in design, operator training and work instructions at Shell Moerdijk. The operators thought that the problem was caused by ethylbenzene, but the Shell incident investigation concluded that the runaway was caused by a hydrogen leak, with the main recommendation related to modifying the hydrogen system. The fact that the temperature increased way beyond the supposed maximum did not prompt further analysis of the risks nor did it lead Shell to explore the possibility of a reaction between ethylbenzene and the new catalyst. One of the recommendations after the Nanhai incident was to assess the use of a single central pump. The accident report says that based on the safety studies during 2010-2011, it does not appear that this assessment was actually done. The single central pump in Unit 4800 was a factor in the accident.	*What type of Safety Information System does Shell Global and Shell Moerdijk (which I assume is a subset of the global information system) have? How is information about related incidents at Shell plants around the world disseminated? Are there procedures to retrieve this information and triggers to distribute it to those who could use it? Is there assigned responsibility for doing these things? Did the Shell Moerdijk safety managers know about the Nanhai incident or did they choose to ignore it?* *Why didn't these events lead someone to question their assumptions about ethylbenzene and the catalyst?*
One month after the initial 1999 start-up at Moerdijk, Shell restarted the MSPO2 plant using hydrogen. Hydrogen was introduced too	*Again, why did these events not lead to further*

rapidly and in excessive quantities during normal operation, triggering a reaction. This runaway was investigated by Shell Projects and Technology and resulted in additional temperature safety devices being installed. Shell continued to assert that a runaway could not take place in these reactors. The fact that a runaway had occurred during the start-up did not prompt further analysis or a review of these assumptions.	*analysis or questioning of the assumptions? What is wrong with the risk management process or the safety culture that even having something occur similarly in the past did not get past their risk assessment blinders?*

Process Model Flaws

- 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.
- 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.

Summary of the Role of Shell Moerdijk Safety Management 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 with the minimum required by the Dutch regulators. 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 MOC procedures were not followed or implemented effectively. Risks resulting from changes made to the plant, the catalyst, the processes, and the procedures were not identified and managed.
- Number of leaks was used as the primary leading indicator of process safety. This practice is common in the petrochemical industry.
- Lessons from similar incidents at Nanhai and at Shell Moerdijk were not used to reduce risk.
- They did not provide proper oversight of the generation of work instruction, which allowed unsafe work instructions to be provided to the operators.

Recommendations:

While the problems specific to the explosions on 3 June 2014 should be fixed, there was a lot of weaknesses in the Shell Moerdijk safety management design and especially practices that were 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 HA 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 leading indicators of risk need to be established.
- Procedures for incorporating and using lessons learned need to be established or improved.

1.8 Operations Management

According to legislation called the Major Accidents Decree, Shell Moerdijk is responsible for taking all measures necessary to prevent major accidents.

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 making sure 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 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.

Unsafe Control Actions

UCA: Did not identify the flaws in the risk analyses performed or the procedures used for these risk analyses [*Why not? Was this a one-time flaw or did it happen continually?*

Why? (Context)	Questions Raised
The risk analyses satisfied the Dutch legal and regulatory requirements.	*Why was Shell Moerdijk management satisfied*

	with the minimum risk assessments and hazard analyses required by law? Did they think they were adequate?
The government regulators of Shell Moerdijk provided no indication that there were flaws in their risk assessment procedures or their safety management system (see Section 1.11.1)	
The hazard analyses and risk assessments used were standard in the petrochemical industry.	
Like everyone else, they thought that the start-up phase was low risk (process model flaw). The evidence from the two previous incidents (one at Shell Moerdijk) did not shake this belief.	

UCA: Did not enforce Shell Management of Change (MOC) procedures. Allowed work instructions to change over time and omit important required information necessary to safely operate the plant during a maintenance stop. Did not require new analyses by Safety Management when changes occurred that affected the prior analyses.

Why? (Context)	Questions Raised
Accidents often occur after changes, both planned and unplanned. This fact is well-known and, in fact, is the reason for the near-universal adoption of MOC policies. Nobody seemed to be aware of the risks involved in this start-up (process model flaw) or the need for special care to be taken, including the regulatory authorities.	
Modifications were made to the production process, including switching to a different catalyst, without retesting the assumptions of the past.	*Were the assumptions recorded? Were they aware of the indications that the assumptions were flawed?*
Over time, the understanding (process model) of the most appropriate procedures relating to Unit 4800 changed: A part of the procedure was not considered critical to safety, and it was no longer included in the amended work instructions. These changes were never assessed for new risks in accordance with the MOC procedure. While the actual reassessment is the responsibility of safety management, operations management is responsible for ensuring they are getting appropriate and correct information for decision making. Because work instructions are for each maintenance stop are created from the previous set used, it is not surprising that they may have changed and omitted information over time.	*Were the omissions in the work instructions deliberate, were they an attempt to simplify the operators' job, or were they simply the common unintentional changes that occur when instructions are modified starting from the previous instructions each time?*

UCA: Allowed work instructions to change over time and omit important required information needed to safely operate the plant during a maintenance stop.

Why? (Context)	Questions Raised
Over time, the understanding of the most appropriate procedures relating to Unit 4800 changed. A part of the procedure was not considered critical to safety, and it was not included (or was no longer included) in the amended work instructions. These changes were never assessed for new risks in accordance with the MOC procedure.	*Why were the changes not assessed for new risk? Simply an oversight? Another reason?*
The general work procedure, referred to as a job analysis (WOL), is drawn up by experienced panel operators in preparation for a maintenance stop. The job analysis contains all relevant processes and process conditions for the commissioning of the installation. The WOL for this maintenance stop was drawn up by panel operators of the relevant plant and approved by the staff of the Shell Projects and Technology process owner.	*What experience did the operators who did the job analysis have in start-up of the plant? Were they the same operators who performed the start-up in June 2014? Who at Shell Moerdijk reviews the WOL? Why are operators drawing up their own work instructions without at least some participation from engineering and safety management?*
The work instructions created for the maintenance stop in June 2014 were largely based on the 2011 job analysis, which in turn was based on the 2007 job analysis. Information from the Design Book[14] was not used because, the accident report says, was too detailed and "intricately presented" and was not understandable by the operators charged with drawing up the work instructions.	*If the operators could not understand the Design Book, why were they assigned the task of drawing up the work instructions? Was there no engineer(s) who could assist them in this task?*
Shell provides detailed instructions about how a job analysis should be done. These instructions are called the SMART 2 ((Specific, Measurable, Achievable, Relevant, Time-bound) Principles. Each task step must be defined in such a way that a controlled, safe situation exists after the task has been completed. Criteria for activities must be clearly recorded. The job analysis completed for the 2014 turnaround was not consistent with the SMART requirements.	*Who is responsible for ensuring that the SMART Principles are followed? Why was the obviously deficient job analysis (e.g., missing required information) approved?*
The job analysis did not contain all the important criteria for the activities such as heating rate and nitrogen flow. <u>Heating rate</u>: The Design book stated that heating had to be performed at 30°C per hour, but this was not recorded in the	*Why were the omissions not detected by whoever reviewed the work instructions either for this maintenance turnaround*

[14] The Design Book, created by Shell Projects and Technology, contains detailed information about the design and operation of the reactor.

work instructions. The operators during the start-up chose to at a rate of 50°C based on past experience. The Design Book heating rate had been removed from the work instructions over time. Nitrogen flow was ignored in the work instructions. A too low flow was one of the physical factors in the accident. Again, the requirements regarding nitrogen flow were removed during the periodic update of the procedures. The accident report states that the omission was done in an attempt to limit the content of the job analysis to information that was believed to be essential and to focus attention on what was thought to be the most important from a safety and operational point of view. The accident report states that there was an assumption that, in principle, the Operators needed to be able to adjust the nitrogen flow during the heating phases at their own discretion in order to be able to adjust other processes. The nitrogen flow was not considered critical and was not included in the work instructions. Central Pump: After the Nanhai incident in 2010, one of the recommendations was to reassess the design of a single central pump. According to the accident report, it does not appear that a reassessment was ever done (based on the safety studies performed during 2010-2011). In any event, there was still a single central pump in the MSPO2 in 2014. The turnaround of 2011 had demonstrated that circulating and heating were difficult to control. However, the difficulties experienced in the past were not included in the 2014 job analysis and clear instructions were not provided about how the filling and circulation was to be done. The only clear instruction was that the central pump was not allowed to run "dry." Otherwise, it would break.	*or for others in the past when they were originally removed? Who controls the updating process? There must have been someone beyond the operators who were actually doing the updating. What engineers were involved in this decision making?*

UCA: Made a decision to configure the process control system to control the plant during the normal production phase but not during non-production and high-risk operations.

