GETTY IMAGES

How to Learn More From Accidents

Prof. Nancy Leveson

Aeronautics and Astronautics
MIT

From KWTX

WHY ARE WE NOT LEARNING ENOUGH FROM ACCIDENTS?

Common Problems in Accident Analysis

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

Root Cause Seduction

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

Oversimplification of Causes

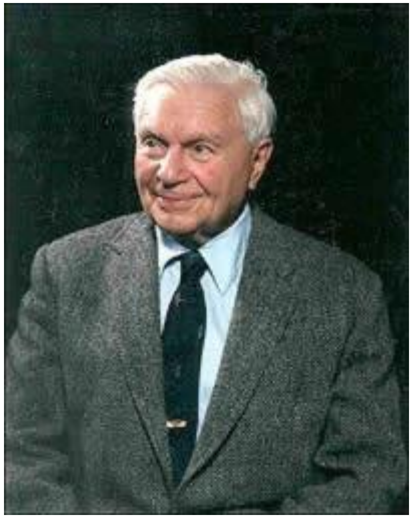
- Almost always there is:
  - Operator “error”
  - Flawed management decision making
  - Flaws in the physical design of equipment
  - Safety culture problems
  - Regulatory deficiencies

Basically flaws throughout the safety control structure

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,



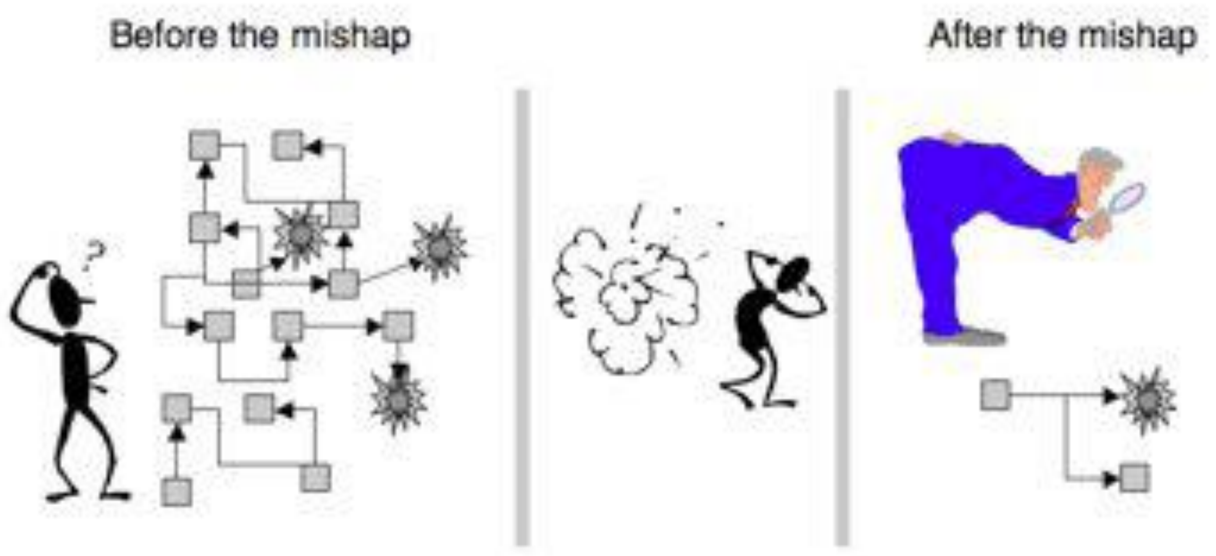
Mr. Aviation Safety

- 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.”

Hindsight Bias



(Sidney Dekker, Richard Cook)

“should have, could have, would have”

