STAMP-Based Analysis of a Refinery Overflow Accident

Nancy Leveson, Margaret Stringfellow, and John Thomas

As an example of STAMP, we have taken an accident report produced for a real refinery overflow accident and reanalyzed it using STAMP. The original accident report is shown in the Appendix, with all identifying parts removed. The results of the two different accident analyses are compared at the end of this paper. The reader might find it easiest to read the appendix (official) accident report first.

Description of the Physical Process

In the SBS unit, tail gas is burned at 1200^o F with excess air and natural gas in the tail gas combustor F-700. This converts the H_2S to SO_2. [A physical diagram could be inserted here, but we did not have one that we could use.]

Hot gas effluent from F-700 is cooled in the waste heat boiler E-701. Effluent gas from the boiler enters the venturi quench tower V-703 where it is quickly cooled by direct contact with a 30% sulfuric acid solution to approximately 181^o F. The 30% acid solution comes from the bottom of the T-704 quench separator and is pumped to V-703 via the quench circulating pumps P-704A/B/C in a continuous loop. The acid concentration is maintained at 30% by purging a small (< 2 gpm) slip stream to Tank-731 acid tank and replacing it with water to maintain the process temperature near 181^o F. The acid from Tank 731 is then removed either by draining to the process sewers (used as Lakefront pH control) or used as a product elsewhere. As the acid enters Tank 731, it is saturated with SO_2. The design of Tank 731 allows for the gas that is entrained in the acid to degas off to another tower, T 707, where it can be further treated. On Thursday August 7th, when tank 731 tank overfilled, there was not sufficient residence time for the SO_2 entrained in the solution to degas properly. As a result, the acid evolved sulfur dioxide to atmosphere as it overfilled to the ground.

Events:

The analysis starts, like any accident analysis, with identifying the proximate events including the physical failures and operator actions (or missing actions) related to the loss. But stopping after identifying these, often the end point in accident investigation, usually leads to attributing the cause to operator error, which, as stated earlier, does not provide enough information to prevent accidents in the future. The operators may be fired or reprimanded, subjected to additional training, or told not to make the same mistake in the future, none of which lead to long term prevention of the same behavior if problems exist in the other parts of the safety control system design. It also leads to identifying and fixing specific hardware design flaws, e.g., the redesign of a relief valve or the replacement of a flow meter, but not the flaws in the engineering design and analysis process or the maintenance issues that led to that particular manifestation of a flawed design. Examining the rest of the control structure will provide more information about the flaws in the larger company safety management structure that need to be fixed.

The events below are from the original accident report:
08:33 - Board Operator attempts to open control valve F-47706, to begin an acid drawdown from the quench recirculation system. The flow meter does not indicate a flow, so the Board Operator

calls the Outside Operator to check and see if the manual block valves at the control valve station are closed. Note: The Board Operator stated/believed that the block valves are normally left in the open position to facilitate conducting this operation remotely.

09:11 - Outside Operator finds that the manual block valves are lined up (open) and has the Board Operator open the control valve to different settings in an effort to troubleshoot the situation. Outside Operator also sees no indication of flow on the flow meter and makes an effort to visually verify that there is no flow. He then begins to work (open and close) the manual block valves in an effort to fix the problem. Note: Process control data indicates that the tank level indicator begins to show an increase in the tank liquid level around this time. Acid level in the tank is approximately 7.2 ft. at this time. Per the interviews, neither the Board Operator nor the Outside Operator had any discussion about opening the bypass valve. The Board Operator did not call for the bypass valve to be opened, and the Outside Operator states that he did not open the bypass valve.

09:25 - Outside Operator finishes his effort to work (open and close) the manual block valves. He reports having heard a clunking sound and thought something might have "broke loose" so he asks the Board Operator to try opening the control valve again. Outside Operator still sees no flow on the flow meter but does not make another effort to visually verify this condition. Note: the tank level is now at approximately 7.7 ft. at this time. Outside Operator gets a call to perform other unit duties and tells the Board Operator to call him when he wants to try again. Outside Operator leaves the manual block valves at the control valve station in the open position. Board Operator leaves the control valve in the closed position (confirmed by process control data).

09:37 - Tank 731 high level alarm sounds in the control room Tank level is at approximately 8.5 ft. Board Operator acknowledges the alarm. About a minute and a half later the alarm is disabled.

09:49 - Alarm B45002L on the Beavon-Stretford unit sounds, indicating an Emergency RGG-One Fire Eye went out. This event and alarm is associated with on-going unit operations to move Pit Sweep from the SBS to Beavon-Stretford.

09:50 - Tank 731 appears to overflow (i.e., chart flat lines).

10:00 - SO_2 alarm (A47710) sounds at 4 ppm, but quickly climb to 25 ppm (maximum instrument reading). At about the same time, emergency alarm B45002LL at the Beavon-Stretford goes off, indicating both fire eyes on the RGG went off, causing it to trip. Board Operator contacts Outside Operator via radio and asks him to check it out at the Beavon-Stretford unit

~10:25 Based on interviews, at approximately this time exposed workers make their way to area southeast of affected area and report odor and irritation problems to their Job Rep.

~10:31 Based on interview with Outside Operator, at approximately this time the manual block valves around the control valve were closed by Outside Operator.

10:48 Ambulance requested

10:54 Unit evacuation alarm sounded by unit asset supervisor

11:33 SO_2 concentration drops below 4 ppm (alarm set-point) on analyzer (A47710).

13:18 SO_2 concentration is non-detectable at analyzer (A47710).

Safety Control Structure

The safety control structure (process safety management system) consists of the controls that have been implemented to prevent hazards. In order 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 6 shows our best reconstruction of the safety control structure from what we could glean in the accident report and from our knowledge of the process industry in general. It is very general and we realize there are almost surely many errors in it, but this was the best we could do. It is adequate for our demonstration.

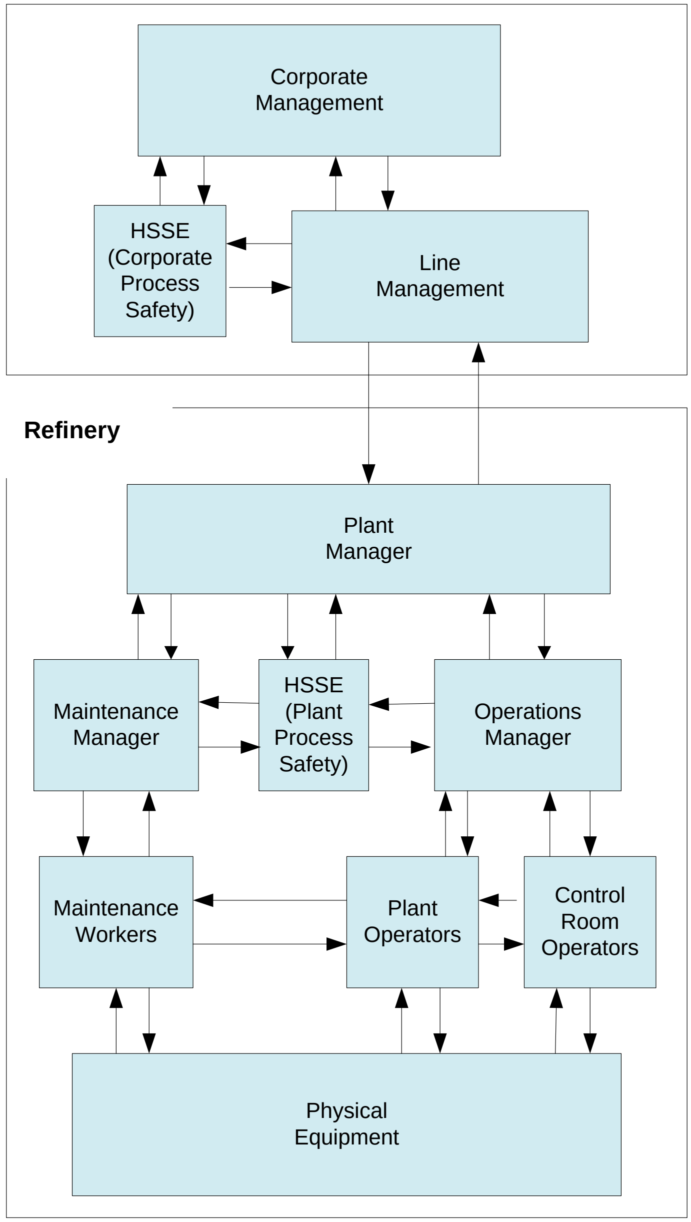

Figure 6. A Simplified Safety Control Structure (almost surely incorrect)

Each of the components in the safety control structure has particular responsibilities with respect to safety. As we have very little information about the actual responsibilities assigned to each group at the company, we inferred responsibilities that seemed reasonable to us. For example, we assumed that the maintenance group was responsible for maintaining safety-critical equipment (as opposed to some special group being given this responsibility) and that HSE (safety engineering) was responsible for performing hazard analyses and risk assessments and producing safety-related operator procedures. An accident analysis using STAMP involves determining whether these responsibilities were carried out and, if not, why not. If we have inadvertently mis-assigned responsibilities, it has 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.