Why? (Context)	Questions Raised
Like everyone else at Shell contributing to this accident, they thought that the start-up phase (including heating) was low risk and that the operators could handle it under manual control.	*Why did they not provide assistance from the process control system anyway? Was it a cost issue? Why was the specified standard procedure to put the process control system on "manual" during start-up?*
There was a lack of automated control circuits in the heating phase.	*Why were these missing? Were they infeasible or impractical*

	to provide? Was it a cost reduction issue?

UCA: Allowed two employees from different contractors to work in the adjacent Unit during the start-up.

Why? (Context)	Questions Raised
The accident report does not mention this problem except to note that employees were injured in the explosion and that they were from different contractors.	*Was this simply a one-time coordination problem or was it a symptom of a larger problem in coordinating crews during safety-critical operations? Because they workers were from different contractors, was their management not notified or not aware of the maintenance activity going on in Unit 4800? Or was the decision related to the misunderstanding about the risk involved in the startup?*

UCA: Flawed assignment of operators to the turnaround (or at least the start-up).

Why? (Context)	Questions Raised
The Safety Report for Unit 4800 stated that only experienced operators were to be allowed to start-up and shut-down the plant, using the work instructions provided for this purpose. The operators operating the start-up in this accident did not have the requisite experience and expertise. There is no explanation in the accident report of why this breach of procedures occurred.	*Were there no such operators available? Was management unaware of this requirement? Did they have bad information about the skill and experience levels of those they tasked to perform the startup? The answers to these questions will determine the appropriate recommendations to prevent future incidents.*

UCA: Did not effectively incorporate lessons learned from similar incidents at other plants in changes to avoid them at Shell Moerdijk.

Why? (Context)	Questions Raised
As with safety management, no actions were taken after the Moerdijk incident in 1999 and the Nanhai incident in 2011.	*Why? Was the information not available to the decision makers? Did they decide to ignore the information?*

DCA: Did not design an effective Safety Management System (SMS) for Shell Moerdijk. The safety management system did not prevent unsafe situations from being overlooked and internal procedures not being properly followed.

Why? (Context)	Questions Raised
No details about the design of the Shell Moerdijk SMS (which is required by the regulatory authorities in the Netherlands) is provided in the accident report. The report only describes (very briefly) the action management procedures, audits, and the measurements used (number of large leaks and lost time due to injury).	
Guidelines for plant safety management systems are imposed by Shell Corporate and by regulators.	*Do the flaws in the Shell Moerdijk SMS stem from flaws in the Shell corporate and government regulatory guidelines that Shell Moerdijk follows?*
The accident report states that Shell Moerdijk has a Business Management System in which safety management is integrated. Without more details it is difficult to comment, but integrating safety and management decision making and management is dangerous and has been a factor in major petrochemical company accidents (such as Deepwater Horizon). Clearly someone needs to make decisions about tradeoffs between safety and business decisions, but those decisions should be made by the responsible decision makers with full information about all the factors that must be considered and not lost by integrating risk information in a nontransparent way.	*How is the safety management system integrated into the business management system? Are they separated enough that risk-related decision making is not impeded by the way the information is created and displayed (e.g., by risk assessments that combine business and safety risks below the appropriate decision-making level?*

UCA: Audits (both internal Shell Moerdijk audits, those by the parent company, and external audits) did not show any evidence of the shortcomings in the safety studies, the management of changes, the lessons learned from incidents, and other important factors in the accident.

Why? (Context)	Questions Raised
The details were provided in the accident report about how audits are performed that would be useful in identifying any potential deficiencies.	*How are audits performed? Why did the audits that were done miss the problems? Could any audit have identified them?*
Audit findings are recorded in the action management system. The investigators concluded that actions in the action management plan are promptly settled.	

Process Model Flaws

- 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, have an inaccurate view of the risk that existed in the plant.
- Feedback:
  - 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.

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 risks 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.
- Made a decision 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 that manual operation would suffice. The reasons for this decision are not in the accident report.
- Allowed two employees from different contractors to work in the adjacent unit during the start-up, probably because they did not believe that phase was dangerous.
- 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.
- 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 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.

Recommendations:

- Establish and enforce proper MOC procedures. 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.

1.9 Shell Corporate

Three basic functions are examined 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, although they may be distributed throughout the Shell Global management structure differently than assumed here. The bottom line is that they need to be somewhere.

1.9.1 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 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.

Unsafe Control Actions

UCA: Shell Projects and Technology did not provide design information in a form that could reliably be translated into safe operating procedures.

Why? (Context)	Questions Raised
The operators creating the work instructions for the Unit 4800 maintenance stop could not understand the technical details in the Design Book provided by Shell Projects and Technology, resulting ultimately in incomplete and unsafe work instructions.	*Were the designers in Shell Projects and Technology aware that operators and not designers were creating the work instructions? Was there any feedback or a feedback mechanism to alert them that the Design Book content was not understandable to those who were using it in plant operations? What type of feedback channels exist and where is the responsibility at the corporate level for ensuring that the right information is provided to subsidiaries to operate the licensed designs safely?*

UCA: Several MSOP2 design flaws contributed to the accident including a lack of pressure relief devices that would have been capable of mitigating a runaway (they were not designed for the pressure increases that occurred) and an inadequate number of temperature sensors in the reactor. Nitrogen flow requirements provided to the licensees were incorrect. Flaws identified in the central pump design after the Nanhai incident were never fixed.

Why? (Context)	Questions Raised
The accident report states that the designers assumed it was impossible for a runaway to occur during the normal production phase. On the basis of this assumption, Unit 4800 of the MSPO2 was not fitted with pressure relief devices that would have been capable of mitigating a runaway. The pressure relief valves that were provided on the separation vessels were not designed for the rapid pressure increases that occurred.	*Was this simply a design miscalculation or was it a result of the mistaken assumption about the reactivity of ethylbenzene and the catalyst or perhaps lack of emphasis on start-up hazards?*
Shell Projects and Technology included an inadequate number of temperature sensors in the reactor. Because of too few temperature sensors, automatic detection of hot spots is not possible. This design deficiency contributed also to the Panel Operator not noticing the hot spots.	*Why? There is no information provided in the report about whether additional sensors were impossible to provide or whether this was a decision based on some unstated rationale.*[15]
Important lessons that should have been learned from the Nanhai incident (2011) and the Shell Moerdijk incident (2011) were either not understood or did not trigger re-examination of the design and the design assumptions. The fact that temperatures in these incidents exceeded what engineers thought was possible did not prompt any further analysis nor examination of the incorrect assumptions about the possibility of a runaway during reheating of the reactors in a start-up. After the Shell Moerdijk incident, the reactors were fitted with additional temperature sensors but basic assumptions used in the hazard and risk analyses were not altered and the analyses performed at the corporate level do not seem to have been redone.	*How is information passed on to the licensees about any deficiencies identified during operations at other locations? Was the information from the Shell Moerdijk 1999 incident passed to Shell Projects and Technology? If it was passed on to them (and almost surely it was), why did they not respond appropriately to it and why did Shell Projects and Technology or some other corporate entity not ensure that they did respond?*
The catalyst pellets had not been adequately wetted prior to the incident. To wet the catalyst pellets properly, enough ethylbenzene and nitrogen had to pass through a distribution plate into the reactors in the correct ratio. It was (incorrectly) established in the design phase that a nitrogen flow of 475 kilograms per hour was required to achieve this requirement. At 240 kilograms per hour, the nitrogen flow on 3 June was not only too low, it was significantly lower. However, after the incident, Shell Moerdijk determined that a significantly higher	*Where were the flaws in the design process that allowed this incorrect flow rate to be determined? Was it possible to have identified this incorrect calculation before the accident through feedback or was this simply the result of a lack of*

