System Safety Introduction

Uberlingen Mid-Air Collision

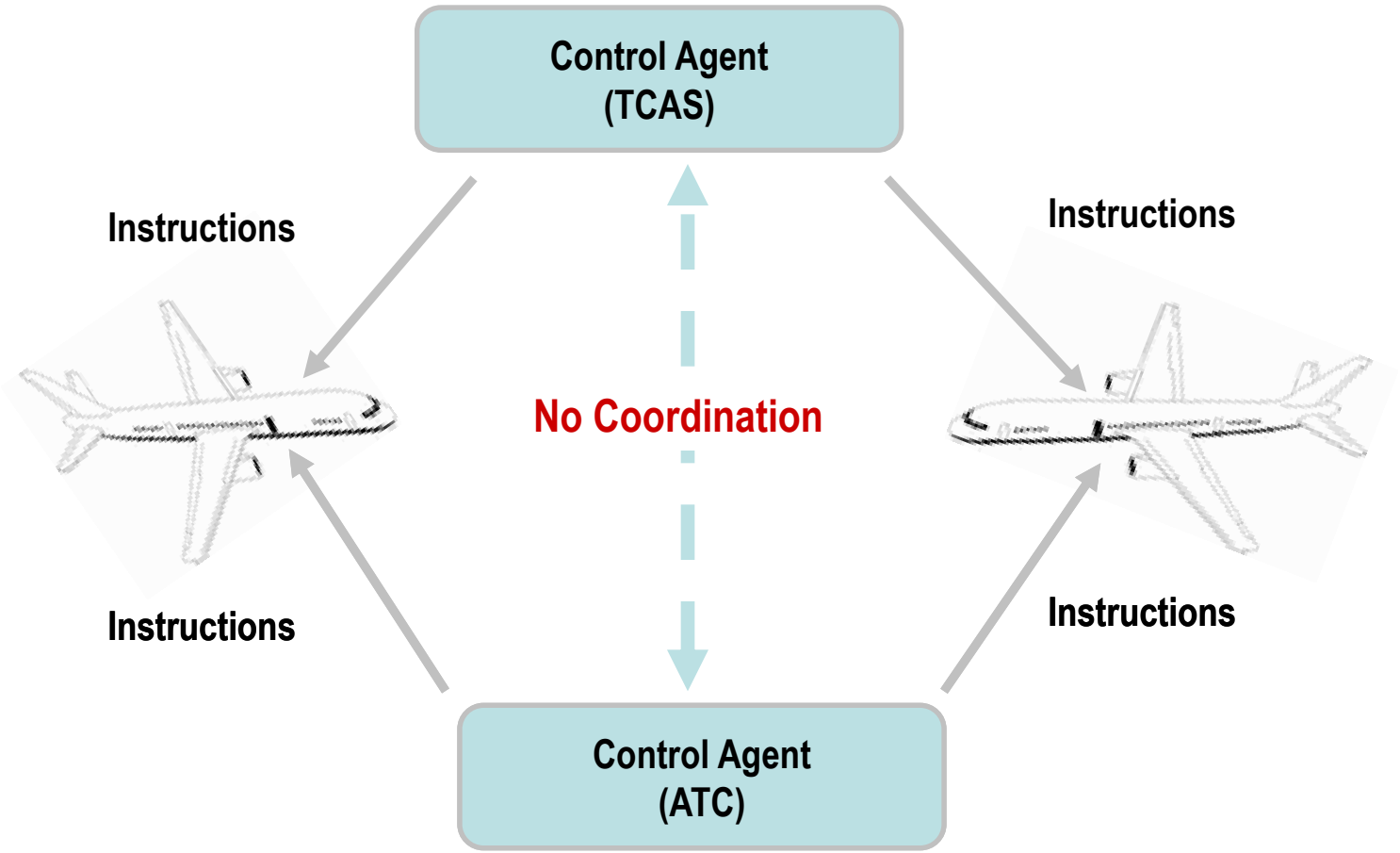
https://www.youtube.com/watch?v=CHjqun9c4Pc

(khchung787)

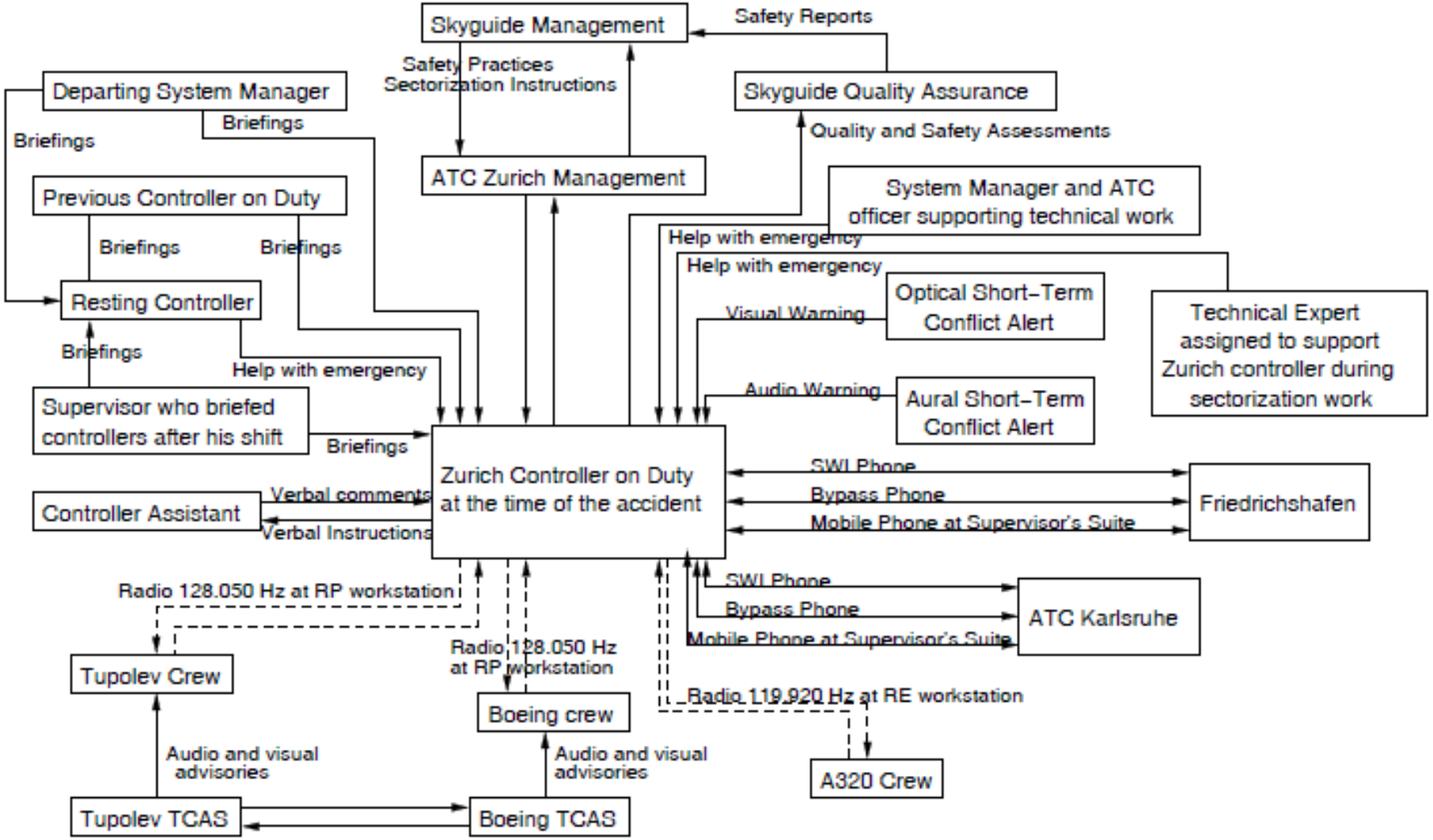
What were some of the causal factors in the Uberlingen accident?