The component responsibilities are identified in the analysis of each component that follows.

Physical Process Analysis

After the control structure has been constructed, the next step is to examine each component, starting with the lowest physical controls and progressing upward to the social and political controls.

The analysis of the physical controls does not differ significantly from that done in most accident analyses. We start by looking at the physical plant safety controls at the bottom of the safety control structure and work upward. We include only those controls related to the specific SO_2 event although we tried to include general responsibilities as far as we could deduce them. The report is not as complete as it would have been if we had collected more information than that provided in the original accident report and in the response to a few questions we were able to ask about the incident. But it serves to demonstrate the power of this approach compared to a standard accident analysis.

SO_2 is a colorless gas with a pungent odor. The acid evolved sulfur dioxide to atmosphere as it overfilled to the ground. SO_2 causes respiratory tract, skin, and eye burns at high concentrations. Workers who were exposed during the incident reported feeling a burning sensation in their eyes, nose, throat, and lungs.

The design of Tank 731 allows for vapor that is entrained in the acid to degas off to another tower, T707, where it can be further treated. As this tank overfilled, SO_2 entrained in the solution did not have sufficient residence time to degas properly. As a result, the acid evolved sulfur dioxide to atmosphere as it overfilled to the ground. The drain was blocked and thus the SO_2 could not flow into the process sewer.

The plant safety equipment (controls) was 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 provide emergency equipment to treat exposed individuals. It appears that this refinery has the standard types of safety equipment installed.

Physical Controls and Safety Related Equipment

Requirements (roles/responsibilities): 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. Convert released chemicals into a non-hazardous or less hazardous form
4. Contain inadvertently released toxic chemicals
5. Provide feedback to operators and others about the state of safety-critical equipment
6. Provide indicators (alarms) of the existence of hazardous conditions
7. Provide protection against human or environmental exposure after release
8. Provide emergency treatment of exposed individuals

Emergency and Safety Equipment (controls): Only those related to the Tank 731 overflow and subsequent events are included.

- Flow meter and level transmitter
- Block valves, bypass valve
- SO_2 alarm
- High level alarms
- SO2 alarm (analyzer): Strobe light
- Unit evacuation alarm
- Drain from containment area to process sewers
- Process vent routed to T-707 from T-731.
- Overflow pipe with gooseneck
- RV

Failures and Inadequate controls: (the links below refer to the requirements above)

- SO_2 released to atmosphere (→ 2)
- Control flow valve may have stuck open (→ 2)
- Level transmitter L47731A for Tank 731 was not working properly. Readings had been erratic for a year and a half. This meant that one of the high level alarms was effectively disabled. (→ 5)
- Flow meter FT47706 was not working properly (→ 5)
- Drain to emergency containment sewer clogged. (could not send excess gas to safe containment area) (→ 4)
- Alert for harmful release of toxic SO_2 is visual and could not be seen by workers in path of released gas. SO_2 analyzers on the SVS alarm trigger flashing strobe lights on the unit, but no audible alarm so they are only effective if they are within the workers line of sight. Several of exposed workers were over 100 yards from the unit and were not able to see the flashing lights. (Because SO2 is a gas, it has the potential to travel away from the unit and around objects to reach workers who may not be able to see the flashing strobe lights.) (→ 5)

Physical Contextual Factors:

- Wind was from NNE at about 9 mph.

(The links in the Failures and Inadequate Controls section refer to the requirements listed above it.)

While there was a reasonable amount of physical safety controls provided, much of this equipment was inadequate or not operational, as noted on the previous page. For example, the level transmitter on the tank was not working properly, the flow meter was not working properly, and the drain to the emergency containment sewer was clogged. The report does not go into why the sewer was clogged and whether this was a common occurrence. While the sewer would not have prevented the overflow, it seems to us that the pooling of the SO_2 in the containment area contributed to the amount of gas in the air and the level of exposure of the workers to this gas.

The failures and inadequate controls raise many questions not included in the original accident report. Were non-functioning or inadequately functioning critical physical controls unusual or was it common at the plant? What types of operational policy exists (in written form or implicit in the culture) about operating a unit with safety equipment out of order? Is a risk assessment done when operations occur under those conditions? What types of inspections are performed on safety-critical equipment? How is safety-critical equipment identified? What was the maintenance policy and why was safety-critical equipment non-operational or operating erratically for relatively long periods of time? Most of these questions are raised later under each of the appropriate safety control structure components.

Safety Control Structure Analysis

The next step in the accident analysis is to determine why the physical system events occurred by examining the higher level control components. The analysis uses the identified responsibilities to determine any inadequate control provided by the component that might have contributed to the loss event. For each component in the safety control structure, the following are identified:

- The safety-related responsibilities of the component
- The component's control actions related to the loss
- The context in which those actions occurred
- Potential process model flaws that led to the inadequate control actions by the component

We start from the assumption that most people have good intentions and do not purposely cause accidents. We need to understand, then, why they did the wrong thing in the particular situation in which they found themselves. In particular, we are interested in the contextual or systemic factors and flaws in the safety control structure that influenced that behavior. For example, the operator or manager may have a mental model that is inconsistent with the real process state and therefore they provide inadequate control. At this refinery, for example, the Board Operator thought that there was no flow because the flow meter showed no flow. There also was missing feedback about the state of the controlled process such as the level of liquid in the tank. The same is true at higher levels of the control structure. For example, the accident report says that there had been previous instances of the units not being properly evacuated in situations where workers may have been at risk. Did the higher levels of management responsible for safety at the refinery know about these instances and just not do anything about it or were they missing feedback about inadequate evacuation procedures and behavior at the refinery? If they had known, we suspect they might have done something about it before the Tank 731 overflow although we cannot know this for sure. We can determine, however, the changes that need to be made to improve the chances that it will not happen again.

In order to minimize hindsight bias, our emphasis in explaining human actions is on understanding why it made sense at the time for the people to act the way they did. We get this information by looking at the context in which the actions took place and the mental (process) model flaws that contributed to the inadequate control.

Board Operator

***Safety-Related Responsibilities*:**

- Provide control actions that avoid hazardous states in the plant.
- Respond appropriately when a potentially hazardous condition or event arises.
- Report incorrectly functioning equipment.

***Context*:**

Related to Tank Level:

- Flow meter was broken: Indicated no flow
- Level transmitter L47731A and its high-level (7.5ft) alarm were not functioning properly. The level transmitter had been erratic since January 2006 but a work order was not written to repair it until July 2008.
- Level transmitter L47731 and its high-level (8.5ft) alarm were functioning.
- Level transmitters gave conflicting information regarding tank level.

Related to Risk and Procedures:

- No written unit procedure for responding to an SO_2 alarm. The "standard response" to an SO_2 alarm on the SBS unit is to have operator conduct a field assessment of the situation.
- No written procedure for ordering evacuation when an SO_2 alarm sounds or criteria established for the level of SO_2 that should trigger an evacuation alarm.
- Unit training material does contain information on the hazards of SO_2, including IDLH information, but this information has not been instituted in standard operating/emergency procedures.
- Block valves normally left open to facilitate remote operations.

Related to Alarms:

- Distracted by other duties related to transferring the Pit Sweep from the SBS to the Beavon-Stretford, which demanded his attention during the time of this incident.
- An alarm indicating that the RGG fire eye went out sounded just before the operating level sensor reached maximum value (no alarm generated).
- Ten minutes later, an alarm indicating that both RGG fire eyes went out sounded at approximately the same time as the SO_2 alarm. This means that multiple alarms were going off at the same time.
- Previous SO_2 alarms were attributed to minor releases that did not require a unit evacuation. Such alarms occur approximately once a month.
- None of alarms were designated as critical alarms, "which may have elicited a higher degree of attention amongst the competing priorities of the Board Operator."
- Upper detectable limit on SO_2 analyzers is 25 ppm. During the incident, analyzer A47710 maxed out at 25 ppm almost instantly, making it impossible to determine the actual SO_2 concentration during the incident.
- There is no established criteria in a written procedure for what SO_2 levels and/or alarms constitutes an emergency condition that should trigger sounding the evacuation alarm. There is also no specific SO_2 ppm threshold for unit evacuation.
- In past, units were not evacuated by blowing the horn, but rather by operations personnel walking through the unit and stopping work.
- Evacuation alert must be sounded by hand, no written procedure for doing so.

***Control actions related to the loss*:**

Control Valve:

- Opened control valve at 8:33. Flow meter does not indicate a flow.
- At 09:25 opened control valve to 44% of open position for about 2 minutes, then closed it.

Alarm:

- At 9:37-9:39: Board Operator acknowledges and disables tank 731 high level alarm. Takes no other action.
- Did not communicate the high-level tank alarm to the Outside Operator
- Delayed sounding evacuation alarm until 54 minutes after the SO_2 was detected by analyzer A47710.

