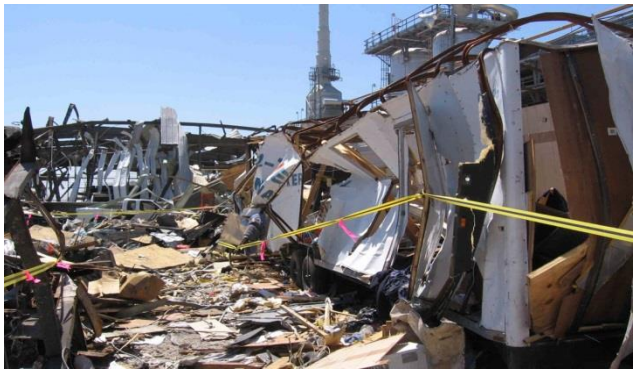


How to Learn More From Accidents

Prof. Nancy Leveson

Aeronautics and Astronautics
MIT





WHY ARE WE NOT LEARNING ENOUGH FROM ACCIDENTS?

Common Problems in Accident Analysis

- Root cause seduction and oversimplification of causes
- Hindsight bias
- Focus on blame
- Narrow view of human error
- Inadequate model of accident causality

Root Cause Seduction

- Assuming there is a root cause gives us an illusion of control.
  - Usually focus on operator error or technical failures
  - Ignore systemic and management factors
  - Leads to a sophisticated “whack a mole” game
    - Fix symptoms but not process that led to those symptoms
    - In continual firefighting mode
    - Having the same accident over and over

Oversimplification of Causes

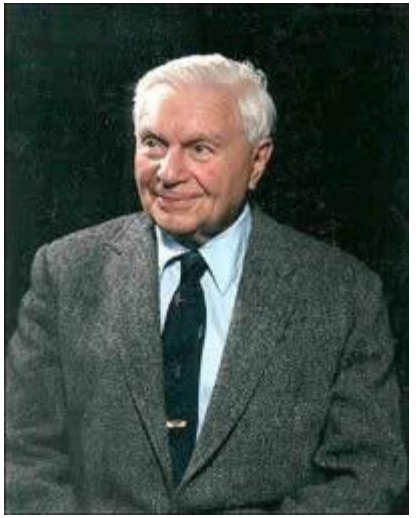
- Almost always there is:
  - Operator “error”
  - Flawed management decision making
  - Flaws in the physical design of equipment
  - Safety culture problems
  - Regulatory deficiencies

  Basically flaws throughout the safety control structure (SMS)

Jerome Lederer (1968)

"Systems safety covers the total spectrum of risk management. It goes *beyond the hardware* and associated procedures of systems safety engineering. It involves:

- Attitudes and motivation of designers and production people,
- Employee/management rapport,
- The relation of industrial associations among themselves and with government,
- Human factors in supervision and quality control
- The interest and attitudes of top management,

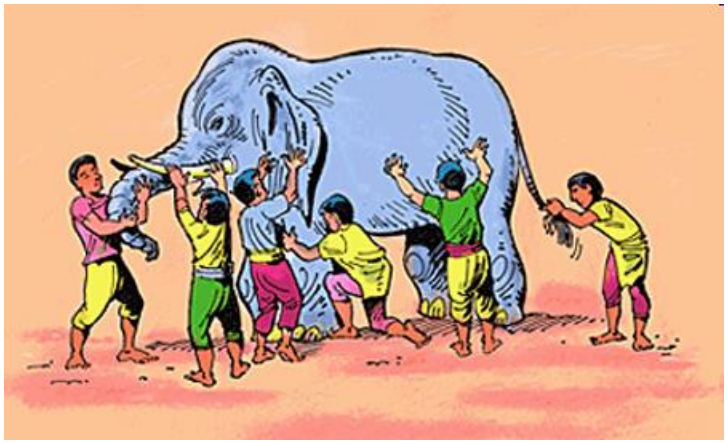


Mr. Aviation Safety

- The effects of the legal system on accident investigations and exchange of information,
- The certification of critical workers,
- Political considerations
- Resources
- Public sentiment

And many other non-technical but vital influences on the attainment of an acceptable level of risk control. These non-technical aspects of system safety cannot be ignored.”

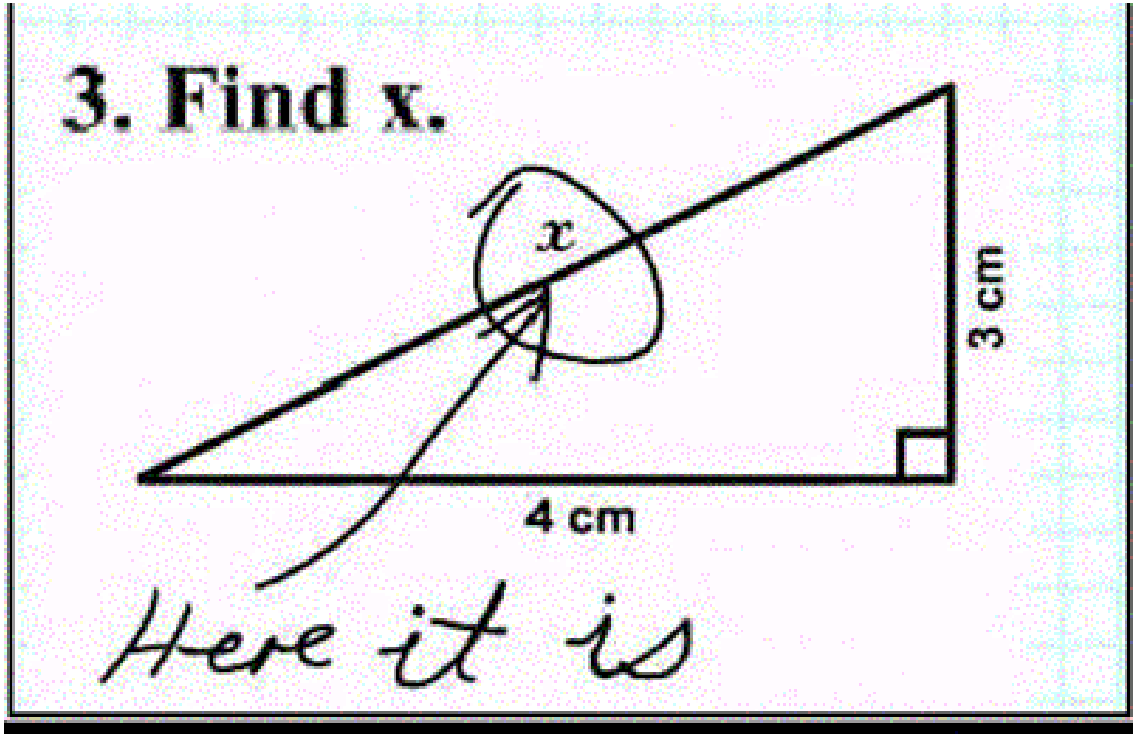
To understand and prevent accidents, must consider system as a whole



And so these men of Hindustan
Disputed loud and long,
Each in his own opinion
Exceeding stiff and strong,
Though each was partly in the right
And all were in the wrong.

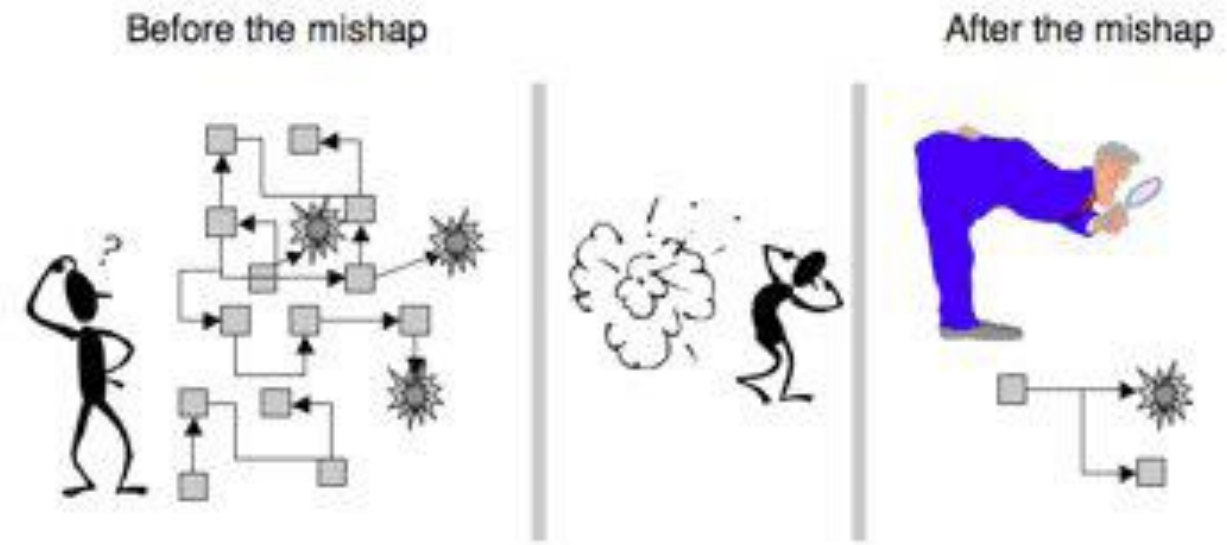
John Godfrey Saxe (1816-1887)

We want simple answers to complex questions.



