Have you learned enough STPA to use it?

- Probably not, but there are other sources.
- Takes longer to learn if you know more about safety engineering
- Not hard to learn. Most of effort is in unlearning.
- STPA stretches the mind. John class at FAA during MAX accident analysis.

Common Mistakes in Using STPA

- Identifying component hazards instead of system hazards
  - Software adds chemicals before adding catalyst
    - vs. Overheating/overpressurization of reactor (M-1)
  - Relief valve opens inadvertently
    - vs. Release of chemicals within or outside plant (M-2, M-3)

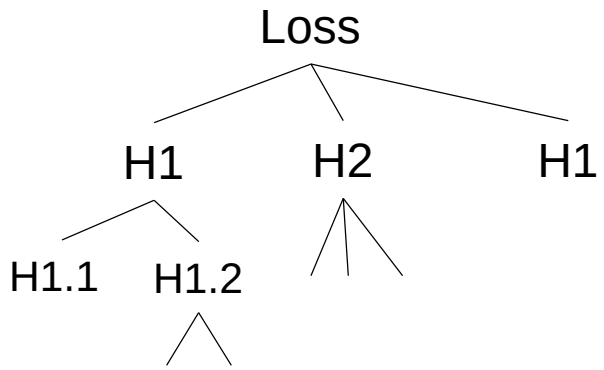
Why a problem? Potential Incompleteness

- May miss other causes of overpressurization
- STPA is a step-by-step process to assist in the analysis

Will only be a few (usually less than 10

- If more, then go to a higher level of abstraction

Creating a “Tree” Structure



Helps organize the search so don’t omit things

Human factors consideration: This is a way humans

- Organize their thoughts
- Review things

Common Mistakes (2)

- Failures as hazards
  - "Valve fails closed" or "Reactor fails"
  - "Human fails"
    Humans do not "fail"
    Leads to missing human factors problems
  - "Software fails"
    Says nothing
    Omits all important software-related causes
    Specific incorrect wrong behavior is what you need to identify
    Unsafe software behavior usually related to unsafe requirements
    (requirements implemented correctly)

In general, avoid use of "fails" unless hardware (even then, not in system hazard list because this is not a hazard or system state, it is a cause of a hazard).

Common Mistakes (3)

- Causes as hazards
  - Correct:
    - Overpressurization
  - Incorrect:
    - Relief valve does not open
    - Chemicals added before catalyst

  Again, will miss things, not an organized method

- Needs to be within the system scope

System Safety Engineering (Def. of Hazard)

Hazard/vulnerability**:** A system state or set of conditions that, together with some worst-case environmental conditions, will lead to a loss

- Hazard is within the system and thus under our control
- Loss/accident has components that are not under our control

Hazard Analysis: Identifying operational scenarios that can lead to a hazard/vulnerability

Safety Engineering: Eliminating or controlling hazard scenarios in the system design and operations

Risk: Potential for a loss so includes both hazard state plus environmental state

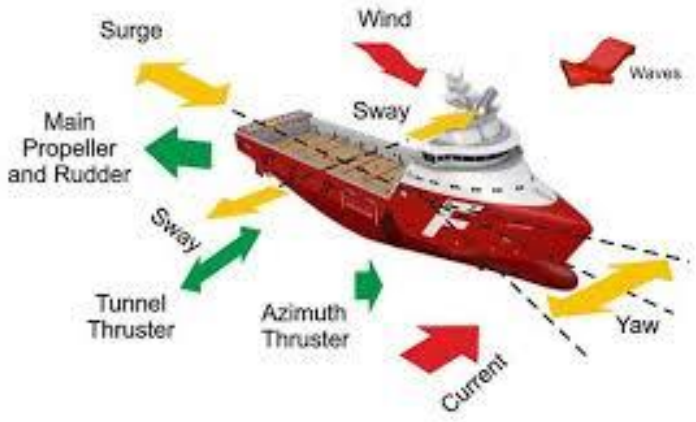
Note: The goal is not to prevent failures; we are preventing and controlling hazards

Prioritization

SAFETY RISK		Severity				
Probability		Catastrophic	Hazardous	Major	Minor	Negligible
		A	B	C	D	E
Frequent	5	5A	5B	5C	5D	5E
Occasional	4	4A	4B	4C	4D	4E
Remote	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extremely improbable	1	1A	1B	1C	1D	1E

- Impossible to get likelihood before design is complete (and even then, probably not feasible)
- No such thing as the probability of software leading to a loss
- We have found these on real systems to be totally wrong

Navy Escort Vessels (Lt. Blake Abrecht)



- Dynamic positioning system
- Ran into each other twice during test
- Performed a CAST analysis (on two incidents) and STPA on system as a whole
- Contractors had accident as not credible (low likelihood).
- Navy admiral rejected our findings saying “We’ve used PRA for 40 years and it works just fine”
- Put into operation and within 2 months ran into a submarine
- Scenario was one we had found

UH-60MU (Blackhawk)

- Analyzed Warning, Caution, and Advisory (WCA) system

- STPA results were compared with an independently conducted hazard analysis of the UH-60MU using traditional safety processes described in SAE ARP 4761 and MIL-STD-882E.
  - STPA found the same hazard causes as the traditional techniques and
  - Also identified things not found using traditional methods, including design flaws, unsafe human behavior, and component integration and interactions flaws

UH-60MU SAR Hazard Classification

UH-60MU SAR marginal hazards

- Loss of altitude indication in DVE
- Loss of heading indication in DVE
- Loss of airspeed indication in DVE
- Loss of aircraft health information
- Loss of external communications
- Loss of internal communications

UH-60MU SAR identified various hazards as marginal that could lead to a catastrophic accident

STPA Unsafe Control Action

The Flight Crew does not provide collective control input necessary for level flight, resulting in controlled flight into terrain

Scenario 1: The Flight Crew has a flawed process model and believes they are providing sufficient control input to maintain level flight. This flawed process model could result from:

a) The altitude indicator and attitude indicator are malfunctioning during IFR flight and the pilots are unable to maintain level flight

b) The Flight Crew believes the aircraft is trimmed in level flight when it is not

c) The Flight Crew has excessive workload due to other tasks and cannot control the aircraft

d) The Flight Crew has degraded visual conditions and cannot perceive slow rates of descent that result in a continuous descent

e) The Flight Crew does not perceive rising terrain and trims the aircraft for level flight that results in controlled flight into terrain

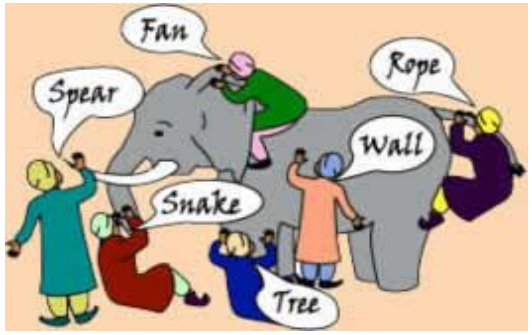
Extra Comments:

- Didn’t look at valve failure etc. as causes of the accidents in chemical reactor.
- Need to do that also, but everyone already does that. The problem is getting people to look at design errors.
- Reduces the types of failures need to consider.
- Recent FVL (future vertical lift vehicles) experiences

MIL-STD-882 (A-E)

- Set of tasks
- Included software (in hazard analysis, etc.)
- Does not say how to do it
- After C, Sec. of Defense Perry, outlawed all standards
- Came back with 882D which was almost empty
- Then 882E, which in my opinion, went off the rails (too influenced by industry)
  - Allowed PRA instead of tasks
  - Appendix on software is nonsense
  - Other parts (about software) are simply wrong
- There is a draft 882F that is worse

How to Learn More 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

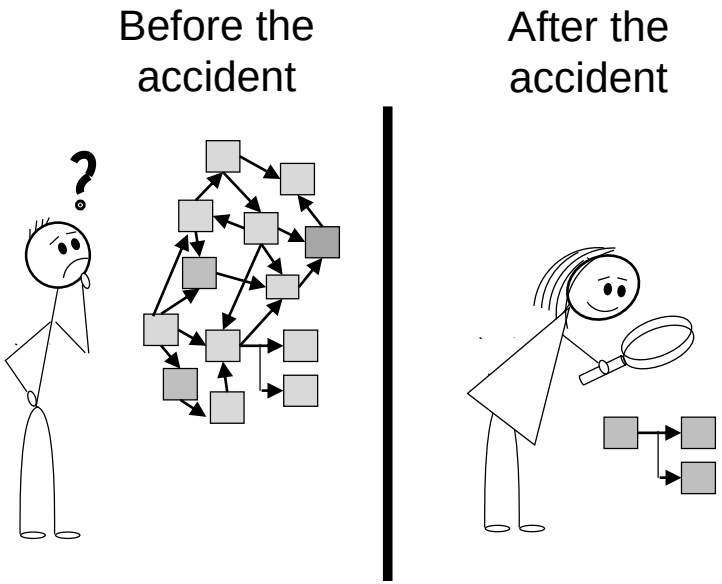
- Assuming there is a root cause gives us an illusion of control.
  - Usually focus on operator error or technical failures
  - Ignore systemic and management factors
  - Leads to a sophisticated “whack a mole” game
    - Fix symptoms but not process that led to those symptoms
    - In continual firefighting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

Hindsight Bias



"S/he could have…," If s/he would have…," "S/he should 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

- Data availability vs. data observability (Dekker)
  - "The available evidence **should have** been sufficient to give the Board Operator a clear indication that Tank 731 was indeed filling and required immediate attention."

Board Control Valve Position: closed	Flow Meter: *shows no flow*
Manual Control Valve Position: *open*	Flow: *none*
Bypass Valve: *closed*	SO_2 alarm: *off*
Level in tank: 7.2 feet	High level alarm: *off*

Data Availability vs. Data Observability (2)

[So I asked, how could the operators have known?]

– "Operators **could have** trended the data on the control board"

– But

- There was no reason to think the tank was still filling (no alarm, no data, …)
- A potentially serious alarm in another part of plant at the same time that the operators attended to

Other Hindsight Bias Examples

- SO_2 did finally sound but operators went to investigate instead of immediately evacuating the plant.
- *"Interviews with operations personnel did not produce a clear reason why the response to the SO_2 alarm took 31 minutes. The only explanation was that there was not a sense of urgency since, in their experience, previous SO_2 alarms were attributed to minor releases that did not require a unit evacuation."*
- Company operations policy said that it was up to the operators to determine when an emergency existed.

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

Focus on Blame

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]

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.

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.

Analysis

- Who or what as primarily responsible for this accident?

Analysis

- Note the use of the word “failure”
  - A pejorative word: a negative judgment
  - Assigns blame

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

Analysis

- Note the use of the word “failure”
  - A pejorative word: a negative judgment
  - Assigns 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]

Another way of describing this accident:

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?

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.**

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

Accusatory:	**vs.**	**Explanatory**:
Who		What
Why		Why

- Don’t use “failed” unless hardware

Do Operators Really Cause Most Accidents?

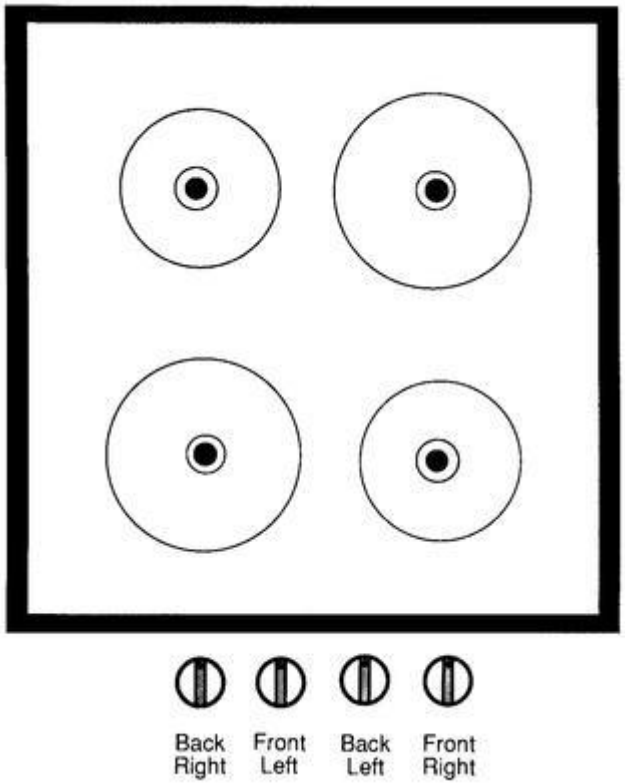
Operator Error: Systems View (1)

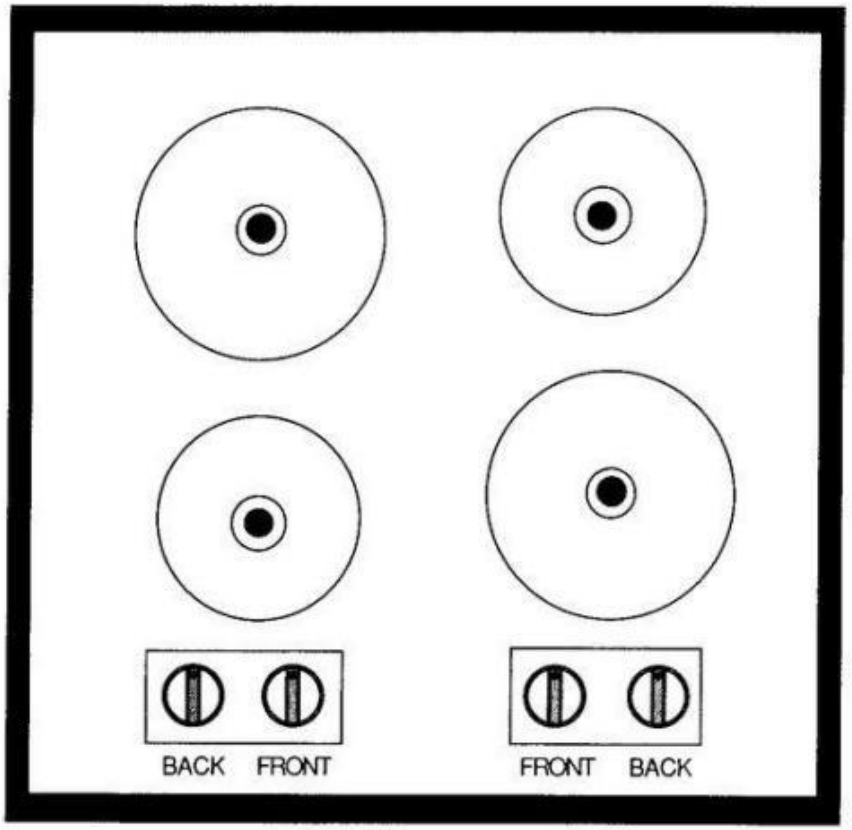
- Human error is a symptom, not a cause
- All behavior affected by context (system) in which occurs
- Role of operators in our systems is changing
  - Supervising rather than directly controlling
  - Systems are stretching limits of comprehensibility
  - Designing systems in which operator error inevitable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

