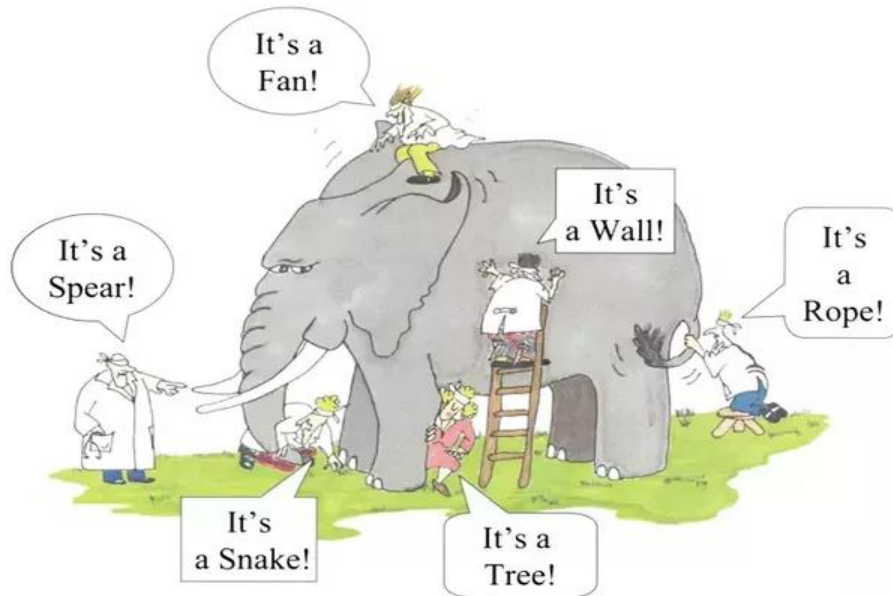


Analyzing Accidents and Incidents with CAST

STAMP Workshop Tutorial March 27, 2017

Nancy Leveson, MIT

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



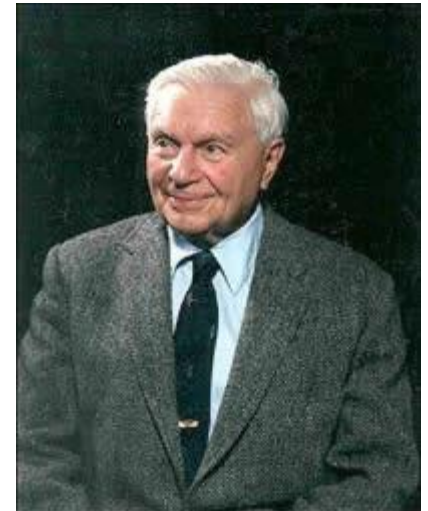
And so these men of Hindustan
Disputed loud and long,
Each in his own opinion
Exceeding stiff and strong,
Though each was partly in the right
And all were in the wrong.

John Godfrey Saxe (1816-1887)

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



Jerome Lederer

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.”

Common Traps in Understanding Accident Causes

- Root cause seduction
- Hindsight bias
- Focus on blame
- Narrow views of human error

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
 - Etc.

“Blame is the Enemy of Safety”

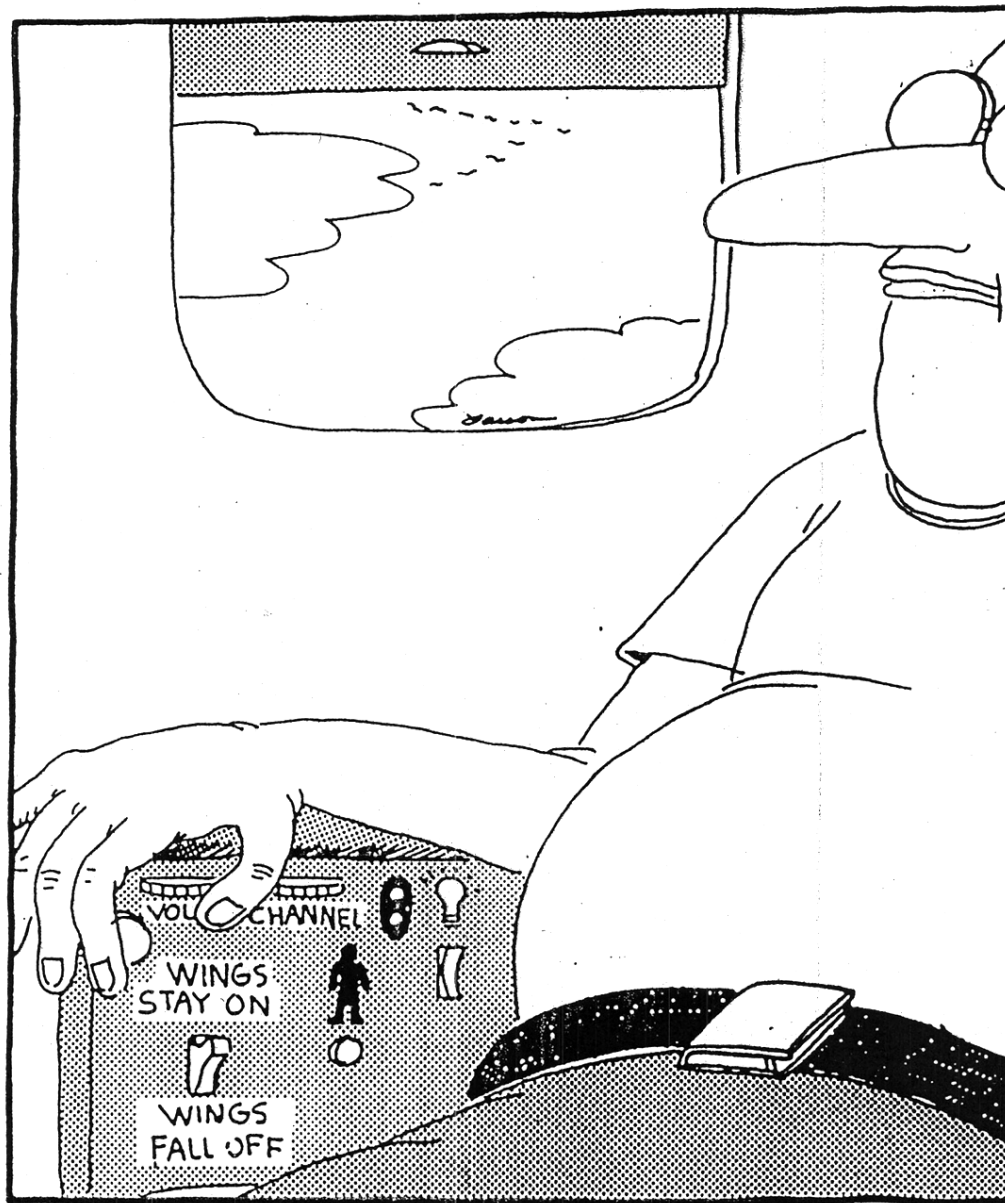
- To prevent accidents in the future, need to focus on why it happened, not who to blame
- Blame is for the courts, prevents understanding what occurred and how to fix it.

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

Operator Error: **Traditional View**

- Human error is cause of incidents and accidents
- So do something about human involved (suspend, retrain, admonish)
- Or do something about humans 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)**

