Instrumentation & Control Disasters

Lessons Learned & What You Can Do To Avoid Them

Paul Gruhn, PE, CFSE
L&M Engineering, Houston, TX

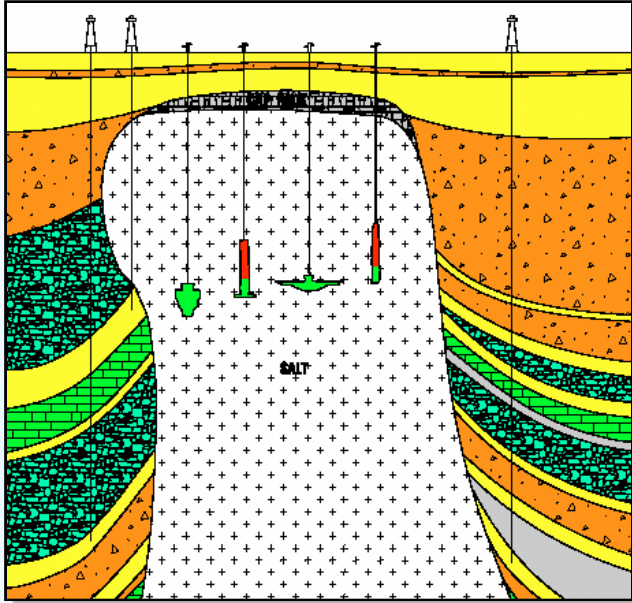
© 2003

Question

- Would you rather learn from the mistakes of others, or make them all yourself?
- Accidents are not due to lack of knowledge, but failure to use the knowledge we already have *(Kletz)*
- The risks involved in our industries are simply too great to be learned by trial and error
- We must learn from the mistakes of others

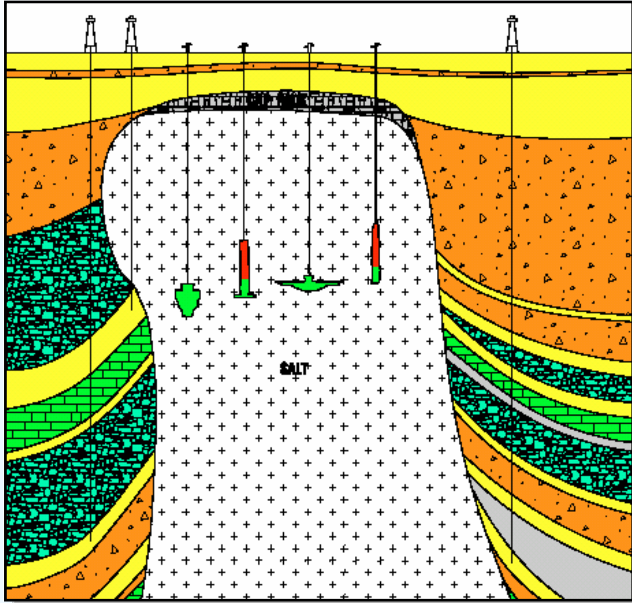
© 2003

Brenham Gas Explosion



- LPG storage in salt dome
- Gas cloud explosion in '92
- Estimated force of 3-kiloton bomb
- 3 deaths & 23 injuries
- > $150 million in damages
- Control room 90 miles away
- No remote way to shut in well
- No local breathing apparatus
- No flare system

Brenham Gas Explosion



- No clear idea of inventory
- Single pressure switch to detect backflow
  - Range of 160 – 2,000 psi
  - Set at 100 psi
  - Frequently did not function when tested
  - Improperly maintained
- Back flow not detected
- Car drove into gas cloud

© 2003

Questions Raised

1. Do you have an accurate indication of your capacity and/or throughput and is it within your design limit?
2. Are your safety devices installed, set, functioning and maintained properly? Are your maintenance records adequate enough to indicate if they weren't?
3. Do you have adequate safety layers?