Most stove tops

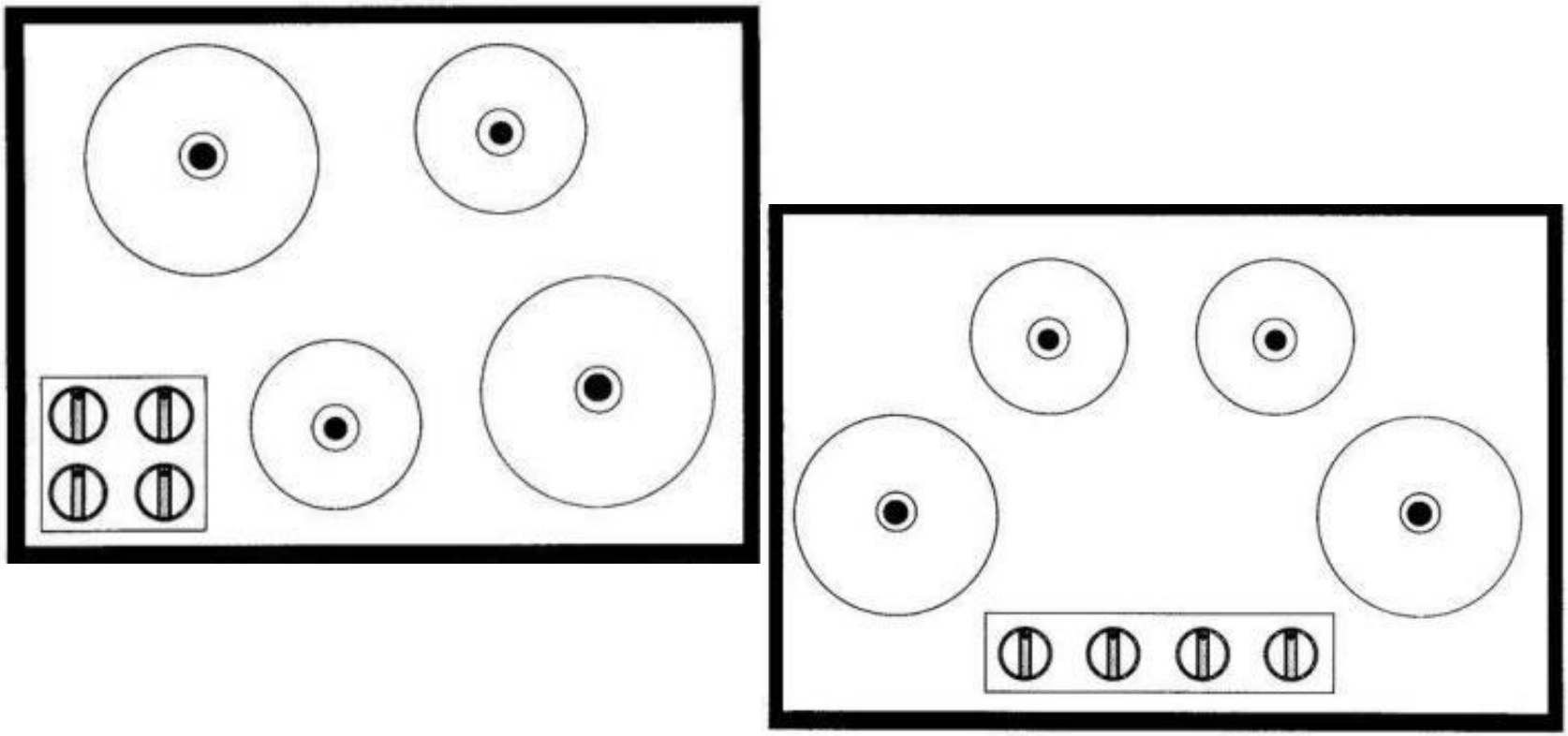




Is this a design problem or just human error?

*Image from D. Norman, 1988

More Natural Mapping



The right design will reduce human error

*Image from D. Norman, 1988

Poor design or human error?

Jedi Entrance

Events are Not Enough

Need to look at ***why*** events occurred, identify questions to ask

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.	???

Events are Not Enough

Need to look at ***why*** events occurred, identify questions to ask

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?*

CAST: Causal Analysis based on Systems Thinking/Theory

A step-by-step process for learning more from accidents

Disclaimer: This is not a training course to do CAST and does not provide the level of practice required for such training.

Goals for CAST

- Minimize hindsight bias
- Structured process to expand search for causes
- Get away from blame ("who") and shift focus to "why" and how to prevent in the future
- Determine:
  1. Why people behaved the way they did
  2. Weaknesses in the safety control structure that allowed the loss to occur

Comair 5191 (Lexington Airport) Sept. 2006

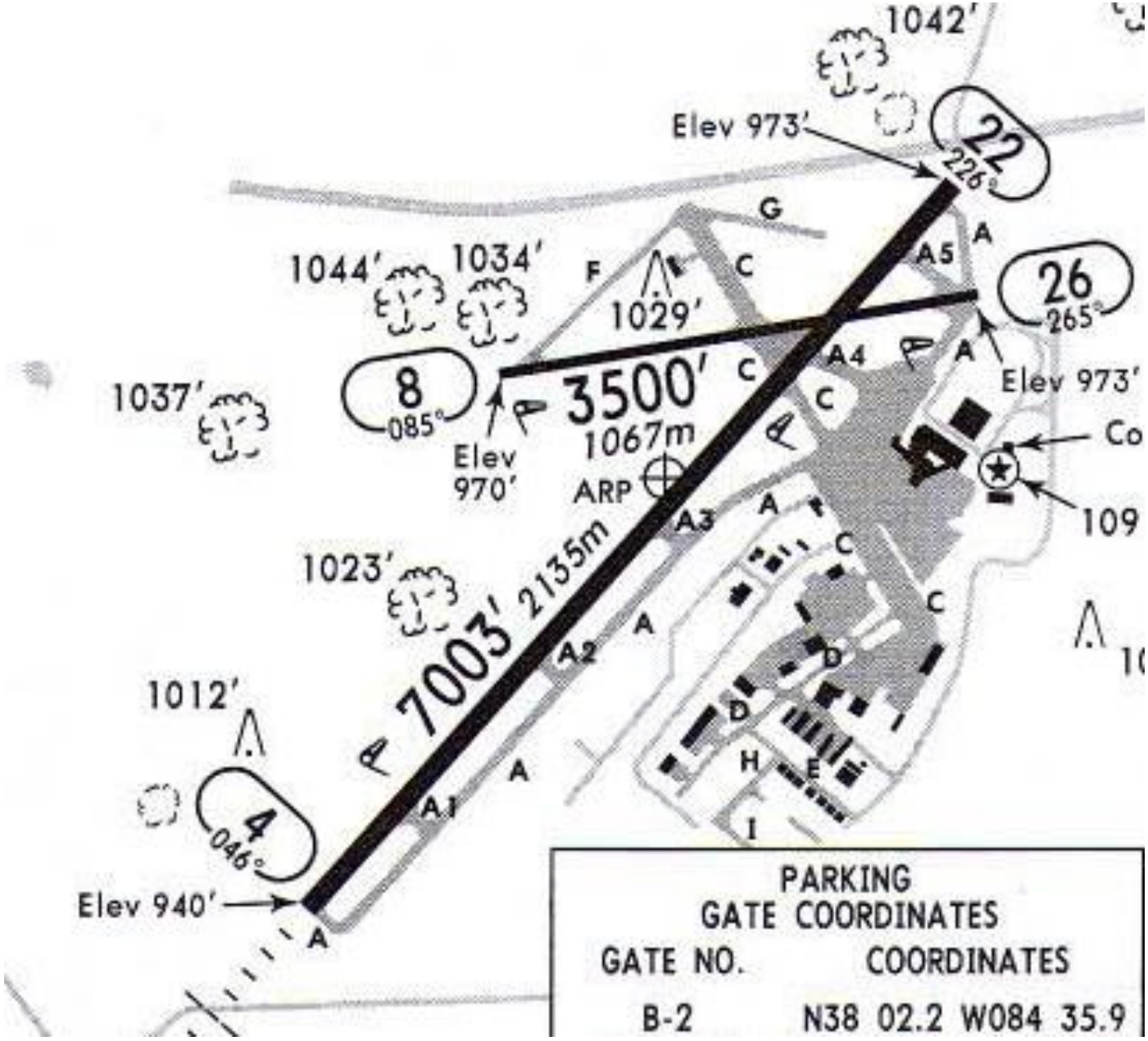
CAST analysis by Paul Nelson, Former Comair Pilot

Events

- Captain arrived at airport as deadhead crew member and released from duty at 1546 Aug. 26, 2006.
- FO arrived as acting crew member and released from duty at 0200 on Aug. 26, 2006.
- Crew met in lobby and took 0500 hotel bus to airport.
- Third flight day for each crew member but first flight together.
- Near last part of gate preparations, FO mentioned that “lights were out all over the place” when had flown in 2 nights before.
- FO gave taxi briefing, saying they would take taxiway Alpha to runway 22 and that it would be a short taxi.
- When pushed back, still dark out (an hour before sunrise).
- Called for taxi clearance. Tower controller said “taxi to runway two two.” FO orally confirmed clearance.

Events (2)

- Captain called for taxi check list and established that on taxiway Alpha.
- Captain called for start of “before takeoff” check list.
- At this time, 40 second conversation about other airline hiring practices by Captain. A continuation of conversation interrupted 15 minutes earlier. Deemed “nonessential” and violation of sterile cockpit rule.
- Captain brought aircraft to a stop short of runway 22 but were actually short of runway 26.
- Checklist items completed and FO called tower for takeoff clearance.
- Tower controller scanned runway to assure no conflicting traffic, then cleared 5191 for takeoff.
- Take off (details omitted) and impacted line of trees, erupted into flames. FO was only one who survived.


1042'
Elev 973'
22
226°
1044'
1034'
F
1029'
C
G
A5
A
26
265°
1037'
8
085°
3500'
1067m
Elev
970'
ARP
C
A4
A
Elev 973'
Co
109
A3
A
C
1023'
7003'
2135m
A2
A
C
D
1012'
D
H
E
4
046°
A1
A
I
Elev 940'
A
PARKING
GATE COORDINATES
GATE NO. COORDINATES
B-2 N38 02.2 W084 35.9

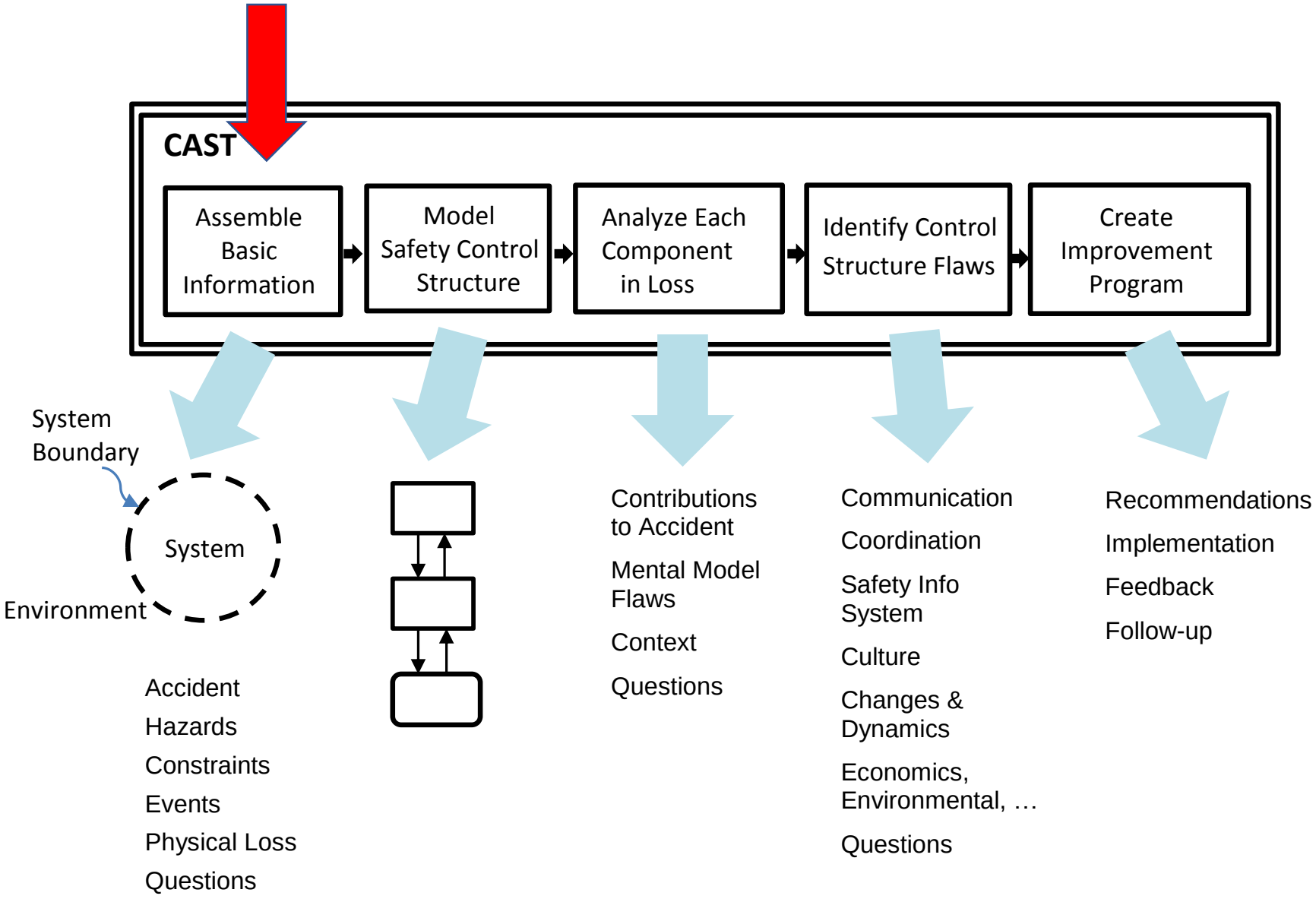
NTSB Findings

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.