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

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

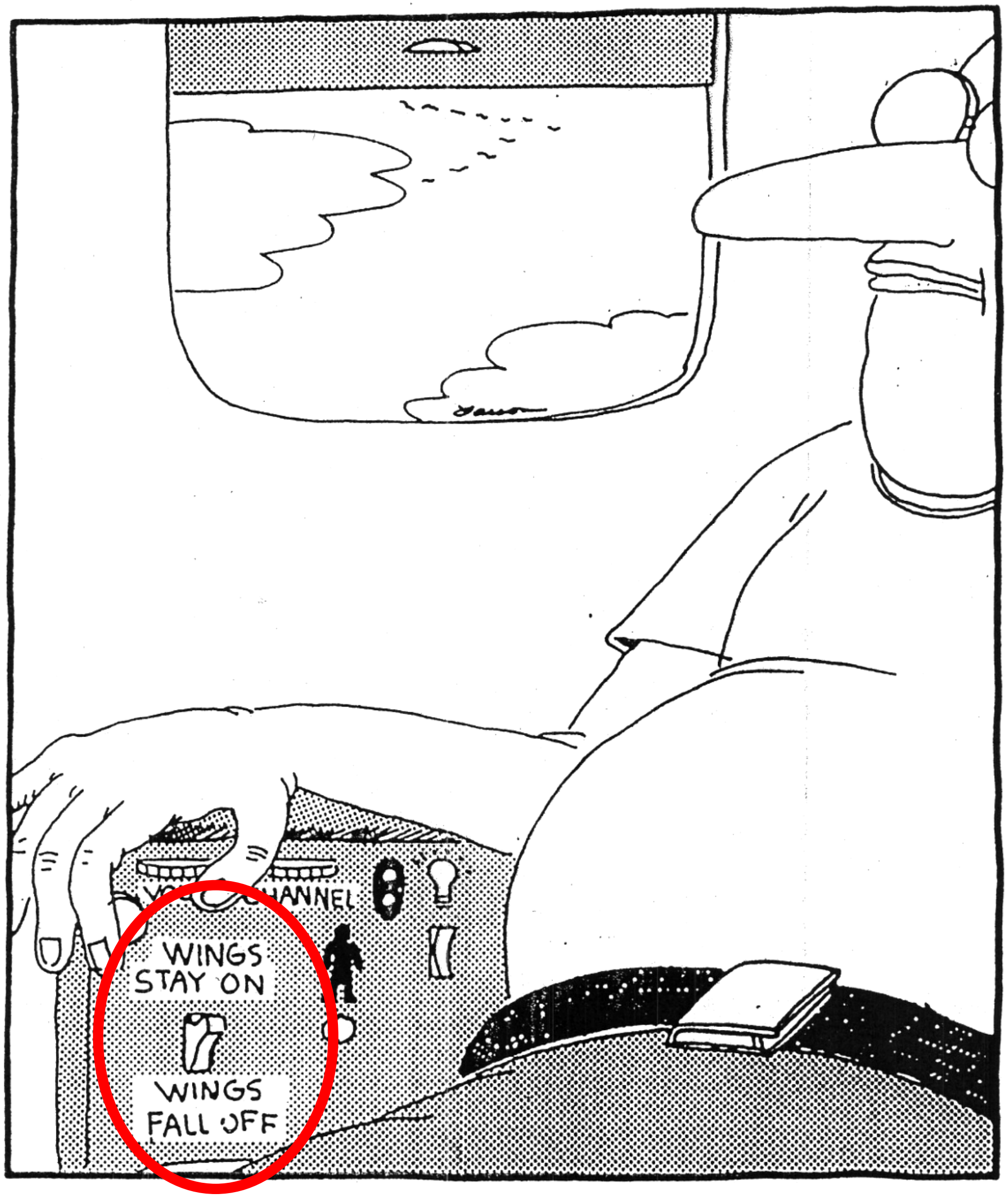
Hindsight Bias

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

Do Operators Really Cause Most Accidents?

Operator Error: Traditional View

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



Fumbling for his recline button Ted unwittingly instigates a disaster

Operator Error: Systems View (1)

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

Operator Error: Systems View (2)

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

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

Blame is the Enemy of Safety

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

- Goal of engineering is to understand why accidents occur in order to prevent them

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

WHO

NTSB determined probable cause of this accident was:

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

WHY

Contributing Factors:

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

Conclusions

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

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

Conclusions

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

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

vs.

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

- Accusatory approach to accident analysis (“who”)

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

WHAT

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

WHY

Reason for the thrust deficiency:

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

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

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

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

Reason for the wing contamination: …

1. Deicing/anti-icing procedures.

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

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

Conclusions

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

Accusatory:

Who

Why

Explanatory:

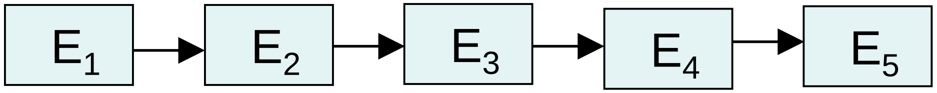
What

Why

- Do you think the recommendations will be different?