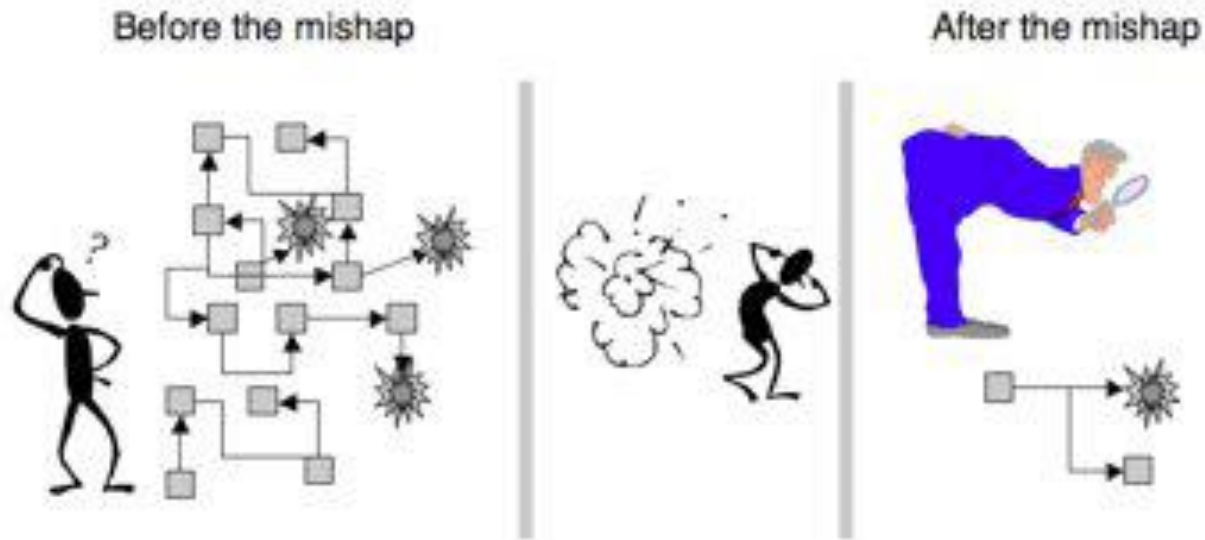
- To do something about error, must look at system in which people work:
 - Design of equipment
 - Usefulness of procedures
 - Existence of goal conflicts and production pressures
- **Human error is a symptom of a system that needs to be redesigned**

Cali American Airlines Crash

Identified causes:

- Flight crew's failure to adequately plan and execute the approach to runway 10 at Cali and their **inadequate use of automation**
- Failure of flight crew to discontinue the approach into Cali, despite numerous cues alerting them of the inadvisability of continuing the approach
- **Lack of situational awareness of the flight crew regarding vertical navigation, proximity to terrain, and the relative location of critical radio aids**
- **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.**

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”

Overcoming Hindsight Bias

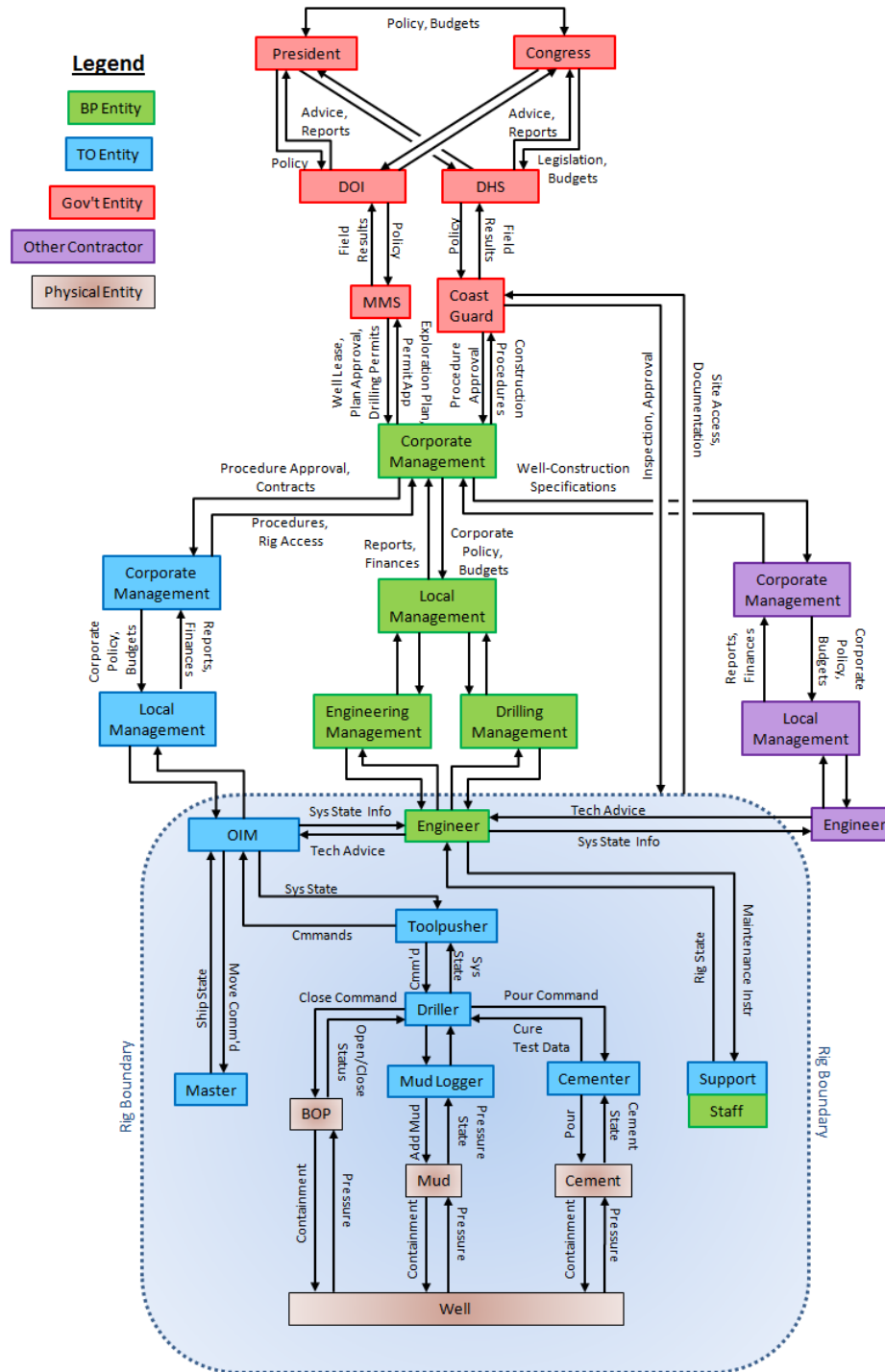
- Assume nobody comes to work to do a bad job.
 - Assume were doing reasonable things given the complexities, dilemmas, tradeoffs, and uncertainty surrounding them.
 - Simply finding and highlighting people's mistakes explains nothing.
 - Saying what did not do or what should have done does not explain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

Goals for an Accident Analysis Technique

- 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
- Goal is to determine
 - Why people behaved the way they did
 - Weaknesses in the safety control structure that allowed the loss to occur