Generating and Documenting Questions

- At each step, generate questions from what you know so far.
- Will generate new questions as proceed with analysis
- Goal at end is to answer all the questions
- At this point, what questions do you have?


CAST
Assemble Basic Information
Model Safety Control Structure
Analyze Each Component in Loss
Identify Control Structure Flaws
Create Improvement Program
System Boundary
System
Environment
Accident
Hazards
Constraints
Events
Physical Loss
Questions
Contributions to Accident
Mental Model Flaws
Context
Questions
Communication
Coordination
Safety Info System
Culture
Changes & Dynamics
Economics, Environmental, …
Questions
Recommendations
Implementation
Feedback
Follow-up

First identify the system hazard and safety constraint violated

What was the

1. System hazard
2. System safety constraint

violated in this accident?

Hazard and Safety Constraint Violated

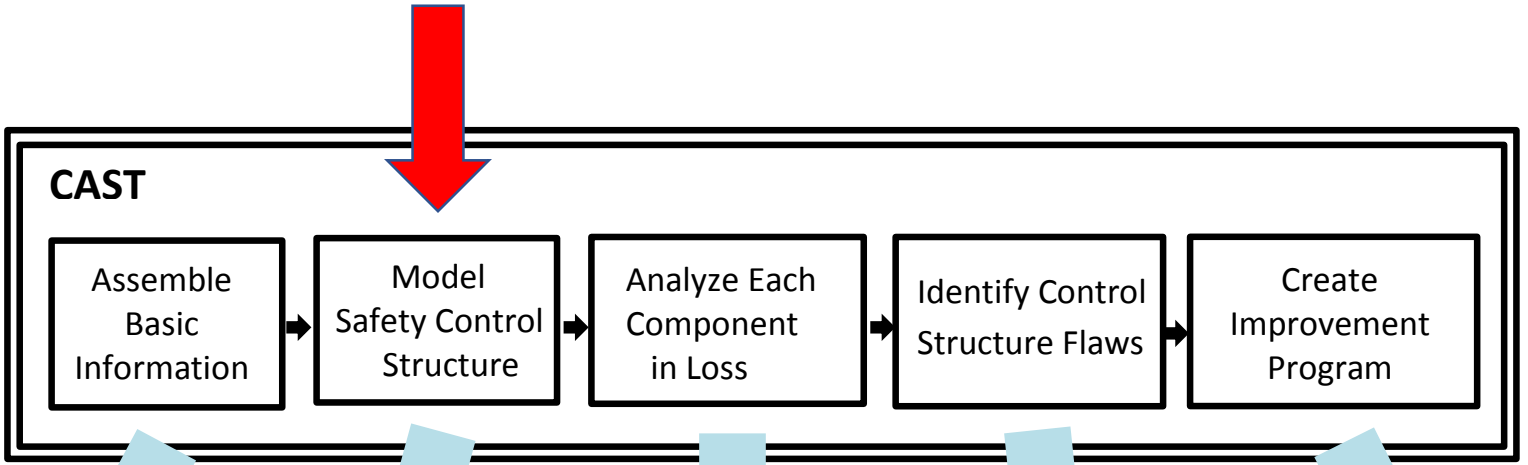
- Accident: death or injury, hull loss
- System hazard: Runway incursions and operations on wrong runways or taxiways.
- System safety constraint: The safety control structure must prevent runway incursions and operations on wrong runways or taxiways.

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

Controls to Prevent Runway Incursion

Controls to Prevent Runway Incursion

- Charts (maps) of airport
- Crew procedures, checklists
- FC Training
- Tower controller providing clearance and visual checks
- Markings on taxiway and runway
- L(local) NOTAMs
- …



System Boundary

System

Environment

Accident
Hazards
Constraints
Events
Physical Loss
Questions

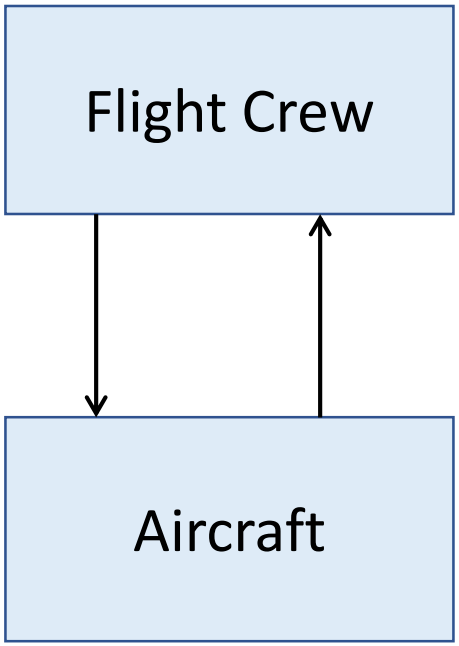
Contributions to Accident
Mental Model Flaws
Context
Questions

Communication
Coordination
Safety Info System
Culture
Changes & Dynamics
Economics, Environmental, …
Questions

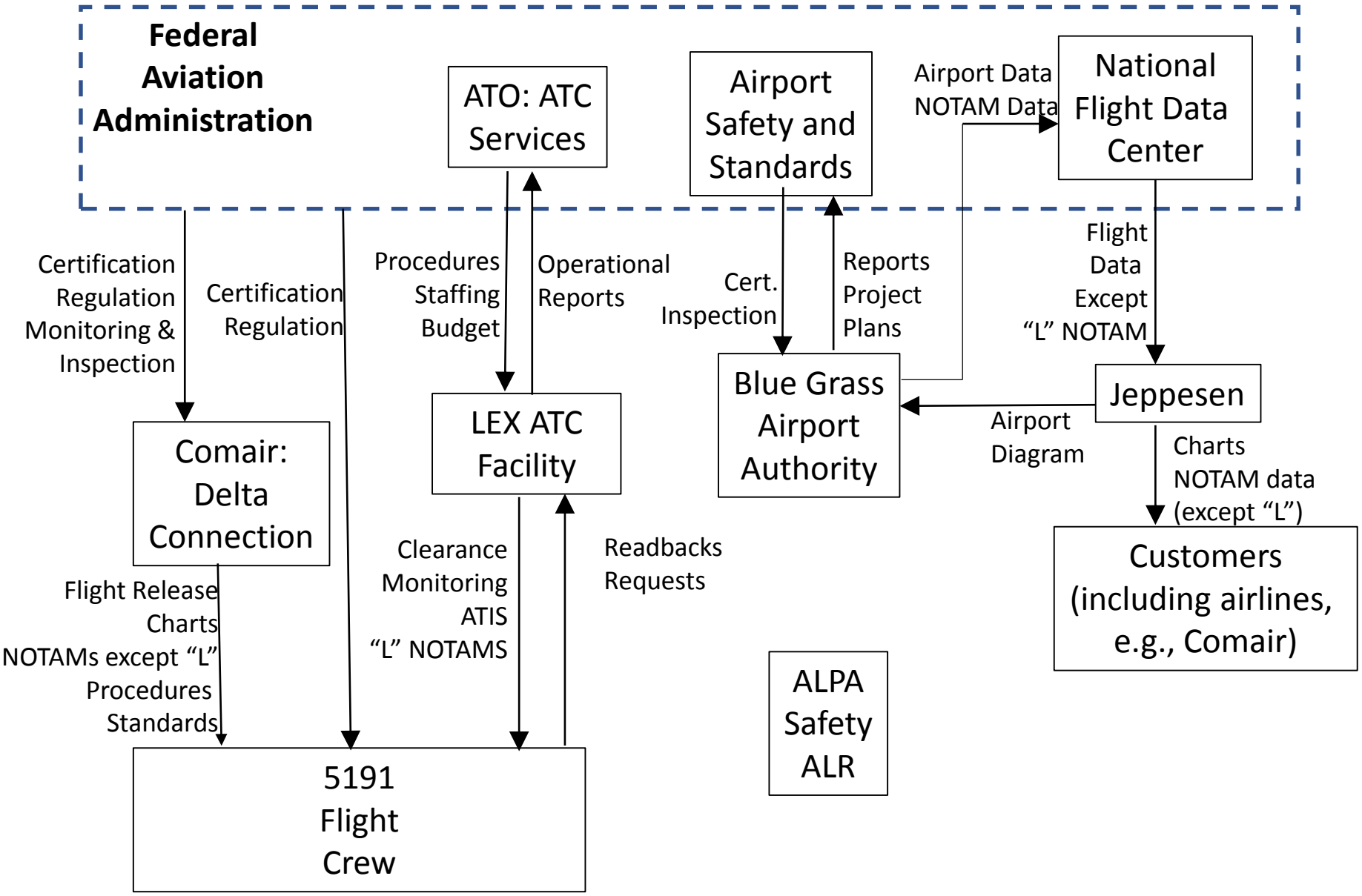
Recommendations
Implementation
Feedback
Follow-up

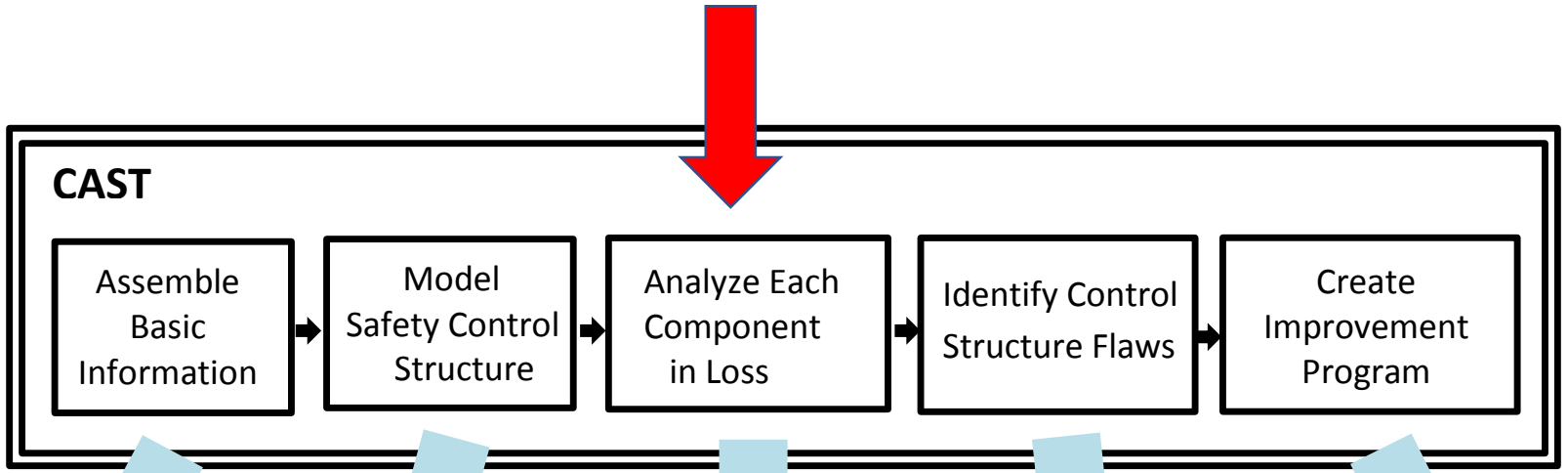
Identifying Components to Include

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



(Might also include the taxiways, runways, and physical infrastructure)


Federal Aviation Administration
ATO: ATC Services
Airport Safety and Standards
Airport Data
NOTAM Data
National Flight Data Center
Certification
Regulation
Monitoring &
Inspection
Certification
Regulation
Procedures
Staffing
Budget
Operational
Reports
Cert.
Inspection
Reports
Project
Plans
Flight
Data
Except
"L" NOTAM
Blue Grass Airport Authority
Jeppesen
Airport
Diagram
Charts
NOTAM data
(except "L")
Comair: Delta Connection
LEX ATC Facility
Clearance
Monitoring
ATIS
"L" NOTAMS
Readbacks
Requests
Customers (including airlines, e.g., Comair)
Flight Release
Charts
NOTAMs except "L"
Procedures
Standards
ALPA Safety ALR
5191 Flight Crew



System Boundary

System

Environment

Accident
Hazards
Constraints
Events
Physical Loss
Questions

Contributions to Accident
Mental Model Flaws
Context
Questions

Communication
Coordination
Safety Info System
Culture
Changes & Dynamics
Economics, Environmental, …
Questions

Recommendations
Implementation
Feedback
Follow-up

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

For Each Controller

Safety Responsibilities:

…

Role in Loss:

…

Why?

Process/Mental Model Flaws	Questions

Contextual Factors	Questions

Flight Crew

Safety Responsibilities:

- 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

Role in Loss:

- 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 most accident reports stop) looks very bad for the crew.
- What questions might you want answered to explain why they behaved this way?

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

Mental Model Flaws:

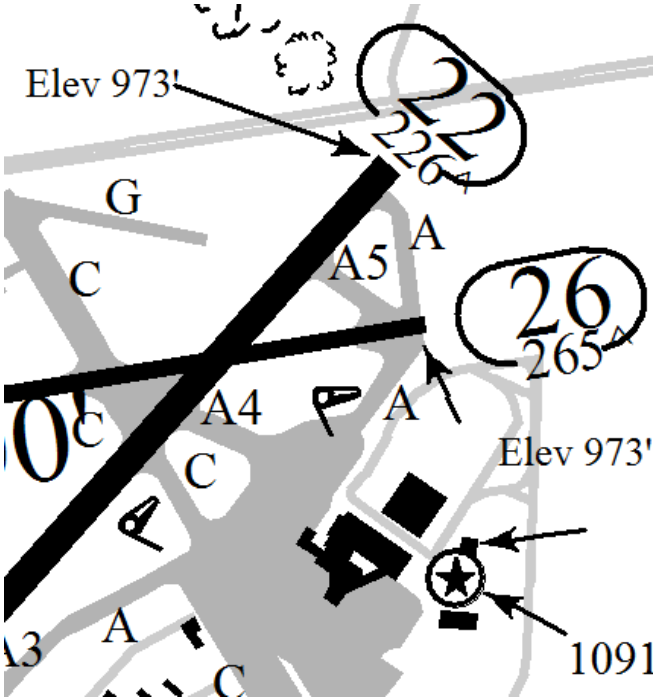
- Believed they were on runway 22 when the takeoff was initiated.
- Thought the taxi route to runway 22 was the same as previously experienced.
- Believed their airport chart accurately depicted the taxi route to runway 22.
- Believed high-threat taxi procedures were unnecessary.
- Believed “lights were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

Questions?