[15] Insufficient sensors above a specific point in the ISOM tower was a factor in the Texas City refinery explosion. In that case, more sensors were possible but were omitted in the design. Apparently, the additional sensors were not considered necessary, perhaps because of an assumption that the liquid would never rise above the maximum level in the tower. Is there a lack of adequate worst-case analysis being used in the petrochemical industry?

nitrogen flow is necessary—of approximately 1700 kilograms per hour—to enable the distribution plate to function properly. So the original calculation appears to be incorrect.	*scientific knowledge that could not be corrected before the loss?*
Because the central pump has a considerable pump capacity compared to the capacity of the separation vessels, work has to be performed with the shut-offs and valves almost closed. The accident report says that "Shell was aware of this but took no further action," but does not qualify whether this knowledge was at Shell Moerdijk or at Shell Projects and Technology. The accident report says that the design data and the system configuration of the process controls do not provide adequate information for the filling and circulation phase. After the Nanhai incident in 2010, one of the recommendations was to reassess the design of single central pump. Based on the safety studies (period 2010-2011), it does not appear that this was actually done. In any event, there was still only a single central pump in the MSPO2 in 2014. A turnaround was carried out in 2011, clearly revealing that circulating and heating were not simple matters. The nearly complete closure of the valve under the separation vessel and the containment which had a negative impact on the stability were points of attention. However, these points were neither examined in sufficient detail nor were they included (by Shell Moerdijk) in the 2014 job analysis.	*Who knew this? How do Shell Projects and Technology work together with Shell Moerdijk engineering and project management to resolve identified weaknesses?* *Again, does Shell Projects and Technology or Shell Global Safety Management review the installation job analyses?*
Insufficient information is provided in the accident report about the reason the design flaws (e.g., incorrect assumptions about operating conditions or limited scientific knowledge at the time), why they were not detected in the design review process, and why they were not fixed adequately after the incidents at Shell Moerdijk in 1999 and Nanhai in 2011.	*What type of worst case and hazard analysis is used in design? What type of design reviews are conducted? Why were the identified flaws not fixed after the incidents showed that the design and underlying design assumptions were flawed?*

UCA: Modifications were made to the production process, including switching to a different catalyst without retesting the assumptions of the past.

Why? (Context)	Questions Raised
In 1977, Shell performed a reactivity test which involved warming up ethylbenzene and the catalyst type used at that time to 130°C. During the test, Shell established that there was no possible chemical reaction between ethylbenzene and the catalyst used. In the following years, modifications were made to the plants and procedures involved in this chemical process and changes made to the	*What are the MOC procedures at Shell Projects and Technology and how are they implemented?*

composition of the catalyst. These modifications did not always lead to a new risk analysis.	
It appears that the incorrect assumption could have been detected by feedback from earlier incidents.	*Were the assumptions about the catalyst recorded? If so, what process is used to detect invalid assumptions through feedback?*

UCA: The work instructions for this maintenance stop were drawn up by Shell Moerdijk panel operators, but the accident report says that this WOL was "approved by the staff of the Shell P&T process owner."

Why? (Context)	Questions Raised
No information is provided beyond the fact that they were approved by Shell Projects and Technology.	*Why did Shell Projects and Technology not notice the flaws in the work instructions? Could this review process be improved?*

UCA: After investigating incidents, Shell P&T did not identify relevant signs regarding process conditions and provide an adequate response to improve safety.

Why? (Context)	Questions Raised
No information is provided in the accident report about how Shell Corporate stores information about incidents and accidents and how it uses it.	

UCA: The risks involved in opting for a trickle-bed reactor and its associated design choices were not recognized and managed properly.

Why? (Context)	Questions Raised
During the development of the SMPO process from 1973 to 1977, engineers at Shell Projects and Technology investigated two reactor designs: • The liquid full reactor: catalyst pellets are located entirely in the liquid, so that the catalyst pellets are always fully wetted. • Trickle-bed reactor: liquid is sprayed onto the catalyst pellets in the reactor from above, as a result of which a thin layer of liquid forms around the catalyst pellets.	*Who actually made the decision to use a trickle-bed reactor at Shell Moerdijk: was it local or made by Shell Corporate?* *What information about the risks was communicated to Shell Moerdijk?*
Tests showed the performance of the catalyst in the liquid full reactor was the best. Therefore, this type of reactor was chosen in 1976 for the	*Was there a technical reason for not using*

MSPO1 plant at Shell Moerdijk as well as the first trickle-bed reactor in Seraya. With the prospect of more SMPO plants, however, all using the trickle-bed design, they needed an alternative catalyst supplier. During the test phase of the MSPO2 plant between 1999 and 2000, Shell compared three catalyst from three different manufacturers. During these tests, the conditions during the start-up phase were not considered. The tests also deviated greatly from the plant conditions. For example, during testing the catalysts were dry reduced using hydrogen and nitrogen, and therefore they were not tested in the presence of ethylbenzene. Furthermore, the tests focused mainly on assessing the normal production phase. Shell selected a catalyst known as G22-2 from a new supplier as an alternative to the catalyst used so far and decided that it could be used as a "drop in"[16] in the SMPO plants. In 2011, the manufacturer of the G22-2 catalyst implemented changes in their production process. As a result, the catalyst contained considerably more hexavalent chromium compounds compared to the previous G22-2 catalyst. Based on the Safety Information Sheet provided with the catalyst, it could be deduced that the new catalyst might contain more hexavalent chromium compound. The accident report notes that the manufacturer did not explicit report this change to Shell Moerdijk [and I assume Shell Projects and Technology]. Around 1990, Shell decided to develop the second SMPO plant in Seraya in Singapore. In the meantime, knowledge had evolved. Research showed that the production process in the liquid full reactor was less effective than had previously been expected. There were also new developments surrounding the trickle-bed reactor. • The performance of the catalyst had been substantially improved. • It was possible to carry out production at much lower pressure and temperature, which improved safety. The liquid full reactor had disadvantages with regard to conversion time and the amount of methyphenyl ketone that had to be circulated over the catalyst bed to get methylphenylcarbinol. Shell opted for a trickle-bed reactor for the Seraya plant and shortly thereafter, for the MSPO2 plant. The new, inherent risk involved in using a trickle-bed reactor rather than a full liquid reactor included: insufficient wetting, followed by the development of hotspots, potentially resulting in a runaway. This risk was in fact identified for the reduction and production phase, but not for the heating phase. It was not recognized before the accident on June 3, 2014.	*ethylbenzene in the tests of the catalysts?*

[16] "Drop in" means that no changes to equipment or procedures are needed before using this catalyst.

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 using the technology. The design had safety-critical design flaws that were not found in hazard analyses during the initial design phase and were not fixed after receiving information about serious problems in operations at some Shell plants such as an inadequate number of temperature sensors and pressure relief valves that could not handle the pressure that occurred. Unsafe and incomplete work instructions were approved by Shell Projects and Technology for the Unit 4800 turnaround at Shell Moerdijk.

Without more information about the operations at Shell Corporate, 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 used if it is produced by another group)? 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 adequate 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 analysis 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 the design and design review process. Fix the design book to be understandable by those who are writing the work instructions and to be comprehensive in 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.

1.9.2 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. This CAST analysis takes the unsafe control actions at the local Shell Moerdijk level and projects what would normally be the responsibility at the corporate level of a well-designed SMS to control them. 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

- 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.

Unsafe Control Actions

UCA: Inadequate risk analysis and/or risk control at the corporate level.

Why? (Context)	Questions Raised
Shell Corporate has overall responsibility for the safety activities in their plants.	*What kind of oversight was provided for the inadequate safety management activities at Shell Moerdijk?*
The design flaws in the MSPO2 reactor were not identified in the original or later hazard and risk analyses.	*Why?*
The accident report says that Shell uses the outdated HEMP and bow tie model. There is little information about what other hazard analysis 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 45 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.	

UCA: The safety information system appears to be inadequate, but no information is provided in the accident report about it. See Section 1.12.2.

Why? (Context)	Questions Raised
Unknown	

UCA: Learning from incidents: After investigating incidents, Shell did not identify relevant signs regarding process conditions and did not incorporate these into new risk analyses for MSP02 or make requisite changes to ensure the incidents did not happen again or lead to a major accident.

