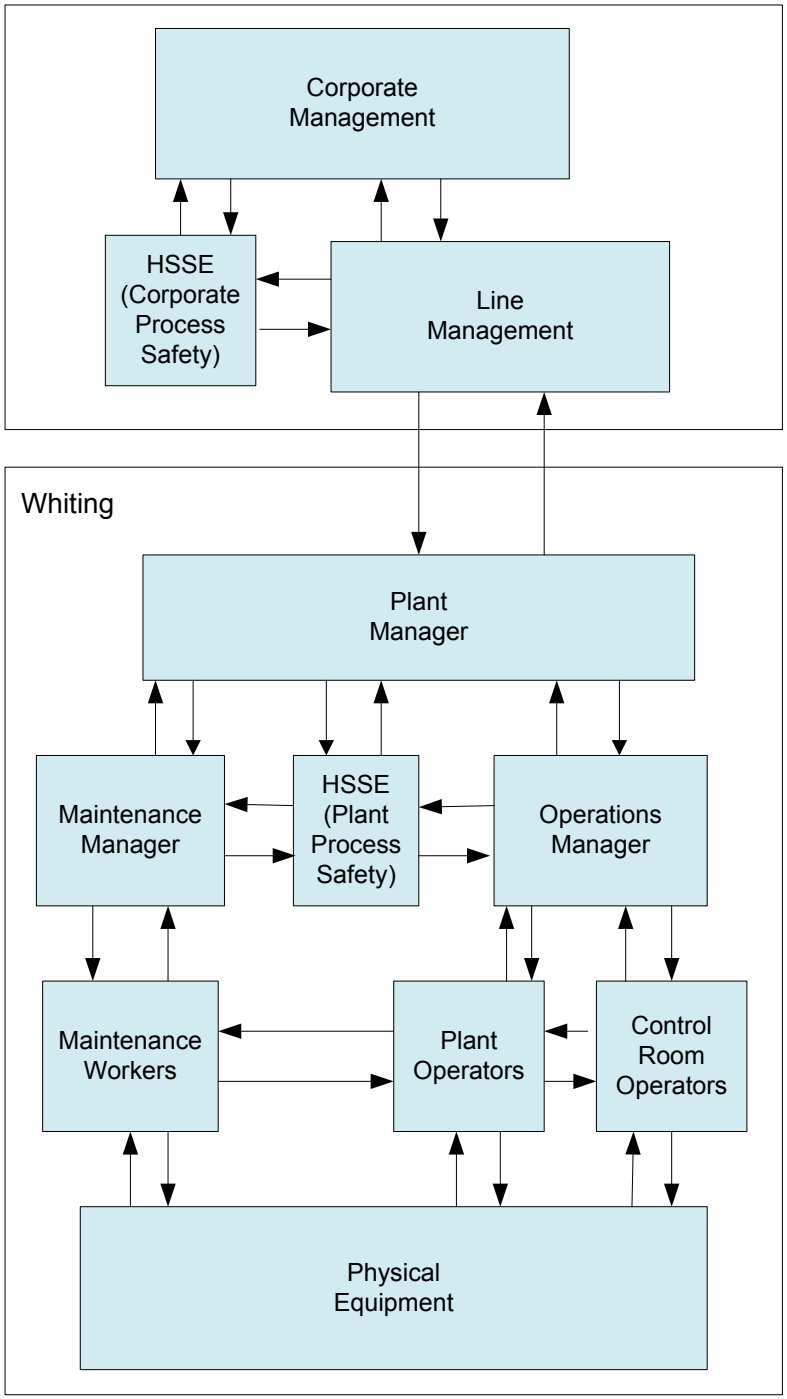
Corporate Management
HSSE (Corporate Process Safety)
Line Management
Whiting
Plant Manager
Maintenance Manager
HSSE (Plant Process Safety)
Operations Manager
Maintenance Workers
Plant Operators
Control Room Operators
Physical Equipment

For the Tank Overflow Accident

- Examine the physical level.
- What were the responsibilities (requirements) of the physical equipment?
- What emergency and safety equipment (controls) existed? How did these relate to the requirements (constraints)?
- What failures or unsafe interactions occurred in the accident?
- Evaluate the physical level controls.
- What additional questions were raised by your analysis so far? (What would you ask if you were investigating this accident?)

Physical Process in SO_2 Overflow

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

Physical Equipment (2)

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.