***Process Model Flaws*:**

Tank:

- Believed there was no flow into tank.
- Did not know that flow meter was not functioning.
- Did not know that level transmitter L47731A was not functioning.
- Did not know that level transmitter L47731 indicated a rising tank level. Believed the liquid level was "tickling" the sensor and triggering a false alarm.

SO_2 Risk

- Was not aware of hazards to human health due to SO_2 exposure.
- Was not aware of risk of SO_2 release via tank overflow.
- Did not know the process sewers were clogged, which would increase the amount of SO_2 in the air in case of a tank overflow.
- Did not know SO_2 release warranted evacuation order.
- Was not aware of actual levels of SO_2 but only maximum reading of 25 ppm.

Plant:

- During the incident, did not appear to have a "full awareness" of all the work being performed by people near the unit.

The operator clearly was confused about the level and flow of SO_2. One way to help clarify why this occurred is to examine the information the operator had at each point in time where critical decisions were made. The Board Operator first attempted to open the control valve to begin the acid drawdown at 8:33. The operator's process model at the time looked like the following:

Board Control Valve Position: ***open***	Flow Meter: ***shows no flow***
Manual Control Valve Position: ***open***	Flow: ***none***
Bypass Valve: ***closed***	SO_2 alarm: ***off***
Level on tank: **7.2 feet**	High level alarm: ***off***

We have left the two redundant level indicators off the process model because we are not sure what information they actually provided. The report says that one was behaving erratically and providing fluctuating readings at the time of the incident. If at least one did provide accurate information, then the question that needs to be answered is why that information was not used by the Board Operator. There are so many different possible explanations for this omission that it would not be helpful to guess; the reason needs to be carefully investigated. We left it out of his process model as apparently the Board Operator did not use that information or discounted it in preference to the other information he had. We were told that the operational level indicator did indicate 7.2 feet but we do not know if or how that reading changed over time or whether the Board Operator even looked at it.

At this time the flow meter shows no flow, so the Board Operator calls the Outside Operator to see if the manual block valves are perhaps closed. He believes they are usually left open to facilitate remote operation.

Between 9:11 and 9:25, the Outside Operator works the manual block valves to see if he can fix the problem. He hears a clunk and asks the Board Operator to try opening the control valve again. He tries, but they both still see no flow on the flow meter. The Outside Operator gets a call to do something else and leaves the manual valve in the open position. The Board Operator's process model at this time is:

Board Control Valve Position: ***open***	Flow Meter: ***shows no flow***
Manual Control Valve Position: ***open***	Flow: ***none***
Bypass Valve: ***closed***	SO_2 alarm: ***off***
Level in tank: **7.2 feet**	High level alarm: ***off***

At 9:25, when the Outside Operator left, the Board Operator closes the Board Control Valve. There is no way for the Board Operator to get confirmation that the valve has actually closed—the valve was not equipped with a valve stem position monitor so the Board Operator only knows that a signal has gone to the valve for it to close. The operators in many accidents, including Three Mile Island, have been confused about the actual position of the valve due to similar designs. While obtaining actual position information adds extra expense, the cost may be justified for critical information.

Board Control Valve Position: **closed**	Flow Meter: ***shows no flow***
Manual Control Valve Position: ***open***	Flow: ***none***
Bypass Valve: ***closed***	SO_2 alarm: ***off***
Level in tank: **7.2 feet**	High level alarm: ***off***

The report writers calculate that the flow actually started sometime between 9:11 and 9:25. So clearly the Board Operator's process model was now incorrect but there was no feedback or information available to the Board Operator to use to detect this mismatch. The report calculates that the actual level in the tank was 7.7 feet at 9:25. There is an alarm at 7.5 feet, but it was not working at the time. In answer to our questions, we were told that the operator did not know that the alarm was not working so it seems reasonable to us that the operator would conclude that the level in the tank had not risen above 7.5 feet given that he believed there was no flow into the tank and the 7.5 foot alarm had not sounded.

At 9:37 (twelve minutes later), the Tank 731 high-level alarm sounds in the control room. The tank level must have been at 8.5 feet at the time as that is the level of the second alarm (which was working). The Board Operator's process model now is:

Board Control Valve Position: **closed**	Flow Meter: ***shows no flow***
Manual Control Valve Position: ***open***	Flow: ***none***
Bypass Valve: ***closed***	SO_2 alarm: ***off***
Level in tank: **7.2 feet**	High level alarm: **on**

Note that the information the Board Operator has is that the input valve is closed, there is no flow into the tank, and the bypass valve is closed. He acknowledges the alarm, assumes it is spurious, and one and a half minutes later turns the alarm off. He takes no action because he says he believed the liquid level was "tickling" the sensor and triggering a false alarm. In response to our questions, we were told that it is possible for the Board operator to determine the liquid level by "trending the data on the control board" (calling up the trend level data) but the operator did not do this. From what we can determine, the operator must request the trend data—it is not normally shown on the control panel by default. The Board Operator at this point had no reason to believe he needed it. His process model now at 9:39 is:

Board Control Valve Position: **closed**	Flow Meter: ***shows no flow***
Manual Control Valve Position: ***open***	Flow: ***none***
Bypass Valve: ***closed***	SO_2 alarm: ***off***
Level in tank: **7.2 feet**	High level alarm: **off**

At 9:49, an alarm on another unit sounded and the operator switched his attention to that. At 9:50 Tank 731 overflowed. At 10:00, the SO_2 alarm sounded at 4 ppm but quickly climbed to 25 ppm, which was the maximum reading. At the same time, there was another emergency alarm at another unit. The Board operator calls the Outside Operator to tell him to check out the other unit.

At this point we need more information than we were able to obtain from the accident report to try to determine why later actions or non-actions occurred. It is clear, however, that the Board Operator's process model was incorrect. To prevent such a mismatch in the future, changes need to be made in the system in order to get better information to him. Such changes may involve different training, different procedures, different feedback channels, control room changes, engineering changes, maintenance changes, etc. Simply saying the operator made a mistake is not helpful without a careful analysis of why and how to prevent it in the future.

Hindsight bias often plays a role in the analysis of accident causes. Knowing the outcome of a sequence of events can easily bias an investigation toward those data points that after the accident we know were significant and showed the real nature of the situation. Without knowledge of the outcome, however, those data points may appear much less significant. Accident investigators need to put themselves in the situation of the operators at the time, with multiple interleaving and overlapping of tasks, other indications and alarms that need attention, and often ambiguous and conflicting data upon which to make decisions.

Hindsight bias occurs because accident investigators know and start from the outcome and trace back to the assessments and decisions that led up to it. Tracing back through the causal flow, it is easy to see where operators could have done something to avoid the outcome—where, as Dekker says, they could have zigged instead of zagged [Dekker 2009]. The question that needs to be answered in the investigation is not what the operators should have done in order to avoid the outcome we now know given our later understanding of the situation. The question needing to be answered is why the operators did what they did given their understanding of the situation at the time (which did not include the outcome) and what changes can be made to help them make better decisions under those same circumstances in the future.

There are several instances of hindsight bias in the official accident report relevant to the operators' role in the incident. For example, the report says:

> "The available evidence should have been sufficient to give the Board Operator a clear indication that Tank 731 was indeed filling and required immediate attention."

The report does not expound on what that evidence was. From our reading, the majority of the evidence the operators had did not indicate the tank was filling and, in fact, indicated the opposite as shown above. The operator did not use his data trending tool, but there was little reason to do so before the actual emergency (overflow) occurred and after that time it was irrelevant.

Another example was the statement:

> "Interviews with operations personnel did not produce a clear reason why the response to the SO_2 alarm took 31 minutes. The only explanation was that there was not a sense of urgency since, in their experience, previous SO_2 alarms were attributed to minor releases that did not require a unit evacuation."

We are confused by the conclusion that there was no clear reason for the delayed response as the explanation provided in the second sentence seems completely clear and reasonable to us, particularly as nuisance alarms were relatively common (they occurred about once a month).[1] The delay in responding to the alarms seems understandable given the fact that past alarms had not been important, other (unrelated) alarms were sounding at the same time that required the operators attention, and all the information the operator had about lack of flow into the tank supported the conclusion that the tank level alarm was spurious and (after the analyzer alarm sounded) the release was minor and did not require a unit evacuation. The analyzer alarm maxed out at 25 ppm so the Board Operator had no indication of the real level (which was much higher).

To understand completely why the Board Operator's process model was so clearly incorrect and his behavior not what was, in hindsight, desirable, a full human-factors analysis of the operator interface to the plant is required. Such a human factors investigation should be part of all accident investigations where, as in this case, the operator was confused or unaware of the actual state of the plant or made assumptions that were incorrect. There is probably a reason for each of these mistakes and they need to be carefully investigated so that appropriate changes can be made for the future. There are very likely a lot of explanations for the operator's behavior related to system and plant interface design that a full human factors analysis would detect. We could not perform such an analysis due to lack of information about the design of the control room and the Board Operator's control interface.