Uncoordinated “Control Agents”

“UNSAFE STATE”
BOTH TCAS and ATC provide uncoordinated & independent instructions

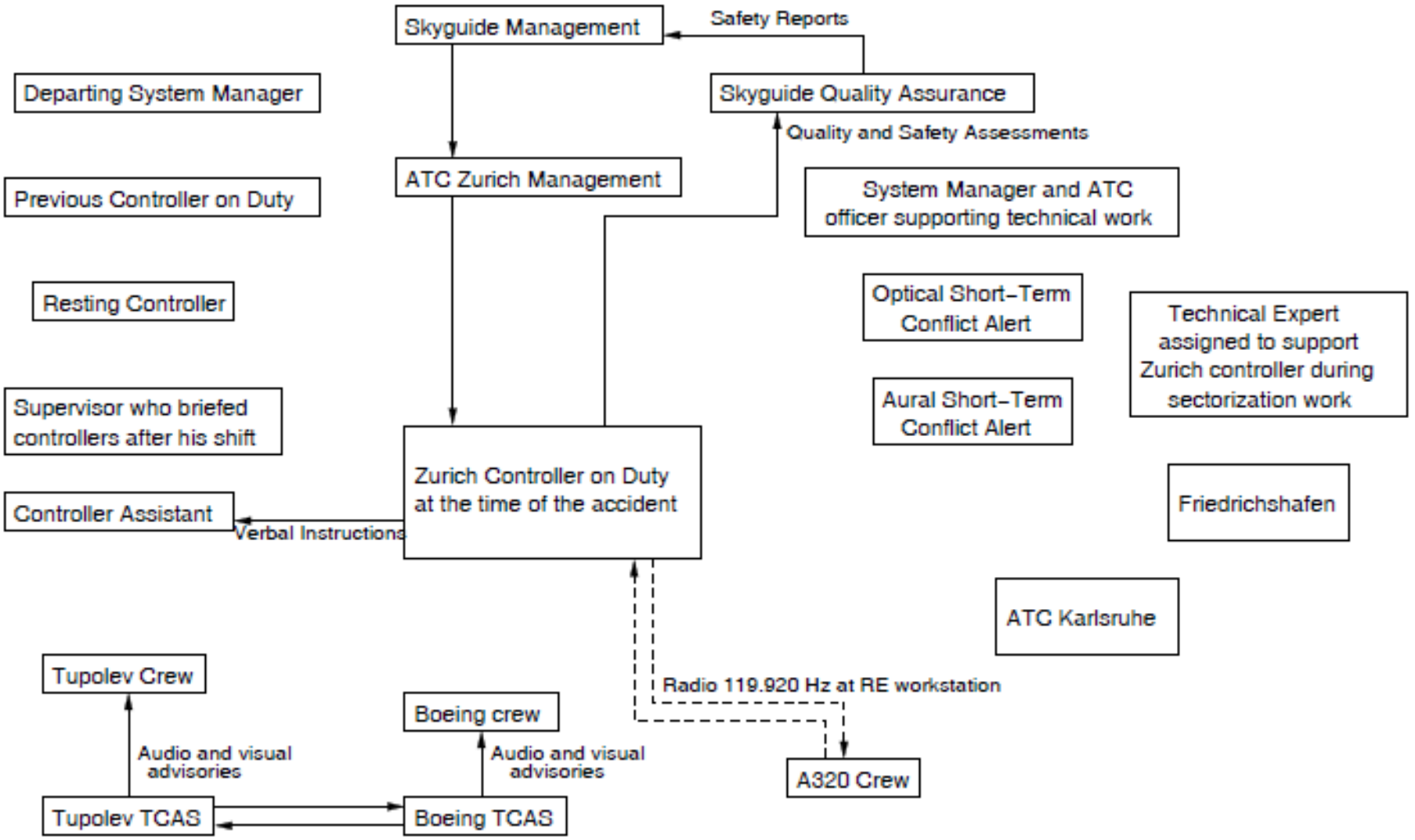


Communication Links Theoretically in Place in Uberlingen Accident



From Leveson, Nancy (2012). Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, © Massachusetts Institute of Technology. Used with permission.

Communication Links Actually in Place



From Leveson, Nancy (2012). Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, © Massachusetts Institute of Technology. Used with permission.