Why? (Context)	Questions Raised
The safety information system is an important way for corporations to pass safety-related information to everyone who needs it (see Section 1.12.2). There is no information provided in the accident report about the format and use of a	*Was there assigned responsibility for this type of communication? Were the inadequacies in learning in this case the fault of a poor safety information system, poor*

Shell safety information system. How are lessons learned at one Shell site communicated to other sites?	*investigation, a culture of denial, not part of Shell defined procedures and responsibilities, etc.?*
Lessons learned from the previous incidents at Shell Moerdijk were not incorporated into the design of the related plants and procedures. Repeated statements were made that such events could not happen in that reactor.	*What is wrong with the risk assessment process that even having something occur similarly in the past did not get past their risk assessment blinders?*

UCA: Management of Change policies were not implemented adequately in this case.

Why? (Context)	Questions Raised
Modifications were made to the production process, including switching to a different catalyst without retesting the assumptions of the past	*Who was responsible for these changes (Shell Corporate or Shell Moerdijk)? Were the assumptions recorded? Did the Corporate MOC procedures omit this type of change or were they inadequately followed? Who in safety management is responsible for ensuring that the management of change procedures are being followed?*

UCA: Audits and Shell internal safety supervision procedures did not reveal the shortcomings related to safety studies and the management of change and lessons learned procedures.

Why? (Context)	Questions Raised
Inadequate information is provided in the accident report to understand why the audits were not more effective.	How are audits carried out? Why were all the deficiencies in the safety management system not identified?

UCA: Did not identify and use effective leading indicators.

Why? (Context)	Questions Raised
Shell used the standard leading indicator of number of leaks for process safety (and lost time injuries for workplace safety). Leaks were going down.	Why is this the only leading indicator of process safety used?

<u>Summary of the Role of Corporate Safety Management</u>: There appears to have been a flawed view of the state of risk and the effectiveness of the safety management system in Shell plants. The flawed process model is most likely related to inadequate feedback (including audits and leading indicators). 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 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.

1.9.3 Executive-Level Corporate Management

Responsibilities:

- Take all measures necessary 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.

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.

Unsafe control: 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 not effective. There is nothing included in the accident report about the assigned safety-related responsibilities for corporate management. The Baker Panel report on the Texas City explosion found that BP corporate management did not have assigned responsibilities for safety, which instead was treated as a local responsibility. This abdication of responsibility (a practice promoted by HRO, which BP follows) was identified as a major contributor to the Texas City explosion [Baker 2007]. Is this a problem in general in the petrochemical industry?

There is also nothing included about context in the accident report that might explain why standard executive-level responsibilities for safety were not effectively carried out. There seems, however, to be a safety culture problem at Shell. See Section 1.12.3 for an 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, 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 violations of procedures. 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.

1.10 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.

Unsafe Control Actions:

UCA: Changes to catalyst made by manufacturer were not reported to Shell Moerdijk although they were specified in the Catalyst Safety Information Sheet.

Why? (Context)	Questions Raised
In 2011, the manufacturer of the G22-2 catalyst implemented changes in their production process. As a result, the catalyst contained considerably more hexavalent chromium compounds compared to the previous G22-2 catalyst. Based on the Safety Information Sheet provided with the catalyst, it could be deduced that the new catalyst might contain more hexavalent chromium compound. The accident report notes that the manufacturer did not explicit report this change to Shell Moerdijk [and presumably Shell Projects and Technology]. The catalyst manufacturer did not report changes because they fell within the scope of the specifications that had been agreed between Shell and the manufacturer.	
As noted in the Shell Moerdijk safety management analysis, the 2014 Shell Moerdijk risk screening for the new G22-2 catalyst in the MSPO2 plant did not involve any laboratory tests or other investigations. Shell Moerdijk Safety Management did not notice the change in the Safety Information Sheet and assumed the properties of the new catalyst were the same as those of the previous catalyst.	

UCA: Did not think catalyst change would affect safety for Shell

Why? (Context)	Questions Raised

Without knowing the details of the Shell reactor design, the catalyst manufacturer cannot determine the safety of the use of their product.	

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 are on a customer, there should be some clear alert (other than simply changing information in a document) that changes have been made and what they are so that the customers are aware of them.

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

1.11 External Oversight and Emergency Services

1.11.1 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 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.

Unsafe Control Actions

UCA: Did not identify shortcomings at Shell. Assessed Shell as a well-functioning company in which they had a great deal of confidence.

Why? (Context)	Questions Raised

Brzo supervision was tightened after incidents at Chemie-Pack (a chemical fire in Moerdijk on 5 January 2011) and Odfjell (serious safety deficiencies contributed to a large gasoline spill at a Rotterdam tank terminal). The changes in oversight of chemical activities that resulted from these events did not prevent the Shell Moerdijk explosion or the unsafe control actions listed above.	
The regulatory agencies had scarce resources and time for oversight.	
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 procedures in place (on paper) and spot check that they are being used.	
There is no statutory standard for determining whether the supervision of a Brzo company is adequate.	
Under Brzo, the regulators 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 (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. And so on.	*Do the regulators also check whether the SMS is effective? What feedback do they get about efficacy? Is there feedback (required reporting) about incidents and inadequacies?*
In terms of safety management system, Shell Moerdijk was one of the highest scoring Brzo companies. The regulators were unanimous in their positive appraisal. Shell Moerdijk was known to take any identified shortcomings seriously and to rectify them quickly and effectively. The Brzo inspections (inspections of companies that are subject to the Major Accidents (Risks) Decree) during the preceding five years were conducted in this context.	
The number of Brzo inspections is determined by (1) company risks (nature and size of plants, volume of	

hazardous substances, and activities of company), (2) Quality of the safety management system, whereby less supervision may be required if the management level is high and more may be required if the management level is low. Shell Moerdjk ranks highest in terms of risks of all the 72 companies subject to Brzo in the Province. It also scored high on the judged quality of its safety management system.	
Shell Moerdijk had only one violation of Brzo between 2010 and 2014, a low number compared to other Brzo companies. The company always initiated an improvement action when a problem was identified. The shortcoming was either immediately rectified or the regulators felt it was clearly on its way to be rectified and was being systematically monitored in the Shell Moerdijk action management system. The regulators considered Shell Moerdijk to be a company with a good safety performance.	
There were several shortcomings at Shell Moerdijk that regulators did not label as violations. Not identifying violations contributed to the positive impression of Shell Moerdijk's operational safety.	
Less intensive supervision was required for companies whose safety management systems were judged to function well. But if there are fewer supervision days allotted, external regulators have more difficulty forming an opinion of the risks in the company with sufficient depth.	
Even under system-oriented supervision, the inspectors could have observed that changes and upgrades to the plants were not consistently subjected to risk analyses and that the safety management system indeed did not function well.	
"Identification of hazards and assessment of risks" was covered only once in a Brzo inspection in the last five years, which was in 2011. The inspectors gave a score of "moderate" and did not follow up to check whether Shell Moerdijk had improved.	