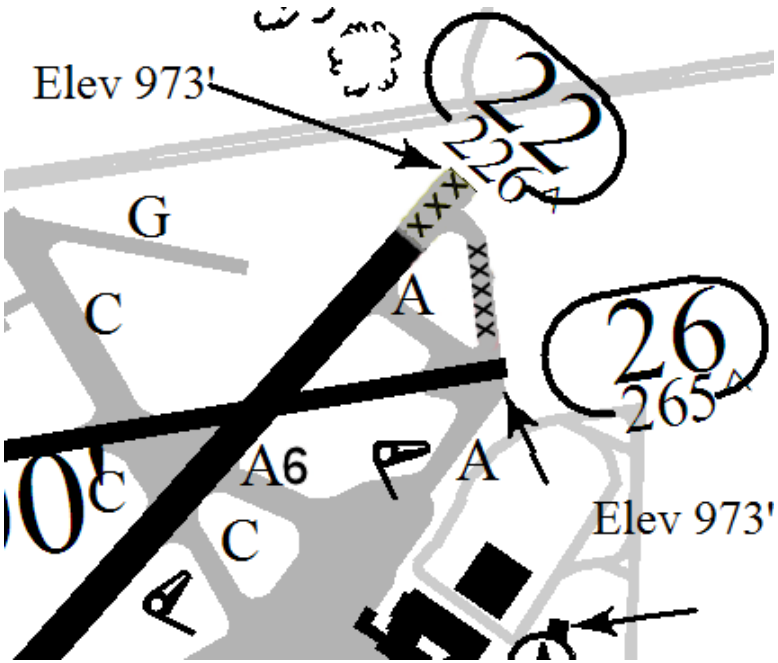
- What maps did they have? Did they match the actual state of the airport?
- Why did they think high-threat procedures were unnecessary?
- Why the 40 second conversation?
- Etc.

The Airport Diagram

What The Crew Had



What the Crew Needed

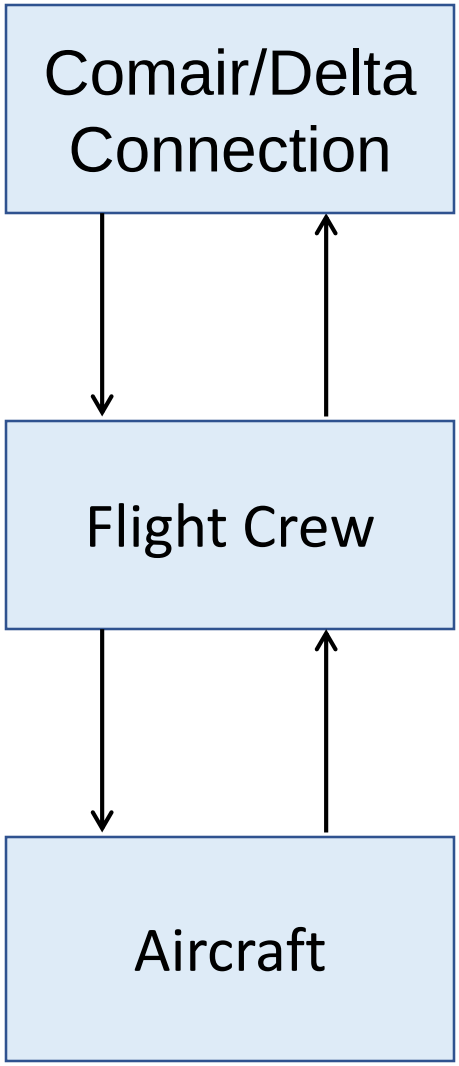


Context in Which Decisions Made:

- No communication that the taxi route to the departure runway was different than indicated on the airport diagram
- Dark out
- No known reason for high-threat taxi procedures
- 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)

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
Flight Crew
Aircraft

Comair (Delta Connection) Airlines

Safety Responsibilities

- 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 and train procedures to ensure proper taxi route progression and runway confirmation

Comair (Delta Connection) Airlines (2)

Role in Loss:

- Internal processes did not provide LEX L (local) NOTAM on the flight release, even though it was faxed to Comair from LEX (ATC)
- 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 or require high-threat taxi procedures.

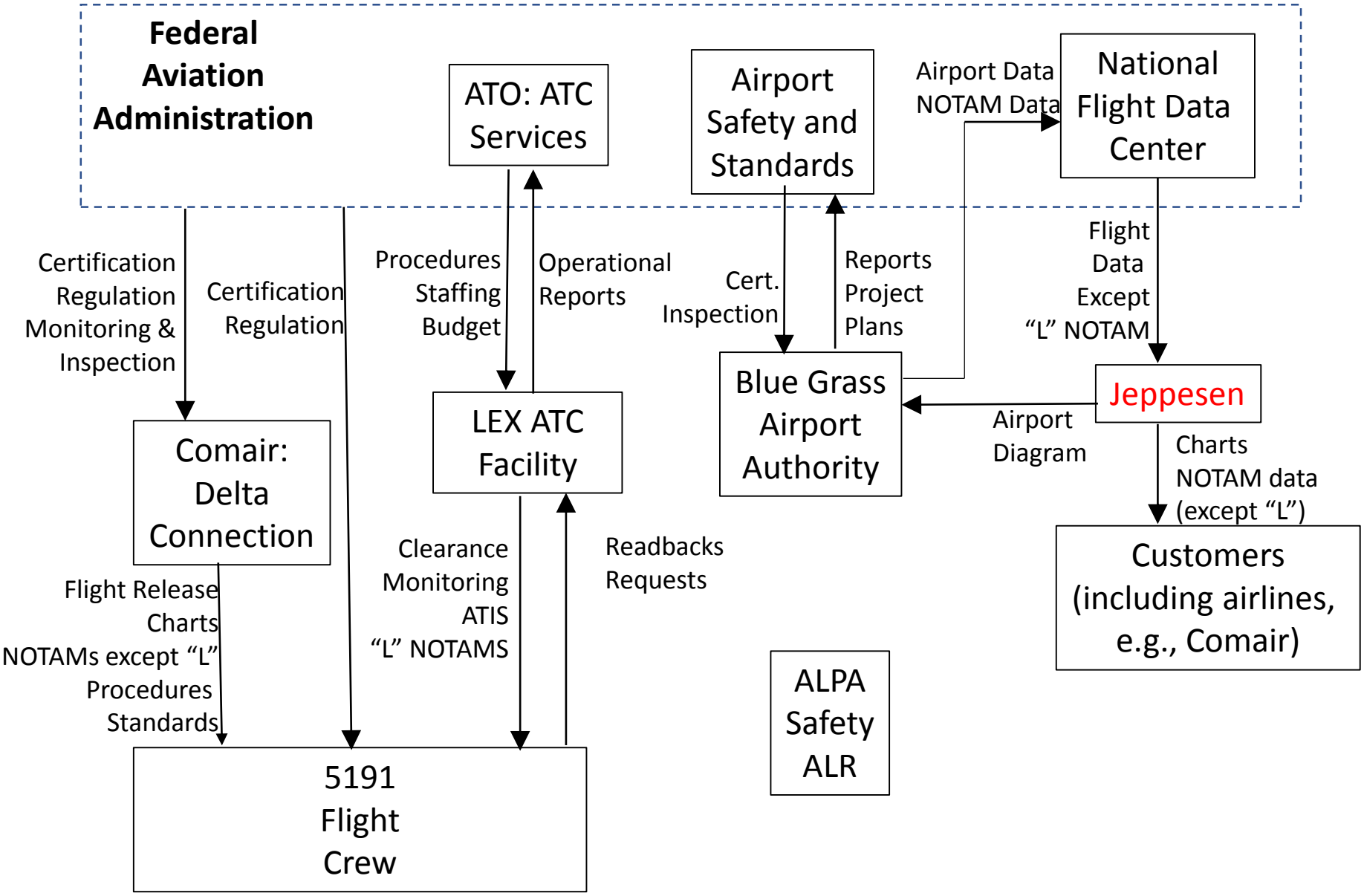
Comair (3)

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.


Federal Aviation Administration
ATO: ATC Services
Airport Safety and Standards
National Flight Data Center
Airport Data
NOTAM Data
Certification
Regulation
Monitoring &
Inspection
Certification
Regulation
Procedures
Staffing
Budget
Operational
Reports
Cert.
Inspection
Reports
Project
Plans
Flight
Data
Except
"L" NOTAM
Comair: Delta Connection
LEX ATC Facility
Blue Grass Airport Authority
Jeppesen
Airport
Diagram
Charts
NOTAM data
(except "L")
Customers (including airlines, e.g., Comair)
Flight Release
Charts
NOTAMs except "L"
Procedures
Standards
Clearance
Monitoring
ATIS
"L" NOTAMS
Readbacks
Requests
ALPA Safety ALR
5191 Flight Crew

Jeppesen

Safety Responsibilities:

- Creation of accurate aviation navigation charts and information data for safe operation of aircraft in the NAS.
- Assure Airport Charts reflect the most recent NFDC data

Role in Loss:

- Insufficient analysis of the software which processed incoming NFDC data to assure the original design assumptions matched those of the application.
- Not making available to the NAS Airport structure the type of information necessary to generate the 10-8 “Yellow Sheet” airport construction chart.

Jeppesen (2)

Process Model Flaws

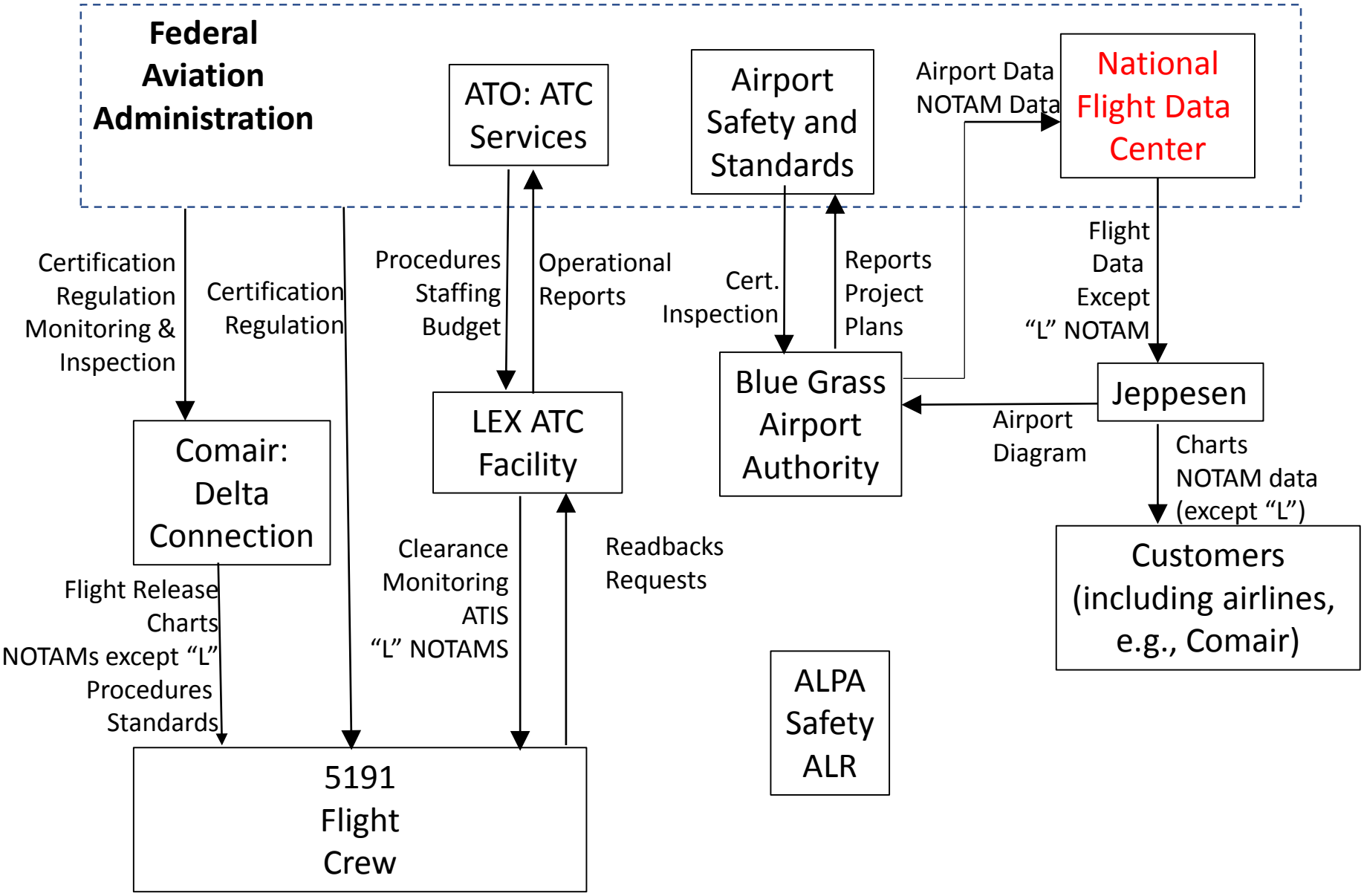
- Believed Document Control System software always generated notice of received NFDC data requiring analyst evaluation.
- Any extended airport construction included phase and time data as a normal part of FAA submitted paper work.

Context in Which Decisions Made

- The Document Control System software generated notices of received NFDC data.

Feedback

- Customer feedback channels are inadequate for providing information about charting inaccuracies.


Federal Aviation Administration
ATO: ATC Services
Airport Safety and Standards
National Flight Data Center
Airport Data
NOTAM Data
Certification
Regulation
Monitoring &
Inspection
Certification
Regulation
Procedures
Staffing
Budget
Operational
Reports
Cert.
Inspection
Reports
Project
Plans
Flight
Data
Except
"L" NOTAM
Comair: Delta Connection
LEX ATC Facility
Blue Grass Airport Authority
Jeppesen
Airport
Diagram
Charts
NOTAM data
(except "L")
Customers (including airlines, e.g., Comair)
Flight Release
Charts
NOTAMs except "L"
Procedures
Standards
Clearance
Monitoring
ATIS
"L" NOTAMS
Readbacks
Requests
ALPA Safety ALR
5191 Flight Crew

National Flight Data Center

Safety Responsibilities:

- Collect, collate, validate, store, and disseminate aeronautical information detailing the physical description and operational status of all components of the National Airspace System (NAS).
- Operate the US NOTAM system to create, validate, publish and disseminate NOTAMS.
- Provide safety critical NAS information in a format which is understandable to pilots.
- NOTAM dissemination methods will ensure pilot operators receive all necessary information.

Role in Loss

- Did not use the FAA Human Factors Design Guide principles to update the NOTAM text format.
- Limited dissemination of local NOTAMs (L-NOTAM).
- Used multiple and various publications to disseminate NOTAMs, none of which individually contained all NOTAM information.