Use of Inappropriate Accident Models

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



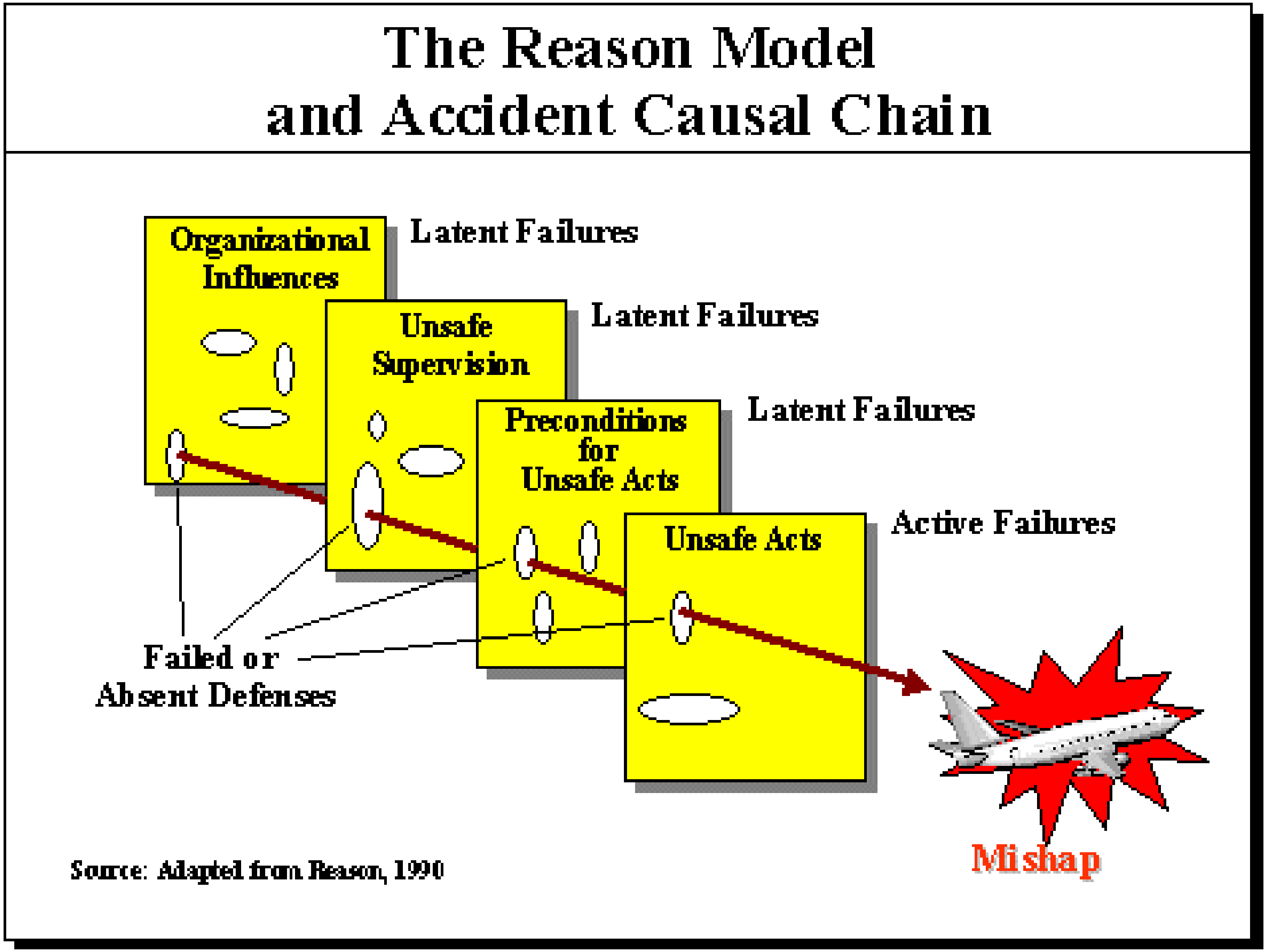
E_1 → E_2 → E_3 → E_4 → E_5

Each event is the direct result of the preceding event

Domino Model

Heinrich, 1932

Reason Swiss Cheese = Domino Model


The Reason Model
and Accident Causal Chain

Source: Adapted from Reason, 1990

Events are Not Enough

Need to look at ***why*** events occurred

Event	Questions Raised
An automatic protection system was triggered that was designed to prevent liquid from entering the exhaust gas system (flare). But preventing the liquids from entering the flare also prevented the gases in the system from being discharged, increasing pressure in the reactor.	???

Events are Not Enough

Need to look at ***<u>why</u>*** events occurred

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

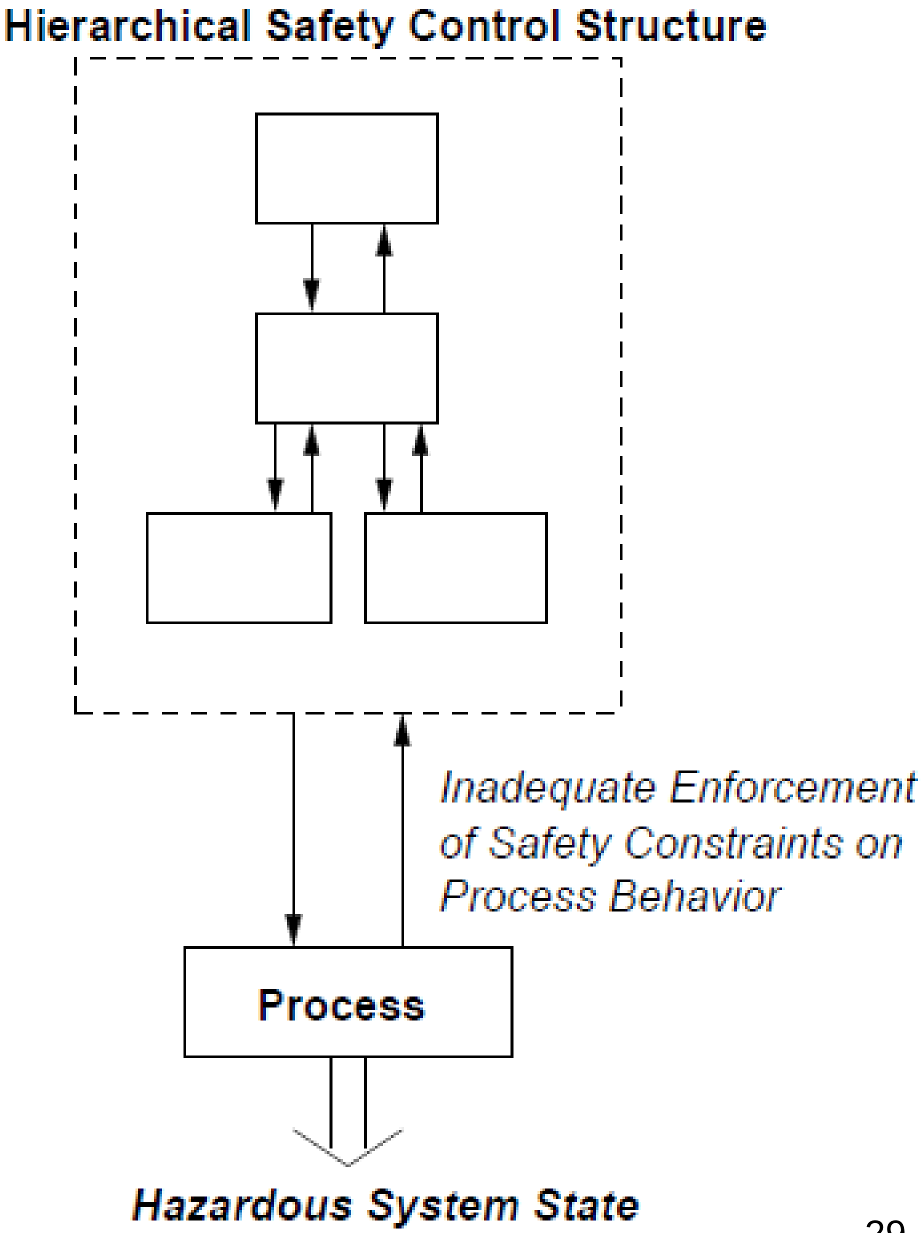
Another Example

Event	Questions Raised
Continued warming up of the reactors caused more chemical reactions to occur between the ethylbenzene and the catalyst pellets, causing more gas formation and increasing pressure in the reactor.	???