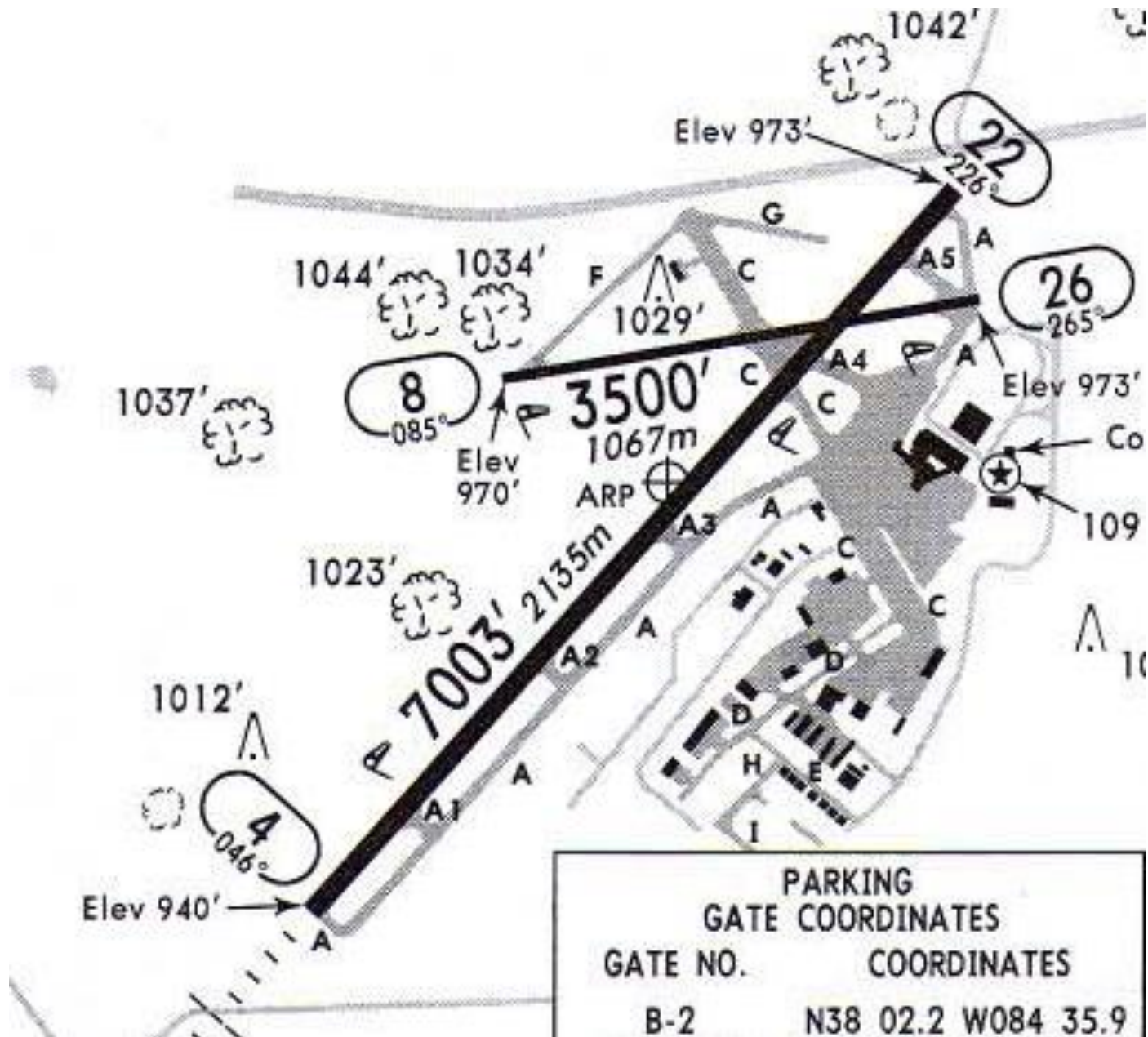
Analysis Results Format

- For each component, will identify:
 - Safety responsibilities
 - Unsafe control actions that occurred
 - Contextual reasons for the behavior
 - Mental (process) model flaws that contributed to it
- Two examples will be done in the tutorial. Lots more examples are in the ESW book (chapters 6 and 11 as well as the ESW appendices) and on our website.
 - Comair Lexington crash
 - Shell Moerdijk Refinery Explosion

ComAir 5191 (Lexington) Sept. 2006



**Analysis using CAST by Paul Nelson,
ComAir pilot and human factors expert
(for report: <http://sunnyday.mit.edu/papers/nelson-thesis.pdf>)**



First identify the system hazard and safety constraint violated

What were the

1. System hazard
2. System safety constraint

violated in this accident?

Identify Hazard and Safety Constraint Violated

- Accident: death or injury, hull loss
- System hazard: *Runway incursions and operations on wrong runways or taxiways.*
- System safety constraint: *The safety control structure must prevent runway incursions and operations on wrong runways or taxiways*

Goal: *Figure out why the safety control structure did not do this*

Identifying Components to Include

- Start with physical process
- What inadequate controls allowed the physical events?
 - Physical
 - Direct controller
 - Indirect controllers
- Add controls and control components as required to explain the inadequate controls already identified.

Physical Components

- Aircraft
- Runway and airport infrastructure

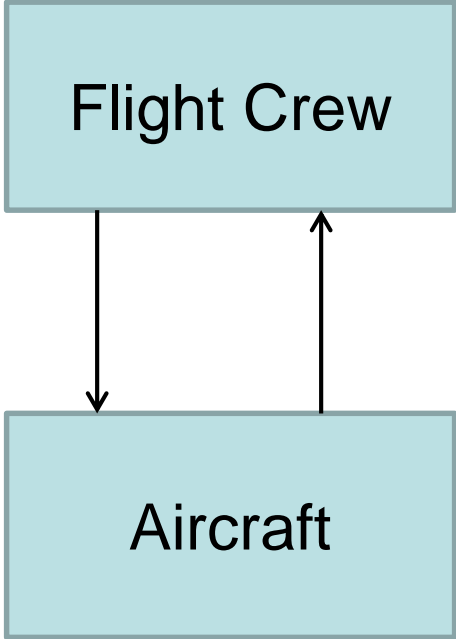
What physical failures occurred?

What unsafe interactions?

Physical System (Aircraft)

- Failures: None
- Unsafe Interactions
 - Took off on wrong runway
 - Runway too short for that aircraft to become safely airborne

Then add direct controller of aircraft to determine why they were on that runway



5191 Flight Crew

Safety Requirements and Constraints:

- Operate the aircraft in accordance with company procedures, ATC clearances and FAA regulations.
- Safely taxi the aircraft to the intended departure runway.
- Take off safely from the planned runway

Unsafe Control Actions:

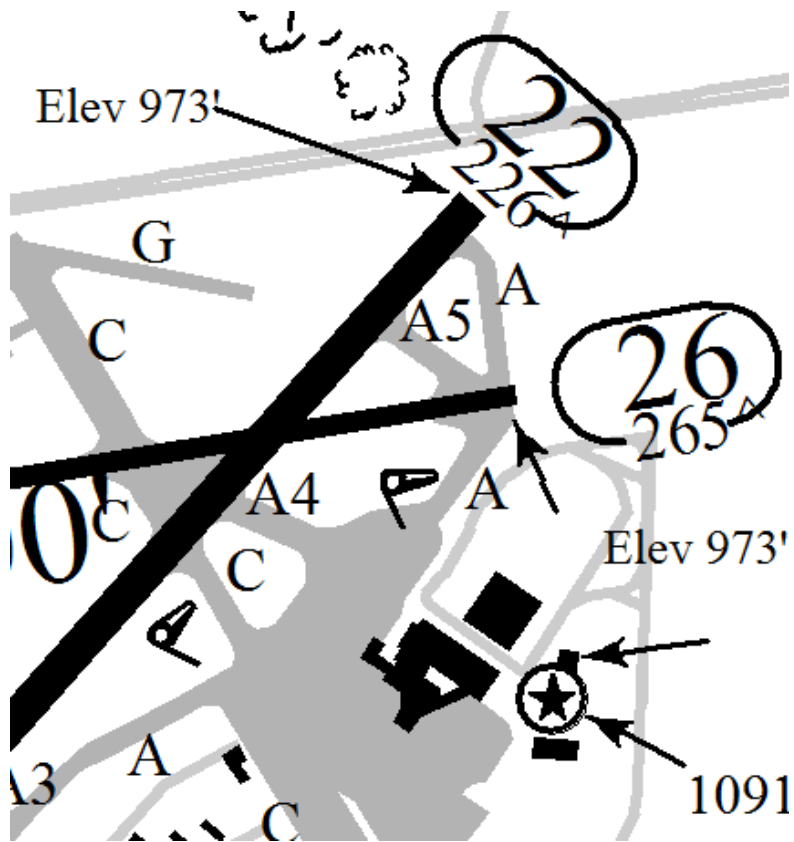
- Taxied to runway 26 instead of continuing to runway 22.
- Did not use the airport signage to confirm their position short of the runway.
- Did not confirm runway heading and compass heading matched (high threat taxi procedures)
- 40 second conversation violation of “sterile cockpit”

- Stopping here (where many accident reports stop) looks very bad for the crew.
- What questions might you want answered to explain why they did these terrible things?

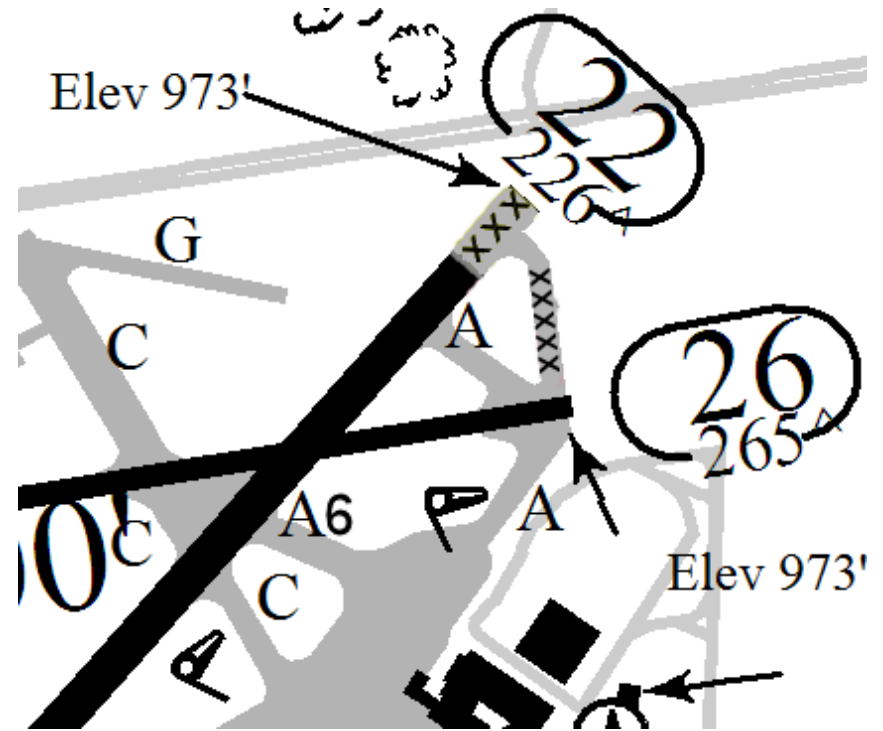
[The next step is to try to explain their actions]