Uberlingen continued

- A year prior there was a near miss due to conflicting TCAS and ATC commands
  - Two Japanese airliners
  - One pilot made evasive maneuvers based on visual judgement.
    - Aircraft came within 300 ft
    - Evasive maneuvers caused ~100 injuries
  - Japan called for changes, but ICAO did not take action until after Uberlingen
- Four other near misses in Europe before Uberlingen collision

Uberlingen continued

- TCAS Pilot's Guide was ambiguous about TCAS / ATC precedence
- Tu-154 Flight Operations Manual had contradictory sections
  - Chapter 8.18.3.2 forbids maneuvers contrary to TCAS
  - Chapter 8.18.3.4 says "most important tool" is executing ATC instructions. TCAS described as an additional instrument.

Syllabus

Assignments and Grading

- Reading assignments and exercises
- Two group assignments: accident analysis and project
- One take home exam (on accident analysis and hazard analysis)

Textbooks and Readings:

- "Safeware"
- "Engineering a Safer World" (published by MIT Press
- Download free from the MIT Press website
- STPA Primer (draft) for reference only
- Optional readings just if you are interested

Acident Causes are Complex

- The vessel Baltic Star, registered in Panama, ran aground at full speed on the shore of an island in the Stockholm waters on account of thick fog. One of the boilers had broken down, the steering system reacted only slowly, the compass was maladjusted, the captain had gone down into the ship to telephone, the lookout man on the bow took a coffee break, and the pilot had given an erroneous order in English to the sailor who was tending the rudder. The latter was hard of hearing and understood only Greek.

  Le Monde

Were there also larger organizational and economic factors?

Components of System Safety Engineering

- Investigating accidents
- Preventing Accidents
  - Hazard Analysis
  - Design for Safety
- Operations
- Management

Investigating/Understanding Accidents

- What are ALL the factors involved?
- Are there tools to help us find all the factors?
- How do we minimize hindsight bias?
- How do we learn from accidents in order to prevent them in the future?

Hazard Analysis

- “Investigating an accident before it occurs”
- Identify potential scenarios
- Worst case analysis vs. average (expected) case analysis
- Use results to prevent losses

Design for Safety

- Eliminate or control scenarios (causal factors) identified by hazard analysis
- Fault Tolerance
  - Failures will occur
  - Need to make sure they don't result in an accident
- Design to prevent operator error
  - Human errors will occur
  - Need to make sure they don't result in an accident
  - Design so that don't induce human error

Understanding Accident Causality

Bhopal

- Worst industrial accident in history
  - Conservative estimate of 2000-3000 killed, 10,000 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)

Safety Features

- UC specified requirements to reduce hazards:
  - MIC was to be stored in underground tanks encased in concrete
  - Bhopal used three double-walled, stainless steel tanks, each with a capacity of 60 tons.
  - Operating manual specified that tanks were never to contain more than half their maximum volume or a standby tank was to be available to which some of chemical could be transferred in case of trouble.
  - Bhopal tanks were interconnected so that MIC in one tank could be bled into another tank.
  - As specified in operating manual, tanks embedded in concrete.

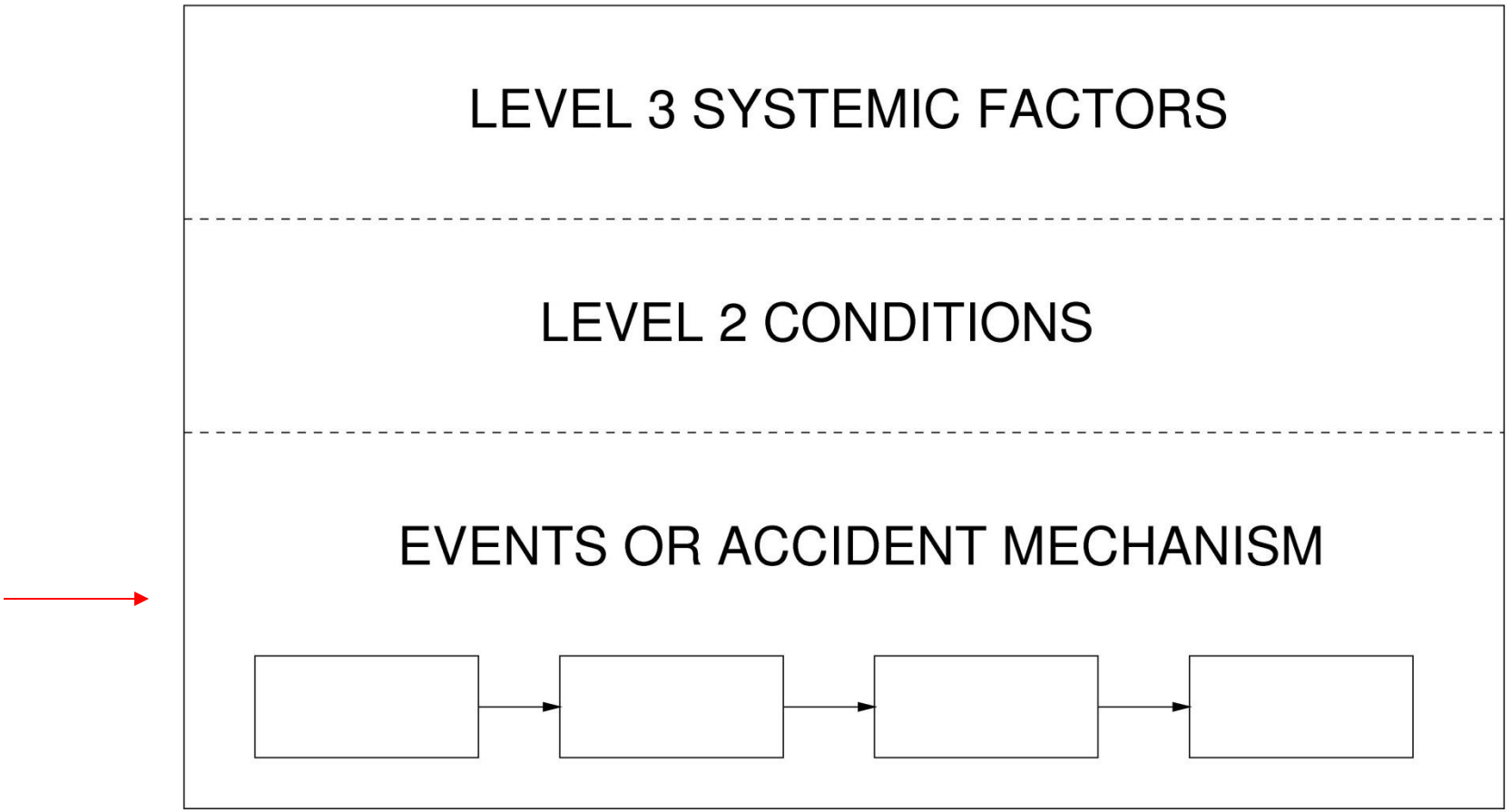
Safety Features (con't)