Within the framework of the Safety Report required by law, Shell Moerdijk subjected all containment systems to a risk assessment. In principle, this process should have led to thousands of potential plant scenarios. Legislation requires the company to prepare 10 scenarios per plant (such as MSPO2). In so doing, the company must select the hazards with the greatest risks and the nature of the risks must be varied. [How do they select the 10 to analyze?]	*Why only 10? How are the 10 to be analyzed selected? By definition, accidents occur when the assumptions about what is most risky are wrong, as in this case. Note that there was evidence that the assumptions were wrong in the form of accidents at plants with a similar design. Do the regulatory authorities get information about accidents at other similar Shell plants? Can examining only a few risks that one thinks are the most important ensure anything about safety and not simply lead to a perfunctory and useless exercise performed on the risks that are already well understood and handled and thus unlikely to lead to an accident? Does the regulatory authority have any oversight about which scenarios are selected?*
Several shortcomings were identified that should have been deemed violations, but were not: for example, the plant scenarios were not up to date or were incomplete and the catalyst was not being stored according to the guidelines. The inspectors gave a score of "good" or "reasonable" for the majority of their assessments. Deficiencies in the scenarios were noted during an inspection in 2011, but no new inspections were performed to determine if the problems were corrected.	
Under system-related supervision, it is assumed that the inspectors are not able to identify "deep-seated shortcomings at Shell Moerdijk if Shell itself has not identified these." Under these assumptions, the regulators do not review things such as written procedures for hazardous activities like start-up, the information passed from the designers to the operators, change management activities, whether learning is being incorporated from similar incidents. And so on. Even under system-related supervision, it was possible for inspectors to see that the work instructions did not follow the format required by Shell and to identify that Shell's own safety rules were being violated, such as assigning operators to a turnaround that did not have the necessary knowledge and experience.	*Exactly what is examined in the safety management system evaluation? Why were the safety management system shortcomings, especially in the implementation of the requirements, not detected by the regulators?*

At Shell Moerdijk, the Safety Report is approximately 1,000 pages long and the safety management system has approximately 350 procedures and guidelines.	*Are each of these equally important? How were these organized? Was it possible to identify and review the most critical aspects of the report and the most critical procedures and guidelines?*

UCA: There was no in-depth investigation of the operation of the specific maintenance-stop-related procedures although maintenance stops are high risk. No special attention was paid to hazardous (critical) activities such as maintenance and startup.

Why? (Context)	Questions Raised
No explanation is provided in the accident report but inadequate resources probably played a role as well as their system-oriented supervision model.	

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."

Summary: The accident report implies that regulators gave Shell Moerdijk a pass on behavior that might have 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. So what is wrong with the supervision model that the regulators did not detect them?

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 they are doing something that is effective in preventing accidents like the Shell Moerdijk explosions and fire.

1.11.2 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.

Unsafe Control Actions

UCA: Inadequate emergency alerting of local population.

Why? (Context)	Questions Raised
NL-Alert message did not reach everyone. • Cell broadcast did not function optimally; for example, it does not operate in the 4G network • Mobile phones were unsuitable or were not set to receive NL-alert • Mobile phones were switched off at 23:49---the time at which the first NL-alert was sent.	*Why were the flaws not identified in previous incidents or in testing? Was the NL-alert not a factor then? Were the deficiencies noted but not acted upon for some reason (low priority, no resources, denial)?*

UCA: A number of parties did not make consistent use of the LCMS (National Crisis Management System) for sharing information: the municipalities did obtain information but did not always share information via the LCMS.

Why? (Context)	Questions Raised
Not all the emergency teams actively used the LCMS. However, in some areas, the system also contained incomplete, insufficient, and at times even incorrect information. Information was not always verified before it was entered into the LCMS.	
National Crisis Management System (LCMS) had several deficiencies: • Lack of experience working with LCMS played a role at various locations. • There were technical and facility-level problems regarding the authorization for the LCMS: a number of officials were unable to log in • Not all of the emergency teams had an information manager available during deployment. In some teams, this meant that the LCMS was not actively used. • The status of the information was not always clear. It was also often unclear whether the info was only exclusively intended for internal use or whether it could be shared externally. • Not all the emergency teams actively used the LCMS. Reasons ranged from the lack of an information manager in the emergency team to a lack of time to actively populate or to read the LCMS within the meeting cycle. Parts of LCMS were used effectively. However, in some areas, the system also contained incomplete, insufficient, and at times even incorrect information.	

• Clear agreements about the use of LCMS were lacking and the officials were not sufficiently familiar with it.	

UCA: Problems occurred in the assessment of hazardous substances and the subsequent communication surrounding them.

Why? (Context)	Questions Raised
No information provided.	

UCA: Some teams also used WhatsApp on their cell phones and thus that information could not be used in developing an inter-regional information overview.

Why? (Context)	Questions Raised
The status of information communicated via WhatsApp is difficult to determine and is usually not recorded and impossible to trace afterwards.	*Why did people use WhatsApp? Was it easier to use? More convenient? What made it more likely to be used than the official system? The answers to these questions can be used to improve the official system.*

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.

Recommendations: Several deficiencies were uncovered in LCMS and NL-Alert during this incident. While they did not lead to loss of life because of the nature of the accident in this case, they could under other circumstances and what was learned from this case should be used to improve the system, including why many people used WhatsApp instead and how the official system can incorporate those features. 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.

1.12 Factors Spanning System Components

The bulk of a CAST analysis is spent examining the contributions of individual components to the loss events. But there are also important factors in the operation of the safety control structure as a whole that need to be considered: the design of the SMS, the safety information system, the safety culture, coordination and communication, and dynamics and changes over time.

1.12.1 Overall Safety Management System

It is difficult to identify flaws in the Shell safety management system (SMS) without detailed information about its design, which is not included in the accident report. The CAST analysis, however, did find several potential deficiencies related to the Shell Global and Shell Moerdijk safety management systems. The Shell Moerdijk SMS is a subset of the overall Shell Global SMS. Clearly, neither one operated effectively.

There is no right or wrong design for a safety management system: A SMS 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 management system to be effective [Leveson, 2012], many of which do not appear to be reflected in the Shell SMS. Shell would be well served by reviewing the design of its SMS to determine whether these principles are implemented.

Even without details provided in the accident report about the Shell and Shell Moerdijk safety control structure, clear deficiencies can be identified from the factors leading to the accident. The accident report notes that unsafe situations were overlooked, internal procedures were not properly followed, lessons were not learned from previous incidents, incorrect assumptions about basic 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.

Finally, while there is no information beyond a cryptic comment in the accident report that the Safety Management System is integrated with the Business Management System, in general this is a poor practice and can undermine good decision making.

1.12.2 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].[17] 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.

The Shell Moerdijk accident report does not provide any information about the Shell or Shell Moerdijk safety information system(s), but it does describe many instances of deficiencies that could have been prevented with a well-designed safety information system, such as not learning from incidents and previous maintenance stops, not identifying flaws in 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 also notes that “A discrepancy therefore occurred between the available information during the design phase and the operations management that was ultimately conducted.” It is these kinds of problems that a well-designed safety information system should be able to prevent. The accident report recommends that they “organize the communication of process knowledge and lessons learned from actual and near incidents to employees who are responsible for managing safety risks.”

Recommendation: The company safety information should be evaluated and improved.

1.12.3 Industry and Organizational Safety Culture

An organizational culture is the set of shared assumptions, values, and beliefs that govern how people behave in organizations [Schein 1986]. The safety culture is a subset of the organizational culture; it is the value system that underlies the safety management structure and upon which the safety policies and practices are developed. The safety culture is mostly set by the organization’s leaders, and it can change quickly when leadership changes. Paul O’Neill, for example, valued safety as one of his primary goals when made the head of Alcoa in 1989. Within one year Alcoa became the safest

[17] The highest ranking factor was top-level management concern about safety.

(and one of the most profitable) in that industry [Duhigg 2012]. The opposite can occur when leaders are selected who do not value safety with respect to other organizational goals.

The accident report briefly mentions the Shell safety culture and does not do an in-depth examination of it. But what is included in the accident report raises important questions and doubts about the strength of this culture in Shell.

Shell was one of the founders of a safety culture program called Hearts and Minds. It was initially created by Shell Exploration and Production in 2002. Figure 6 shows what they call the “culture ladder,” which is described as the “maturity” level of the organization’s safety culture. Maturity level appears to be borrowed from the current “process maturity” movement. But cultures are not processes, they are value systems and describing one value system as more “mature” than another makes little sense or one set of behaviors as more mature than another makes no sense. The employees of a company or participants of an industry either value safety highly or not. Value systems cannot be compared with others or ranked on a scale of maturity, but simply evaluated on whether they are successful in achieving specific goals such as preventing accidents.

Limited information is provided in the accident report, but with respect to the stated goals in the Shell Hearts and Minds culture ladder, Shell seems to have major weaknesses. The accident report points to unsafe behavior that seems to imply safety was not a high priority: overlooking unsafe behavior and warnings, not adhering to internal procedures, not making changes after previous incidents, and not evaluating assumptions after changes occur.