The Airport Diagram

What The Crew Had



What the Crew Needed

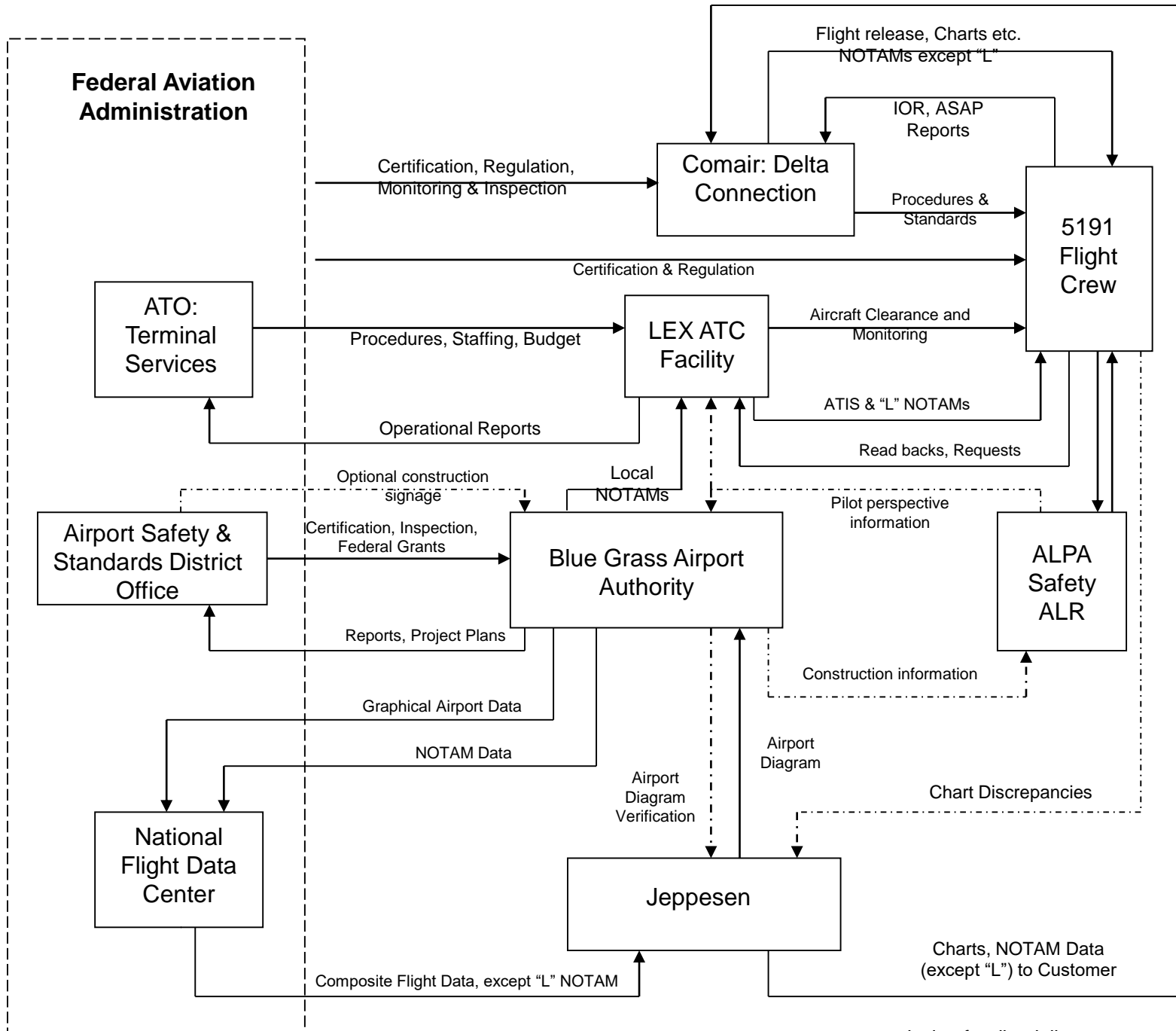


Mental Model Flaws:

- Believed they were on runway 22 when the takeoff was initiated.
- Thought the taxi route to runway 22 was the same as previously experienced.
- Believed their airport chart accurately depicted the taxi route to runway 22.
- Believed high-threat taxi procedures were unnecessary.
- Believed “lights were out all over the place” so the lack of runway lights was expected.

Context in Which Decisions Made:

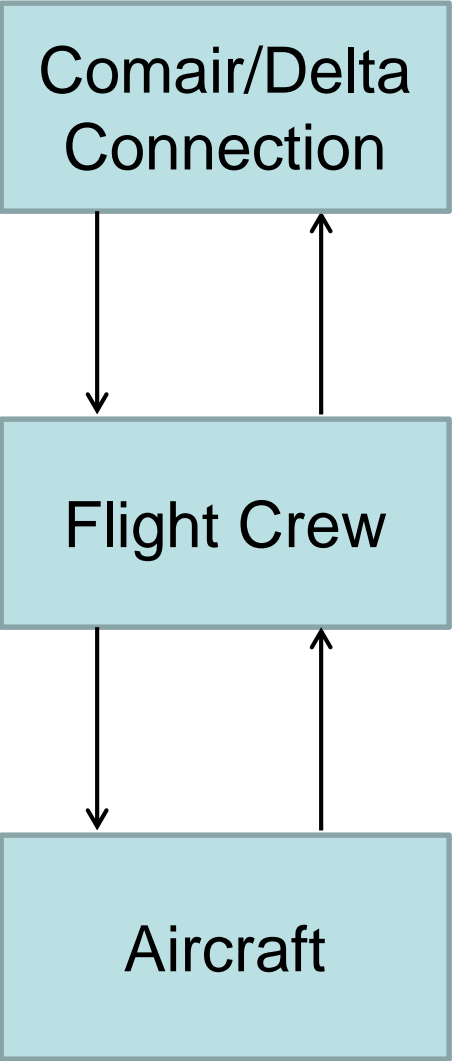
- No communication that the taxi route to the departure runway was different than indicated on the airport diagram
- No known reason for high-threat taxi procedures
- Dark out
- Comair had no specified procedures to confirm compass heading with runway
- Sleep loss fatigue
- Runways 22 and 26 looked very similar from that position
- Comair in bankruptcy, tried to maximize efficiency
 - Demanded large wage concessions from pilots
 - Economic pressures a stressor and frequent topic of conversation for pilots (reason for cockpit discussion)



Now what additional questions might you ask?

Some Questions to Answer

- Why was the crew not told about the construction?
- Why didn't ATC detect the aircraft was in the wrong place and warn the pilots?
- Why didn't the pilots confirm they were in the right place?
- Why didn't they detect they were in the wrong place?



Comair (Delta Connection) Airlines

Safety Requirements and Constraints

- Responsible for safe, timely transport of passengers within their established route system
- Ensure crews have available all necessary information for each flight
- Facilitate a flight deck environment that enables crew to focus on flight safety actions during critical phases of flight
- Develop procedures to ensure proper taxi route progression and runway confirmation

Comair (Delta Connection) Airlines (2)

Unsafe Control Actions:

- Internal processes did not provide LEX local NOTAM on the flight release, even though it was faxed to Comair from LEX
- In order to advance corporate strategies, tactics were used that fostered work environment stress precluding crew focus ability during critical phases of flight.
- Did not develop or train procedures for take off runway confirmation.

Comair (3)

Process Model Flaws:

- Trusted the ATIS broadcast would provide local NOTAMs to crews.
- Believed tactics promoting corporate strategy had no connection to safety.
- Believed formal procedures and training emphasis of runway confirmation methods were unnecessary.