Evaluation of Physical Level Controls

- Reasonable amount provided but much was inadequate or non-operational, e.g.,
  - Tank level transmitter not working properly
  - Flow meter not working properly
  - Drain to emergency containment sewer clogged
- Questions:
  - Why was sewer clogged? Is this a common occurrence?
  - Were non-functional or inadequately functioning controls common at the plant?
  - What types of policy existent about operating plant with non-functioning safety equipment? Is risk assessment done when this occurs?
  - What types of inspections done on safety-critical equipment?
  - How is safety-critical equipment identified?
  - What is maintenance policy? Why was safety-critical equipment non-operational or operating erratically for relatively long periods of time?

Hindsight Bias at Operator Level

- What are some examples of hindsight bias in the report?

Hindsight Bias Examples

- Data availability vs. data observability (Dekker)
  - "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."

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*

  - "Operators could have trended the data" on the control board

Hindsight Bias Examples

- Another example
  - "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."

Analyze Board Operator

- Start from assumption that most people want to do the right thing and not purposely cause accidents
- So why did wrong thing in situation in which they found themselves?
  - Contextual and systemic factors
  - Mental model flaws
  - Missing feedback
- To minimize hindsight bias, try to understand why it made sense for them to act the way they did.
  - For example, why didn't evacuate immediately?
  - Did higher levels of control structure know about previous instances of this behavior?

Board Operator Analysis

- I separated contextual issues into those related to:
  - Tank level
    - Didn't know tank was filling. Responded incorrectly to alarm. Why?
  - Procedures and Alarms
    - Didn't evacuate plant immediately. Why?

Contextual Factors for Board Operator: Related to Tank Level

- Flow meter broken. Indicated no flow.
- Level transmitter and high-level alarm not functioning
  - Erratic behavior since January 2006 but work order not written to repair it until July 2008 (year and a half later). Why?
- Another level transmitter and high-level alarm (8.5 ft) were functioning
  - But level transmitters gave conflicting information regarding tank level

Contextual Factors for Board Operator: Related to Alarms

- Distracted by other duties related to transferring pit sweep
- Another alarm in plant he had to attend. Multiple alarms at same time.
- Previous SO_2 alarms attributed to minor releases did not require an evacuation alarm. Occur approximately once a month.
- None of alarms designated as critical alarms “which may have elicited a higher degree of attention …”

Contextual Factors for Board Operator: Related to Alarms (2)

- Upper limit of SO_2 analyzers is 25 ppm which occurred almost immediately. No way to determine actual SO_2 concentration during incident.
- In past, units not evaluated by blowing horn but by operations personnel walking through unit and stopping work.
- No written procedure for sounding alarm.

Contextual Factors for Board Operator: Related to Procedures

- No written unit procedure for responding to SO_2 alarm.
- No written procedure for ordering evacuation when SO_2 alarm sounds nor criteria established for level of SO_2 that should trigger an evacuation alarm.
- Unit training materials contains info about hazards of SO_2 but no standard operating/emergency procedures
- Block valves normally left open to facilitate remote operations.

Company Safety Policy

"*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.*"

What problems do you see with this policy?

Problems with Policy

- Responsibility not assigned to anyone.
  - Need someone with responsibility, accountability, and authority
  - Plus backup procedures for others to step in when necessary
- Normal human behavior is to try to diagnose situation first.
  - When overwhelmed with information, will try to digest and understand it first.
  - If want immediate behavior, then need to require it (or automate it) and not leave it up to employee to “evaluate situation.”
- If want flexibility inherent in real-time decision making then will need to provide
  - More extensive training
  - Better real-time information to operators

Outside Operator

- No more info than board operator and in hurry to get to simultaneous (but unrelated) trip of equipment in another part of unit
- Primary mistake (in hindsight) seems to be delay in evacuation alarm and attempt to clean up instead of immediately seeking help.
  - Report says he was not sure conditions bad enough to make that call
  - "Poor understanding of risks of an SO_2 release"
    - Is this unique to these two operators?
    - Is this unique to risks associated with SO_2 and not other risks?
  - Normal response is to try to fix problem rather than call emergency personnel immediately

Other Things Not Mentioned

- Very likely coordination problems about who should be doing what, but not enough info in report
- Dynamics (migration):
  - When I asked about why no criteria for SO_2 alarm levels, told that “didn’t think of it before – perhaps not needed before when lots of experienced personnel in units”
  - Had experience level decreased?

Recommendations

- Report recommendations very limited
- We came up with lots more even without additional information (see STAMP analysis of same accident)

16.683J / ESD.863J System Safety
Spring 2016