The report notes that during the four years before the accident, only one safety culture measurement effort was carried out (in 2011). And in that small effort, only 28 of the more than 800 employees participated. This measurement was conducted during a middle-management meeting where all 28 individuals attending the meeting took part in the survey, which was then discussed. The report says that “Shell Moerdijk has not performed any other safety culture measurements in order to assess the effects of its safety culture efforts.” There was another employee satisfaction survey, containing eight questions, that gave some evidence of culture-related elements, but it was not a safety culture survey that would “provide deeper insight into the areas of values, attitude, and behavior as regards safety” [Dutch Safety Board, 2015].

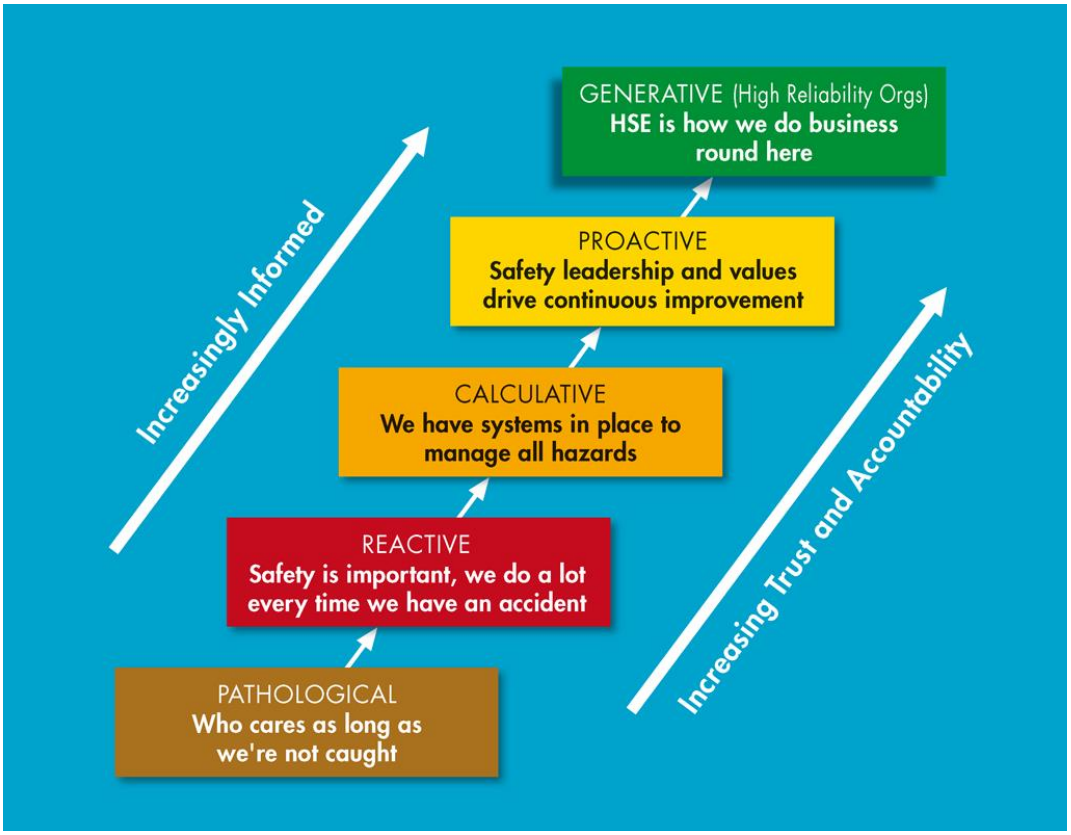
GENERATIVE (High Reliability Orgs)
HSE is how we do business round here
PROACTIVE
Safety leadership and values drive continuous improvement
CALCULATIVE
We have systems in place to manage all hazards
REACTIVE
Safety is important, we do a lot every time we have an accident
PATHOLOGICAL
Who cares as long as we're not caught
Increasingly Informed
Increasing Trust and Accountability

Figure 6. The Hearts and Minds Culture Ladder

In lieu of a direct examination of the Shell safety culture, indirect evidence must be used to identify safety culture flaws. The company seems to be satisfied with their self-assessed current level on the Hearts and Minds "culture ladder" of Calculative (which is described in the accident report as the "required" level), but even that level does not seem to have been achieved (nor the so-called "lower" levels).

The reactive level, defined as "We do a lot every time we have an accident" leaves undefined what "a lot" is. Reacting after an accident is not very useful, and what was done after the Nanhai and Shell Moerdijk 1999 incidents was clearly inadequate in terms of preventing the same thing from happening again.

The accident report says that "In Shell Moerdijk's estimation, its safety culture is at the required level (calculative). This level is defined as "we have systems in place to manage all hazards," but they clearly did not achieve this level either as they did not have systems in place to manage the hazards involved in starting up Unit 4800 on 3 June 2014. In addition, the fact that they are satisfied with not achieving the top two steps in their own program, i.e., using leadership and values to continuously drive safety improvement and making safety an integral part of the way business is done at Shell,[18] is not encouraging in terms of the state of Shell's actual safety culture.

[18] HRO is controversial with respect to whether it promotes safety or simply reliability (these are two different and sometimes conflicting properties). For example, the Baker Panel Report on the Texas City explosion [Baker 2007] found that the treatment of safety as a local responsibility, a practice promoted by HRO, contributed to the losses. An evaluation of HRO can be found in [Leveson et.al. 2009].

The accident report says that the company deduces the level of its own safety culture from the safety performance indicators based on number of leaks and industrial accidents resulting in absenteeism. Neither is a good indicator of process safety.

To evaluate the safety culture at Shell requires looking in depth at the company and employee behavior, not simply giving surveys of what some people think. How they behave is a much better indicator of their internal value system than what they answer on surveys. The accident report did not cover the safety culture in depth, but what is included seems to point to what has been labeled as a "compliance culture," where the bulk of the effort is simply complying with standards and the requests of regulators and not proactively taking steps to improve safety because it is a basic value in the company. The accident report says that they always fixed immediately what was found to be lacking by government inspectors. Did they aggressively search for problems internally without being prompted by a regulatory agency?

The words on paper do not matter with respect to safety culture, but how the employees behave and how they see their leaders behaving.

Recommendation: Shell Moerdijk and Shell Corporate should do a thorough study of their safety culture and why it was not strong enough to prevent the events in 2014.

1.12.4 Communication and Coordination

Communication and coordination problems are often implicated in accidents. 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 lack of effective communication between Shell Projects and Technology and Shell Moerdijk and within Shell Moerdijk. In addition, the changes to the catalyst by the manufacturer was not communicated to Shell.

The accident report does not provide any information about whether the fact that two employees from different contractors were allowed to work in the adjacent unit at the time of the start-up was a coordination problem or simply the result of complacency about the risk of a start-up. There also is a dearth of information about possible coordination confusion when the operators were using a process control system that was on manual but still had some automated functions. Many questions were raised in the CAST analysis about human factors aspects of both the feedback provided to the operators and the tasks they had to perform in manual mode.

Recommendations: Communication channels, especially feedback channels, should be examined to determine whether they are effectively conveying the information necessary to operate safely. An important part of this includes performing a human factors analysis of the information provided to the operators and the potential for human errors created by the design of the process and particularly by the design of the process control system.

1.12.5 Dynamics and Changes over Time

As has been repeatedly stressed throughout this report, accidents usually occur after some type of change. The change(s) may be in the physical process, the operating procedures, the safety procedures, the management process, or in the oversight (both internal and external).

Changes may be planned or unplanned. Both need to be controlled. If the changes are planned, a strong management of change policy that is enforced and followed can be effective. In this accident, the management of change procedures do not appear to have been either enforced or effective. Examples include the switch to a new catalyst without testing it or reconsidering that assumptions regarding it may no longer be true and the removal of parts of the work instructions for Unit 4800 (again without assessment) because they were not considered critical. For example, 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 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 may also be unplanned and must therefore be detected. There needs to be a way to detect unplanned changes that affect safety or 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. In this accident, the leading indicators were inadequate and too narrow (number of leaks), 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 here 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.

Recommendation: The Management of Change procedures should be evaluated to determine why they were not effective in this case and appropriate improvements implemented.

Recommendations Stemming from the CAST Analysis

There are many questions that need to be answered to complete the CAST analysis. One of the goals of an accident analysis technique should be to guide the investigation so that the investigators can provide the information necessary to learn as much as possible to prevent more losses in the future.