Context in Which Decisions Made:

- In bankruptcy.

Blue Grass Airport Authority (LEX)

Safety Requirements and Constraints:

- Establish and maintain a facility for the safe arrival and departure of aircraft to service the community.
- Operate the airport according to FAA certification standards, FAA regulations (FARs) and airport safety bulletin guidelines (ACs).
- Ensure taxiway changes are marked in a manner to be clearly understood by aircraft operators.

Airport Authority

Unsafe Control Actions:

- Relied solely on FAA guidelines for determining adequate signage during construction.
- Did not seek FAA acceptable options other than NOTAMs to inform airport users of the known airport chart inaccuracies.
- Changed taxiway A5 to Alpha without communicating the change by other than minimum signage.
- Did not establish feedback pathways to obtain operational safety information from airport users.

Airport Authority

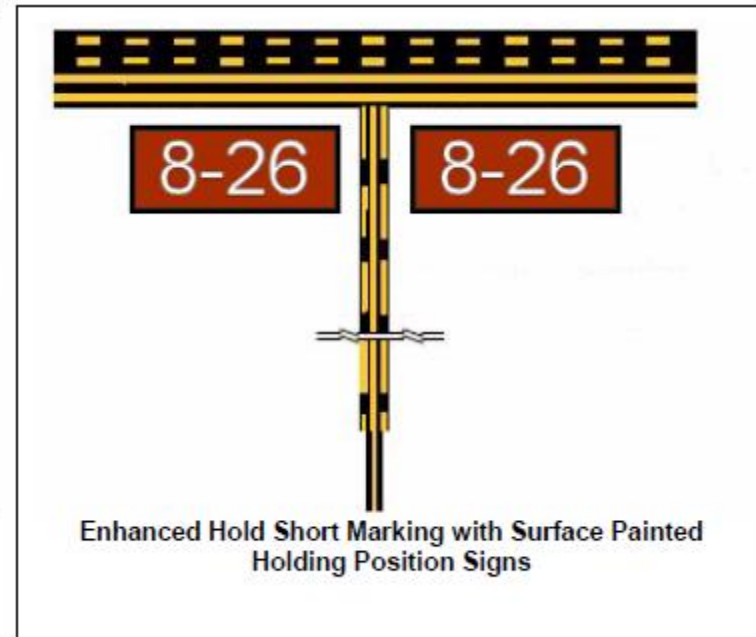
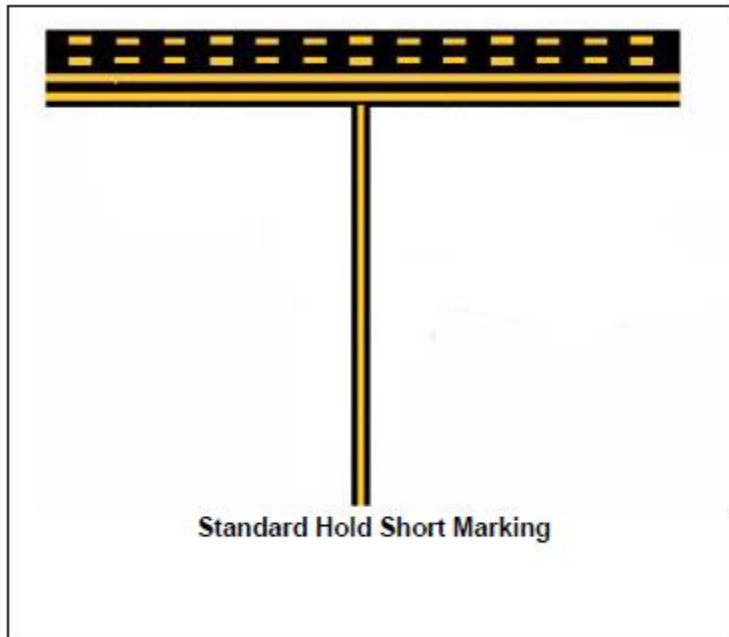
Process Model Flaws:

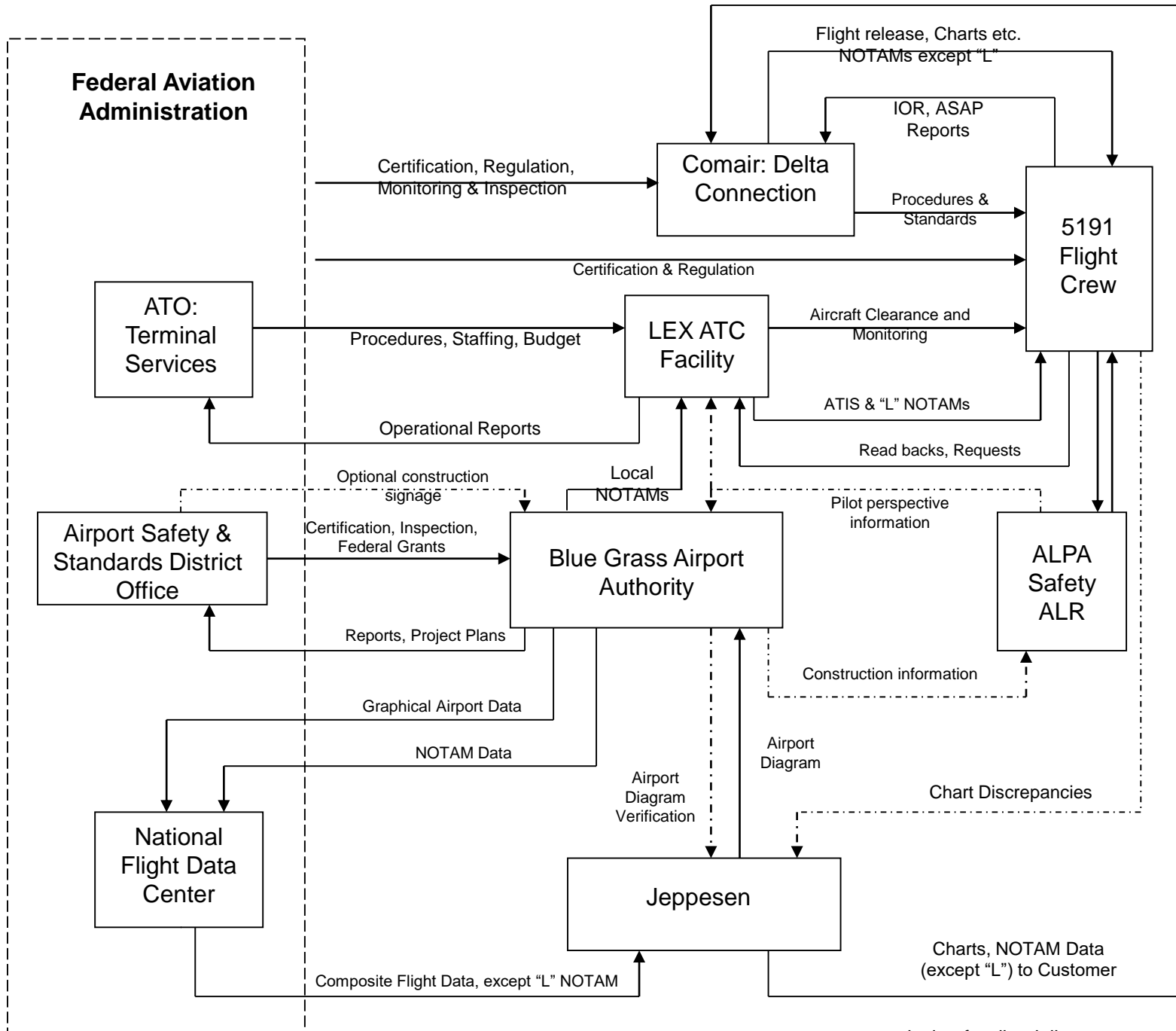
- Believed compliance with FAA guidelines and inspections would equal adequate safety.
- Believed the NOTAM system would provide understandable information about inconsistencies of published documents.
- Believed airport users would provide feedback if they were confused.

Context in Which Decisions Made:

- The last three FAA inspections demonstrated complete compliance with FAA regulations and guidelines.
- Last minute change from Safety Plans Construction Document phase III implementation plan.