© 2003

Ocean Ranger

- Largest floating offshore drilling rig when it was built in 1976
- Sank of the eastern coast of Canada in 1982
- Loss of all 84 aboard
- Ballast control room in middle leg 27’ above water surface
  - 4 glass windows
  - Electric panel used to control rig trim

© 2003

Ocean Ranger

- Operator not formally trained on ballast systems
  - Additional backup system operation not documented
- Large chain lockers at the top of each outer leg
  - No means of detecting water entering chain locker
- Full-immersion exposure suits not available
  - 180 miles offshore in North Atlantic in winter

© 2003

Ocean Ranger

- Poor evacuation training
- Crew prepares for approaching storm
- Wave breaks window in ballast control room
  - Storm covers not in place
  - Water shorts out ballast system
  - Improper understanding of systems operation exacerbates rig list

© 2003

Ocean Ranger

- Water eventually enters chain locker and fills up leg
- Crew attempts evacuation
  - Wind and waves damage lifeboats
  - Supply vessel takes 1 hour to reach rig
  - Sole lifeboat crew perishes attempting to board vessel

The world's largest, supposedly unsinkable rig, was lost with all aboard, due to a small porthole

© 2003

Questions Raised

1. How many undocumented systems do you have operating in your facility?
2. Have your personnel been formally trained on their operation?
3. What would happen is people were to use these systems without a full understanding of their operation?
4. Have you done a complete HAZOP?

© 2003

Chernobyl

- Soviet reactor exploded in ’86
- > 24 operators & firefighters die within days
- Thousands estimated to have died downwind
- > 70,000 people contaminated
- Operators performing undocumented test
  - Assumed to be safe
  - Lack of system understanding

Chernobyl

- Designers knew such operation was not safe
  - Safety systems installed
- Operators intentionally disable safety systems
  - Violation of safety policies

Questions Raised

1. How well do your operators understand the operation of their facility?
2. Are safety policies being violated? How would you even know if they were?
3. Does Engineering and Management *really* know what Operations is doing?
4. Is the design of your facility inherently safe? Could it be modified to be safer?

© 2003

Terra Industries

- Ammonium nitrate unit in Port Neal, Iowa
- Explosion in '94 killed 4 and hospitalized 18
- 5,700 tons of anhydrous ammonia and 25,000 gallons of nitric acid released
- Residents evacuated
- Plumes detected miles away

© 2003

Terra Industries

- pH probe out of service for two weeks, yet operations continued
- Operators unable to determine acidic conditions, which contributed to the accident
- PHA not performed
- Personnel not aware of hazards
- No Engineer responsible for operations or procedures

© 2003

Questions Raised

1. Have you done a hazards analysis?
2. Are your operators aware of the process risks?
3. Are all of your safety devices operating properly?
4. What procedures are in place for operating with bypassed instrumentation?

© 2003

Mars Polar Lander

- Lander launched in ’99
- Legs deploy prior to landing
- Sensor detect touchdown and turn of rocket motor
- Leg deployment known to create spurious signals
  - Software requirements did not describe this behavior
- Mission cost > $150 million

© 2003

Questions Raised

1. Have all operating parameters been accounted for in your design (e.g., start-up, operation, maintenance, shutdown, etc.)?
2. Have all parameters been fully documented?
3. Has the impact of spurious sensor signals been accounted for in the rest of the system design and operation?

© 2003

Airbus

- A320 crashed in Warsaw in ’93
- 2 deaths, multiple injuries
- Ground spoilers and engine thrust reversers can only be utilized when *both* main landing gear are compressed
- Wheel brakes may be used once both main landing gear are above a certain reference speed

© 2003

Airbus

- Crew unable to override and operate ground spoilers and engine thrust reversers manually
- Plane landed faster than normal to counteract windshear
- Plane touched down beyond normal touchdown point
- Spoilers, reversers and brakes inoperable by design until too late
- Computer had final authority

© 2003

Questions Raised

1. How confident are you that all operating conditions have been accounted for in your automated control system?
2. Are your automation systems operating beyond the capabilities of your operators to adequately override them in the event of an emergency?

© 2003

Conclusion

- There is much to learn from past accidents
- Overconfidence and complacency are attitude we can no longer afford
  - "That won't happen here"
  - "But we've never had an accident"
    - Seveso, Flixborough, Norco, Pasadena, Channelview, Three Mile Island, Chernobyl…

© 2003