- Several backup protection systems and lines of defense
  - Vent gas scrubber designed to neutralize any escaping gas with caustic soda. Scrubber was capable of neutralizing about 8 tons of MIC per hour at full capacity
  - Flare tower to burn off any escaping gas missed by scrubber; toxic gases would be burned high in the air, making them harmless
  - Small amounts of gas missed by scrubber and flare tower were to be knocked down by a water curtain that reached 40 to 50 feet above ground. Water jets could reach as high as 115 feet, but only if operated individually.
  - In case of an uncontrolled leak, a siren was installed to warn workers and surrounding community.

Safety Features (con't)

- MIC was to be stored in an inert atmosphere of nitrogen gas at 2 to 10 psi over atmospheric pressure.
- Regularly scheduled inspection and cleaning of valves specified as imperative
- Storage limited to 12 months maximum.
- If staff were doing sampling, testing, or maintenance at a time when there was a possibility of a leak or spill, operating manual specified they were to use protective rubber suits and air-breathing equipment.
- To limit its reactivity, MIC was to be maintained at a temperature near 0 C.
  - Refrigeration unit provided for this purpose
  - High temperature alarm if MIC reached 11 C.

Hierarchical models



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
  - Maintenance sheet contained no instruction to insert disk
  - Worker assigned task did not check to see whether pipe properly isolated because said it was not his job to do so.
  - He knew valves leaked, but safety disks were job of maintenance department.

- 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.
  - Leaky valves were common and were not considered significant

- Workers looked for leak and saw a continuous drip on outside of MIC unit.
  - Reported it to the MIC supervisor
  - Shift 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.

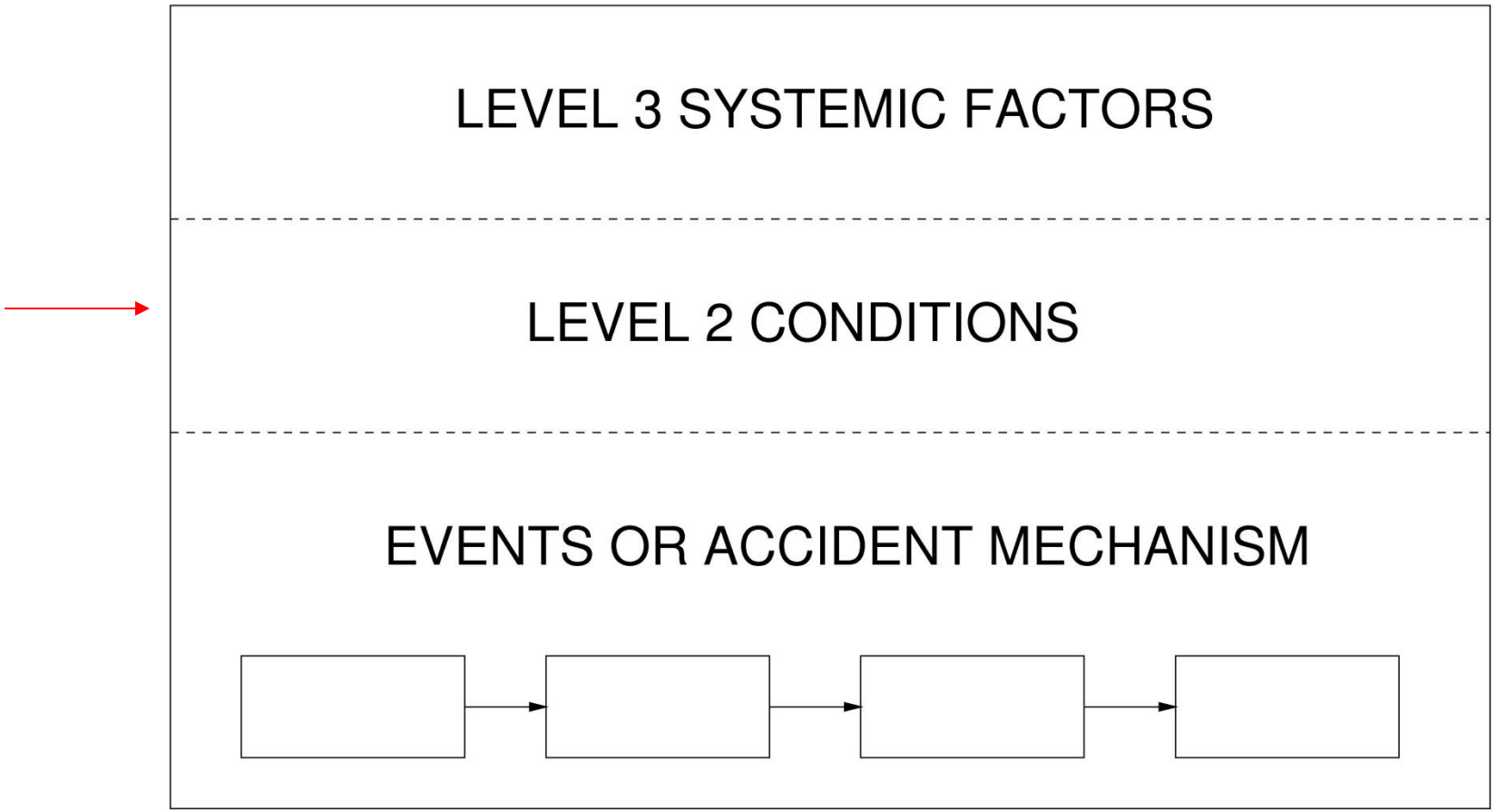
- MIC supervisor could not find his oxygen mask and ran to boundary fence, where he broke his leg attempting to climb over it.
- Control room supervisor stayed in control room until the next afternoon, when he emerged unharmed.
- Toxic gas warning siren not activated until 12:50 am when MIC seen escaping from vent stack.
  - Turned off after only 5 minutes, which was Union Carbide policy.
  - 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 were the causes of this accident given what you know so far?