There is one other clue provided in the accident report to explain some of the Board Operator's behavior. The report notes that the Board operator "did not demonstrate an awareness of risks associated with overflowing the tank and potential to generate high concentrations of SO_2 if the surfuric acid was spilled." There is no explanation of why this might have been true. Is there a deficiency in the training procedures about the hazards associated with his job responsibilities? If the explanation is that this particular operator is simply incompetent and although exposed to effective training did not profit from it, then the question becomes why such an operator was allowed to continue in that job and why the evaluation of his training outcomes did not detect this deficiency.

[1] This information was not in the accident report but was provided in a response to one of our questions Apparently such nuisance alarms are caused by sampling errors or other routine activities.

One of the common problems in systems with multiple controllers is confusion and coordination problems about who should be doing what and what the other people are doing. It is very likely that coordination problems occurred here, but we cannot tell from the information in the accident report alone. As will be noted later, the safety policy, as currently written, seems to ensure that such coordination problems will occur.

One other inadequate control action related to the loss was the lack of a work order reporting the erratic behavior of the level transmitter for a year and a half after it started acting erratically (January 2006). We have too little information to understand why this time lag occurred, but it is an important question that should have been answered in the accident report.

Outside (Field) Operator:

Safety-Related Responsibilities:

- Provide control actions that will avoid chemical release
- Sound evacuation alarm when an exposure occurs

Context:

Related to Risk and Procedures:

- No written unit procedure for responding to an SO_2 alarm. The "standard response" to an SO_2 alarm on the SBS unit is to have operator conduct a field assessment of the situation.
- No written procedure for ordering evacuation when an SO_2 alarm sounds or criteria established for the level of SO_2 that should trigger an evacuation alarm.
- Unit training material does contain information on the hazards of SO_2, including IDLH information, but this information has not been instituted in standard operating/emergency procedures.
- Time required to conduct a field assessment varies based on specific circumstances.
- Some said it was standard operating procedures to leave the manual block valves open while others said it was SOP to leave them closed. No written procedures or protocols provided

Related to Alarms:

- Distracted by other concerns related to transferring the Pit Sweep from the SBS to the Beavon-Stretford, which demanded his attention during the time of this incident. An alarm indicated that the RGG fire eye went out.
- No way to determine actual level of SO_2. Alarm maxes out at 25 ppm.
- Previous SO_2 alarms were attributed to minor releases that did not require a unit evacuation. Such alarms occur approximately once a month.
- In past, units were not evacuated by blowing the horn, but rather by operations personnel walking through the unit and stopping work so a "reluctance to hit the evaluation horn is apparent among some operations personnel."
- None of alarms designated as critical alarms. No established criteria in a procedure for what SO_2 levels constitute an emergency condition that should trigger sounding the evacuation alarm.

Control actions related to the loss

Control Valve:

- Leaves manual block valves in open position.
- At 10:00 Field Operator checks on the Beavon-Stretford unit at behest of board operator

Emergency Response:

- 31 minutes transpired from time SO_2 alarm sounded until Outside Operator reached unit, conducted an assessment, and implemented measures to stop the release.
- Put himself at risk by entering the immediate area to close the manual block valves instead of allowing properly equipped emergency personnel to handle the release.

Process Model Flaws:

Tank:

- Believed there was no flow into tank.
- Did not know flow meter was not working so thought tank was not filling when it was.
- Did not know that board operator had erratically functioning level indicators and a non-functioning alarm.

SO_2 Risk

- Knew a significant release was occurring but did not know analyzer had maxed out at 25 ppm or that IDLH concentration for SO_2 was 100 ppm.
- Was not aware of risk of SO_2 release via tank overflow.
- Did not know SO_2 release warranted evacuation order.

Emergency Response:

- Felt he had the authority to call for a unit evacuation but was not sure that conditions were bad enough to make that call during this incident.

Plant:

- Did not have "full awareness" of all work being performed on or near the unit

The process model for the Outside Operator could be used to understand his behavior as was done for the Board Operator. But his model is pretty simple: he believed there was no flow because the (non-functioning) flow meter said that was so. The Board Operator and Outside Operator both see the output from the same sensor indicating flow. In this case, that sensor was faulty. The only other information he had came from the Board Operator, whose process model and process feedback information was also incorrect. The Outside Operator has no other direct indicator of the level in the tank. He did not make a second effort to visually verify the flow at 9:25 because he was in a hurry to get to the simultaneous but unrelated trip of equipment in another part of the unit.

The primary mistake (in hindsight) made by the Outside Operator concerned the delay in the evacuation alarm and his attempt to clean up the spill instead of immediately seeking help. The official accident report says that the evacuation signal was delayed because the field operator was not sure the conditions were bad enough to make that call. The Outside Operator also seemed to have a poor understanding of the risks of an SO_2 release. Once again, several reasons could exist for this, but no matter what the reason, it is clearly something that needs to be remedied—not just for SO_2 but also for the risks of the plant in general. An audit should be performed to determine if SO_2 release is the only hazard that is not understood and if these two operators are the only ones who are confused.

In addition to examining the training and understanding of the hazards by the operations personnel, the procedures for sounding evacuation alarms need to be examined. If there is a potential for operators to make poor decisions in safety-critical situations, then they need to be provided with the criteria to make such a decision. Expecting operators under stress and perhaps with limited information and training to make such critical decisions based on their own judgment is unrealistic: It simply ensures that operators will be blamed when their decisions turn out, in hindsight, to be wrong.

The other training or procedural deficiency here beyond not sounding the alarm, i.e., the operator trying to fix the problem rather than calling in emergency personnel immediately, also needs to be more carefully examined. In fact, this response is the *normal* one for humans; if it is not the desirable response then procedures and training must be used to ensure that a different response is elicited. The role of the current company safety policy is discussed later.

If the company wants the flexibility inherent in real-time decision making rather than strict procedures, then they will need to provide much more extensive training and better real-time information to the operators.

HSE (Process Safety):

Safety-Related Responsibilities:

- Perform hazard analyses and identify safety-critical procedures and equipment
- Conduct risk assessments and develop operating procedures that adequately control the risk associated with safety-critical operations.
- Inform operators about critical processes and alarms.
- Audit safety-related equipment
- Provide MoC and CoW procedures for safety-critical operations.
- Ensure that all plant personnel have adequate training about:
  - The risks of chemicals and materials at their place of work
  - The risks associated with their job
  - How to perform their job safely
  - Proper emergency response

Context: Unknown

Control actions related to the loss

- Unit training information does contain information on the hazards of SO_2 but this information has not been instituted in standard operating/emergency procedures.
- None of the high level alarms were designated as critical alarms
- Did not provide any risk-assessed operating procedure for drawing down acid and filling Tank 731.
- No specific unit procedures or other protocols that define critical operational parameters were provided
  - Sequence to initiate the drawdown process (e.g., notification of Outside Operator, manual block valve positioning, etc.)
  - Process control parameters (e.g. drawdown initiation and endpoint, specified flow rate into the tank, safe level at which Tank 731 is considered full)
  - Sequence of steps necessary to conclude and secure the tank filling process (e.g., closing block valves)
  - Appropriate response to alarms (e.g. high level alarm, SO_2 alarm)
  - Clear conditions for evacuation, including SO_2 ppm level "There is not established criteria in a procedure for what SO_2 levels and/or alarms constitutes an emergency condition which should trigger sounding the evacuation alarm"

Process Model Flaws: Unknown

Because the report focused on the operators' role in the incident and not on the role of other groups, we cannot provide information about the context or the process model flaws that might have existed for components of the safety control structure that were involved in the accident process but were not examined in the accident report. The inadequate control actions included on the previous page did occur, but there is no way to determine the reason for them. This would be important information to obtain in determining how to fix any systemic problems. For example, how are critical alarms identified and why were these alarms not identified as such when they clearly were involved in a serious incident? Is such a determination done using HAZOP? If so, are there problems in performing HAZOP effectively in these circumstances? Alternatively, are the problems perhaps in the criteria used to label alarms as critical?

We asked whether the HAZOP had identified the alarms as critical and were told that it had not identified a critical alarm for this application. A hypothesis for why not is that it was "probably because it was an infrequent batch operation." If HAZOP is not useful for infrequent batch operations, then a different hazard analysis method should be used or the HAZOP procedures changed or augmented.

We were told that the omission of criteria for which SO_2 levels and/or alarms constitutes an emergency that should trigger sounding the evacuation alarm was simply an oversight. What procedures are in place to detect or prevent such oversights? It seems that any identified hazards should have procedures in place for responding if the hazard occurs so either the hazard was not identified or there was no procedure for checking that there is a response for all identified hazards.

What criteria have been established at the company for determining what emergency procedures are provided to the operators? The report says that there is a safety policy (C-13) that states: *"At units, any employee shall assess the situation and determine what level of evacuation and what equipment shutdown is necessary to ensure the safety of all personnel, mitigate the environmental impact and potential for equipment/property damage. When in doubt, evacuate."* There are two problems with such a policy.