Process Model Flaws:

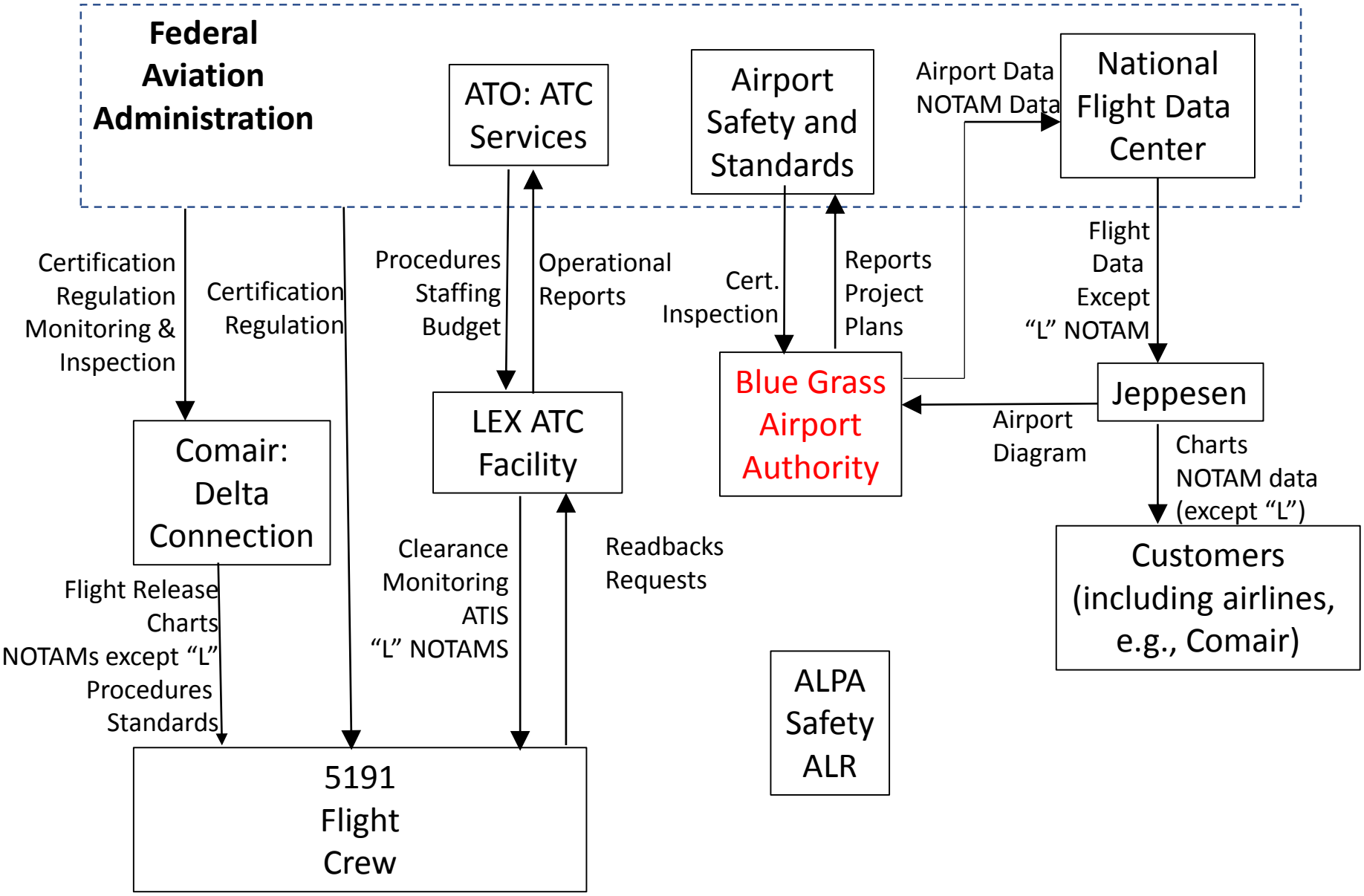
- Believed NOTAM system successfully communicated NAS changes.

Context in Which Decisions Made

- The NOTAM systems over 70 year history of operation. Format based on teletypes

Coordination

- No coordination between FAA human factors branch and the NFDC for use of HF design principle for NOTAM format revision.


Federal Aviation Administration
ATO: ATC Services
Airport Safety and Standards
Airport Data
NOTAM Data
National Flight Data Center
Certification
Regulation
Monitoring &
Inspection
Certification
Regulation
Procedures
Staffing
Budget
Operational
Reports
Cert.
Inspection
Reports
Project
Plans
Flight
Data
Except
"L" NOTAM
Blue Grass Airport Authority
Jeppesen
Airport
Diagram
Charts
NOTAM data
(except "L")
Comair: Delta Connection
LEX ATC Facility
Clearance
Monitoring
ATIS
"L" NOTAMS
Readbacks
Requests
Customers (including airlines, e.g., Comair)
Flight Release
Charts
NOTAMs except "L"
Procedures
Standards
ALPA Safety ALR
5191 Flight Crew

Blue Grass Airport Authority (LEX)

Safety Responsibilities:

- 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

Role in Loss:

- 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

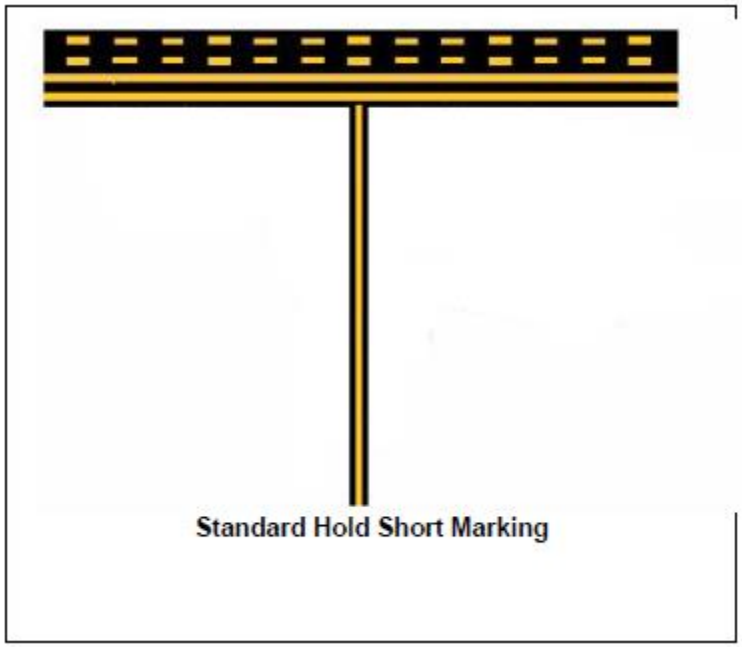
Process Model Flaws:

- 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.

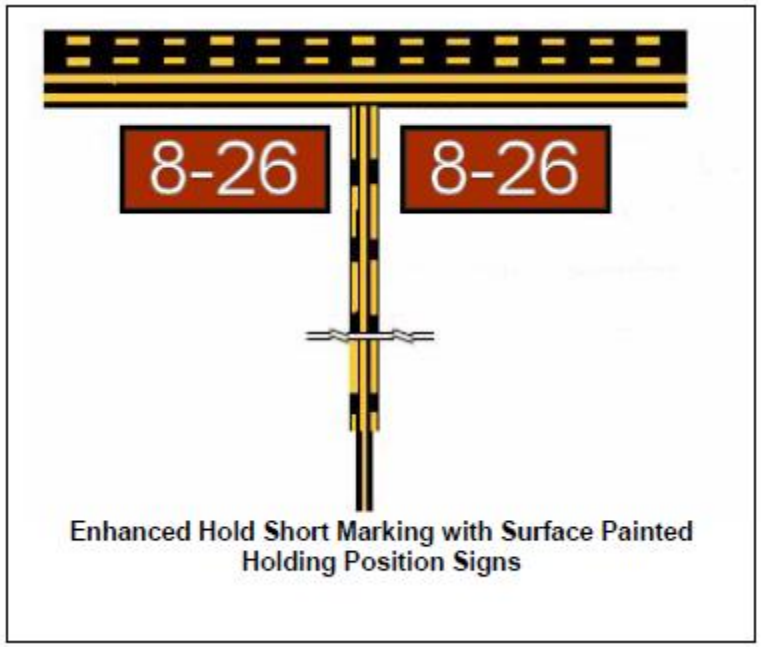
Context in Which Decisions Made:

- 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.

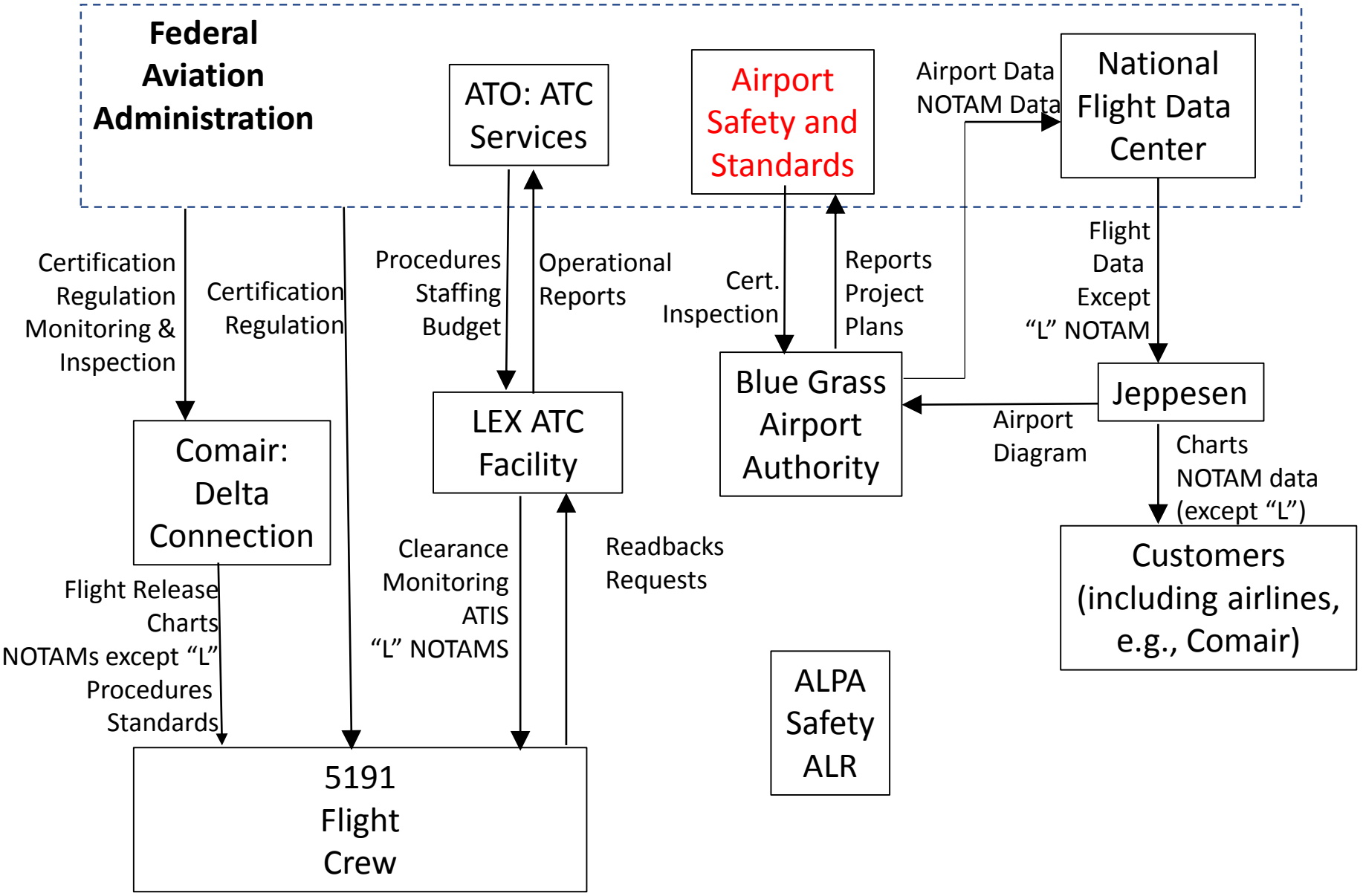
Standard and Enhanced Hold Short Markings



Standard Hold Short Marking



Enhanced Hold Short Marking with Surface Painted Holding Position Signs


Federal Aviation Administration
ATO: ATC Services
Airport Safety and Standards
National Flight Data Center
Airport Data
NOTAM Data
Certification
Regulation
Monitoring &
Inspection
Certification
Regulation
Procedures
Staffing
Budget
Operational
Reports
Cert.
Inspection
Reports
Project
Plans
Flight
Data
Except
"L" NOTAM
Comair: Delta Connection
LEX ATC Facility
Blue Grass Airport Authority
Jeppesen
Airport
Diagram
Charts
NOTAM data
(except "L")
Customers (including airlines, e.g., Comair)
Clearance
Monitoring
ATIS
"L" NOTAMS
Readbacks
Requests
Flight Release
Charts
NOTAMs except "L"
Procedures
Standards
ALPA Safety ALR
5191 Flight Crew

FAA Airport Safety & Standards Office

Safety Responsibilities:

- Establish airport design, construction, maintenance, operational and safety standards and issue operational certificates accordingly.
- Ensure airport improvement project grant compliance and release of grant money accordingly.
- Perform airport inspections and surveillance. Enforce compliance if problems found.
- Review and approve Safety Plans Construction Documents in a timely manner, consistent with safety.
- Assure all stake holders participate in developing methods to maintain operational safety during construction periods.

FAA Airport Safety & Standards Office

Role in Loss:

- The FAA review/acceptance process was inconsistent, accepting the original phase IIIA (Paving and Lighting) Safety Plans Construction Documents and then rejecting them during the transition between phases II and IIIA.
- Did not require all stake holders (i.e. a Pilot representative was not present) be part of the meetings where methods of maintaining operational safety during construction were decided.
- Focused on inaccurate runway length depiction without consideration of taxiway discrepancies.
- Did not require methods in addition to NOTAMs to assure safety during periods of construction when difference between LEX Airport physical environment and LEX Airport charts.