What additional questions were raised by what you have seen so far?

Hierarchical models



What about all the safety devices and procedures?

- How could the vent scrubber, flare tower, water spouts, refrigeration unit, alarms, and monitoring instruments all fail simultanously?
- Not uncommon for a company to turn off passive safety devices to save money; gauges are frequently out of service.
  - At Bhopal, few alarms, interlocks, or automatic shutoff systems in critical locations that might have warned operators of abnormal conditions or stopped the gas leak before it spread.
  - Thresholds established for production of MIC routinely exceeded. e.g., workers said it was common to leave MIC in the spare tank.

- Operating manual said refrigeration unit must be operating whenever MIC was in the system
  - Chemical has to be maintained at a temp no higher than 5 C. to avoid uncontrolled reactions.
  - High temperature alarm to sound if MIC reached 11 C.
  - Refrigeration unit turned off and MIC usually stored at nearly 20 C.
  - Plant management adjusted threshold of alarm, accordingly, from 11 C to 20 C., thus eliminating possibility of an early warning of rising temperatures.
- Flare tower was totally inadequate to deal with estimated 40 tons of MIC that escaped during accident.
  - Could not be used anyway because pipe was corroded and had not been replaced.

- Vent scrubber (had it worked) was designed to neutralize only small quantities of gas at fairly low pressures and temperatures.
  - Pressure of escaping gas during accident exceeded scrubber's design by nearly 2 ½ times
  - Temperature of escaping gas at least 80 degrees more than scrubber could handle.
  - Shut down for maintenance
- Water curtain designed to reach height of 40 to 50 feet. MIC vapor vented over 100 feet above ground.
- Practice alerts did not seem to be effective in preparing for an emergency (ran from contaminated areas and ignored buses sitting idle and ready to evacuate them)

- Pipe-washing operation should have been supervised by second shift operator, but that position had been eliminated due to cost cutting.
- Tank 610 contained 40 to 50 tons of MIC out of total capacity of 60 tons, which violated safety requirements.
  - Tanks were not to be more than half filled
  - Spare tank was to be available to take excess
  - Adjacent tank thought to contain 15 tons according to shipping records, but contained nearer to 21 tons
  - Spare tank (619) contained less than 1 ton, but level gauge showed it was 20 percent full
  - Many of gauges not working properly or were improperly set.

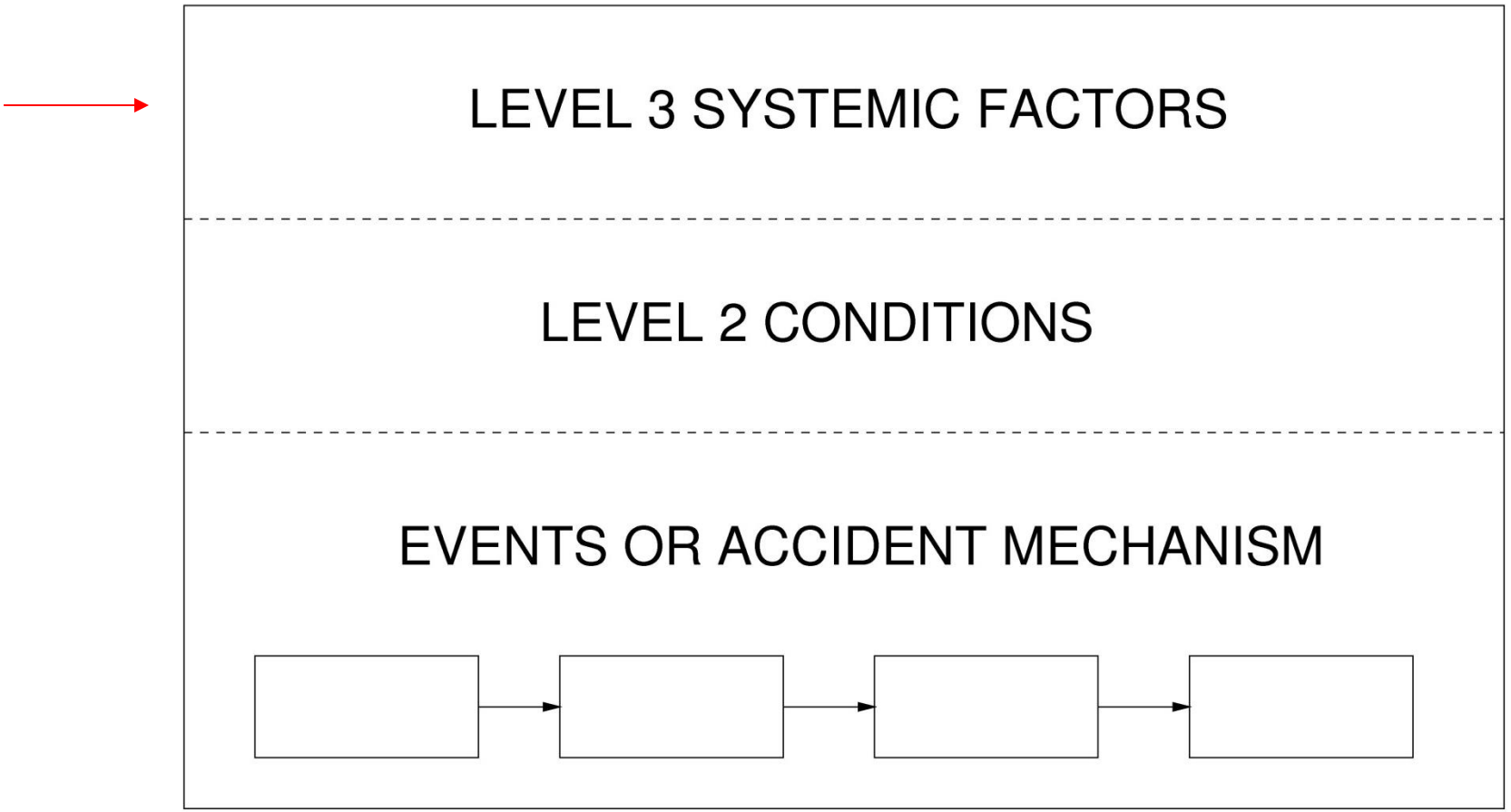
- Alarms sounded so many times a week (20 to 30) that no way to know what the siren signified
  - Emergency signal was identical to that used for other purposes, including practice drills.
  - Not turned on until 2 hours after MIC leak started and then turned off after 5 minutes (company policy)
- Plant workers had only bare minimum of emergency equipment, e.g., shortage of oxygen masks discovered after accident started.
  - They had almost no knowledge or training about how to handle non-routine events.
- Police were not notified when chemical release began
  - When called by police and reporters, plant spokesmen first denied accident and then claimed MIC was not dangerous.
- Surrounding community not warned or prepared

Has your view of this accident changed with this additional information ?