The first problem is that evacuation responsibility does not seem to be assigned to anyone but can be initiated by all employees. The consequence of such lack of assigned control responsibility is usually that everyone thinks someone else will take the initiative. Responsibility for sounding alarms must be assigned to someone. Others may report problems and even sound an evacuation alert when necessary, but there must be someone who has the actual responsibility, accountability, and authority, and there should be backup procedures for others to step in when that person does not execute their responsibility acceptably.

The second problem is that unless the procedures clearly say to sound an alarm, humans are very likely to try to diagnose the situation first. The same problem pops up in many accident reports—the operator is overwhelmed with information that they cannot digest quickly or do not understand and will first try to understand what is going on before they sound an alarm. If the company wants employees to sound alarms expeditiously and consistently, then the safety policy should specify exactly when alarms are required, not leave it up to personnel to "evaluate a situation" in which they probably are confused and unsure about what is going on (as in this case) and under pressure to make quick decisions under stressful situations. How many people, instead of dialing 911 immediately, try to put out a small kitchen fire themselves? That it often works simply reinforces the tendency to act in the same way during the next emergency. And it avoids the embarrassment of the firemen arriving for a non-emergency.

Maintenance:

Safety-Related Responsibilities:

- Ensure that all safety-related equipment is in proper working order.

Context:

- Large backlog of maintenance work orders associated with unit equipment.

Control actions related to the loss

- Did not meet target of 4 weeks (28 days) average age of a "safety" work order. Average age was 86 days. In particular, did not fix flow meter (FT47706) and level transmitter (L47731A) involved in the incident for an extended time.
- The level transmitter L47731A had supposedly been fixed on July 25, but it was not functioning properly at the time of the incident 2 weeks later. Was this a result of inadequate repair or perhaps inadequate testing after the repair?

Process Model Flaws:

Unknown

Questions that need to be answered here are why the level transmitter was not working so soon after it was supposedly fixed, why safety work orders were so delayed, whether plant and corporate management knew this and what they were doing about it (if anything), etc. If the targets are impractical and unobtainable, then the targets need to be re-evaluated or more resources applied. There was a seemingly large number of non-functioning or erratically functioning equipment in this unit. Was this unusual or is it a problem throughout the refinery? Is the problem actually in HSSE because critical alarms are not being properly identified?

In response to our questions, we were told that the Maintenance Manager was aware of the backlogs and was working on reducing them. Some of the problem was bad data—work orders that had been completed but not closed, work orders marked as safety related but not really a safety issue, etc. Because of the difficulty in managing something with bad data, ways to improve the data should be developed.

Operations Management:

Safety-Related Responsibilities:

- Ensure operators have the information they need to carry out their tasks, including information about the current state of the equipment they are operating
- Ensure operators have been given adequate operational procedures and training on how to implement them and audit to ensure that the training is effective.
- Ensure operators understand the hazards associated with the equipment they are operating and audit to ensure that training is effective.
- Provide reporting channels for malfunctions and assign responsibility. Ensure that communication channels are effective and operating correctly.
- Ensure emergency procedures are being executed properly.

Context: Unknown

Control actions related to the loss:

- Allowed unreported malfunctioning safety-related equipment for 2.5 years
- Did not respond properly when past evacuation alarms were provided inadequately (no horn and use of verbal commands only)
- Was appropriate training provided? Were there audits to check the effectiveness of the training? Gun drills were apparently not run on this process.

Process Model Flaws: Unknown

Again, it is difficult to analyze the role of operations management because so much was left out of the accident report.

Emergency procedures are the basis for gun drills at the refinery. But there were no emergency procedures provided for this procedure. We learned that there is a refinery "gun drill" policy and matrix that list requirements (which procedures, how often, etc.). This policy needs to be reviewed as adequate gun drills were not done for this unit. The official accident report recommends running a gun drill on this unit but not evaluating the policy for determining when gun drills are done.

The training coordinator is responsible for training operators on hazards, and we have been told that unit training includes a review of the hazards of the acid stream. The effectiveness of this training should be evaluated given the incident and the operators' responses.

The Control of Work status board was not effective in notifying the operators about where work was occurring around the unit. Why not?

Why the evacuation horn had been delayed or improperly used in the past has not been thoroughly investigated. Two possible reasons provided to us in response to our questions is that (1) the hazard or extent of the situation was not understood and/or (2) the operators tried to handle the situation internal to the unit instead of sounding the evacuation alarm (which calls attention to the incident). This should be investigated further beyond the reasons hypothesized in the report that a precedent had been set. While that may be true, there are many other even more plausible reasons that could have caused it. Solutions can then be proposed. It is also important to understand why management did not know about this behavior or, if they did, why they did not take measures to change it. It seems extremely important to answer such questions.

Plant Management:

Safety-Related Responsibilities:

- Ensure that plant is operated in a safe manner, that appropriate safety responsibilities (and authority and accountability) have been assigned, and that everyone is carrying out their safety-related responsibilities.

Context:

Unknown, probably lots of performance pressures together with less pressure for his or her safety-related responsibilities.

Control actions related to the loss

- Allowed a large maintenance backup of safety-related equipment over the target dates
- Allowed lots of safety lapses in plant operations.

Process Model Flaws:

- Probably lots of wrong information, e.g., did they know about maintenance backlogs? Did they know about lack of risk-assessed procedures? Did they understand the risk in current plant operations?

Plant management has responsibility for ensuring that the plant is run safely. Either the plant management did not know about the inadequacies of operations at the plant (and that is the problem that must be fixed) or they did not take adequate steps to fix the problems. The latter could have resulted from many factors, none of which are included in the accident report so we cannot determine why the necessary steps were not taken. Some common reasons are that the feedback about safety at the plant is inadequate, safety risk is judged to be low and other risks (financial, etc.) are judged to be greater, reward structures for management are not appropriate, etc. In a complete accident/incident report, the role of plant management must be investigated and analyzed as carefully as that of the operators and lower-level managers.

Corporate Management:

Safety-Related Responsibilities:

- Ensure that company facilities are operated in a safe manner, that appropriate safety responsibilities (and authority and accountability) have been assigned, and that plant managers are carrying out their safety-related responsibilities.
- Establish an appropriate reward structure for safe behavior.

Context:

Unknown, probably lots of performance pressures and less pressure for safety-related responsibilities and oversight

Control actions related to the loss

- Allowed at least one refinery to be operated with many safety deficiencies.

Process Model Flaws:

- Probably lots of wrong information, e.g., did they know about maintenance backlogs? Did they know about lack of risk-assessed procedures?

Again, little information is available. And, again, the reasons for the inadequate control over safety at this level needs to be identified and fixed.

Corporate HSE:

Safety-Related Responsibilities:

- Ensure that plant is operated in a safe manner, that appropriate safety responsibilities have been assigned, and that everyone is carrying out their safety-related responsibilities.

Context:

Unknown, probably lots of performance pressures and less pressure for safety-related responsibilities and oversight

Control actions related to the loss

- Did not provide high-level policies for performing effective hazard analysis, etc. or they were provided but did not know about the deficiencies in their execution.

Process Model Flaws:

- Probably lots of wrong information, e.g., did they know about maintenance backlogs? Did they know about lack of risk-assessed procedures?

Once again, there is no information about the role of this group in the incident, but from a systems thinking perspective, they clearly played a role. We will not speculate about the reasons for the inadequate control at this level.

Communication and Coordination

There was inadequate communication from operations to contractors working in the area that an incident involving release of sulfuric acid had occurred and that the SO_2 alarms had sounded. The communications between the Board and Outside operators seem good. Not enough information was provided to evaluate other types of critical communications within the plant and within the company as a whole.

Dynamics and Changes over Time

We have little information about the dynamic aspects of safety that might have contributed to the T-731 overflow incident. But the answers to some questions we asked gave hints that changes over time may have been involved in the problems. For example, to our question about why there was no established criteria in a procedure for what SO_2 levels and/or alarms constitutes an emergency that should trigger sounding the evacuation alarm, the answer provided was “Just not thought of before—perhaps it was ‘not required’ before when there were many experienced personnel in the units.” Has the level of experience of personnel changed significantly over time? In general, has the behavior of the components in the safety control structure degraded and why?

Recommendations from the STAMP-Based Analysis

Equipment:

Not having access to engineering design information for the plant, it is difficult for us to recommend physical design changes not recommended in the original report. For example, we do not know why the sewer was blocked or whether a redesign might eliminate that cause. Nevertheless, three equipment recommendations arise from the STAMP analysis that were absent from the official accident report:

1. Change the SO_2 alarm to be audible and can be heard by people in the affected areas who are not in the line of sight of the strobe light alarm.
2. Determine why the sewer was blocked and improve the design or procedures to avoid this in the future.
3. Safety-critical indicators should show actual state and not just commanded position. A hazard analysis could be used to determine where additions or changes are needed.