FAA Airport Safety & Standards Office

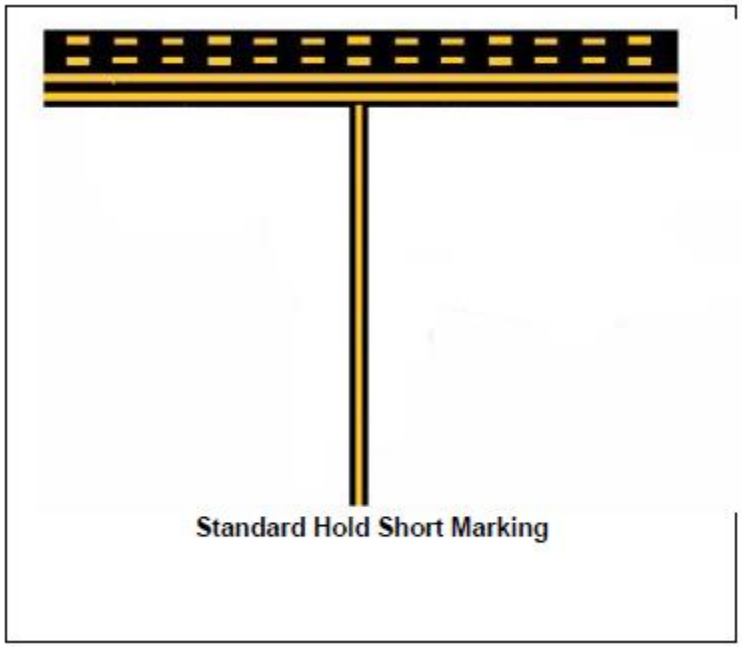
Process Model Flaws

- Did not believe pilot input was necessary for development of safe surface movement operations.
- No recognition of negative effects of changes on safety.
- Belief that the accepted practice of using NOTAMs to advise crews of charting differences was sufficient for safety.

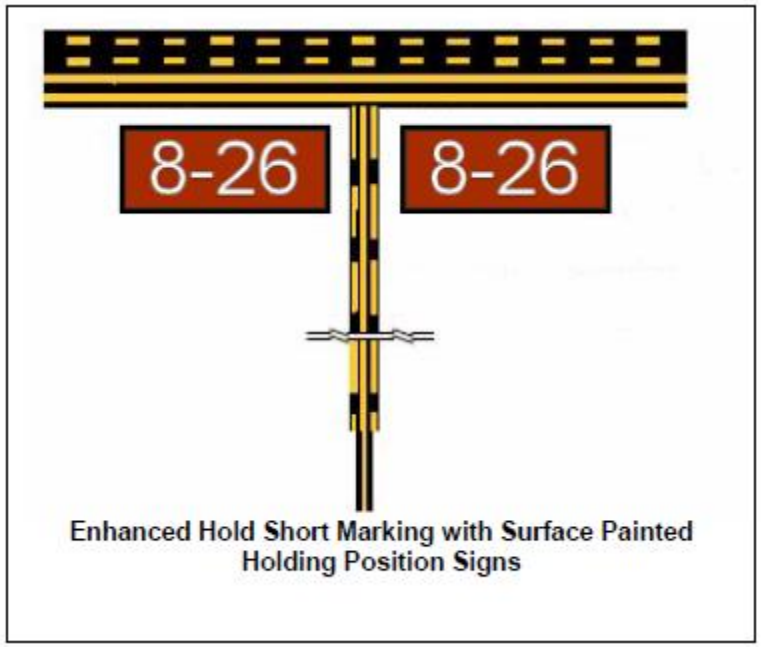
Context in Which Decisions Made

- Priority was to keep Airport Facility Directory accurate.
- Did not see a need for enhanced runway markings when low number of flights

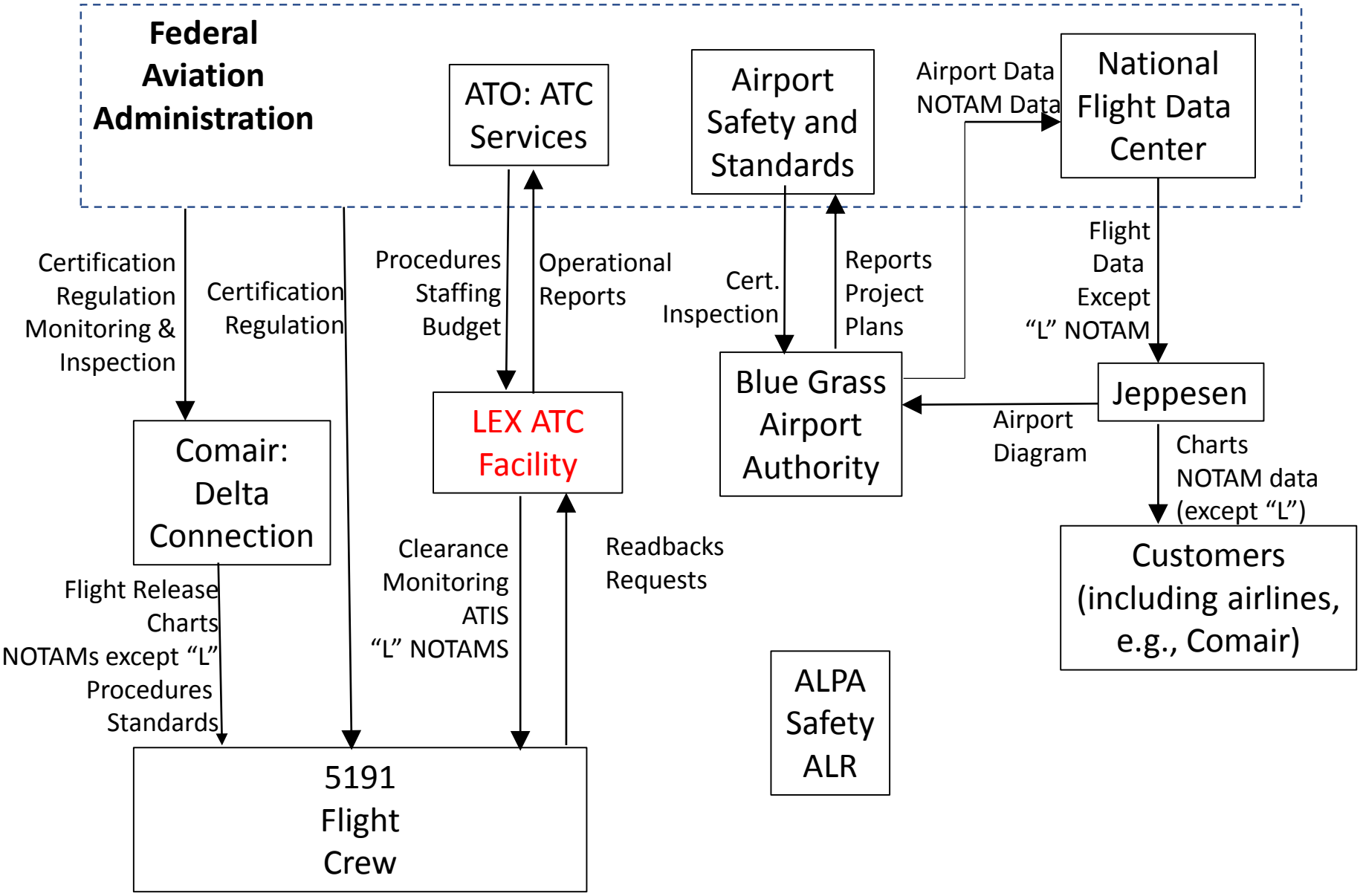
Standard and Enhanced Hold Short Markings



Standard Hold Short Marking



Enhanced Hold Short Marking with Surface Painted Holding Position Signs


Federal Aviation Administration
ATO: ATC Services
Airport Safety and Standards
Airport Data
NOTAM Data
National Flight Data Center
Certification
Regulation
Monitoring &
Inspection
Certification
Regulation
Procedures
Staffing
Budget
Operational
Reports
Cert.
Inspection
Reports
Project
Plans
Flight
Data
Except
"L" NOTAM
Blue Grass Airport Authority
Jeppesen
LEX ATC Facility
Airport
Diagram
Charts
NOTAM data
(except "L")
Comair: Delta Connection
Customers (including airlines, e.g., Comair)
Clearance
Monitoring
ATIS
"L" NOTAMS
Readbacks
Requests
Flight Release
Charts
NOTAMs except "L"
Procedures
Standards
ALPA Safety ALR
5191 Flight Crew

LEX Controller Operations

Safety Responsibilities:

- 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 Tower Controller Operations (2)

Role in Loss:

- Issued non-specific taxi instructions; i.e. “Taxi to runway 22” instead of “Taxi to runway 22 via Alpha, cross runway 26”. [Hindsight bias]
- 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

LEX Air Traffic Control Facility Management

Safety Responsibilities:

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

Role in Loss:

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

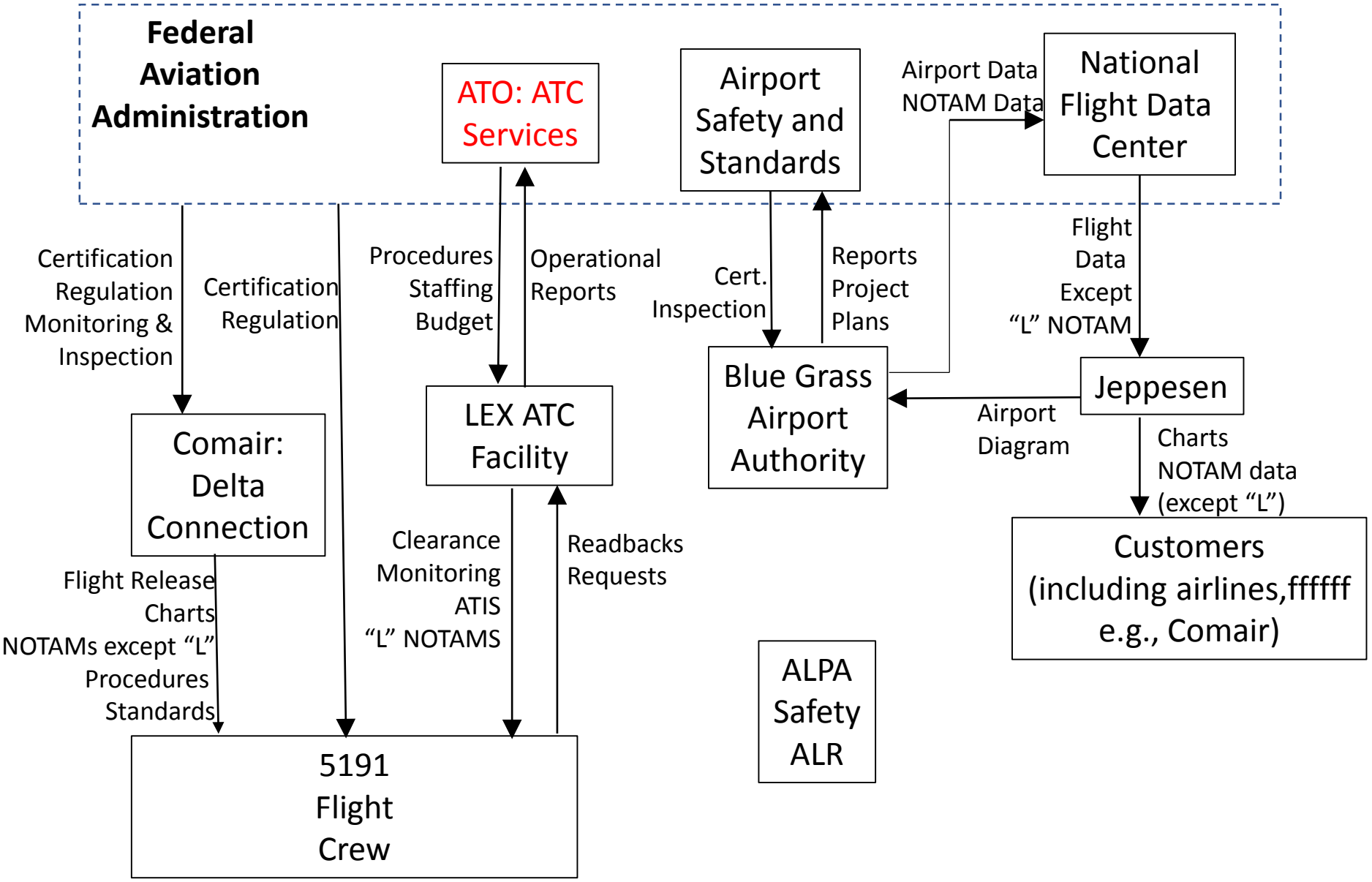
LEX Air Traffic Control Facility Management

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.


Federal Aviation Administration
ATO: ATC Services
Airport Safety and Standards
Airport Data
NOTAM Data
National Flight Data Center
Certification
Regulation
Monitoring &
Inspection
Certification
Regulation
Procedures
Staffing
Budget
Operational
Reports
Cert.
Inspection
Reports
Project
Plans
Flight
Data
Except
"L" NOTAM
Blue Grass Airport Authority
Jeppesen
Airport
Diagram
Charts
NOTAM data
(except "L")
Comair: Delta Connection
LEX ATC Facility
Clearance
Monitoring
ATIS
"L" NOTAMS
Readbacks
Requests
Flight Release
Charts
NOTAMs except "L"
Procedures
Standards
Customers (including airlines,ffffff e.g., Comair)
ALPA Safety ALR
5191 Flight Crew

FAA Air Traffic Organization: Terminal Services

Safety Responsibilities:

- 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.