Standard and Enhanced Hold Short Markings





LEX Controller Operations

Safety Requirements and Constraints

- Continuously monitor all aircraft in the jurisdictional airspace and insure clearance compliance.
- Continuously monitor all aircraft and vehicle movement on the airport surface and insure clearance compliance.
- Provide clearances that clearly direct aircraft for safe arrivals and departures.
- Provide clearances that clearly direct safe aircraft and vehicle surface movement.
- Include all Local NOTAMs on the ATIS broadcast.

LEX Controller Operations (2)

Unsafe Control Actions

- Issued non-specific taxi instructions; i.e. “Taxi to runway 22” instead of “Taxi to runway 22 via Alpha, cross runway 26”.
- Did not monitor and confirm 5191 had taxied to runway 22.
- Issued takeoff clearance while 5191 was holding short of the wrong runway.
- Did not include all local NOTAMs on the ATIS

Mental Model Flaws

- Hazard of pilot confusion during North end taxi operations was unrecognized.
- Believed flight 5191 had taxied to runway 22.
- Did not recognize personal state of fatigue.

Context in Which Decisions Made

- Single controller for the operation of Tower and Radar functions.
- The controller was functioning at a questionable performance level due to sleep loss fatigue
- From control tower, thresholds of runways 22 and 26 appear to overlap
- FAA does not require specific clearances

LEX Air Traffic Control Facility

Safety Requirements and Constraints

- Responsible for the operation of Class C airspace at LEX airport.
- Schedule sufficient controllers to monitor all aircraft with in jurisdictional responsibility; i.e. in the air and on the ground.

Unsafe Control Actions

- Did not staff Tower and Radar functions separately.
- Used the fatigue inducing 2-2-1 schedule rotation for controllers.

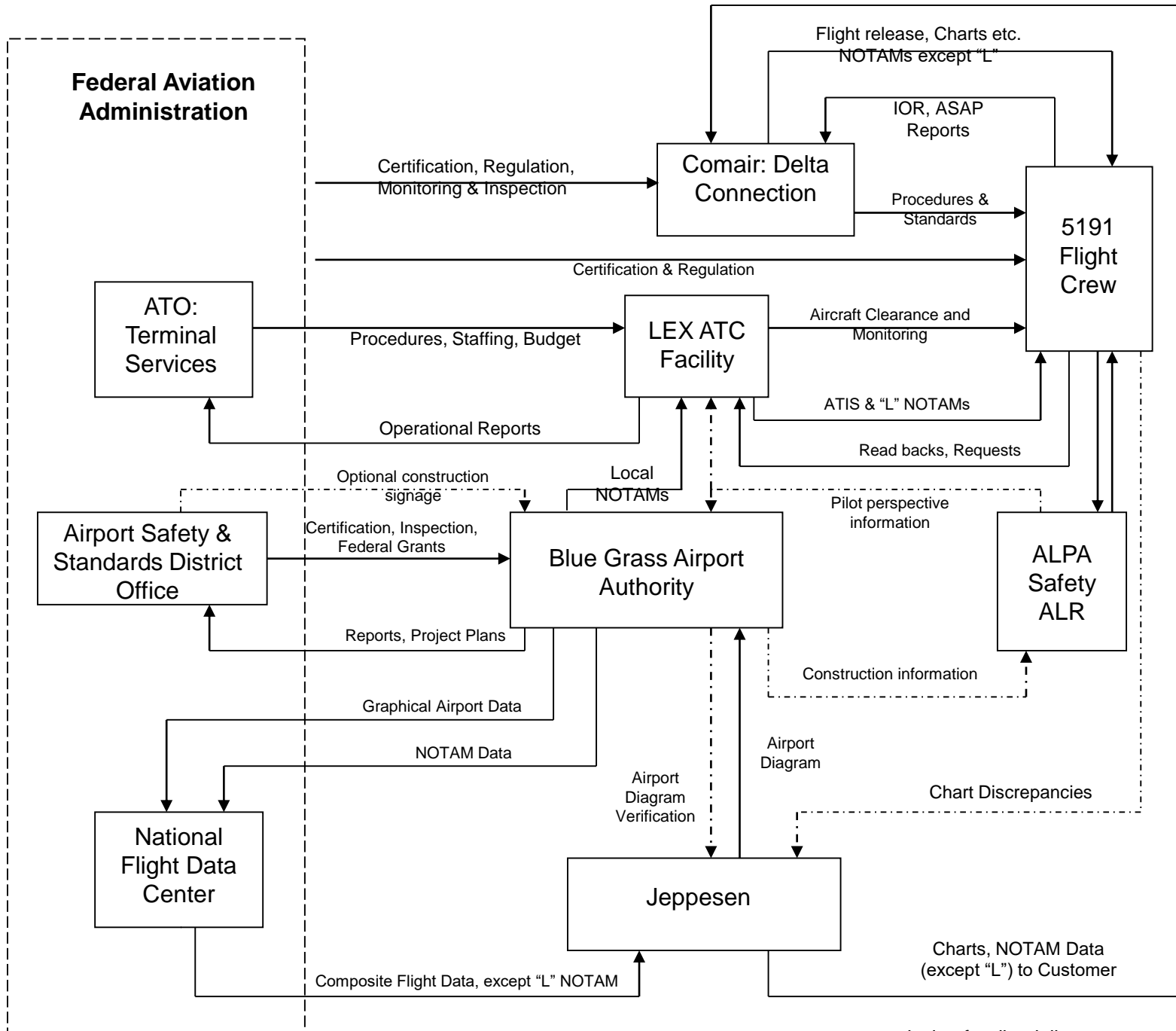
LEX Air Traffic Control Facility (2)

Mental Model Flaws

- Believed “verbal” guidance requiring 2 controllers was merely a preferred condition.
- Controllers would manage fatigue resulting from use of the 2-2-1 rotating shift.

Context in Which Decisions Made

- Requests for increased staffing were ignored.
- Overtime budget was insufficient to make up for the reduced staffing.



Air Traffic Organization: Terminal Services

Safety Requirements and Constraints

- Ensure appropriate ATC Facilities are established to safely and efficiently guide aircraft in and out of airports.
- Establish budgets for operation and staffing levels which maintain safety guidelines.
- Ensure compliance with minimum facility staffing guidelines.
- Provide duty/rest period policies which ensure safe controller performance functioning ability.

Unsafe Control Actions

- Issued verbal guidance that Tower and Radar functions were to be separately manned, instead of specifying in official staffing policies.
- Did not confirm the minimum 2 controller guidance was being followed.
- Did not monitor the safety effects of limiting overtime.

Process Model Flaws

- Believed “verbal” guidance (minimum staffing of 2 controllers) was clear.
- Believed staffing with one controller was rare and if it was unavoidable due to sick calls etc., that the facility would coordinate the with Air Route Traffic Control Center (ARTCC) to control traffic.
- Believed limiting overtime budget was unrelated to safety.
- Believed controller fatigue was rare and a personal matter, up to the individual to evaluate and mitigate.

Context in Which Decisions Made

- Budget constraints.
- Air Traffic controller contract negotiations.

Feedback

- Verbal communication during quarterly meetings.
- No feedback pathways for monitoring controller fatigue.

Federal Aviation Administration

Safety Requirements and Constraints

- Establish and administer the National Aviation Transportation System.
- Coordinate the internal branches of the FAA, to monitor and enforce compliance with safety guidelines and regulations.
- Provide budgets which assure the ability of each branch to operate according to safe policies and procedures.
- Provide regulations to ensure safety critical operators can function unimpaired.
- Provide and require components to prevent runway incursions.

Unsafe Control Actions:

- Controller and Crew duty/rest regulations were not updated to be consistent with modern scientific knowledge about fatigue and its causes.
- Required enhanced taxiway markings at only 15% of air carrier airports: those with greater than 1.5 million passenger enplanements per year.

Mental Model Flaws

- Believed enhanced taxiway markings unnecessary except for the largest US airports.
- Believed crew/controller duty/rest regulations are safe.

Context in Which Decisions Made

- FAA funding battles with the US congress.
- Industry pressure to leave duty/rest regulations alone.