Management and Engineering:

1. Review procedures for deciding when to do risk assessments of operating procedures.
2. Establish and enforce procedures for writing work orders for non-routine operations.
3. Evaluate normal operating levels of tanks and alarm settings (is it appropriate to routinely operate a tank at 0.3 ft below the alarm threshold?).
4. Investigate frequent spurious alarms. Determine the root causes and establish ways to reduce their frequency.
5. Consider adding an alarm to indicate rising tank level when the control valve has been commanded closed.
6. Consider a way to easily and clearly mark malfunctioning gauges/meters for the operators.
7. Consider adding a policy where manual block valves are left closed when it appears that flow is not occurring and should not occur instead of depending on the Board Operator's control valve only (creates a single point of failure).
8. If the standard response to an alarm is to have a field operator check it, then need some instructions on what to do if the field operator is not immediately available. Alternatively or in addition, use dedicated operators for non-routine batch operations (as this was) when practical.
9. Define safe operating limits for all safety-related equipment. Establish corporate policy for doing this and ensure it is being followed.
10. Improve malfunction reporting and communication, e.g., establish a way to communicate information about all current malfunctioning equipment to operators. Determine if there are any barriers to reporting malfunctioning equipment and, if so, eliminate them.
11. Clarify the evacuation alarm procedures. The company should not just leave it up to the operators to assess the situation, particularly when the operator does not have all the necessary information to make a proper decision. Rewrite the general safety policy (C-13) on evacuation procedures. [This recommendation conflicts directly with the related recommendation in the official report, which suggests reinforcing the current policy with the operators.]
12. Investigate why in the past the evacuation alarm was not handled appropriately.
13. Perform a full human-factors analysis of the operator's interfaces to the plant to determine what changes are necessary to ensure improved control by the operators in the

future. This will require a major effort but will be much less effort if such analyses are done (as they should be) at the time the interfaces are originally designed.

14. Redesign maintenance activities or provide additional resources to ensure critical work orders are completed on time. If the targets are impractical and unobtainable, then evaluate the targets and the risk involved in changing them to more realistic values. Improve the procedures for collecting data on target achievement if that is the problem.
15. Create a system to ensure that operators understand the hazards associated with the processes they are controlling. Evaluate their knowledge and revise training procedures if necessary.
16. Evaluate and perhaps improve the CoW procedures with respect to knowing what personnel (contractors) are in the area. Determine how to provide more effective "situation awareness" of all work being performed on or near the units.
17. Evaluate the information operators have about the plant hazards and ensure they have what is required to operate hazardous processes safely both in terms of the design of feedback and in terms of ensuring that feedback channels are operational and working properly.
18. Evaluate current policy with respect to operating processes with safety-critical equipment that is known to be non-operational and establish policy if it does not already exist. While it may at times be necessary, there should be an approval process by someone who has the proper authority to evaluate and accept the risks and information should be provided to corporate management about when and how often this occurs. Before safety-critical, non-routine, potentially hazardous batch operations are conducted, safety policies should require inspection of all safety equipment involved to ensure it is operational, including testing of alarms.
19. Evaluate all operating procedures to determine whether they need to be risk-assessed and, even more important, determine how this will be done for new or changed procedures in the future. This is clearly a very large task and will take time to finish.
20. Evaluate the refinery gun-drill policy.
21. Improve the methods used to identify hazards, critical alarms and parameter values for all hazards (including non-routine batch operations), design feedback to provide operators with the real-time information they need to deal with hazards, and create procedures for operators to deal with all hazards.
22. Evaluate the safety control structure at the refinery and at the company Corporate level to determine whether it is adequate to ensure safety and make improvements if it is not. Ensure explicit specification of each component's responsibilities (and authority and accountability) and make sure each person assigned the responsibilities knows what they are and how to execute them. Determine whether each controller has the information required to effectively carry out their safety-related responsibilities. Establish procedures to periodically audit feedback channels to ensure they are operating correctly.

3.4 Comparison with Recommendations from Official Report

The official accident report identified many causal factors leading to eight recommendations. These eight recommendations are listed below. We compare them with the recommendations we generated using STAMP-based analysis of the accident.

1. Operator duty to respond to alarms needs to be reinforced with the work force.
   [This recommendation ignores the reasons for why the operators did not respond to the alarms and changing the contextual and behavior-shaping factor in the system design.]
2. Two alarm points (high and high/high) should be established for each of the redundant level sensors on Tank 731. The high alarm should be designated as a critical alarm given the risks associated with overflowing this tank.
   [Reasonable, but it ignores the other alarms at the plant. Could there be other incorrectly identified alarms and is there a flaw in the procedures for identifying critical alarms? While necessary, this action will not solve the whole problem. The alarm was ignored because it was believed to be in error, not because it was believed to be non-critical and therefore acceptable.]
3. Consideration should be given to establishing two alarm set-points for the SO_2 analyzers. The current alarm setpoint at 4 ppm provides an important warning of the release of SO_2 gas that should be investigated. Consideration should be given to establishing a second alarm setpoint at a level that triggers an immediate evacuation alarm (e.g., when the instrument maximum reading is reached).
   [Good.]
4. Implement new control of work procedures to achieve better operational awareness and control of work being performed on the unit. Process hazards and potential risks associated with operational activities should be identified by the AA and communicated to the PA for inclusion in risk assessments and crew reviews to improve the awareness of all work groups about the area hazards. Utilize process risk assessment to make more informed decisions about when to best schedule potentially hazardous operations to minimize potential risk to work crews.
   [Good]
5. Develop a risk assessed procedure for the acid drawdown process in accordance with Policy D-22 which defines critical operational parameters such as the sequence of steps required to initiate the drawdown process (e.g., notification of Outside Operator, manual block valve positioning, etc), process control parameters (e.g., drawdown initiation and endpoint, specified flow rate into the tank, etc.), the safe level at which Tank 731 is considered full, the sequence of steps necessary to conclude and secure the tank filling process (e.g., closing block valves), and appropriate response to alarms.
   [Why just this process?]
6. Consideration should be given to conducting a gun drill on the unit with a focus on how to recognize and report emergency response conditions, proper communications, and the circumstances under which a unit evacuation should be conducted.
   [Again, we believe this recommendation should be generalized to evaluating the overall gun drill policy.]
7. Unit evacuation procedure should be revised and emphasize that employees shall assess the situation and determine what level of evacuation is necessary to ensure the safety of all

personnel as stated in Safety Policy C-13. Consideration must include ongoing SIMOPs (as posted on CoW boards) in determining evacuation requirements.

[We disagree with this recommendation as stated earlier.]

8. Convene a cross function team of refinery and OCC personnel to examine "protection of workforce" issues. Areas of focus should include:
   - Evacuation – understanding and awareness of workforce
   - Evacuation – when to activate

   Specific issues to consider include:
   - Identification of potential conditions that could lead to loss of containment by the process unit.
   - Identification and planning to evacuate during unit upsets and transients, loss of instruments/view, exceeding safe operating limits / critical alarms, loss of level or filling a drum / tower, etc.

   Team recommendations should apply site-wide.

   [A good recommendation, but it could be more general. For example, what about the effectiveness of the alarms in evacuation (visual vs. aural) and the reasons why evacuation alarm procedures have not been executed correctly in the past.]

The STAMP analysis of the T-731 accident and resulting recommendations were more general and less focused on this particular incident and fixing the specific problems of this particular refinery unit. While several of the official report recommendations do tackle systemic factors, most are limited strictly to the details of this particular incident. The first one, i.e., to reinforce operator duty to respond to alarms, results from the use of hindsight bias in blaming the operators for not responding without considering the systemic factors that led them to respond inappropriately. Simply telling the operators to respond to alarms without changing those factors will not be very effective.

We were limited to the information contained in the official accident report and could not evaluate why the flawed management control actions and decision making related to the incident occurred at the higher levels of the safety control structure. To do this, we would need more information about the context in which these actions took place and about the information provided by the feedback channels to the controllers.

Appendix: Official Accident Report

SBS Tank 731 Overflow

Executive Summary

On Thursday, August 7, 2008, at approximately 09:50, the Sulfuric Acid Accumulator (Tank 731) on the SBS unit overflowed, eventually releasing approximately 2000 gallons of 30% sulfuric acid into the containment area. Tank 731 contained a 30% sulfuric acid solution which had been drawn off the T-704 quench separator recirculation line. The sulfuric acid was saturated with SO_2 which flashed out of solution into the atmosphere. The SO_2 gas migrated in a southwesterly direction (wind speed approximately 9 mph) setting off fixed SO_2 alarms on the unit. Multiple contract workers immediately downwind of the release area were exposed to SO_2 vapors, eventually resulting in one (1) DAFW [Days Away From Work] case and three (3) first aid cases.

An Incident Report was created following the incident. An investigation team was formed to determine the root/contributing causes of the incident and to suggest proposals for corrective action.

The team consisted of:

Safety Team Lead - Incident Investigation Team Lead
RCA Site Safety Manager, Turnarounds
OCC Root Cause Analyst
SRU Operation Specialist Board (OSB)
Technical Services Engineer, APS Unit
Safety Superintendent

Chronology of Events

<u>Background</u>

In the SBS unit, tail gas is burned at 1200 ^{o}F with excess air and natural gas in the tail gas combustor F-700. This converts the H_2S to SO_2.