Role in Loss:

- 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

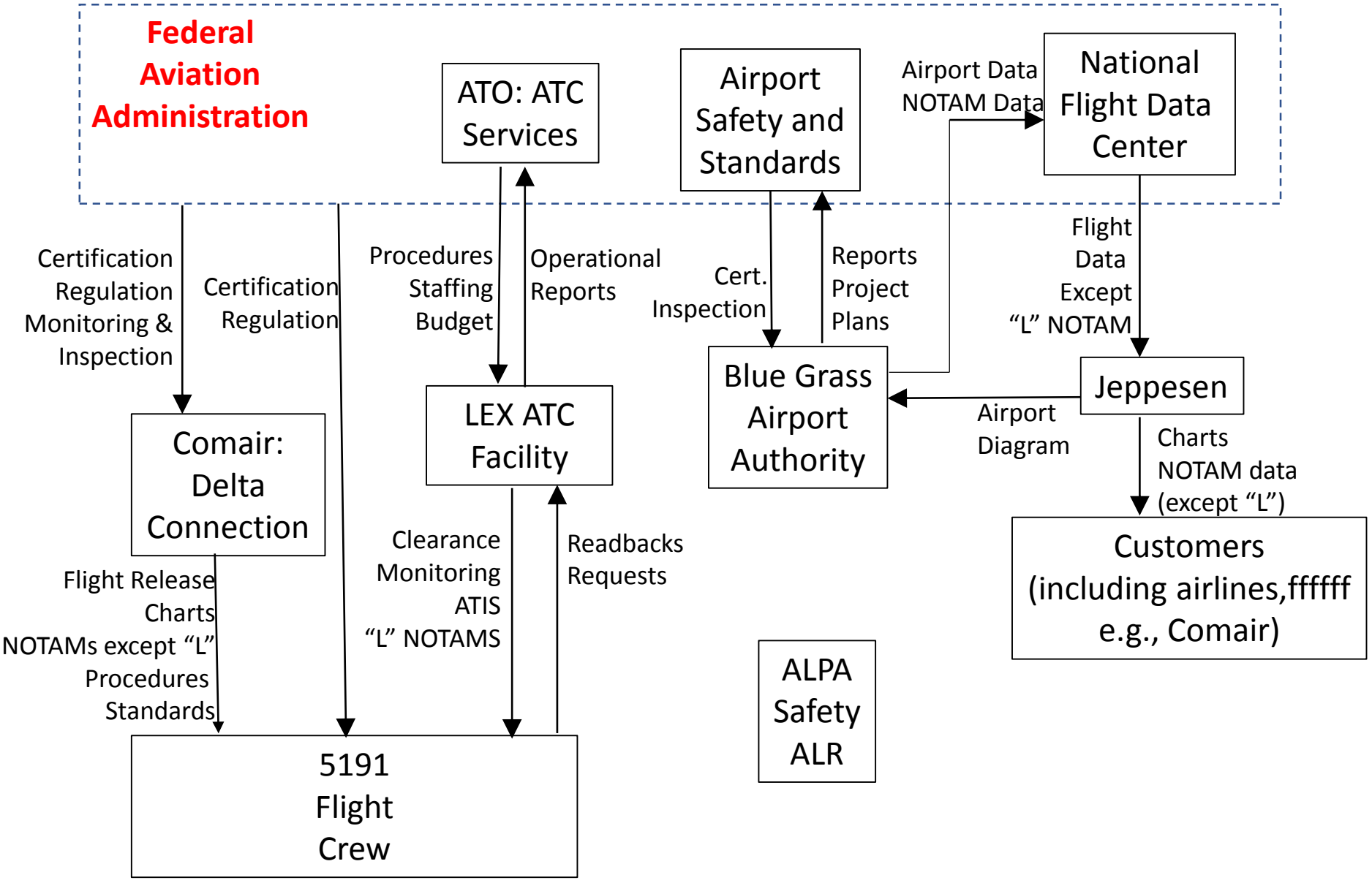
- Believed “verbal” guidance (minimum staffing of 2 controllers) was clear.
- Believed staffing with one controller was rare and if it was unavoidable due to sick calls etc., that the facility would coordinate the with Air Route Traffic Control Center (ARTCC) to control traffic.
- Believed limiting overtime 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
ATO: ATC Services
Airport Safety and Standards
Airport Data
NOTAM Data
National Flight Data Center
Certification
Regulation
Monitoring &
Inspection
Certification
Regulation
Procedures
Staffing
Budget
Operational
Reports
Cert.
Inspection
Reports
Project
Plans
Flight
Data
Except
"L" NOTAM
Blue Grass Airport Authority
Jeppesen
Airport
Diagram
Charts
NOTAM data
(except "L")
Comair: Delta Connection
LEX ATC Facility
Clearance
Monitoring
ATIS
"L" NOTAMS
Readbacks
Requests
Flight Release
Charts
NOTAMs except "L"
Procedures
Standards
Customers (including airlines,ffffff e.g., Comair)
ALPA Safety ALR
5191 Flight Crew

Federal Aviation Administration

Safety Responsibilities:

- 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.

Role in Loss:

- 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.

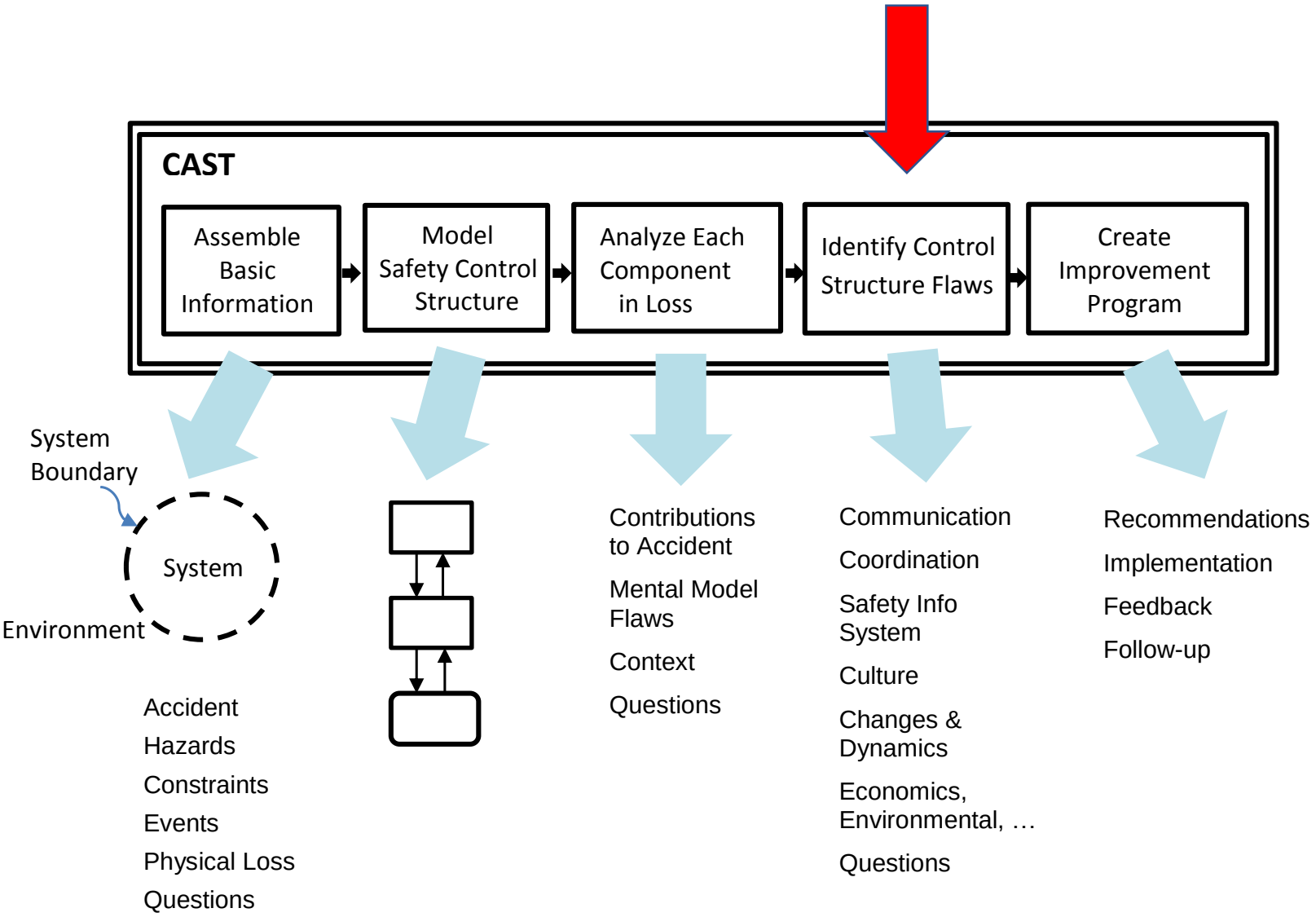
Context in Which Decisions Made

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

NTSB Findings

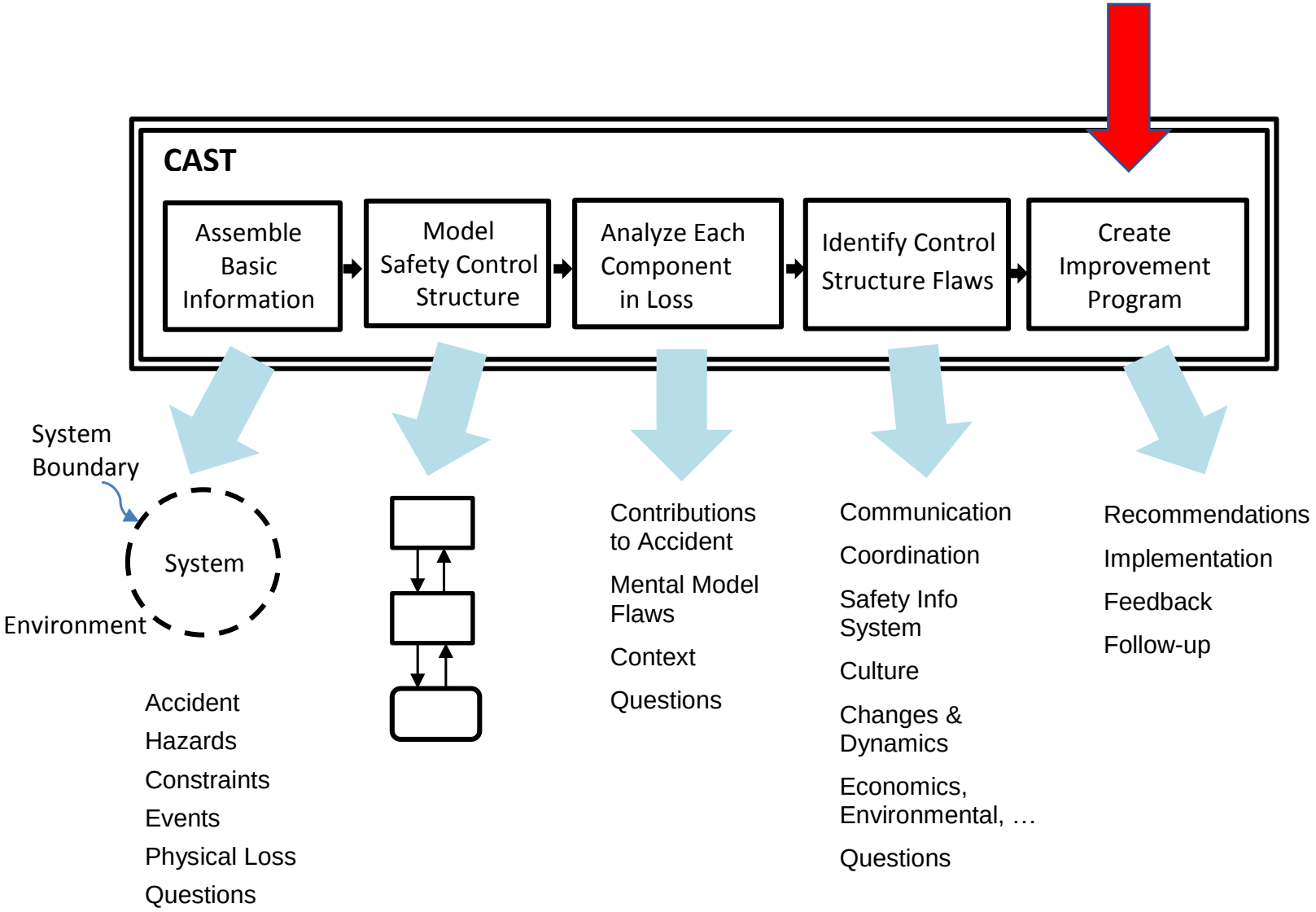
Probable Cause:

- 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.

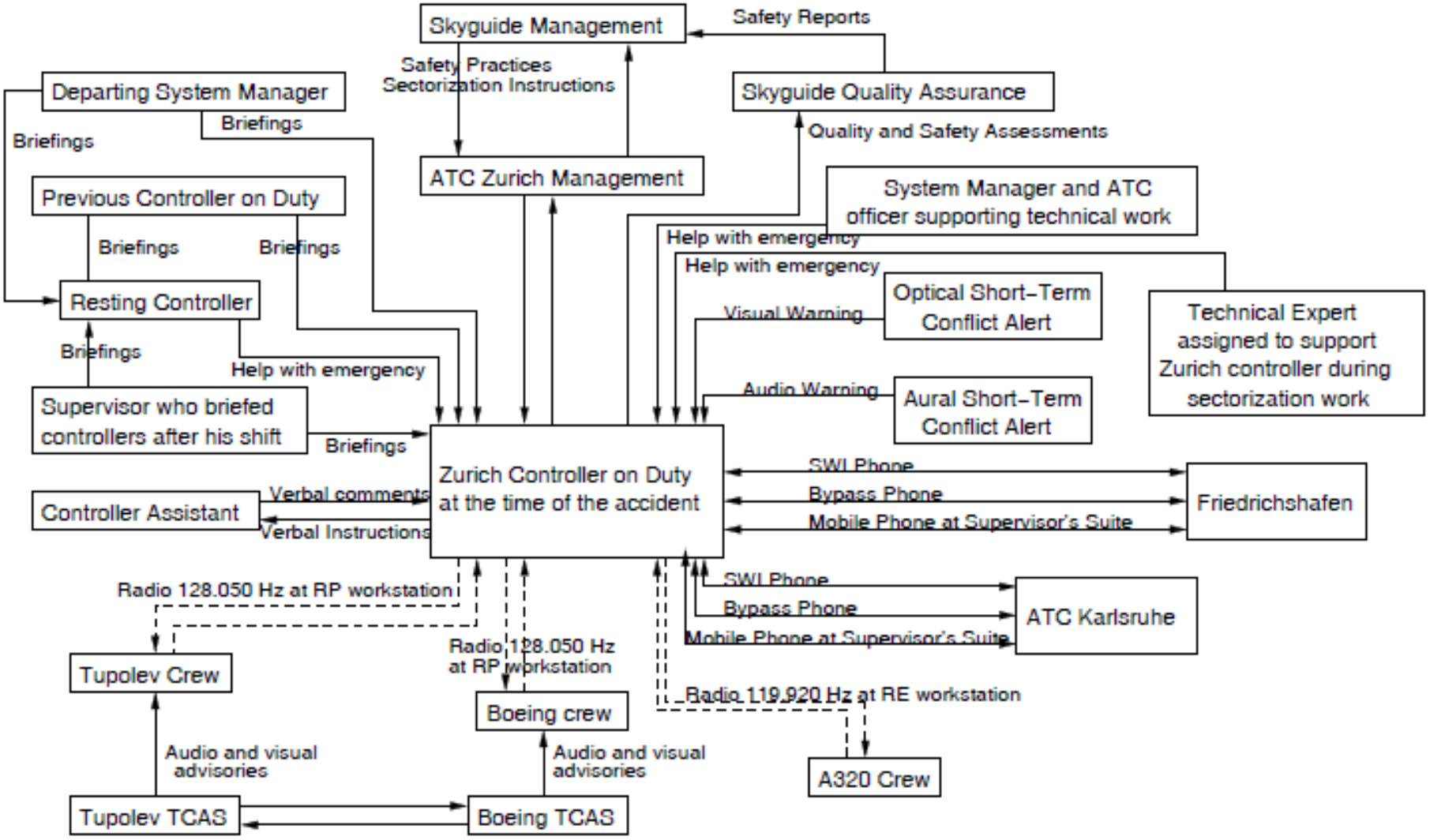

CAST
Assemble Basic Information
Model Safety Control Structure
Analyze Each Component in Loss
Identify Control Structure Flaws
Create Improvement Program
System Boundary
System
Environment
Accident
Hazards
Constraints
Events
Physical Loss
Questions
Contributions to Accident
Mental Model Flaws
Context
Questions
Communication
Coordination
Safety Info System
Culture
Changes & Dynamics
Economics, Environmental, …
Questions
Recommendations
Implementation
Feedback
Follow-up