What additional causal factors would you now include?

What additional questions would you want answered?

Hierarchical models



Additional Information about Systemic Factors

- Demand for MIC dropped sharply after 1981, leading to reductions in production and pressure on company to cut costs.
  - Plant operated at less than half capacity when accident occurred.
  - UC put pressure on Indian subsidiary to reduce losses, but gave no specific details about how this was to be done.
- In response, maintenance and operating personnel cut in half.
  - Top management justified cuts as merely reducing avoidable and wasteful expenditures without affecting overall safety.
- As plant lost money, many of skilled workers left for more secure jobs. They either were not replaced or replaced by unskilled workers.

- Maintenance procedures severely cut back and shift relieving system suspended (if no replacement showed up at end of shift, following shift went unmanned).
- Indian government required plant to be operated completely by Indians
  - At first, UC flew plant personnel to West Virginia for intensive training and had teams of U.S. engineers make regular on-site safety inspections.
  - By 1982, financial pressures led UC to give up direct supervision of safety at the plant, even though it retained general financial and technical control.
  - No American advisors resident at Bhopal after 1982.
- Minimal training of many of workers in how to handle non-routine emergencies.

- Several Indian staff who were trained in U.S. resigned and were replaced by less experienced technicians.
  - When plant first built, operators and technicians had equivalent of two years of college education in chemistry or chemical engineering.
  - In addition, UC provided them with 6 months training.
  - When plant began to lose money, educational standards and staffing levels were reportedly reduced.
- In 1983, chemical engineer managing MIC plant resigned because he disapproved of falling safety standards. He was replaced by an electrical engineer.

- Morale at the plant was low. Management and labor problems followed the financial losses.

  "There was widespread belief among employees that the management had taken drastic and imprudent measures to cut costs and that attention to the details that ensure safe operation were absent."

- Five months before accident, local UC India management decided to shut down refrigeration system.
  - Most common reason given was cost cutting.
  - Local management claimed unit was too small and never worked satisfactorily.
  - Disagreement about whether UC in U.S. approved this measure.
  - High temperature alert reset and logging of tank temperatures discontinued.

- Other examples of unsafe conditions that were permitted to exist:
  - At time of accident, chloroform contamination of MIC was 4 to 5 times higher than specified in operating manual, but no corrective action taken.
  - MIC tanks were not leak-tight to a required pressure test.
  - Workers regularly did not wear safety equipment, such as gloves or masks because of high temperatures in plant. There was no air conditioning.
  - Inspections and safety audits at the plant were few and superficial.

- A review and audit of Bhopal plant in 1982 noted many of deficiencies involved in accident
  - No follow-up to ensure deficiencies were corrected.
  - A number of hazardous conditions were known and allowed to persist for considerable amounts of time or inadequate precautions were taken against them.
  - Report noted such things as filter-cleaning operations without using slip blinds, leaking valves, possibility of contaminating the tank with material from the vent gas scrubber, bad pressure gauges.
  - Report recommended raising capacity of water curtain. Pointed out that alarm at flare tower was non-operational and thus any leakage could go unnoticed for a long time.
  - According to Bhopal manager, all improvements called for in the report had been taken care of, but obviously not true.

- Prior warnings and events presaging the accident were ignored:
  - 6 serious incidents between 1981 and 1984, several of which involved MIC
  - One worker killed in 1981, but official inquiries required by law were shelved or tended to minimize government's or company's role.
  - A leak similar to one involved in the big one had occurred the year before.
  - Journalists and others tried to warn of dangers
  - At least one person within government tried to bring up hazards of plant. He was forced to resign.
  - Local authorities and plant managers did nothing in response.

- UC went into large-scale production of MIC without having performed adequate research on stability of the chemical. Did not know of an effective inhibitor for the type of reaction that occurred.
- After the accident, both UC and OSHA announced same type of accident could not occur at Institute WV plant because of plant's better equipment, better personnel, and America's general "higher level of technical culture."
  - Eight months later a similar accident occurred there. Led to brief hospital stays for 100 people. Consequences less serious only because of incidental factors such as direction of wind and tank contained a less toxic substance at the time.
  - Warning siren delayed and company slow in making information available to public.

- A few months later, leak at another UC plant created a toxic cloud that traveled to a shopping center.
- Several people had to be given emergency treatment, but for two days, doctors and health officials did not know what toxic chemical was or where it came from because UC denied leak's existence.
- OSHA fined UC $1.4 million after Institute accident charging "constant, willful, and overt violations at the plant and a general atmosphere and attitude that "a few accidents here and there are the price of production."

Do you see any additional factors you did not note before?

Are these factors unique to the Bhopal accident?

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

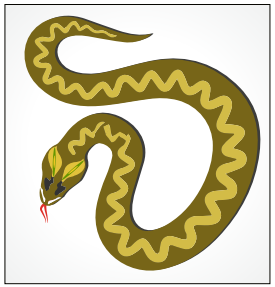


Image by MIT OpenCourseWare.

Image by MIT OpenCourseWare.

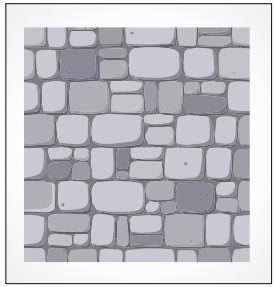


Image by MIT OpenCourseWare.

Image by MIT OpenCourseWare.

Image by MIT OpenCourseWare.