Hot gas effluent from F-700 is cooled in the waste heat boiler E-701. Effluent gas from the boiler enters the venturi quench tower V-703 where it is quickly cooled by direct contact with a 30% sulfuric acid solution to approximately 181 ^{o}F. The 30% acid solution comes from the bottom of the T-704 quench separator and is pumped to V-703 via the quench circulating pumps P-704A/B/C in a continuous loop. The acid concentration is maintained at 30% by purging a small (< 2 gpm) slip stream to Tank-731 acid tank and replacing it with water to maintain the process temperature near 181 ^{o}F. The acid from Tank 731 is then removed either by draining to the process sewers (used as Lakefront pH control) or used as a product elsewhere. As the acid enters Tank 731, it is saturated with SO_2. The design of Tank 731 allows for the gas that is entrained in the acid to degas off to another tower, T 707, where it can be further treated. On Thursday August 7th, when tank 731 tank overfilled, there was not sufficient residence time for the SO_2 entrained in the solution to degas properly. As a result, the acid evolved sulfur dioxide to atmosphere as it overfilled to the ground.

Event Chronology (based on interviews and process control data)

The following chronology represents a best estimate of the sequence of key events associated with this incident. The events and associated time frames were pieced together from witness statements, logs, charts, etc. and may be subject to various sources of error such as memory recall limitations, time discrepancies between different sources of information (e.g. there is a difference in the TDC and the PI times), etc.

08:33 - Board Operator attempts to open control valve F-47706, to begin an acid drawdown from the quench recirculation system. The flow meter does not indicate a flow, so the Board Operator calls the Outside Operator to check and see if the manual block valves at the control valve station are closed. Note: The Board Operator stated/believed that the block valves are normally left in the open position to facilitate conducting this operation remotely.

09:11 - Outside Operator finds that the manual block valves are lined up (open) and has the Board Operator open the control valve to different settings in an effort to troubleshoot the situation. Outside Operator also sees no indication of flow on the flow meter and makes an effort to visually verify that there is no flow. He then begins to work (open and close) the manual block valves in an effort to fix the problem. Note: Process control data indicates that the tank level indicator begins to show an increase in the tank liquid level around this time. Acid level in the tank is approximately 7.2 ft. at this time. Per the interviews, neither the Board Operator nor the Outside Operator had any discussion about opening the bypass valve. The Board Operator did not call for the bypass valve to be opened, and the Outside Operator states that he did not open the bypass valve.

09:25 - Outside Operator finishes his effort to work (open and close) the manual block valves. He reports having heard a clunking sound and thought something might have “broke loose” so he asks the Board Operator to try opening the control valve again. Outside Operator still sees no flow on the flow meter but does not make another effort to visually verify this condition. Note: the tank level is now at approximately 7.7 ft. at this time. Outside Operator gets a call to perform other unit duties and tells the Board Operator to call him when he wants to try again. Outside Operator leaves the manual block valves at the control valve station in the open position. Board Operator leaves the control valve in the closed position (confirmed by process control data).

09:37 - Tank 731 high level alarm sounds in the control room Tank level is at approximately 8.5 ft. Board Operator acknowledges the alarm. About a minute and a half later the alarm is disabled.

09:49 - Alarm B45002L on the Beavon-Stretford unit sounds, indicating an Emergency RGG-One Fire Eye went out. This event and alarm is associated with on-going unit operations to move Pit Sweep from the SBS to Beavon-Stretford.

09:50 - Tank 731 appears to overflow (i.e., chart flat lines).

10:00 - SO_2 alarm (A47710) sounds at 4 ppm, but quickly climb to 25 ppm (maximum instrument reading). At about the same time, emergency alarm B45002LL at the Beavon-Stretford goes off, indicating both fire eyes on the RGG went off, causing it to trip. Board Operator contacts Outside Operator via radio and asks him to check it out at the Beavon-Stretford unit

~10:25 – Based on interviews, at approximately this time exposed workers make their way to area southeast of affected area and report odor and irritation problems to their Job Rep.

~10:31 – Based on interview with Outside Operator, at approximately this time the manual block valves around the control valve were closed by Outside Operator.

10:48 - BP ambulance requested

10:54 - Unit evacuation alarm sounded by unit asset supervisor

11:33 - SO_2 concentration drops below 4 ppm (alarm set-point) on analyzer (A47710).

13:18 - SO_2 concentration is non-detectable at analyzer (A47710).

Root Cause Analysis

In analyzing this incident, the team developed a detailed timeline of key events to help in the identification of critical events and contributing/critical factors.

Findings:

Immediate Causes

Actions:

1.1 Violation (by individual)
At approximately 09:37 a high level alarm sounded on Tank 731. The Board Operator acknowledged the alarm but took no action in response, reporting that he believed the liquid level was "tickling" the sensor and triggering a false alarm. The Board Operator had previously attempted to fill the tank, but believed that there was no flow into the tank because the flow meter to the tank was not working. However, during the previous 26 minutes, the liquid level in the tank had risen 1.3 ft. (from 7.2 ft. to 8.5 ft.) representing a flow rate of approximately 25 gpm (about what would be expected from a fully open control valve or bypass valve). The available evidence should have been sufficient to give the Board Operator a clear indication that Tank 731 was indeed filling and required immediate attention.

4.1 Distracted by other concerns
The Board Operator reported that he was distracted by other concerns related to transferring the Pit Sweep from the SBS to the Beavon-Stretford which demanded his attention during the time of this incident. An alarm indicating that the Emergency RGG-One Fire Eye went out sounded at approximately the same time as the SO_2 alarm.

4.4 No warning provided to workers downwind

No warning was provided to workers downwind of the immediate release area that there had been a release of SO_2 gas at the SBS until the unit evacuation alarm sounded at 10:54 (approximately 54 minutes after SO_2 was detected by analyzer A47710). While there is not a written unit procedure, interviews indicate that the standard response to an SO_2 alarm on the SBS unit is to have an operator conduct a field assessment of the situation. There is not a specific ppm limit designated as must evacuate the unit. Additionally, the time required to conduct this assessment can vary based on the specific unit circumstances. In this case, 31 minutes transpired from the time the SO_2 alarm sounded until the Outside Operator reached the unit, conducted an assessment, and implemented measures to stop the release. **The response time was inadequate to protect adjacent workers from exposure.** SO_2 continued to evolve off the spilled sulfuric acid for another 23 minutes before the evacuation alarm was sounded. By this time the ambulance had already arrived on scene to transport an exposed employee to the hospital.

Interviews with operations personnel did not produce a clear reason why the response to the SO_2 alarm took 31 minutes. The only explanation was that there was not a sense of urgency since, in their experience, previous SO_2 alarms were attributed to minor releases which did not require a unit evacuation.

Conditions:

5.5 Warning Systems not effective

When the SO_2 analyzers on the SBS alarm, they trigger flashing strobe lights on the unit. However, as there is no audible alarm, these strobe lights are only effective if they are within the workers line of sight. Several of the exposed workers were over 100 yards from the unit and were not able to see the flashing lights. As SO_2 is a gas, it has the potential to travel away from the unit and around objects to reach workers who may not be able to see the flashing strobe lights. The upper detectable limit of the analyzers is 25 ppm. During the incident, analyzer A47710 maxed out at 25 ppm almost instantly, making it impossible to determine the actual SO_2 concentration during the incident. The Field Operator has no mechanism for distinguishing between these conditions. The Board Operator can observe the analyzer reading but does not routinely communicate this information to the Field Operator. Additionally, there is not established criteria in a procedure for what SO_2 levels and/or alarms constitutes an emergency condition which should trigger sounding the evacuation alarm. Unit training information does contain information on the hazards of SO_2, including IDLH (Immediate Danger to Life and Health) information, but this information has not been instituted in standard operating / emergency procedures.

Also, as noted below, one of the Tank 731 high level alarms was not functioning. None of the alarms were designated as critical alarms which may have elicited a higher degree of attention amongst the competing priorities of the Board Operator.

6.1 Plant/Equipment malfunction

Significant attention was focused on the functioning of control valve (F47706). Both the Board Operator and the Field Operator stated that they believed that there was no flow entering Tank 731 because they saw no flow reading on the flow meter. However the data shows that the Tank 731 began filling around 09:11 (around the time that the operator began working the block valves) and continued to fill even when the control valve OP indicated it was closed. At about 09:25 the Board Operator opened control valve F47706 to 44% OP for about two minutes, then closed it. The manual block valves were all left in the open position. Tank 731 continues to fill at the rate of about 25 gpm (which is equivalent to the flow through a fully opened control valve or bypass valve) until it overflows at approximately 09:50. Potential explanations for how the tank continued to fill despite the control valve F47706 appearing to be closed, include: 1) a broken valve stem, 2) the by-pass valve was open, 3) instrument air failure, or 4) the valve simply stuck open. In response to scenario #1, control valve F47706 was inspected post incident and found to be in good operating condition. In response to scenario #2, the Outside Operator stated that the by-pass valve was never opened during this operation. In response to scenario #3, it was verified that the control valve would air fail closed so an instrument air failure was ruled out as a potential cause. In response to scenario #4, the control valve did not stick or hang-up during post incident testing. This left the team to conclude that the most likely explanation for why Tank 731 continued to fill being a temporarily stuck control valve or the bypass valve being inadvertently left open (differing from Field Operator interview statements).