So we get simple (and useless) answers

Hindsight Bias



(Sidney Dekker, Richard Cook)

“should have, could have, would have”

-- “Failure of flight crew to discontinue the approach into Cali, despite numerous cues alerting them of the inadvisability of continuing the approach”

-- “The Board Operator should have noticed the rising fluid levels in the tank”

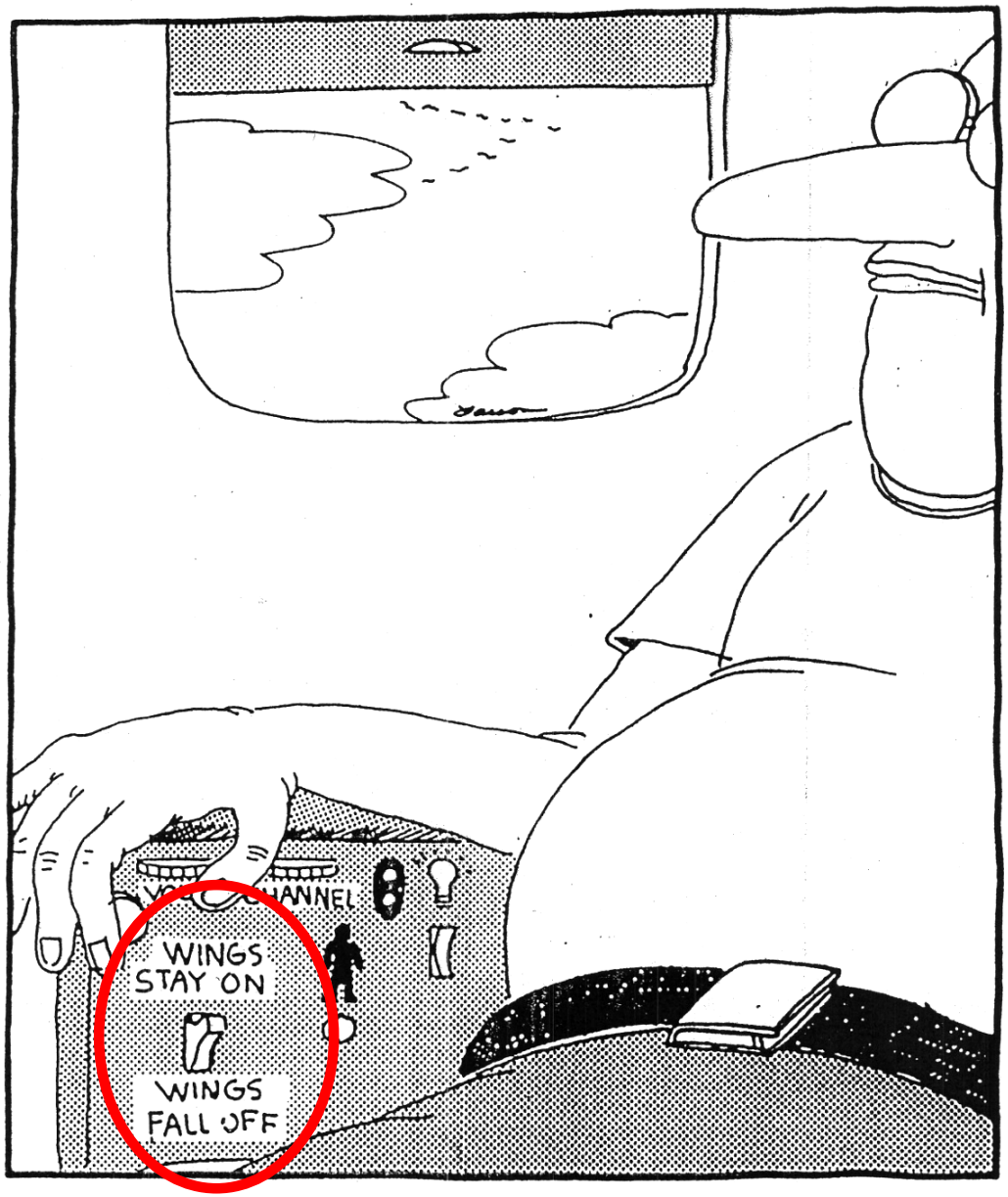
Hindsight Bias

- After an incident
  - Easy to see where people went wrong, what they should have done or avoided
  - Easy to judge about missing a piece of information that turned out to be critical
  - Easy to see what people should have seen or avoided
- Almost impossible to go back and understand how world looked to somebody not having knowledge of outcome
- To learn, need to identify why it made sense for people to do what they did

Do Operators Really Cause Most Accidents?

Operator Error: Traditional View

- Assumption: Operator error is cause of most incidents and accidents
- So do something about operator involved (fire, retrain, admonish)
- Or do something about operators in general
  - Marginalize them by putting in more automation
  - Rigidify their work by creating more rules and procedures



Fumbling for his recline button Ted unwittingly instigates a disaster

Operator Error: Systems View (1)

- Human error is a symptom, not a cause
- All behavior affected by context (system) in which occurs
- Role of operators in our systems is changing
  - Supervising rather than directly controlling
  - Systems are stretching limits of comprehensibility
  - Designing systems in which operator error inevitable and then blame accidents on operators rather than designers

Operator Error: Systems View (2)

- To do something about error, must look at system in which people work:
  - Design of equipment
  - Usefulness of procedures
  - Existence of goal conflicts and production pressures
  - Etc.
- **Human error is a symptom of a system that needs to be redesigned**

Failure of the flight crew to revert to basic radio navigation at the time when the FMS-assisted navigation became confusing and demanded an excessive workload in a critical phase of flight.

Blame is the Enemy of Safety

- Goal of the courts is to establish blame
  - People stop reporting errors
  - Information is hidden
  - Learning is inhibited

- Goal of engineering is to understand <u>why</u> accidents occur in order to prevent them

[Example from Gerry Bruggink and C.O. Miller]

WHO

NTSB determined probable cause of this accident was:

1. The flight crew's failure to use engine anti-icing during ground operations and takeoff
2. Their decision to take off with snow/ice on the airfoil surfaces of the aircraft, and
3. The captain's failure to reject the takeoff during the early stage when his attention was called to anomalous engine instrument readings.

WHY

Contributing Factors:

1. The prolonged ground delay between de-icing and receipt of ATC clearance during which the airplane was exposed to continual precipitation.
2. The known inherent pitch-up characteristics of the B-737 aircraft when the leading edge is contaminated with even small amounts of snow or ice, and
3. The limited experience of the flight crew in jet transport winter operations.

Conclusions

- What was the cause of this accident?
- Note the use of the word “failure”
  - A pejorative word: a judgment
  - Assigning blame

The captain’s failure to reject the takeoff during the early stage when his attention was called to anomalous engine instrument readings.

Conclusions

- What was the cause of this accident?
- Note the use of the word “failure”
  - A pejorative word: a judgment
  - Assigning blame

The captain’s failure to reject the takeoff during the early stage when his attention was called to anomalous engine instrument readings.

vs.

The captain did not reject the takeoff during the early stage when his attention was called to anomalous engine instrument readings.

- Accusatory approach to accident analysis (“who”)

[Example from Gerry Bruggink and C.O. Miller]

WHAT

Based on the available evidence, the Accident Board concludes that a thrust deficiency in both engines, in combination with contaminated wings, critically reduced the aircraft's takeoff performance, resulting in a collision with obstacles in the flight path shortly after liftoff.

WHY

Reason for the thrust deficiency:

1.Engine anti-icing was not used during takeoff and was not required to be used based on the criteria for “wet snow” in the aircraft’s operations manual.

2.The engine inlet probes became clogged with ice, resulting in false-high thrust readings.

3.One crew member became aware of anomalies in cockpit indications but did not associate these with engine inlet probe icing.

4.Despite previous incidents involving false thrust readings during winter operations, the regulator and the industry had not effectively addressed the consequences of blocked engine inlet probes.

Reason for the wing contamination: …

1.Deicing/anti-icing procedures.

2.The crew’s use of techniques that were contrary to flight manual guidance and aggravated the contamination of the wings.

3.ATC procedures that resulted in a 49-minute delay between departure from the gate and takeoff clearance.

Conclusions

- Did you get a different view of the cause of this accident?
- Do you now think it was just flight crew “failures”? Are there other factors?

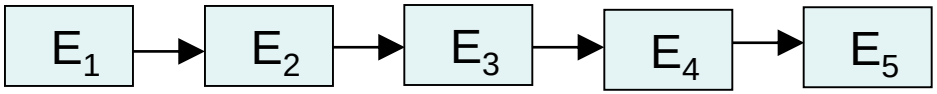
Accusatory:
Who
Why

Explanatory:
What
Why

- Do you think the recommendations will be different?