NTSB “Findings”

Probable Cause:

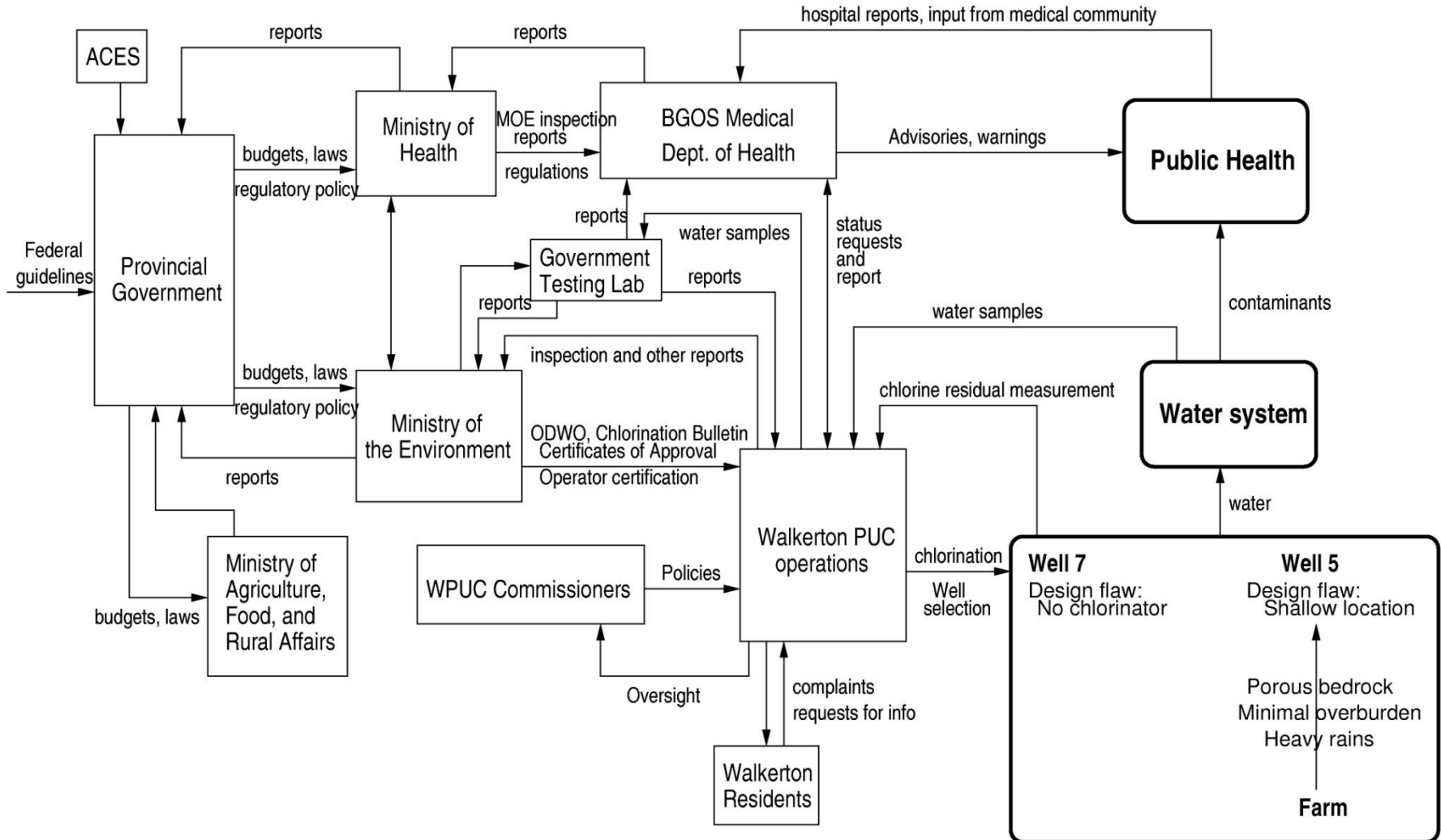
- FC’s failure to use available cues and aids to identify the airplane’s location on the airport surface during taxi
- FC’s failure to cross-check and verify that the airplane was on the correct runway before takeoff.
- Contributing to the accident were the flight crew’s nonpertinent conversation during taxi, which resulted in a loss of positional awareness.
- Federal Aviation Administration’s (FAA) failure to require that all runway crossings be authorized only by specific air traffic control (ATC) clearances.

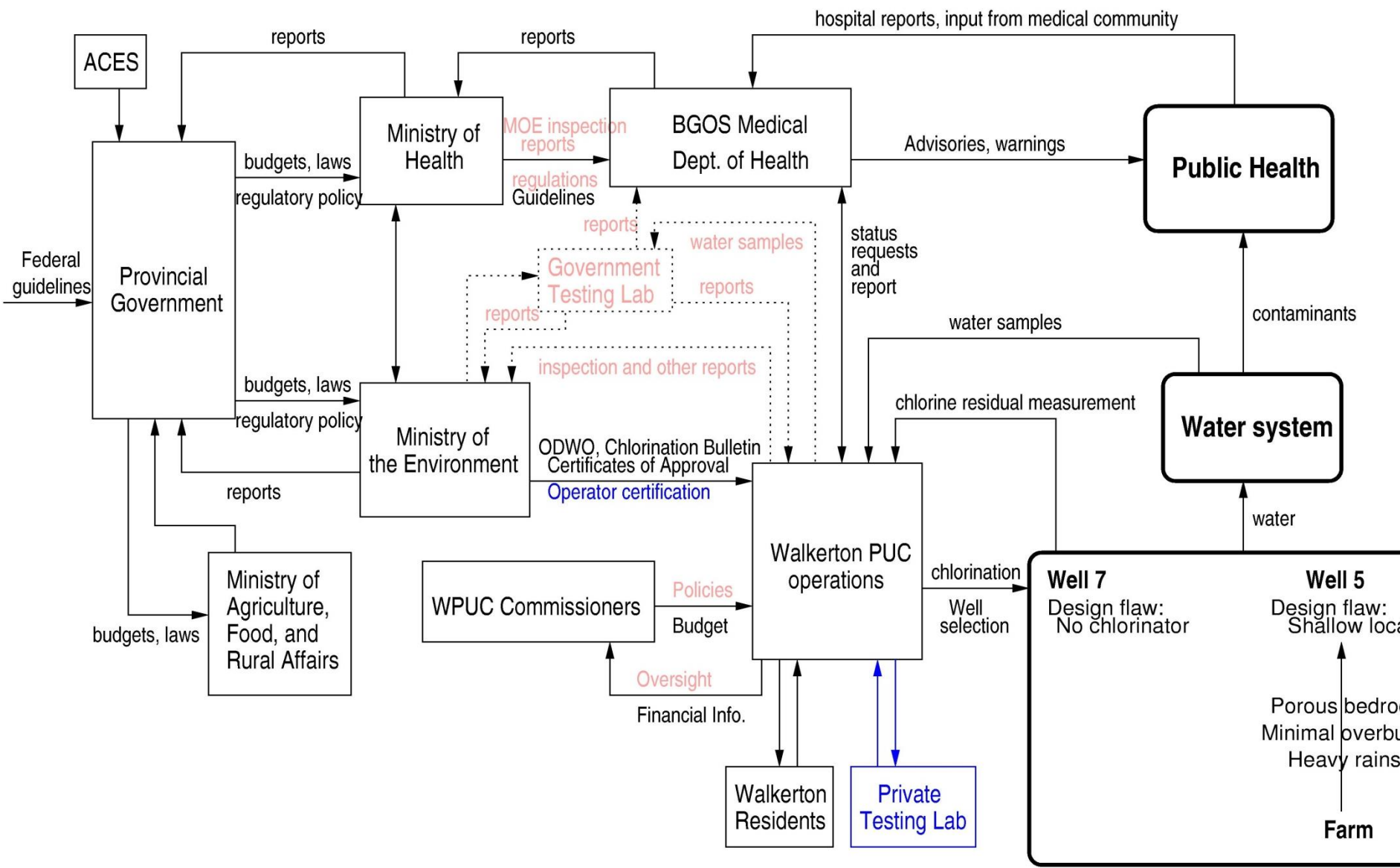
System Hazard: Public is exposed to E. coli or other health-related contaminants through drinking water.

System Safety Constraints: The safety control structure must prevent exposure of the public to contaminated water.