In addition, at the time of the incident, the drain from the containment area to the process sewers was plugged and water had backed up in the containment area flooding the trench that the Tank 731 overflow pipe discharged to. Rather than flow through the trench into the process sewer, the liquid spread out on the ground near the base of the tank. .

7.6 Unanticipated exposure to hazardous chemicals

Unanticipated exposure to hazardous chemicals (SO_2) was the most immediate cause of worker injury associated with this incident. When tank 731 overfilled SO_2 was released to the atmosphere. The design of tank 731 allows for vapor that is entrained in the acid to degas off to another tower, T 707, where it can be further treated. As this tank overfilled there was not sufficient residence time for any SO_2 entrained in the solution to degas properly. As a result of this, the acid evolved sulfur dioxide to atmosphere as it overfilled to the ground. The MSDS describes SO_2 as a colorless gas with a pungent odor. It causes respiratory tract, skin and eye burns at high concentrations. Workers who were exposed to the SO_2 gas during the incident reported feeling a burning sensation in their eyes, nose, throats, and lungs. Figure 1 shows the approximate location of the workers who were exposed to the SO_2 in relation to Tank 731. At the time of the release, the wind was the NNE at about 9 mph.

System Causes

19.1 No work planning or risk assessment performed

The unit could not produce evidence that it had conducted a risk assessment and developed operating procedures that adequately accounted for the risk associated with the acid drawdown and tank filling operation. The design of Tank 731 included controls such as a process vent routed to T-707, the goose neck in the overflow pipe, and RV that adequately controlled the release of SO_2 during normal operations. However, the operators involved in this incident did not demonstrate an awareness of the risks associated with overflowing the tank and potential to generate high concentrations of SO_2 if the sulfuric acid was spilled. Furthermore, during the incident, the both the Outside Operator and Board Operator (who ultimately makes the decision to conduct the acid drawdown) did not appear to have a full awareness of all the work being performed on or near the unit, making decisions concerning the appropriate response more difficult.

21.4 Incorrect adjustment/ repair/ maintenance

At the time of incident, flow meter (FT47706) and level transmitter (L47731A) were not functioning properly. The flow meter (FT47706) appears to have not been working the previous time the tank was filled, however, no work order had been written to fix it. On August 7, neither the Board Operator nor the Outside Operator were aware that the meter was not functioning leading them to believe that the tank was not filling when, in fact, it was.

Level transmitter (L47731A) was a redundant level sensor on the tank. The readings from this transmitter had been erratic since about January 2006. A work order was written to repair the transmitter in July 2008 (D-04304). Work was performed on it on July 25, but it appears that the transmitter still was not functioning properly at the time of the incident leaving only level transmitter (L47731) working properly. Both transmitters had high level alarms. The high level alarm on transmitter (L47731A) was set to alarm at 7.5 ft. The high level alarm on transmitter (L47731) was set to alarm at 8.5 ft. So effectively, one of the high level alarms was not working detracting from the effectiveness of the alarm system.

Concerns were expressed during the interviews about the large backlog of maintenance work orders associated with unit equipment. A review of safety work orders revealed that the average age of a "safety" work order on the unit is about 86 days. The target for completing safety work orders is 4 weeks.

22.1 Lack of SPP for the task

Currently there is no risk assessed operating procedure for drawing down acid and filling Tank 731. The valve configuration on the acid line to Tank 731 includes block valves positioned on the inlet and outlet side of the control valve. The investigation team received conflicting statements about the routine positioning of the block valves at the control valve station. Some employees indicated that it was standard practice to leave the block valves open so that the operator could initiate the acid drawdown process without having to involve the Outside Operator to reposition the valves. Others indicated that it was standard practice to close the block valves when not engaged in filling the tank. The latter practice would have prevented this incident from occurring. There are not specific unit procedures or other protocols which define critical operational parameters such as the sequence of steps required to initiate the drawdown process (e.g., notification of Outside Operator, manual block valve positioning, etc), process control parameters (e.g., drawdown initiation and endpoint, specified flow rate into the tank, etc.), the safe level at which Tank 731 is considered full, the sequence of steps necessary to conclude and secure the tank filling process (e.g., closing block valves), and appropriate response to alarms.

23.1 Communication between work groups not effective

Effective communication is critical to the proper handling of an emergency. The investigation revealed several gaps in communication that occurred during this incident. As noted earlier, there was inadequate communication from BP operations to contractors working in the area that an incident involving the release of sulfuric acid had occurred and that the SO_2 alarms had sounded. There was also a lack of communication back to the Board Operators about worker exposure and the resulting affects. It was not until the Shift Supervisor arrived on-site and received information about both the incident that had occurred and the effect it was having on workers, that a decision was made to sound the unit evacuation alarm.

Safety Policy C-13 “Evacuation / Sheltering Plans for Buildings and Units” states

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

The Outside Operator stated that he felt he had the authority to call for a unit evacuation but was not sure that conditions were bad enough to make that call during this incident. The Outside Operator had no knowledge of the fact that the SO_2 analyzer had maxed out at 25 ppm or even that the IDLH (Immediate Dangerous to Life and Health) concentration for SO_2 was 100 ppm, but he clearly understood there was a significant release ongoing. In his interview, he stated that he smelled the release and saw a considerable amount of material on the ground venting/bubbling. The Outside Operator may have put himself at risk by entering the immediate release area to close the manual block valves. The appropriate course of action would have been to declare an emergency and allow the emergency response team (wearing proper PPE) to handle the situation. Critical time was lost in the assessment of the conditions associated with this incident and the improper communications that entailed.

Finally, the Board Operator failed to communicate the high level tank alarm to the Outside Operator who could have taken steps to close the manual block valves and stop the flow of acid to the tank.

13.4 Incorrect behavior not confronted

Investigation interviews and the team's own recollections concerning previous emergency incidents across the site indicate past examples of where units were not properly evacuated in situations where workers may have been at risk. The team discussed previous examples of where units were not evacuated by blowing the evacuation horn, but rather by operations personnel walking through the unit and stopping work. These past examples have set a incorrect precedent on how to address situations where unit evacuation may be required and are contrary to the C-13 policy statement, "When in doubt, evacuate." Additionally, since these past examples were not confronted and/or corrected at the time, an underlying reluctance to "hit the evacuation horn" is apparent among some operations personnel. In this incident, the Outside Operator stated that he was "not sure that conditions were bad enough to make that call".

Recommended Corrective Actions

1. Operator duty to respond appropriately to alarms needs to be reinforced with the work force.
2. Two alarm points (high and high/high) should be established for each of the redundant level sensors on Tank 731. The high alarm should be designated as a critical alarm given the risks associated with overflowing this tank.
3. Consideration should be given to establishing two alarm set-points for the SO_2 analyzers. The current alarm set-point at 4 ppm provides an important warning of the release of SO_2 gas that should be investigated. Consideration should be given to establishing a second alarm set-point at a level that triggers an immediate evacuation alarm (e.g., when the instrument maximum reading is reached).
4. Implement new control of work procedures to achieve to achieve better operational awareness and control of work being performed on the unit. Process hazards and potential risks associated with operational activities should identified by the AA and communicated to the PA for inclusion in risk assessments and crew reviews to improve the awareness of all work groups about the area hazards. Utilize process risk assessment to make more informed decisions about when to best schedule potentially hazardous operations to minimize potential risk to work crews.
5. Develop a risk assessed procedure for the acid drawdown process in accordance with Policy D-22 which defines critical operational parameters such as the sequence of steps required to initiate the drawdown process (e.g., notification of Outside Operator, manual block valve positioning, etc), process control parameters (e.g., drawdown initiation and endpoint, specified flow rate into the tank, etc.), the safe level at which Tank 731 is considered full, the sequence of steps necessary to conclude and secure the tank filling process (e.g., closing block valves), and appropriate response to alarms.
6. Consideration should be given to conducting a gun drill on the unit (last one conducted in 2005) with a focus on how to recognize and report emergency response conditions, proper communications, and the circumstances under which a unit evacuation should be conducted.
7. Unit evacuation procedure should be revised and emphasize that employee shall assess the situation and determine what level of evacuation is necessary to ensure the safety of all personnel as stated in Safety Policy C-13. Consideration must include ongoing SIMOPs (as posted on CoW boards) in determining evacuation requirements.

8. Convene a cross function team of refinery and OCC personnel to examine “protection of workforce” issues. Areas of focus should include:
   - Evacuation – understanding and awareness of workforce
   - Evacuation – when to activate

   Specific issues to consider include:
   - Identification of potential conditions that could lead to loss of containment by the process unit.
   - Identification and planning to evac during unit upsets and transients, loss of instruments / view, exceeding safe operating limits / critical alarms, loss of level or filling a drum / tower, etc.
     Team recommendations should apply site-wide