Use of Inappropriate Accident Models

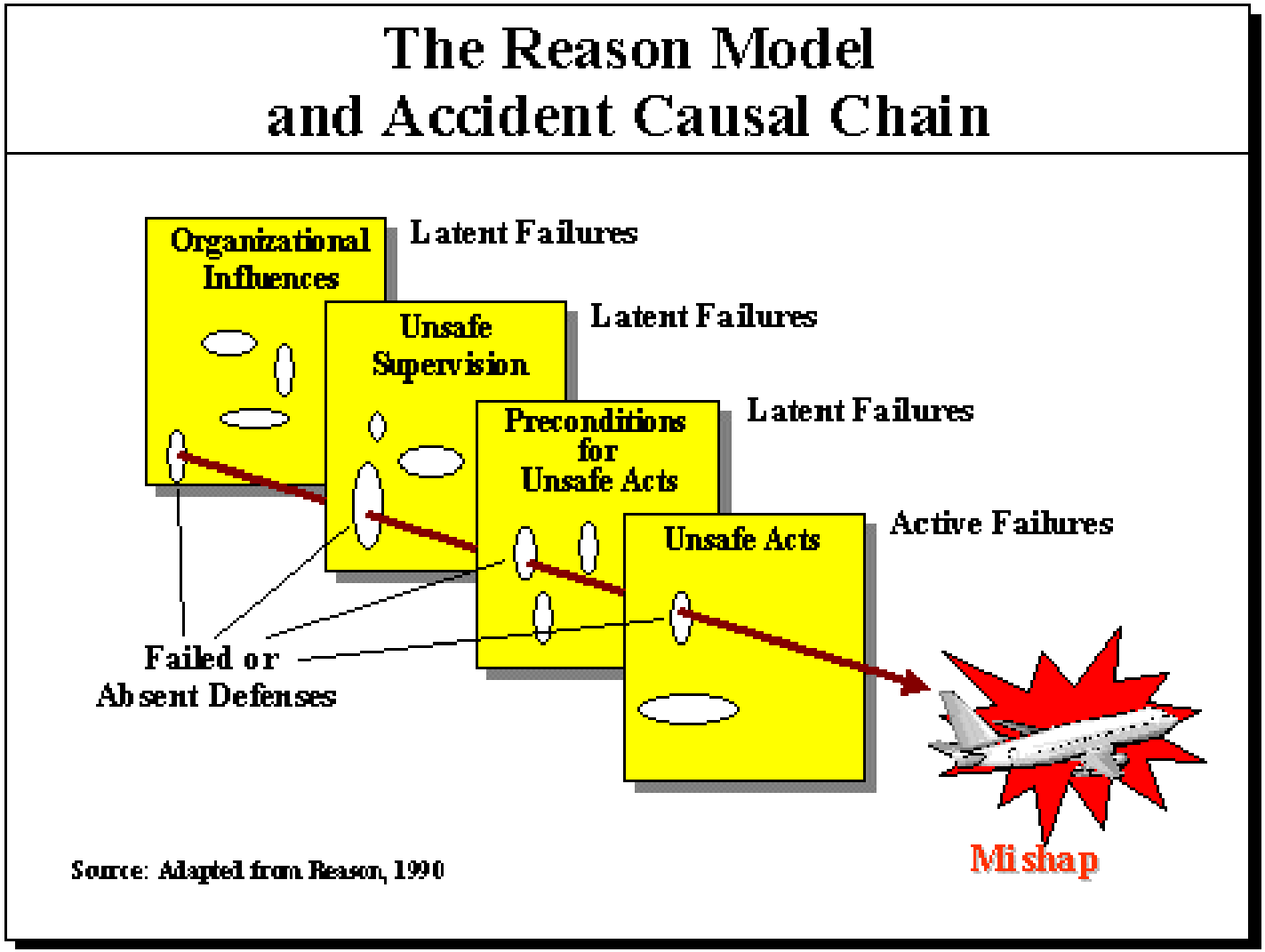
- Identifies how we learn from and try to prevent accidents
- Linear “chain of failure events” is used today



Each event is the direct result of the preceding event

Heinrich, 1932

Reason Swiss Cheese = Domino Model



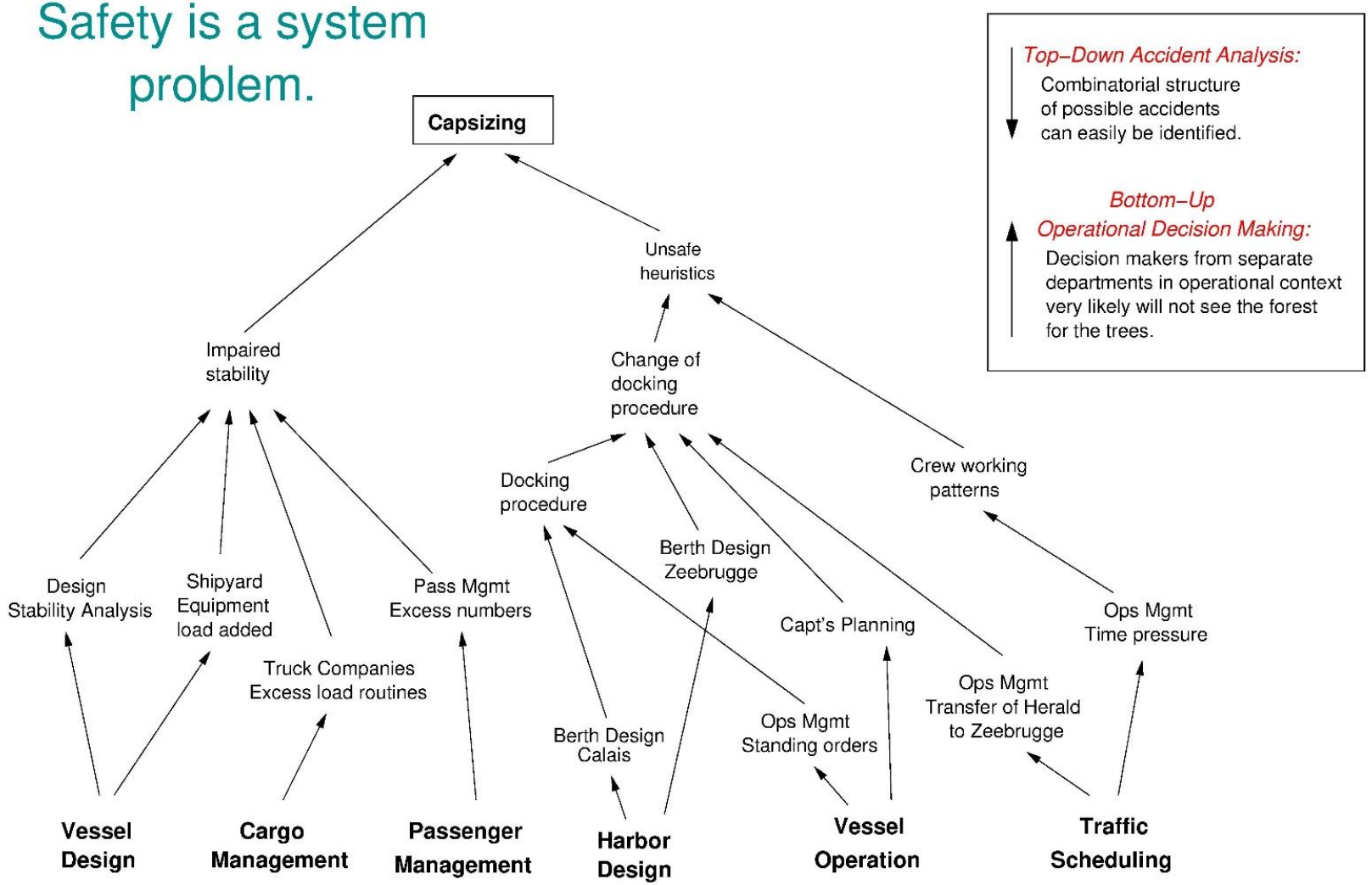
Herald of Free Enterprise (Events)

- Assistant bosun responsible for closing loading doors
- First officer supposed to check that actually closed
- To keep on schedule, the First Officer returned to the wheel house before the ship dropped its moorings (which was common practice), leaving the closing of the doors to the Assistant Bosun, who had taken a short break after cleaning the car deck upon arrival at Zeebrugge. He had returned to his cabin and was still asleep when the ship left the dock.
- The captain could only assume that the doors had been closed because he could not see them from the wheel house due to their construction, and there were no indicator lights in the wheelhouse to show door position.

Jens Rasmussen

Herald of Free Enterprise

Safety is a system problem.