The CAST analysis used the information in the official Dutch Safety Board report so the recommendations are going to be similar. In fact, the Shell Moerdijk accident report written by the Dutch Safety Board is, in my experience, much better than most accident reports. The CAST recommendations are more extensive, however, and more detailed. A CAST analysis encourages a broader and deeper look into the reasons why the accident occurred. Getting answers to the questions raised in the CAST analysis would most certainly create additional recommendations that are not noted here.

In general, there were so many flaws in the Shell Safety Management System and the behavior of almost every component of Shell Global and Shell Moerdijk that a comprehensive redesign of the Shell and Shell Moerdijk safety management system and the safety information system would be appropriate. In addition, there appear to be flaws in the safety culture that should be corrected. The oversight authorities also were ineffective in preventing the accident using their procedures and legislation and a review and redesign of the oversight procedures appears to be appropriate.

Figure 7 shows the safety control structure assumed in the CAST analysis, with flawed control and feedback contributing to the accident shown with dotted lines. As can be seen, almost the entire structure was involved.

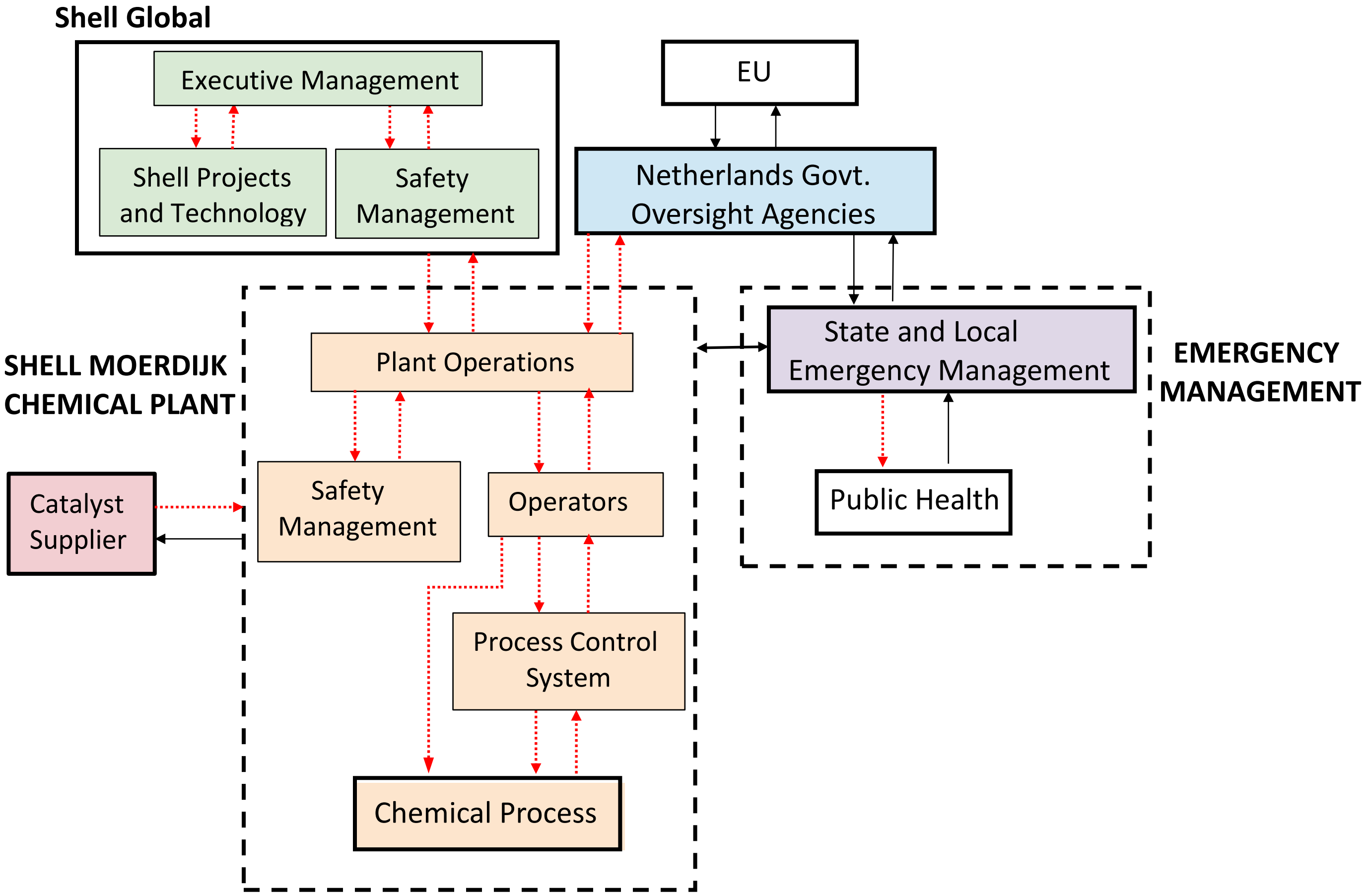

Figure 7. Flawed Interactions in the Assumed Safety Control Structure. Red dotted lines represent missing or inadequate control or feedback. Almost all the interactions were flawed in some way.

As an overview of the CAST analysis results, the following table summarizes each component's role in the accident along with the recommendations generated for that component. The reasons for the component's role in the accident would probably be augmented if the unanswered questions noted in the CAST analysis details had been included in the accident report.

Physical Component	**Role:** None of the physical controls failed. The final physical collapse of the reactor and separation vessel after pressure reached a critical level 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. **Recommendations**: The physical design limitations and inadequate physical controls need to be fixed. (The potential detailed fixes are not included here; they need to be determined by a qualified chemical engineer.)
Process Control System	**Role**: The process control system was not configured 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. **Recommendations**: The operators' knowledge and skill is 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 to provide all necessary assistance to the operators in decision making and taking action and to reduce attention and time pressures.
Operators	**Role**: The operators 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, while 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. The risks were not communicated properly. Management relied on the 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. **Recommendations**: The operators must have the appropriate skills and expertise to perform their assigned activities, and there must be someone assigned the responsibility for enforcing this requirement. A human factors study during the job analysis is needed 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 should be provided in all phases of operation, training should be provided for activities that are known to be hazardous like startup, and work instructions as well as the process for producing them need to be improved.

Plant Safety Management	**Role**: (1) 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 with the minimum required by the Dutch regulators. Safety management did not consider some 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. (2) Although Shell's safety management system includes requirements for dealing with changes, the MOC procedures were not followed or implemented effectively. Risks resulting from changes made to the plant, the catalyst, the processes, and the procedures were not identified and managed. (3) Used the number of leaks as the primary leading indicator of process safety. This practice is common in the petrochemical industry. (4) Lessons from similar incidents at Nanhai and at Shell Moerdijk were not used to reduce risk. (3) Proper oversight of the generation of work instructions was not provided, which allowed unsafe work instructions to be used by the operators. **Recommendations**: While the problems specific to the explosions on 3 June 2014 should be fixed, there was a lot of weaknesses in the Shell Moerdijk safety management design and especially practices that were identified in the official Dutch Safety Agency accident report and in the CAST analysis. These need to be improved. In addition: (1) 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. (2) All work instructions should be reviewed for safety by knowledgeable people using information from the hazard analysis. [In this case, the HA was flawed too, but that is a different problem to fix.] (3) MOC procedures must be enforced and followed. When changes occur, assumptions of the past need to be re-evaluated. (4) Hazard analysis and risk assessment methods need to be improved. (5) More inclusive leading indicators of risk need to be established. (6) Procedures for incorporating and using lessons learned need to be established or improved.
Operations Management	**Role**: (1) 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. (2) Changes over time were not subjected to assessment in accordance with the MOC procedures.

	(3) 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 and nitrogen flow. (4) Made a decision 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 that manual operation would suffice. The reasons for this decision are not in the accident report. (5) Allowed two employees from different contractors to work in the adjacent unit during the start-up, probably because they did not believe that phase was dangerous. (6) 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. (7) 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. (8) Did not follow MOC procedures or perhaps they and the procedures were inadequate. No information in the report to determine this. (9) Conducted internal Shell Moerdijk audits that did not detect any of the clear shortcomings in practices and procedures. Not enough information is provided to determine why the audits were ineffective. **Recommendations**: (1) Establish and enforce proper MOC procedures. 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. (2) Do a thorough review of the Shell Moerdijk SMS 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. (3) 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. (4) Improve the process control system to provide appropriate assistance to operators performing functions that are outside of normal production.