Image by MIT OpenCourseWare.

Image by MIT OpenCourseWare.

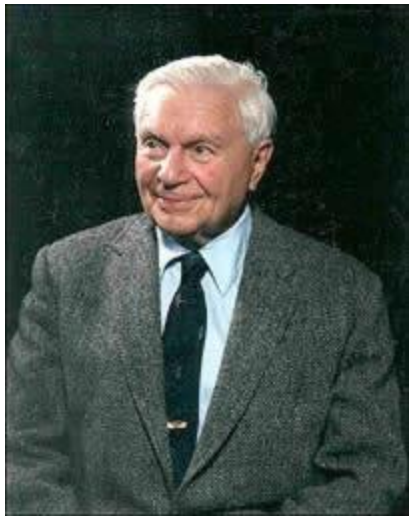
And so these men of Hindustan
Disputed loud and long,
Each in his own opinion
Exceeding stiff and strong,
Though each was partly in the right
And all were in the wrong.

John Godfrey Saxe (1816-1887)

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,



- 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.”

Root Cause Seduction

- Accidents always complex, but usually blamed on human operators
- Cannot prevent them unless understand ALL the factors that contributed
- Always additional factors (sometimes never identified)
  - Equipment failure and design
  - Procedures
  - Management decisions
  - Etc.

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 fire-fighting mode
    - Having the same accident over and over

Blame is the Enemy of Safety

- Goal of the courts is to establish blame
  - People stop reporting errors
  - Information is hidden
- Goal of engineering is to understand why accidents occur in order to prevent them

Exxon Valdez

- Shortly after midnight, March 24, 1989, tanker Exxon Valdez ran aground on Bligh Reef (Alaska)
  - 11 million gallons of crude oil released
  - Over 1500 miles of shoreline polluted
- Exxon and government put responsibility on tanker Captain Hazelwood, who was disciplined and fired
- Was he to “blame”?
  - State-of-the-art iceberg monitoring equipment promised by oil industry, but never installed. Exxon Valdez traveling outside normal sea lane in order to avoid icebergs thought to be in area
  - Radar station in city of Valdez, which was responsible for monitoring the location of tanker traffic in Prince William Sound, had replaced its radar with much less powerful equipment. Location of tankers near Bligh reef could not be monitored with this equipment.

- Congressional approval of Alaska oil pipeline and tanker transport network included an agreement by oil corporations to build and use double-hulled tankers. Exxon Valdez did not have a double hull.

- Crew fatigue was typical on tankers
  - In 1977, average oil tanker operating out of Valdez had a crew of 40 people. By 1989, crew size had been cut in half.
  - Crews routinely worked 12-14 hour shifts, plus extensive overtime
  - Exxon Valdez had arrived in port at 11 pm the night before. The crew rushed to get the tanker loaded for departure the next evening

- Coast Guard at Valdez assigned to conduct safety inspections of tankers. It did not perform these inspections. It's staff had been cut by one-third.

- Tanker crews relied on the Coast Guard to plot their position continually.
  - Coast Guard operating manual required this.
  - Practice of tracking ships all the way out to Bligh reef had been discontinued.
  - Tanker crews were never informed of the change.
- Spill response teams and equipment were not readily available. Seriously impaired attempts to contain and recover the spilled oil.

Summary:

- Safeguards designed to avoid and mitigate effects of an oil spill were not in place or were not operational
- By focusing exclusively on blame, the opportunity to learn from mistakes is lost

Postscript:

Captain Hazelwood was tried for being drunk the night the Exxon Valdez went aground. He was found “not guilty”

Do Operators Really Cause Most Accidents?

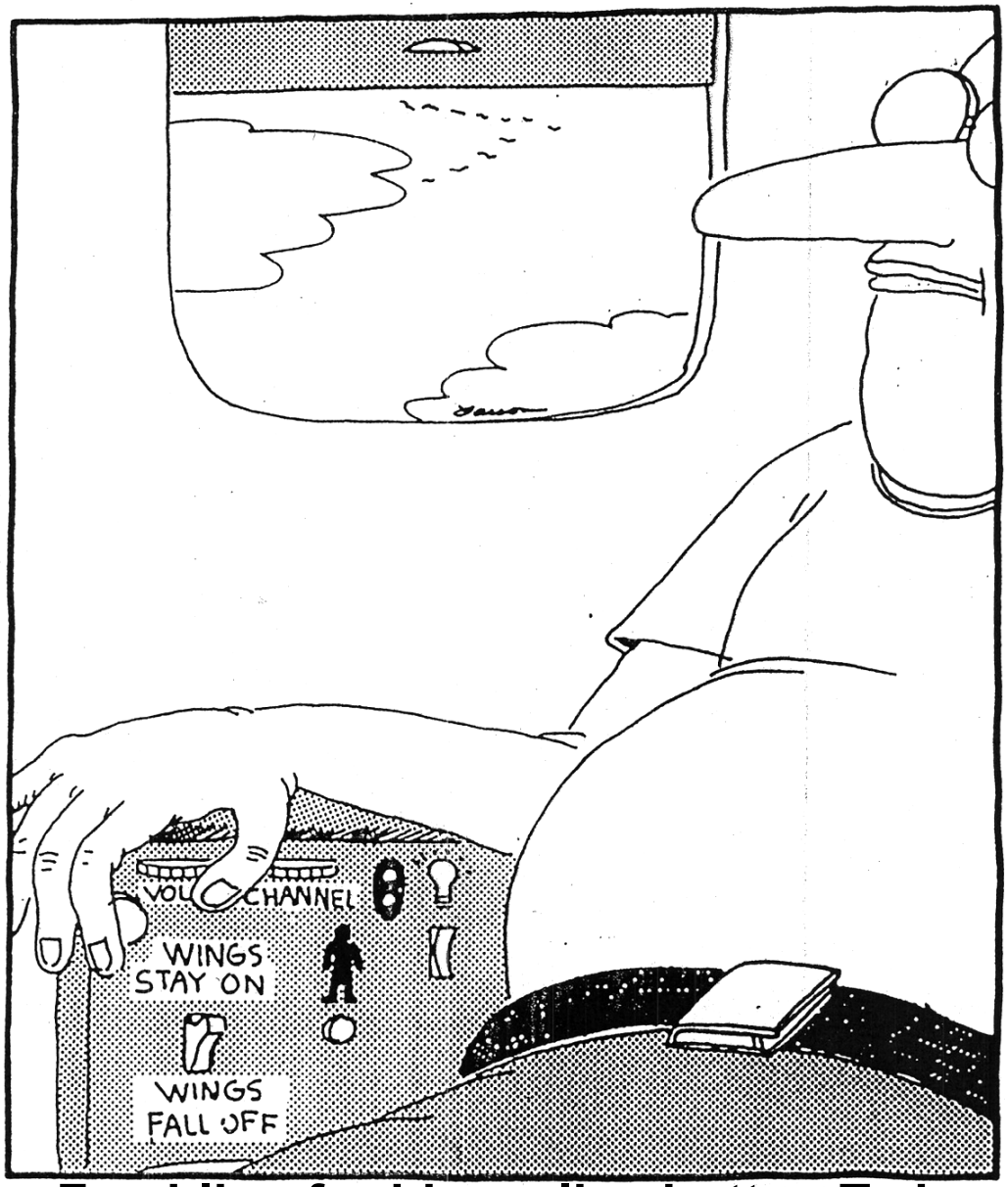
- When say human error, usually mean “operator error”
- Operator error vs. design error
- Hindsight bias