Need to understand interactions among causal factors

Events are Not Enough

Need to look at *why* events occurred

Event	Questions Raised
An automatic protection system was triggered that was designed to prevent liquid from entering the exhaust gas system (flare). But preventing the liquids from entering the flare also prevented the gases in the system from being discharged, increasing pressure in the reactor.	*Did the operators notice this? Was it detectable?* *Why did they not respond?* *This seems like a predictable design flaw. Was the unsafe interaction between the two requirements (preventing liquid from entering the flare and the need to discharge gases to the flare) identified in the design or hazard analysis efforts?* *If so, why was it not handled in the design or in operational procedures?* *If it was not identified, why not?*

Another Example

Event	Questions Raised
Continued warming up of the reactors caused more chemical reactions to occur between the ethylbenzene and the catalyst pellets, causing more gas formation and increasing pressure in the reactor.	*Why wasn't the increasing pressure detected and handled?* *If there were alerts, why did they not result in effective action to handle the increasing pressure?* *If there were automatic overpressurization control devices (e.g., relief valves), why were they not effective?* *If there were not automatic devices, then why not? Was it infeasible to provide them?*

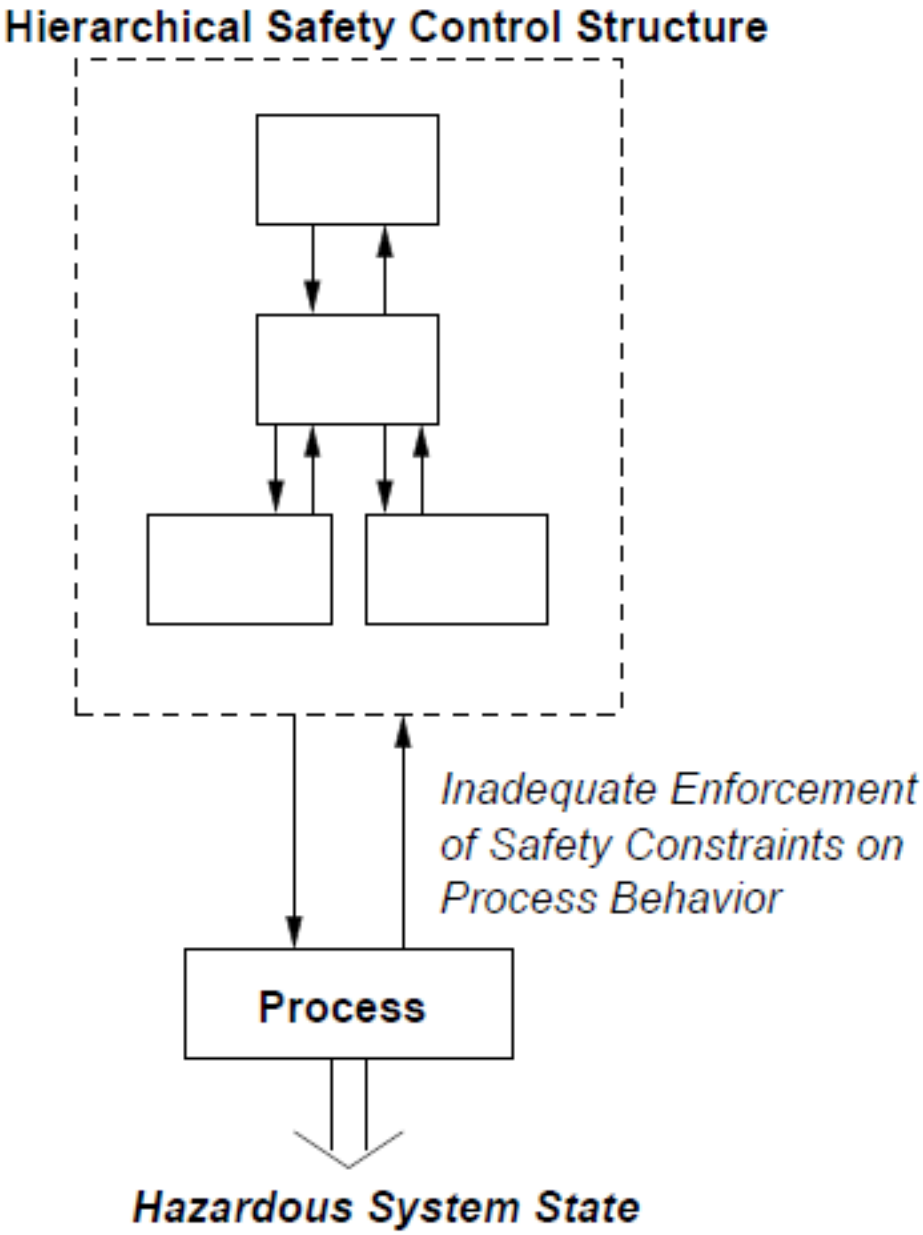
Limitations of Chain-of-Events Model

- Assumption of independence
- End up blaming the human operator or physical failure in the chain
- Cannot handle
  - Complex human behavior
  - Software (system design and requirements flaws)
  - Systemic factors (e.g., managerial/production pressures)
  - Design flaws in complex systems
  - Organizational/social factors, culture
  - Accidents involving non-failures
  - Interactions among causal factors

STAMP

- Accidents are a dynamic control problem rather than a failure problem.
  - Hazards result from lack of enforcement of safety constraints in system design and operations
  - Losses involve interaction of humans, physical components, software, organizational factors, regulatory factors, culture, etc.
- Controls are created to prevent hazards. Accidents occur when the controls are ineffective.

Accident Causality Using STAMP



CAST: INCREASING LEARNING FROM ACCIDENTS/INCIDENTS

Goals for Accident/Incident Analysis

- Minimize hindsight bias
- Provide a framework or process to assist in understanding entire accident process and identifying systemic factors
- Get away from blame (“who”) and shift focus to “why” and how to prevent in the future
- Determine:
  - Why people behaved the way they did
  - Weaknesses in the safety control structure that allowed the loss to occur

CAST (Causal Analysis using System Theory)

- A structured technique to analyze accident causality from a system perspective
  - Helps to generate questions to be asked
  - Paradigm change from what is done by other tools
    - Why didn't designed controls prevent the accident?
    - What changes in the controls are needed to prevent future accidents?
- Identify how each of components in control structure contributed to the loss
- "What-Why" (explanatory) not "Who-Why" (accusatory)

Examples and information at: http://sunnyday.mit.edu/STAMP-publications-sorted.pdf

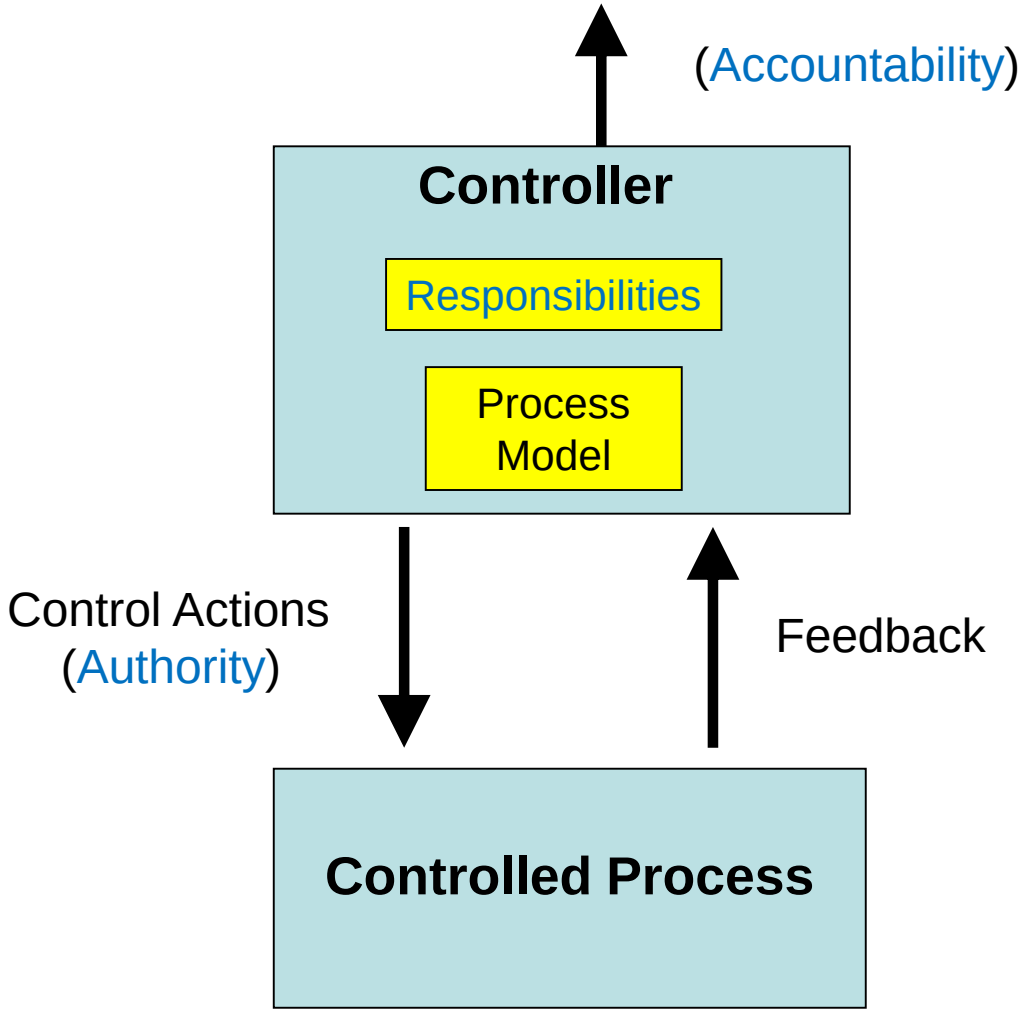
CAST is Based on STAMP

- STAMP is a new model of accident causality
- Accidents are caused by complex interactions among humans, hardware, software, and social structures (not just chains of failure events)
- Change focus:

~~"Examine failures"~~

"Determine why designed controls were ineffective"

SMS is Constructed from Control Loops



Bhopal

- Worst industrial accident in history
  - Conservative estimate of 10,000 killed, 50,000 permanent disabilities (including blindness), and 200,000 injured.
  - Blamed by management on operator error
  - Union Carbide blamed on sabotage
- MIC (methyl isocyanate) used in production of pesticides and polyurathanes (plastics, varnishes, and foams)
  - Highly volatile, vapor heavier than air
  - A major hazard is contact with water, which results in large amounts of heat.
  - Gas burns any moist part of body (throat, eyes, lungs)
  - Keeping it at a low temperature reduces reactivity

Events at Bhopal

- Dec. 2, 1984, relatively new worker assigned to wash out some pipes and filters, which were clogged.
- Pipes being cleaned were connected to the MIC tanks by a relief valve vent header, normally closed
- Worker closed valve to isolate tanks but nobody inserted required safety disk (slip blind) to back up valves in case they leaked
- Night shift came on duty at 11 pm.
- Pressure gauge indicated pressure was rising (10 psi instead of recommended 2 to 3 psi). But at upper end of normal range.

- Temperature in tank about 20 C.
- Both instruments were ignored because believed to be inaccurate. Operators told instead to use eye irritation as first sign of exposure.
- 11:30 pm: detected leak of liquid from an overhead line after some workers noticed slight eye irritation.
- Workers looked for leak and saw a continuous drip on outside of MIC unit.
  - Reported it to the MIC supervisor
  - Supervisor did not consider it urgent and postponed an investigation until after the tea break.

- 12:40 am on Dec. 3: Control room operator noticed tank 610 pressure gauge was approaching 40 psi and temperature was at top of scale (25 C)
- 12:45 am: Loud rumbling noises heard from tank. Concrete around tank cracked.
- Temperature in tank rose to 400 C, causing an increase in pressure that ruptured relief valve.
- Pressurized gas escaped in a fountain from top of vent stack and continued to escape until 2:30 am.
- MIC vented from stack 108 feet above ground. 50,000 pounds of MIC gas would escape.

- Operator turned off water-washing line when first heard loud noises at 12:45 am and turned on vent scrubber system, but flow meter showed no circulation of caustic soda.
  - He was unsure whether meter was working
  - To verify flow had started, he would have to check pump visually.
  - He refused to do so unless accompanied by supervisor
  - Supervisor declined to go with him.
- Operator never opened valve connecting tank 610 to the spare tank 619 because level gauge showed it to be partially full.

- Assistant plant manager called at home at 1 am and ordered vent flare turned on. He was told it was not operational (out of service for maintenance). A section of pipe connecting it to the tank was being repaired.
- Plant manager learned of leak at 1:45 am when called by the city magistrate.
- When MIC leak was serious enough to cause physical discomfort to workers, they panicked and fled, ignoring four buses intended for evacuating employees and nearby residents.
- A system of walkie-talkies, kept for such emergencies, never used.

- MIC supervisor could not find his oxygen mask and ran to boundary fence, where he broke his leg attempting to climb over it.
- Control room supervisor stayed in control room until the next afternoon, when he emerged unharmed.
- Toxic gas warning siren not activated until 12:50 am when MIC seen escaping from vent stack.
  - Turned off after only 5 minutes
  - Remained off until turned on again at 2:30 am.
  - Police were not notified and when they called between 1 and 2, were given no useful information.

- No information given to public about protective measures in case of an emergency or other info on hazards.
  - If had known to stay home, close their eyes, and breathe through a wet cloth, deaths could have been prevented.
- Army eventually came and tried to help by transporting people out of area and to medical facilities.
  - This help was delayed because nobody at plant notified authorities about the release
- Weather and wind contributed to consequences.
- Because happened in middle of night, most people asleep and it was difficult to see what was happening.

What was the “root cause”?

Hazards

System Hazard 1: Inadvertent release of toxic chemicals.

Safety Constraints:

- Chemicals must be under positive control at all time (runaway reactions must be prevented)
- Means must be available, effective, and used to respond to runaway reactions before leads to exposure of workers or the public.

Hazards

System Hazard 2: Exposure of public or workers to released toxic chemicals

Safety Constraints:

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

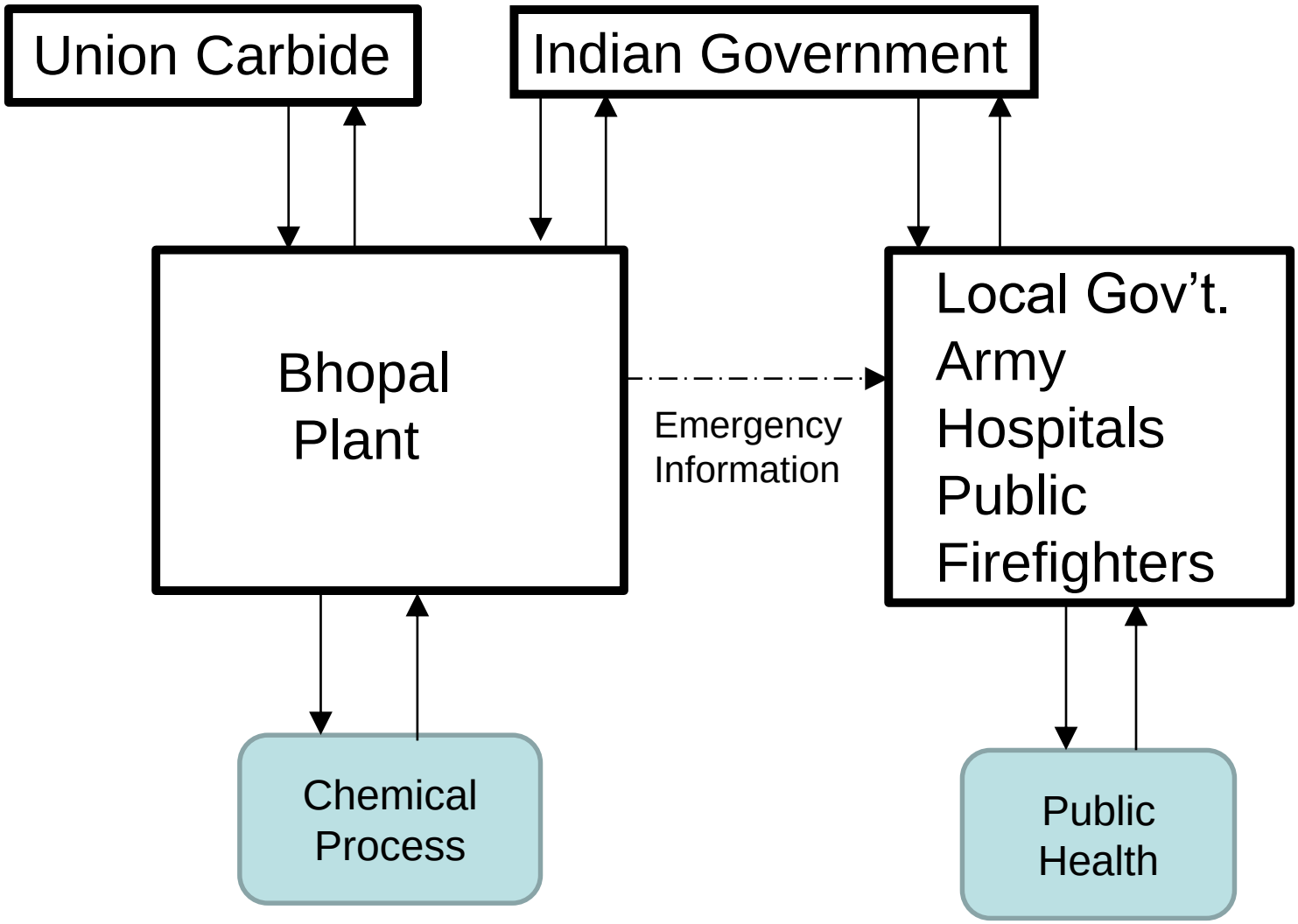
Drawing the Control Structure

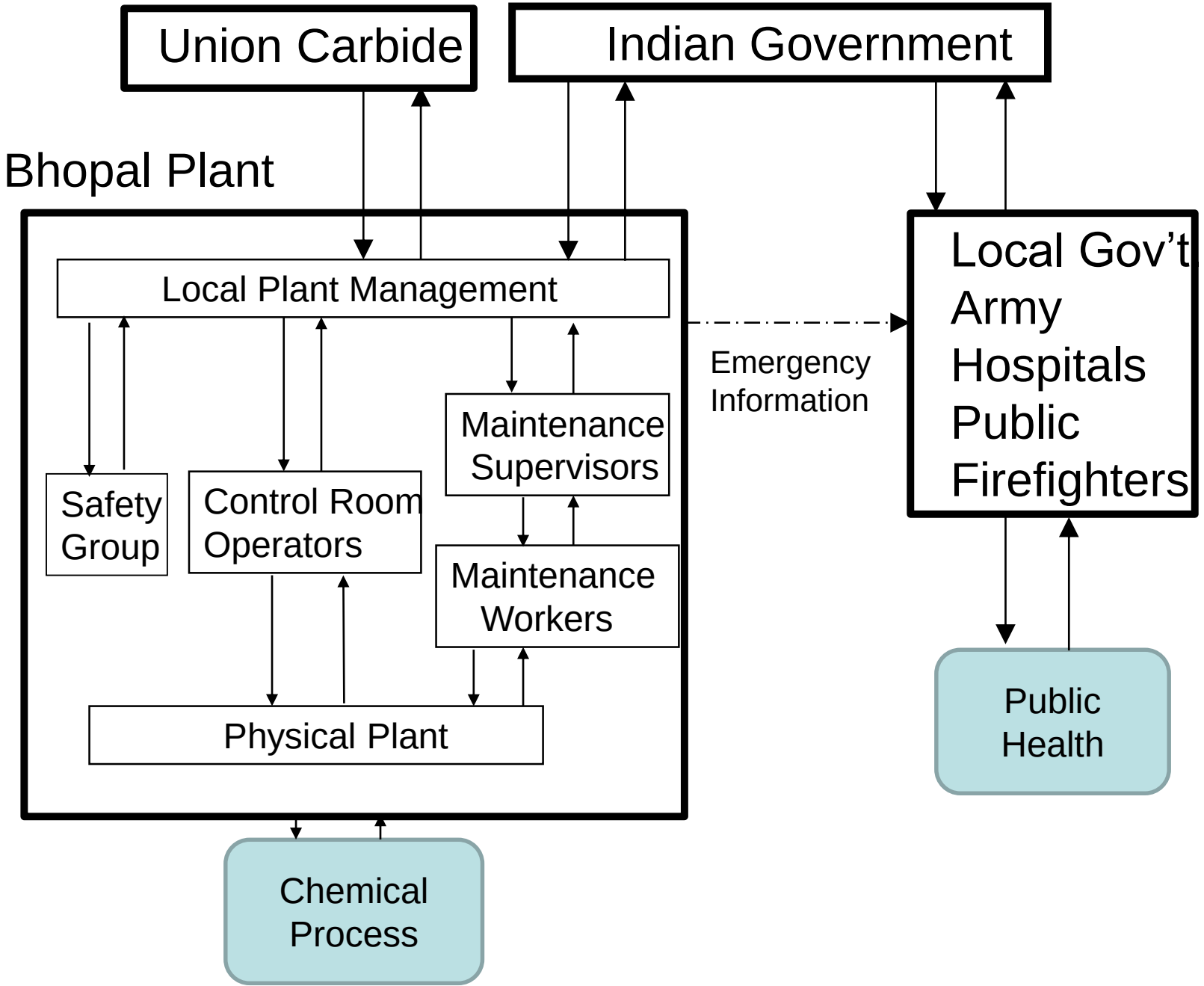
- What are the controlled processes?

- What controls might exist?

Drawing the Control Structure

- What are the controlled processes?
  - Chemical process
  - Public Health
- What controls might exist?


Union Carbide
Indian Government
Bhopal Plant
Emergency Information
Local Gov't.
Army
Hospitals
Public
Firefighters
Chemical Process
Public Health


Union Carbide
Indian Government
Bhopal Plant
Local Plant Management
Safety Group
Control Room Operators
Maintenance Supervisors
Maintenance Workers
Physical Plant
Chemical Process
Emergency Information
Local Gov't
Army
Hospitals
Public
Firefighters
Public Health

Analysis Results Format

- For each component, identify:
  - Safety responsibilities
  - Contributory control actions
  - Mental (process) model flaws that contributed to it
  - Contextual reasons for the behavior
- For control structure as a whole
  - Flaws in coordination and communication among components
  - Industrial and organizational safety culture
  - Safety information system
  - Dynamics and changes over time

Physical Plant

Designed Controls

- MIC storied in underground tanks, double walled, stainless steel, embedded in concrete
- Tanks must never contain more than half max volume
- Standby tank to transfer chemical in case of trouble
- Tanks interconnected so could transfer from one tank to another
- Vent gas scrubber
- Flare tower
- Water curtain
- Siren to warn of danger
- Valves were supposed to be inspected and cleaned regularly
- Limit storage to 12 months
- Staff to wear PPE

Physical Plant (2)

- Maintain MIC at temperature near 0 C.
  - Refrigeration unit
  - High temperature alarm (if reaches 11 C.)
- Relief valve to release pressure if gets higher than a fixed value
- Buses for evacuation in case of emergency
- System of walkie-talkies for emergencies

Failures and Unsafe Interactions

- Valves not isolated for pipe washing in case they leaked. Relief valve header normally closed.
- Water gets into MIC tank, causing runaway reaction (no failure, an unsafe interaction)
- Leak from overhead line
- Concrete around tanks cracked
- Few alarms, interlocks, or automatic shutoff systems in critical locations.

Physical Plant (3)

- Temperature increased (to 400 degrees), causing an increase in pressure that ruptured the relief valve
- Vent scrubber not designed to handle amount of escaping gas
- Vent flare out of service for maintenance (section of pipe connecting it to tank was being repaired
- Flare tower inadequate to deal with amount of MIC that escaped. Pipe corroded and had not been replaced.
- Water curtain not high enough to be effective
- Refrigeration shut down. Alarm was reset to 20 C.
- Weather and wind contributed. Middle of night so dark.

What do you now think is the cause of this accident? Is your view changing?

Control Room Workers

Responsibility:

- Maintain temperature and pressure constraints.

CCAs (Contributing Control Actions):

- Ignored pressure gauge showing pressure was rising. Ignored temperature gauge
- Detected leak but ignored it and went to tea break
- Did not go out to check pump visually
- Did not open valve connecting tank to spare tank

Why?

Process Model:

- Believed pressure and temperature gauges were inaccurate.
- Did not know if vent scrubber was working or not.
- Unsure if meter was working

Control Room Workers (2)

Contextual Factors:

- Pressure gauge at upper end of normal. Temperature high but at high normal
- Instruments often faulty
- Leaky valves common and not considered significant
- Had been told to use eye irritation as first sign of exposure. Only slight irritation at first.
- Temperature scale on gauge only went up to 25 degrees
- Checking pump visually would have been potentially dangerous if there was a runaway reaction
- Level gauge showed spare tank was full
- Turned on vent scrubber, but not sure working because flow meter showed no circulation of caustic soda. Didn't know if meter working or not. To determine this, would have to check pump visually.
- Common to leave MIC in spare tank

MIC Supervisor

Responsibility:

- Ensure control room operations is enforcing constraints on MIC temperature and pressure
- Activate emergency warnings

CCAs:

- Postponed investigation of leak until after tea break
- Did not activate toxic gas warning siren until late in emergency. Then turned it off after 5 minutes.

Process Model: Did not consider leak to be urgent

Context:

- Gauges often faulty
- Followed UC policy with respect to warning siren

Workers at Plant

Responsibilities in case of emergency

- Use walkie talkies, evacuate orderly using buses provided
- Follow emergency procedures when alarms sound

CCAs:

- Panicked and fled, ignoring buses.
- Did not use walkie talkies, etc.

Context:

- Almost no training about how to handle non-routine events
- Could not tell emergency alarm from practice alerts (went off 20-30 times a week)
- Only had minimum of emergency equipment

Maintenance Worker

Responsibilities:

- Perform regularly scheduled maintenance
- Follow procedures provided to him

CCAs:

- Washed pipes without inserting slip blind
- Did not check to see whether pipe was properly isolated

PM:

- Did not think his job was to insert slip blind. He knew the valves leaked, but safety disks were job of maintenance department

Context:

- Relatively new at his job
- No instruction provided to insert slip blind on maintenance sheet
- Told it was not his job to insert slip blind nor to check whether pipe was isolated. Low-skilled worker.