Shell Projects and Technology	**Role**: The design data provided to the licensees was not usable by those creating work instructions at the plants using the technology. The design had safety-critical design flaws that were not found in hazard analyses during the initial design phase and were not fixed after receiving information about serious problems in operations at some Shell plants. These design flaws include an inadequate number of temperature sensors and the use of pressure relief valves that could not handle the pressure that occurred. Unsafe and incomplete work instructions were approved by Shell Projects and Technology for the Unit 4800 turnaround at Shell Moerdijk. Without more information about the operations at Shell Corporate, it is difficult to determine exactly why the unsafe control occurred. More questions than answers

	arise from the CAST analysis here, 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 used if it is produced by another group)? Why were identified design flaws not fixed after the incidents at Shell Moerdijk in 1999 and Nanhai in 2011? What other types of feedback (beyond incidents) 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 adequate 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 specifically about start-up and the hazards of start-up? What types of hazard analysis 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 are the triggers got 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 the design and design review process. Fix the design book to be understandable by those who are writing the work instructions and to be comprehensive in 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 (or fix it elsewhere if this group does not do their own hazard analyses).
Corporate Safety Management	**Role**: There appears to have been a flawed view of the state of risk and the effectiveness of the safety management system in Shell plants. The flawed process model is most likely related to inadequate feedback (including audits and leading indicators). Again, many questions are raised in 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. Almost nothing about safety management at the Corporate level is included in the accident report. **Recommendations**: Improve Shell safety audits. Review all risk assessment and hazard analysis processes and, in general, improve their approach 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	**Role**: Corporate management is responsible to ensure that an effective safety management system is created. Clearly 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 not effective. There is nothing included in the accident report about the assigned safety-related responsibilities for Corporate management. The Baker Panel report on the Texas City explosion found that BP corporate management did not have assigned responsibilities for safety, which instead was treated as a local responsibility. This abdication of responsibility (a practice promoted by HRO, which BP follows) was identified as a major contributor to the Texas City explosion [Baker 2007]. Is this a problem in general in the petrochemical industry? There is also nothing included about context in the accident report that might explain why standard executive-level responsibilities for safety were not effectively carried out. There seems, however, to be a safety culture problem at Shell. Is this a problem in the Oil and Gas industry as a whole? 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, 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 violations of procedures. 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 Manufacturer	**Role**: 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 are on a customer, there should be some clear alert (other than simply changing information in a document) that changes have been made and what they are so that the customers are aware of them.

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

Dutch Regulators	**Role**: The accident report implies that regulators gave Shell Moerdijk a pass on behavior that might have 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. So what is wrong with the supervision model that the regulators did not detect them? **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 they are doing something that is effective in preventing accidents like the Shell Moerdijk explosions and fire.
Emergency Services	**Role**: Emergency services were mostly very effective in carrying out their responsibilities, but some deficiencies, particularly in communication, were uncovered in the accident response. **Recommendations**: Several deficiencies were uncovered in LCMS and NL-Alert during this incident. While they did not lead to loss of life because of the nature of the accident in this case, they could under other circumstances and what was learned from this case should be used to improve the system, including why many people used WhatsApp instead of LCMS and how the official system can incorporate those features. 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.

For the factors that spanned the entire control structure, not much information was included in the accident report that provided the information used in the CAST analysis, but some weaknesses are implied by what is included and some general recommendations can be derived.

Safety Management System	Evidence of an overall inadequate safety control system (safety management system) in the report includes: unsafe situations were overlooked, internal procedures were not properly followed, lessons were not learned from previous incidents, incorrect assumptions about basic 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. In summary, 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 ensuring that it was working properly. **Recommendations**: The design of the entire safety management system should be evaluated and improved. In addition, the integration of the safety management system and the business management system should be carefully examined to ensure that hazard and risk-related information is not being effectively communicated to decision makers by being traded off at inappropriately low levels.
Safety Information System	No information is provided about the safety information system but it appears that people were making decisions without having appropriate information. **Recommendations**: The safety information system is so critical to the achievement of high safety that Shell and Shell Moerdijk should evaluate the existing system and perhaps redesign it.
Safety Culture	The accident report did not cover the safety culture in depth, but what is included seems to point to what has been labeled as a "compliance culture," where the bulk of the effort is simply complying with standards and the requests of regulators and not proactively taking steps to improve safety because it is a basic value in the company. The accident report points to unsafe behavior that seems to imply safety was not a high priority such as overlooking unsafe behavior and warnings, not adhering to internal procedures, not making changes after previous incidents, and not evaluating assumptions after changes occur. The Hearts and Minds Safety Culture Program used by Shell has serious weaknesses. The "culture ladder" is vaguely defined ("we do a lot every time we have accidents"). Strangely, the company seems to be satisfied with their self-assessed current level in this program of Calculative (which is described in the accident report as the "required" level), but even that level does not seem to have been achieved (nor the so-called "lower" levels). **Recommendations**: Shell Moerdijk and Shell Corporate should do a thorough study of their safety culture and why it was not strong enough to prevent the events in 2014.
Communication and Coordination	**Recommendations**: Communication channels, especially feedback channels, should be examined to determine whether they are effectively conveying the information necessary to operate safely. An important part of this includes performing a human

	factors analysis of the information provided to the operators and the potential for human errors created by the design of the process and particularly by the design of the process control system.
Management of Change	**Role**: A large number of both planned and unplanned changes contributing to the accident were not assessed for risk. **Recommendations**: The Management of Change procedures should be evaluated to determine why they were not effective in this case and appropriate improvements implemented.

SUMMARY

CAST is based on a new accident causality model, STAMP, which in turn has a theoretical foundation in systems theory. As such, accidents are treated as resulting from a lack of control over the components and non-enforcement of safety constraints. This assumption is in contrast with the standard causality model which treats accidents as a chain of failure events. STAMP is more general than the chain-of-failure-events models and therefore encompasses more types of accident causes.

The use of CAST helps to guide an accident investigation, to generate questions to answer, and to identify the deep seated problems that need to be fixed to prevent a large number of accidents in the future rather than just preventing very similar ones. The results should help companies get out of the firefighting mode where seemingly different, but actually related accidents, keep occurring.

GLOSSARY [PROBABLY CAN OMIT]

SIS: Safety Information System
SMS: Safety Management System

REFERENCES

1. Baker Panel. *The Report of the BP U.S. Refineries Independent Safety Review Panel*, 2007.
2. Peter Checkland. *Systems Thinking, Systems Practice*, John Wiley & Sons, 1981.
3. Sidney Dekker. *The Field Guide to Understanding Human Error*, Ashgate, 2006.
4. Charles Duhigg. *The Power of Habit: Why We Do What We Do in Life and Business*, Random House, 2012.
5. Dutch Safety Board, *Explosions MSPO2 Shell Moerdijk*, The Hague, 2015.
6. Anthony Hidden. *Investigation into the Clapham Junction Railway Accident*, Dept. of Transportation, London, 1990.
7. Urban Kjellan. An Evaluation of Safety Information Systems at Six Medium-Sized and Large Firms, *Journal of Occupational Accidents*, 3:273-288, 1982.
8. Nancy G. Leveson, *Engineering a Safer World*, MIT Press, 2012.
9. Nancy G. Leveson, *Safeware*, Addison-Wesley, 1995.

10. Nancy G. Leveson, Nicolas Dulac, Karen Marais, and John Carroll. Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems, *Organizational Studies*, 30:227-249, February/March, 2009.
11. Jens Rasmussen. Human Error and the Problem of Causality in Analysis of Accidents, in *Human Factors in Hazardous Situations*, eds. D.E. Broadbent, J. Reason, and A. Baddeley, 1-12, Clarendon Press.
12. Jens Rasmussen, Risk Management in a Dynamic Society: A Modelling Problem. *Safety Science*, 27(2/3):183-213, 1997.
13. Edgar Shein. *Organizational Culture and Leadership*, Sage Publications, 1986.