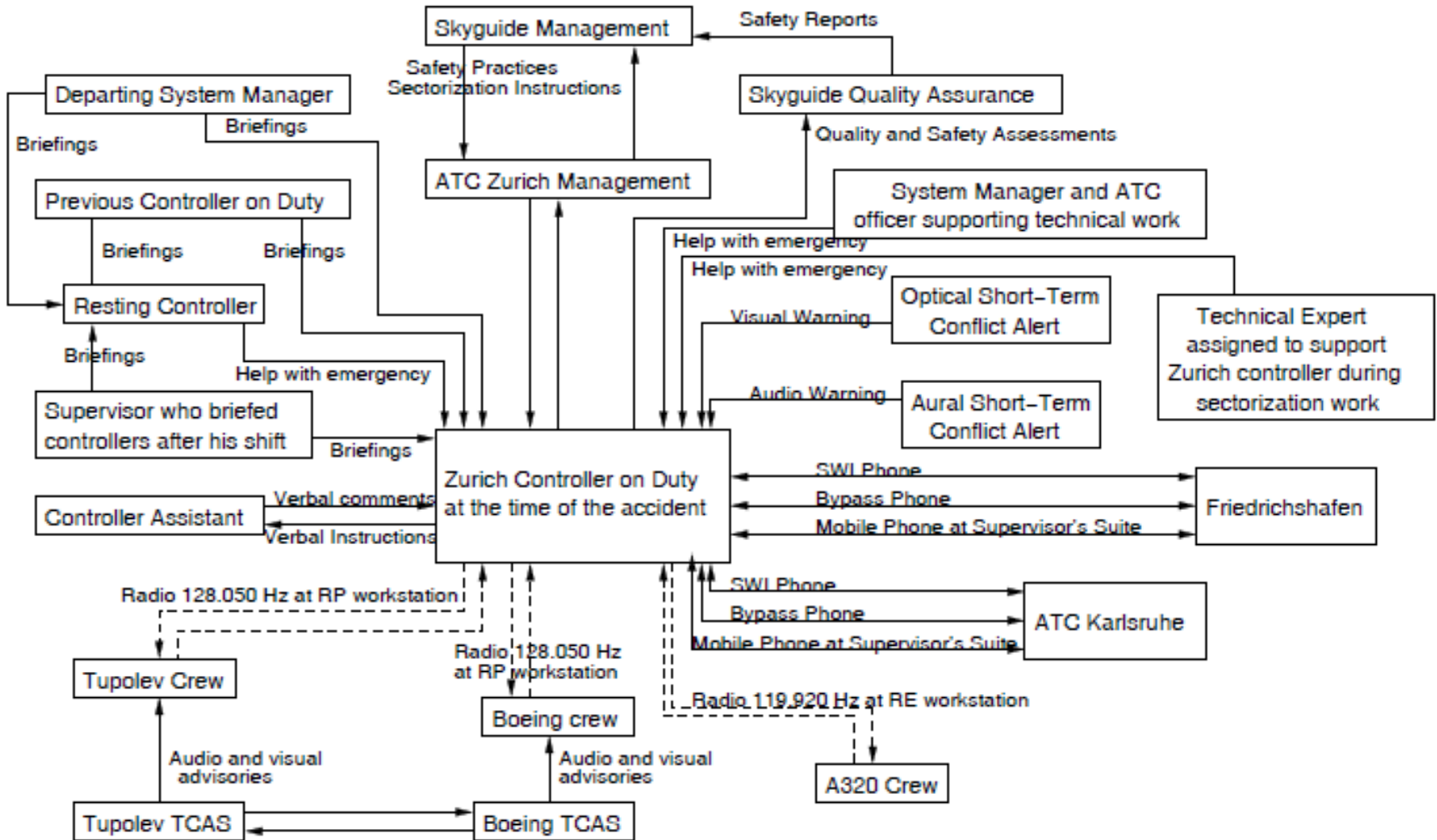
(1) Water quality must not be compromised.

(2) Public health measures must reduce risk of exposure if water quality is compromised (e.g., notification and procedures to follow)

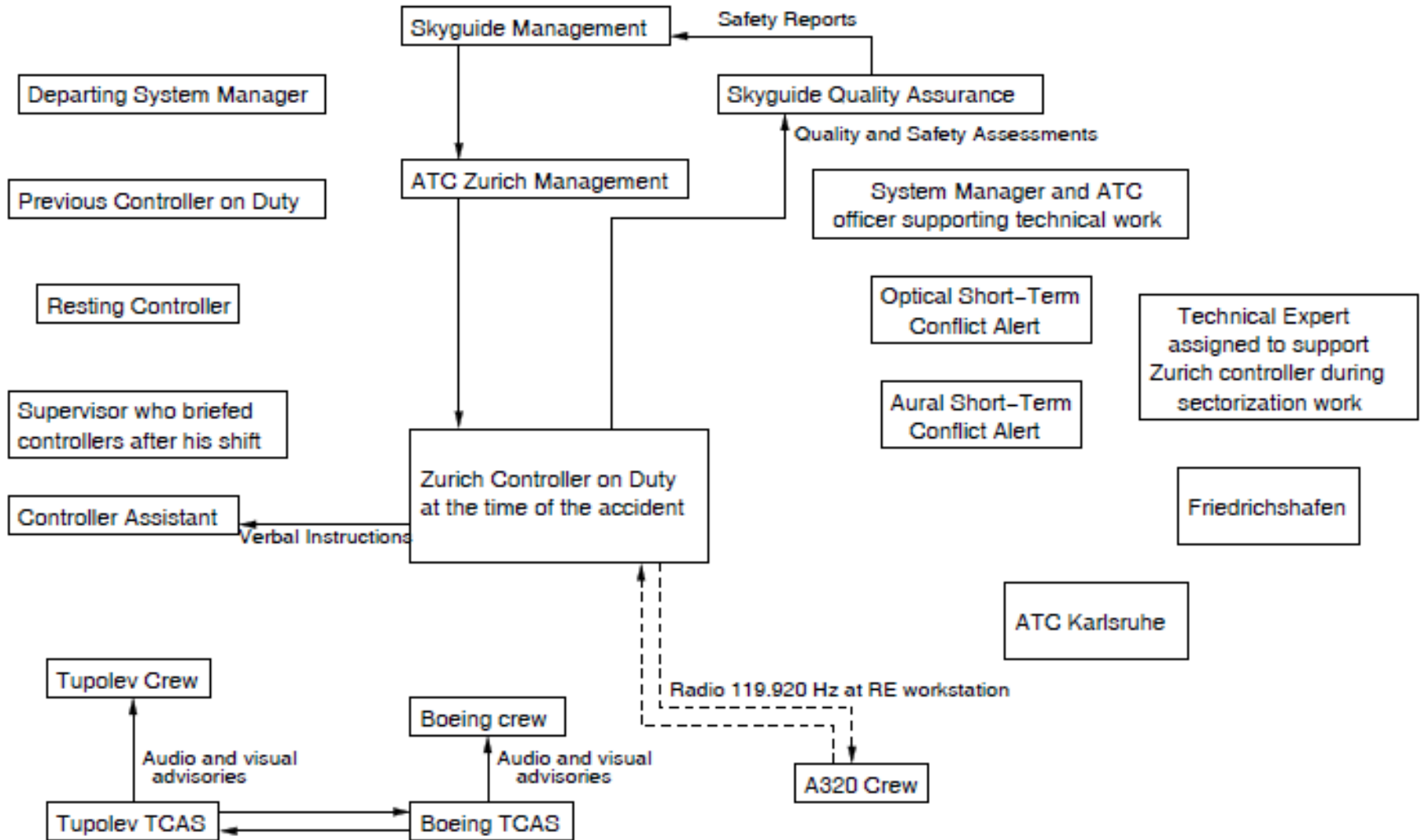




Communication Links Theoretically in Place in Uberlingen Accident



Communication Links Actually in Place



CAST Analysis of the Shell Moerdijk Explosion

A complete example at:

<http://sunnyday.mit.edu/shell-moerdijk-cast.pdf>



Summary

- A “why” analysis, not a “blame” analysis
- Construct the safety control structure as it was designed to work
 - Component responsibilities (requirements)
 - Control actions and feedback loops
- For each component, determine if it fulfilled its responsibilities or provided inadequate control.
 - If inadequate control, why? (including changes over time)
 - Context
 - Process Model Flaws
- For humans, why did it make sense for them to do what they did (do this to reduce hindsight bias)
- Examine coordination and communication

Summary (2)

- Consider dynamics (changes in control structure) and migration to higher risk
- Determine the changes that could eliminate the inadequate control (lack of enforcement of system safety constraints) in the future.
- Generate recommendations
- Continuous Improvement
 - Assigning responsibility for implementing recommendations
 - Follow-up to ensure implemented
 - Feedback channels to determine whether changes effective
 - If not, why not?

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 control structure