Maintenance Supervisors

Responsibilities:

- Insert safety disks when washing pipes (isolate valves)
- Ensure safety-critical equipment is working when MIC in tanks (during critical operations)

CCAs:

- Allowed a lot of deferred maintenance in safety-critical equipment (e.g., flare tower, gauges)
- Gauges and alarms improperly set
- Allowed pipe washing operation with adequate supervision

Context:

- Cost cutting (second shift supervisor position eliminated
- Nobody working on shift when problem arose

Safety Group

Responsibilities:

- Training for emergencies
- Ensure emergency equipment provided and working
- Inspections, safety audits

CCAs:

- Ineffective practice alerts. Lots of emergency drills but ineffective
- Alarm sounded too often. Emergency signal identical to that used for other purposes, including practice drills
- Provided only bare minimum of emergency equipment
- Allowed unsafe conditions to exist (refrigeration turned off)
- Allowed workers to not wear safety equipment
- Few inspections and safety audits, superficial when done

Safety Group (2)

PM:

- Either thought operations were safe as designed or did not know current state

Context: (no information)

- Qualified for their job?
- High temperatures in plant, no air conditioning
- Lots of questions here but few answers

Bhopal Plant Management

Responsibilities:

- Operate plant safely
- Work with local authorities to provide information necessary to protect the public
- Provide alarms and warnings and education to surrounding population

CCAs:

- Police not notified and given no useful info when they called
- Did not turn on toxic gas warning siren until late and then turned off after only 5 minutes
- Did not provide info to public about protective measures or other info on hazards

Bhopal Plant Management (2)

CCAs (con't)

- Help delayed because nobody at plant notified authorities about release
- Turned off refrigeration and adjusted threshold alarms, discontinued logging of tank temperatures
- Allowed threshholds for production to be routinely exceeded
- Allowed plant to be operated with safety-critical equipment out of operation (e.g., flare tower)
- Allowed operation that violated safety rules (e.g., spare tank not empty, filled tanks more than half full)
- Allowed skilled workers to leave, not replaced or replaced with unskilled workers
- Maintenance and operating personnel cut in half
- Maintenance procedures severely cut back and shift relieving system suspended.

Bhopal Plant Management (3)

CCAs (con't)

- Minimal training of many workers in how to handle non-routine emergencies
- Replaced US-trained staff with less experienced technicians
- Reduced educational standards and staffing levels
- Ignored warnings (e.g., plant manager resigned because disapproved of falling safety standards)
- Allowed unsafe conditions to exist (no refrigeration, etc.)
- 1982 safety audit deficiencies never corrected (e.g., gauges didn't work, leaky valves, flare tower and gas scrubber not working, pipe washing without slip blinds, etc.)
- Hazardous conditions were known and allowed to persist for considerable amounts of time or inadequate preparations taken against them.
- Prior warnings and events ignored

Bhopal Plant Management (4)

Process Model:

- Thought they were reducing avoidable and wasteful expenditures without affecting overall safety.
- Poor understanding of risk existing at plant.

Context:

- Losing money
- UC policy to turn off siren
- Turned off refrigeration to save money and reset high-level alarm
- Union Carbide put pressure on them to reduce costs (losses)
- Limited advanced technology industry and good jobs in India at the time

Union Carbide

Responsibilities:

- Oversee safety-critical operations at indian subsidiary
- Provide training, oversight
- Make sure plant is built and operated in a way that can adequately control hazards

CCAs:

- Did not install alarms, interlocks or automatic shutoff systems in critical places that would have warned operators or stopped gas leak before it spread
- Put pressure on Indian subsidiary to reduce losses, but gave no guidance on how this was to be done
- Gave up direct supervision of safety at plant, even though retained general financial and technical control
- Eliminated American advisors at plant, no on-site safety inspections

Union Carbide

CCAs (con't)

- Ignored warnings (e.g., plant manager resigned because disapproved of falling safety standards)
- Did they approve of refrigeration removal?
- No follow-on to 1982 audit report to determine if identified hazardous conditions had been corrected
- Went into full-scale production of MIC without adequate research on its stability or an effective inhibitor for type of reaction that occurred
- Did not learn from events at Bhopal and same thing happened in WV

Union Carbide

PM:

- Thought plant was being run safely
- Did not understand real risk at plant

Context:

- Losing money on plant
- Arrogance about American superiority
- Green revolution was important in feeding the world and provided big profits originally for MIC
- Put very hazardous operations in third world country?

Local Government Authorities

Responsibilities:

- Make sure population is informed about emergency procedures (emergency preparedness)
- Provide emergency procedures

UCA:

- Calling in army for help delayed.

PM:

- Thought the plant was being run safely

Context:

- Nobody at plant notified local authorities

Indian Government Regulators

Responsibilities:

- Provide oversight of plant operation to protect the workers and the public

CCAs:

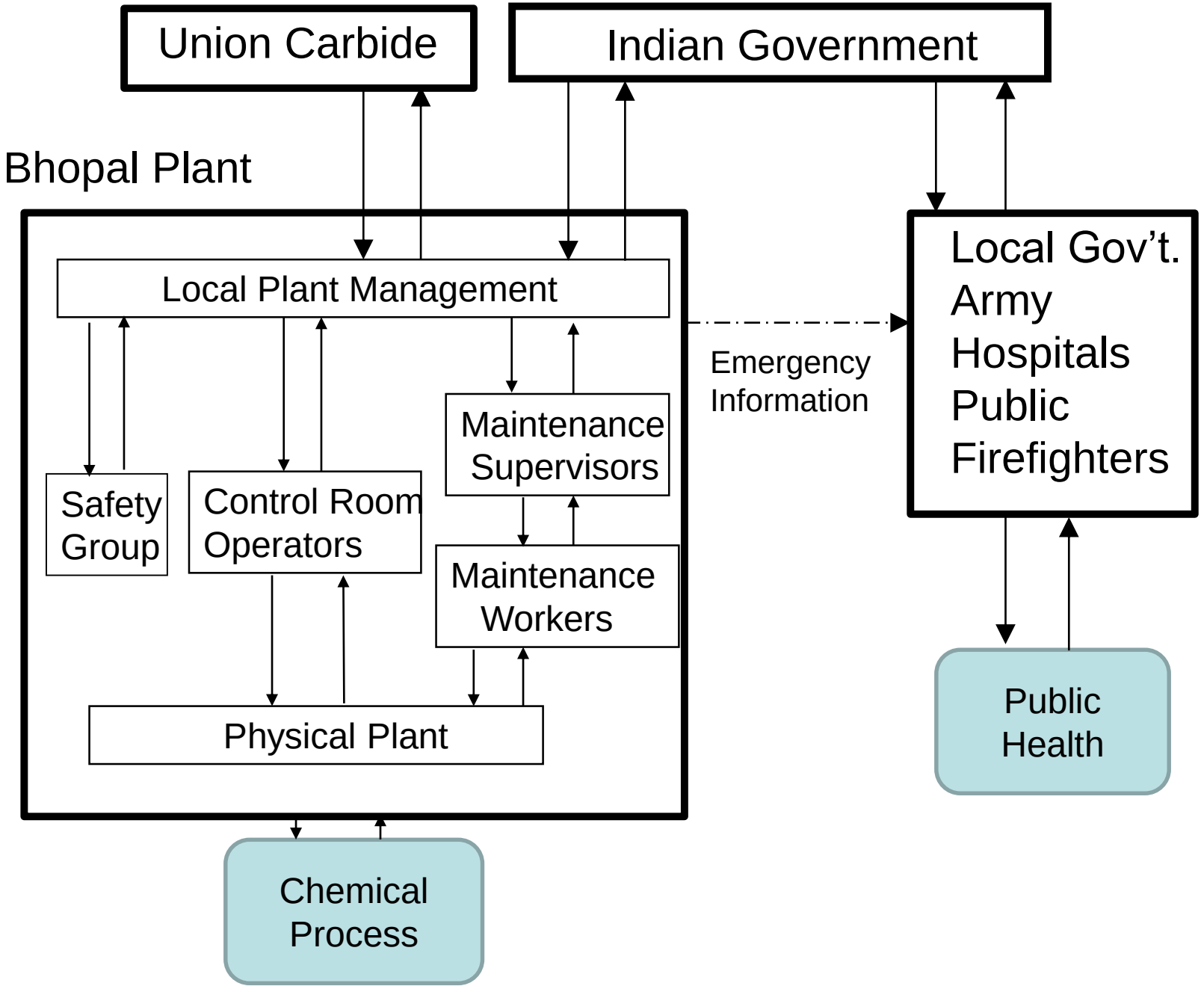
- Required plant to be operated completely by Indians
- Official inquiries into prior accidents were shelved or minimized government's and company's role
- Nothing done in response to previous warnings and events

Context:

- Important source of employment in a poor area

Overview so Far

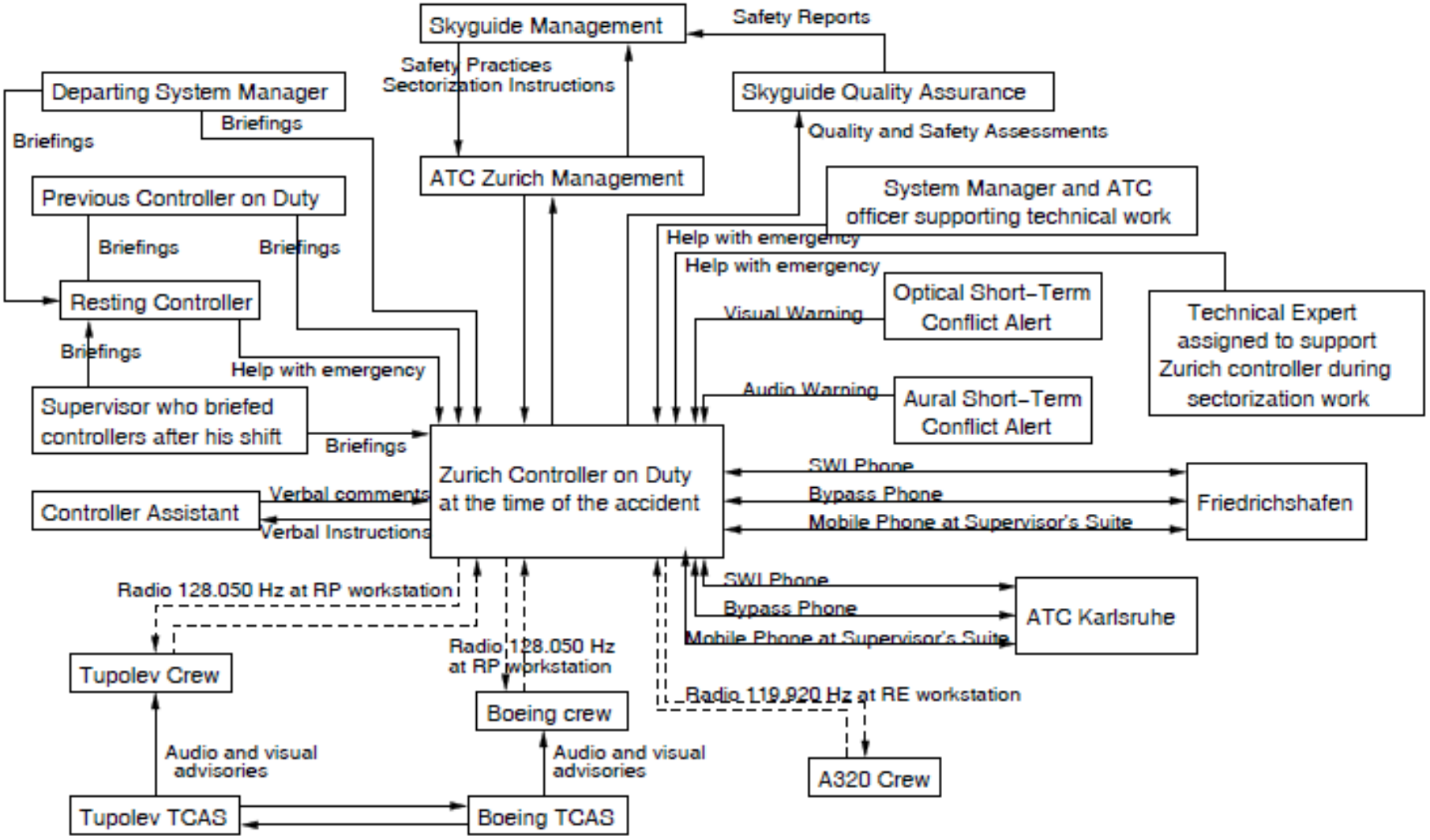
- Has your idea of the cause of this accident given the events changed?
- Was the pipe washer the root cause? The operators and maintainers?
- What is the “root cause”? Is there one?
- STAMP: Cause of all accidents is the same:
  - A safety control structure that does not prevent hazardous states and events.
  - Need to fix as much as you can to prevent future losses
- Still need to consider systemic factors affecting all components of control structure and their interactions


Union Carbide
Indian Government
Bhopal Plant
Local Plant Management
Safety Group
Control Room Operators
Maintenance Supervisors
Maintenance Workers
Physical Plant
Chemical Process
Emergency Information
Local Gov't.
Army
Hospitals
Public
Firefighters
Public Health

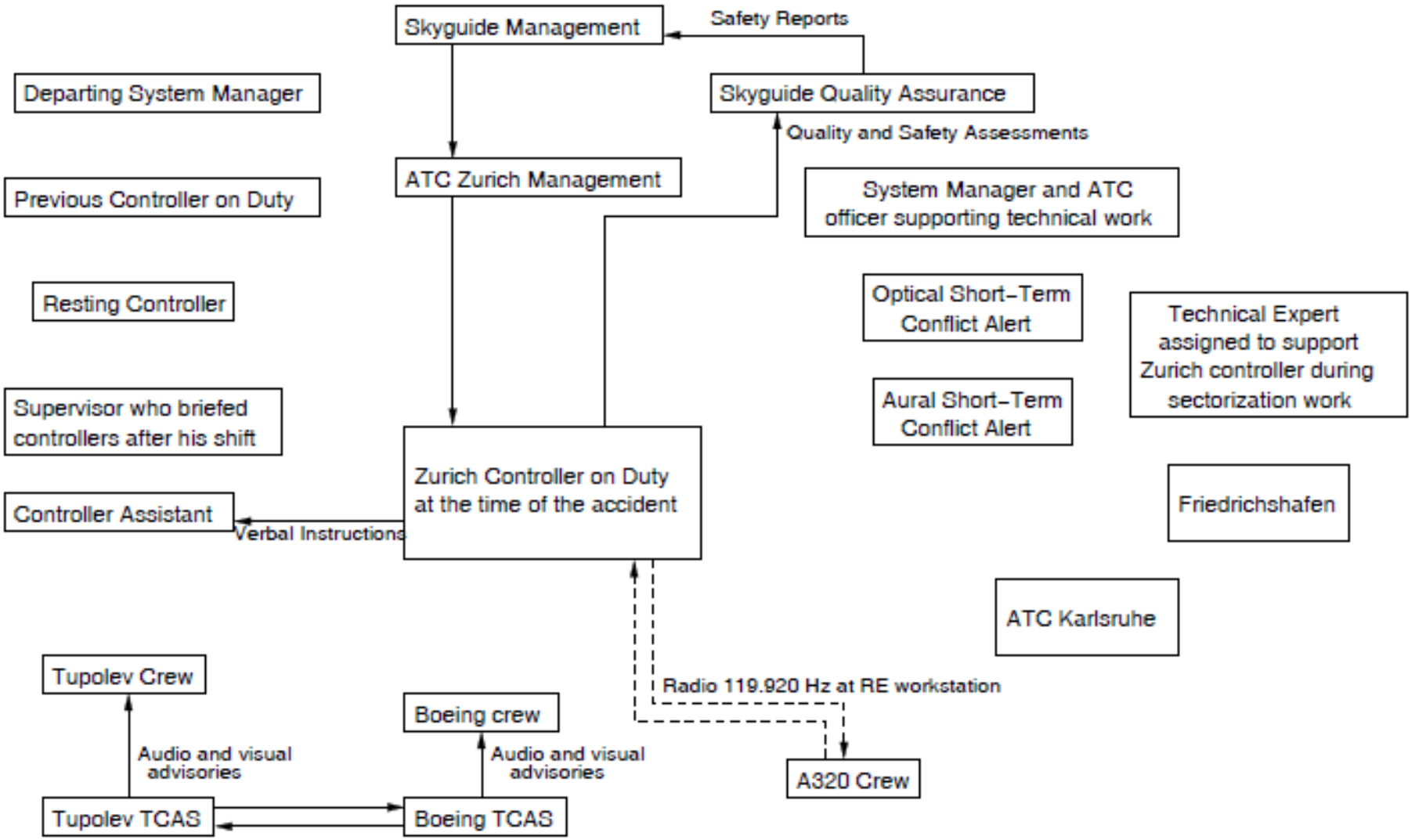
Flaws in Interactions Among SMS Components

- Safety Information System
- Safety Culture
- Dynamics and Changes over Time
  - Management of change
- Communication and Coordination

Communication Links Theoretically in Place in Uberlingen Accident



Communication Links Actually in Place



Conclusions

- The model used in accident or incident analysis determines what we what look for, how we go about looking for “facts”, and what facts we see as relevant.
- A linear chain-of-events promotes looking for something that broke or went wrong in the proximal sequence of events prior to the accident.
  - A stopping point, often, is arbitrarily determined at the point when something physically broke or an operator “error” (in hindsight) occurred.
  - Unless we look further, we limit our learning and almost guarantee future accidents related to the same factors.
- Goal should be to learn how to improve the safety controls (safety control structure) and not to find someone or something to blame.

Conclusions

- We need to use accident analysis processes that:
  - Avoid root cause seduction and oversimplification
  - Minimize hindsight bias (provide a structured process)
  - Are explanatory rather than accusatory
  - Emphasize a broad, contextual view of human behavior
    - Why did the person think it was the right thing to do at the time?

Discussion

- Generates more comprehensive list of causes and recommendations. But common complaints about this:
  - Too many causes?
    - Learning more from each accident
    - Can prioritize recommendations, do not need to respond to all immediately
  - Politics?
    - Partly now because blame now included in reports
    - Do we want to let this hinder learning from accidents?
  - Liability?
    - CAST takes out blame factor
    - Liability should be determined by courts, not by accident reports
    - Liability injects more politics in what should be an engineering process
  - Too much time?
    - Control structures are reused
    - Reports now take a long time to produce and are usually very comprehensive. CAST just generates <u>different</u> questions to ask.