Operator Error: Traditional View

- Operator error is cause of most incidents and accidents
- So do something about operator involved (suspend, 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

The second important factor is system design vs. operator error

All human behavior is affected by the context in which it occurs.



Fumbling for his recline button Ted unwittingly instigates a disaster

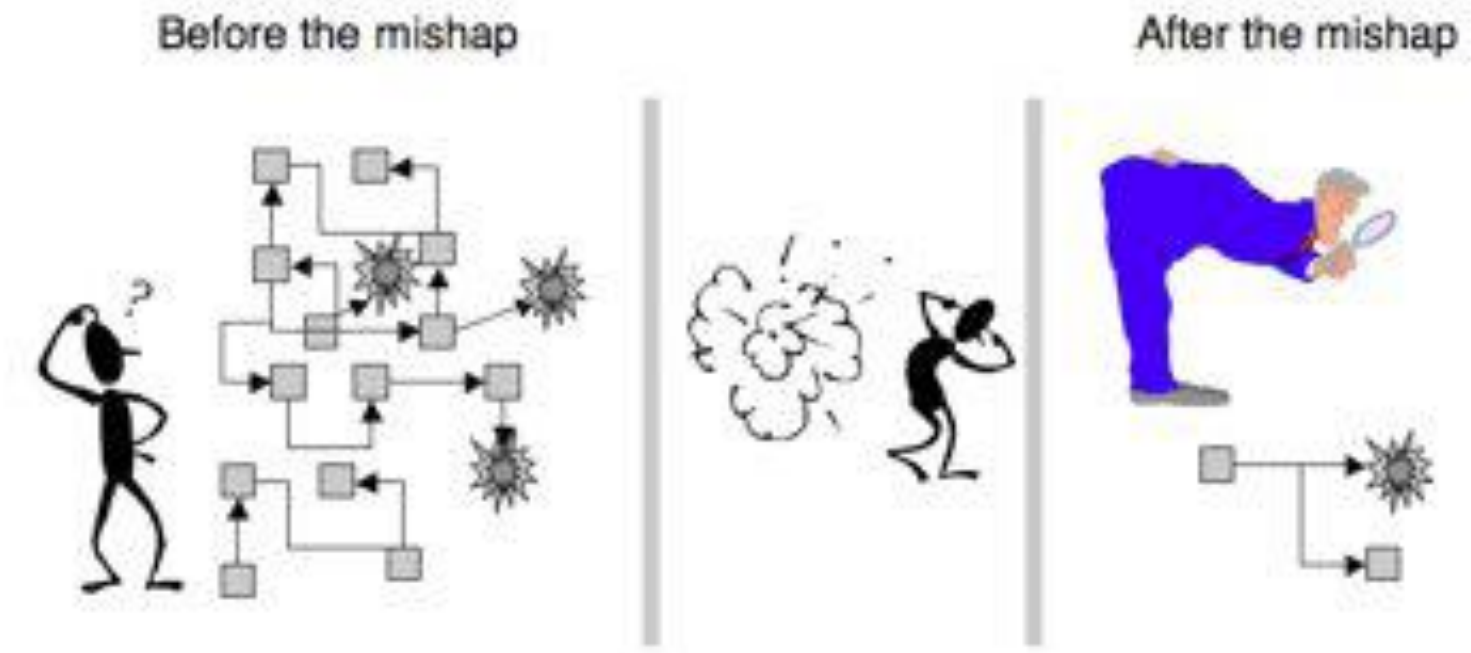
Operator Error: Systems View (1)

- 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
- **Human error is a symptom of a system that needs to be redesigned**

Hindsight Bias



Courtesy of Sidney Dkker. Used with permission.

(Sidney Dekker, 2009)

“should have, could have, would have”

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

Hindsight Bias

- Almost impossible to go back and understand how world looked to somebody not having knowledge of outcome
  - Oversimplify causality because start from outcome and reason backward
  - Overestimate likelihood of the outcome and people's ability to foresee it because already know outcome
  - Overrate rule or procedure "violations"
  - Misjudge prominence or relevance of data presented to people at the time
  - Match outcomes with actions that went before it: if outcome bad, actions leading to it must have been bad too (missed opportunities, bad assessments, wrong decisions, and misperceptions)

Overcoming Hindsight Bias

- Assume nobody comes to work to do a bad job.
  - Assume were doing reasonable things given the complexities, dilemmas, tradeoffs, and uncertainty surrounding them.
  - Simply finding and highlighting people's mistakes explains nothing.
  - Saying what did not do or what should have done does not explain why they did what they did.

Overcoming Hindsight Bias

- Need to consider why it made sense for people to do what they did
- Some factors that affect behavior
  - Goals person pursuing at time and whether may have conflicted with each other (e.g., safety vs. efficiency, production vs. protection)
  - Unwritten rules or norms
  - Information availability vs. information observability
  - Attentional demands
  - Organizational context

16.63J / ESD.03J System Safety
Spring 2016