Flaws in Interactions Among Components

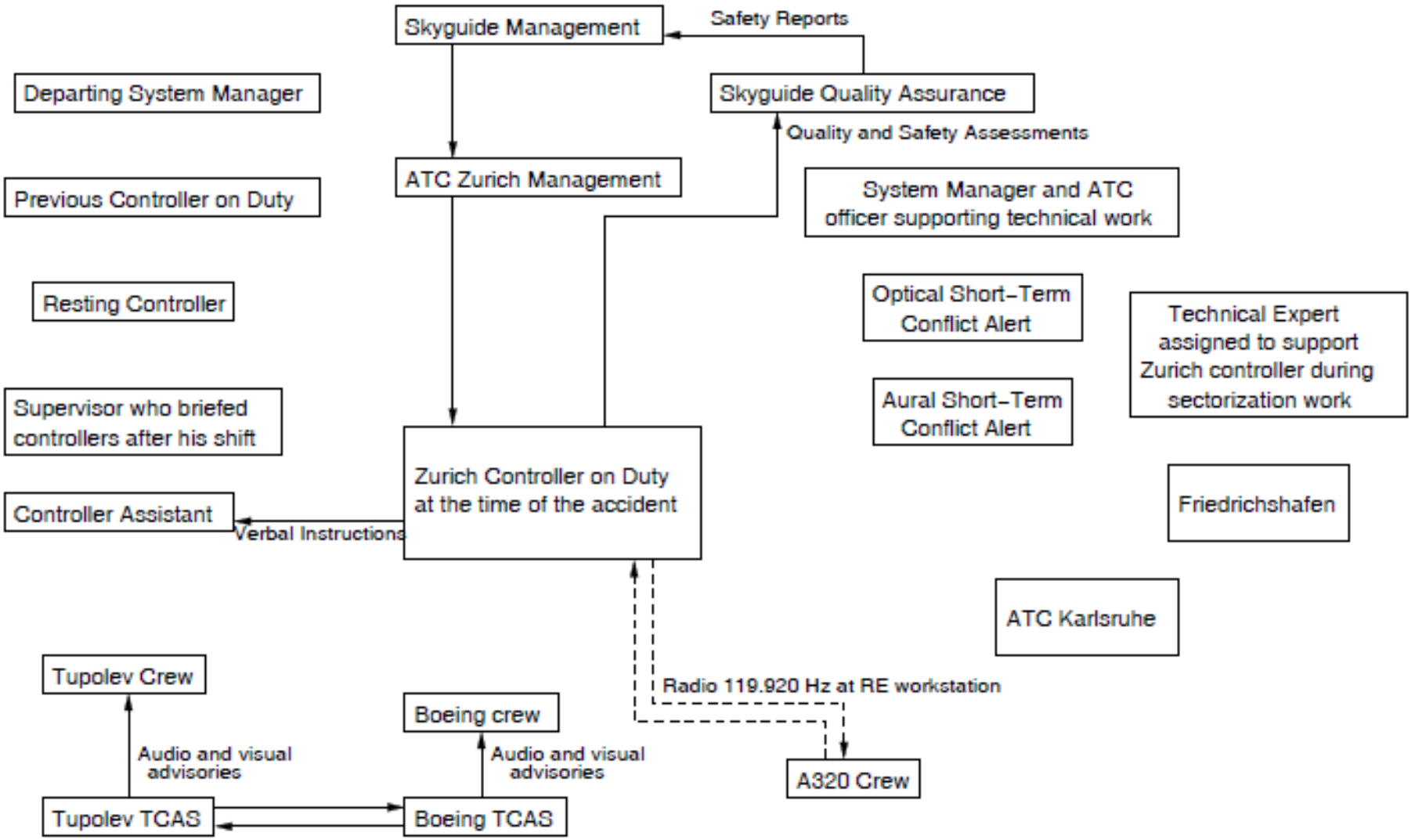
- Safety Information System
- Communication and Coordination (including feedback)
- Confusion about Responsibilities (accidents often in interfaces between departments, components)
- Safety Culture
- Changes and Dynamics over Time
- Economics, Environmental, …
- Safety Culture


CAST
Assemble Basic Information
Model Safety Control Structure
Analyze Each Component in Loss
Identify Control Structure Flaws
Create Improvement Program
System Boundary
System
Environment
Accident
Hazards
Constraints
Events
Physical Loss
Questions
Contributions to Accident
Mental Model Flaws
Context
Questions
Communication
Coordination
Safety Info System
Culture
Changes & Dynamics
Economics, Environmental, …
Questions
Recommendations
Implementation
Feedback
Follow-up

Communication Links Theoretically in Place in Uberlingen Accident



Communication Links Actually in Place

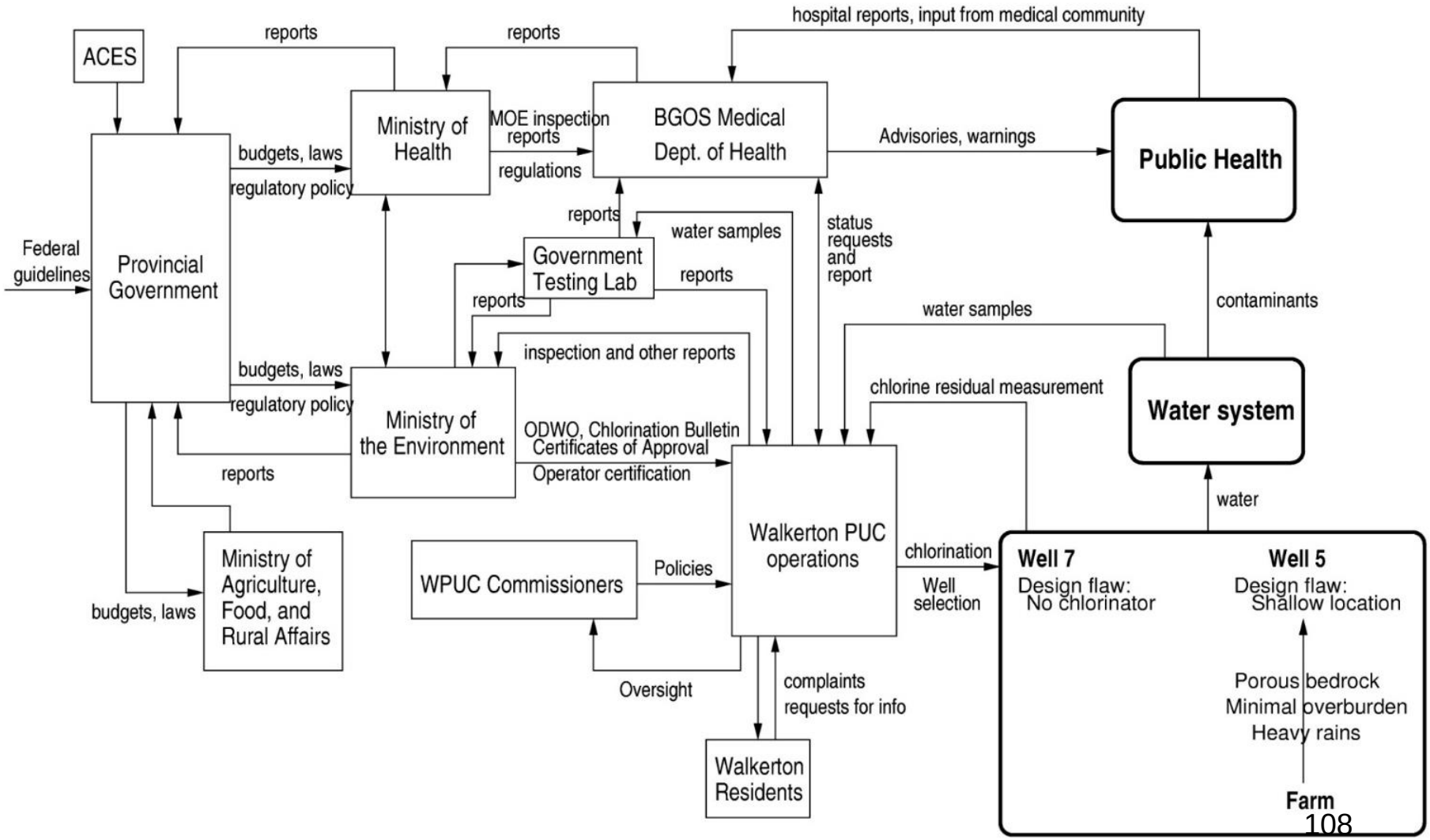


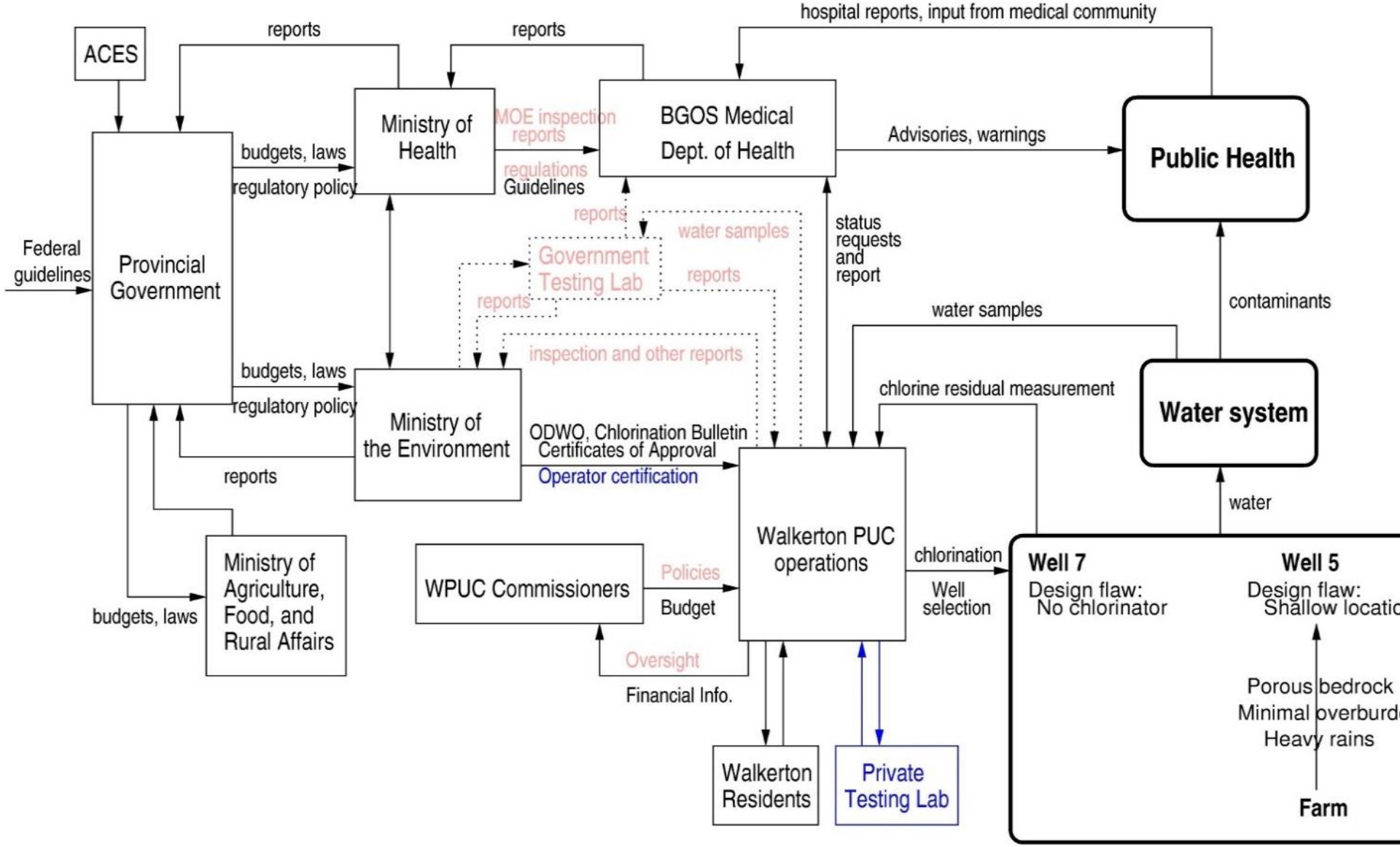
System Hazard: Public is exposed to E. coli or other health–related contaminants through drinking water.

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)




ACES
reports
reports
hospital reports, input from medical community
Ministry of Health
MOE inspection reports
regulations Guidelines
BGOS Medical Dept. of Health
Advisories, warnings
Public Health
budgets, laws
regulatory policy
Federal guidelines
Provincial Government
reports
water samples
Government Testing Lab
reports
reports
status requests and report
contaminants
water samples
inspection and other reports
budgets, laws
regulatory policy
Ministry of the Environment
chlorine residual measurement
Water system
ODWO, Chlorination Bulletin
Certificates of Approval
Operator certification
reports
water
Walkerton PUC operations
chlorination
Well 7
Design flaw:
No chlorinator
Well 5
Design flaw:
Shallow locatio
Ministry of Agriculture, Food, and Rural Affairs
WPUC Commissioners
Policies
Budget
Well selection
budgets, laws
Oversight
Financial Info.
Porous bedrock
Minimal overburd
Heavy rains
Farm
Walkerton Residents
Private Testing Lab

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
- Liability?
  - CAST takes out blame factor
  - Liability should be determined by courts, not by accident reports
  - Liability injects 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 generates
    - Different questions to ask
    - Different conclusions and recommendations

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.

Conclusions (2)

- Goal should be to learn how to improve the safety controls (safety control structure) and not to find someone or something to blame.
- 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?
- CAST provides a structured process for learning more from accidents. Generates questions that need to be answered during investigation.