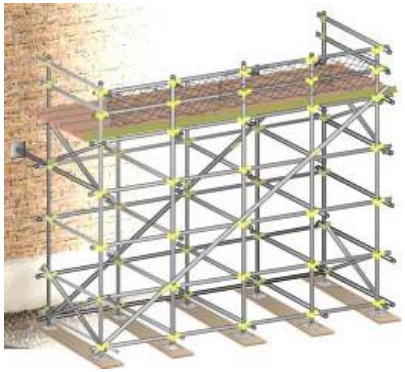
Another Example

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

Accident Causality Using STAMP

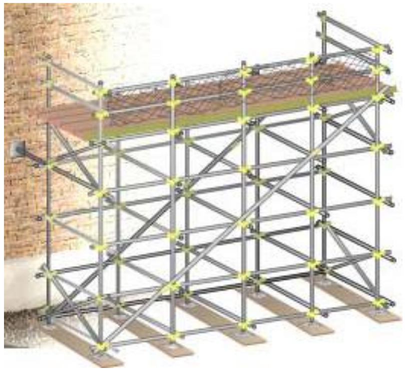

Hierarchical Safety Control Structure
Inadequate Enforcement of Safety Constraints on Process Behavior
Process
Hazardous System State

Scaffolding Accident



- Assembling a large, complex product
- Part was not available when needed so decision made to add it later
- When part arrived, had to disassemble a large piece of product to insert missing part
- Scaffolding constructed during previous shift
- When went to remove large piece, the scaffolding kept it from being removed.
- Took floorboards out of scaffolding
- Removed piece and four workers were holding the piece while they moved it to the end of the scaffolding to take it down to the shop floor
- All four turned and one fell through hole in scaffolding

Scaffolding Accident (Analysis)



- Identified “root cause”
  - Lack of experience doing job
  - Did not know there was a shop aid for this job
  - Did not perceive any undue risk and did not ask for help
- Recommendations:
  - Tell workers not to remove floorboards from scaffolding.
  - Add tool information to job instructions
  - During daily kickoff meeting, discuss potential hazards and ensure safe work practices for assigned tasks of the day
- Causal analysis tool:
  - Error: Worker stepped in a hole?
  - Why?
    - “Lack of situational awareness”
    - “Made a mistake”

Note focused on victim and workers themselves

Scaffolding Accident (2)

- Report did not ask:
  - Why were they doing a job for which they had no experience and without oversight from someone who did?
  - Why did they not know about proper job aids?
  - Whose responsibility was it to ensure right equipment was available and used?
  - Why did they not ask for advice when scaffolding prevented them from doing their job? [“Find a way” culture]
  - Who provides oversight for “out-of-sequence” work?
  - Why was blame for not understanding risks involved placed on them and not their supervisors?
  - Why was incorrect scaffolding for job constructed in the first place?

Scaffolding Accident (2)

- Why were the people constructing it not aware of what scaffolding was required?
- Who evaluates the hazards of out-of-sequence jobs?
- Was there documentation of tools needed for job?
- Why was the job not done when it originally was supposed to be done?
- Why was there no oversight of this out-of-sequence job?
- There was supposed to be a meeting about how to accomplish this work. Why was it never held? Why didn’t the work wait until it could be?
- Are workers often expected to jury rig solutions with no oversight or input from others?

STAMP

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

CAST: INCREASING LEARNING FROM ACCIDENTS/INCIDENTS

Goals for Accident/Incident Analysis

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

CAST (Causal Analysis using System Theory)

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

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

Change in Focus

~~“Examine failures”~~

⇩

“Determine why designed controls were ineffective”

- Accidents are caused by complex interactions among humans, hardware, software, and social structures (not just chains of failure events)

Patient Safety: Root Cause Analysis

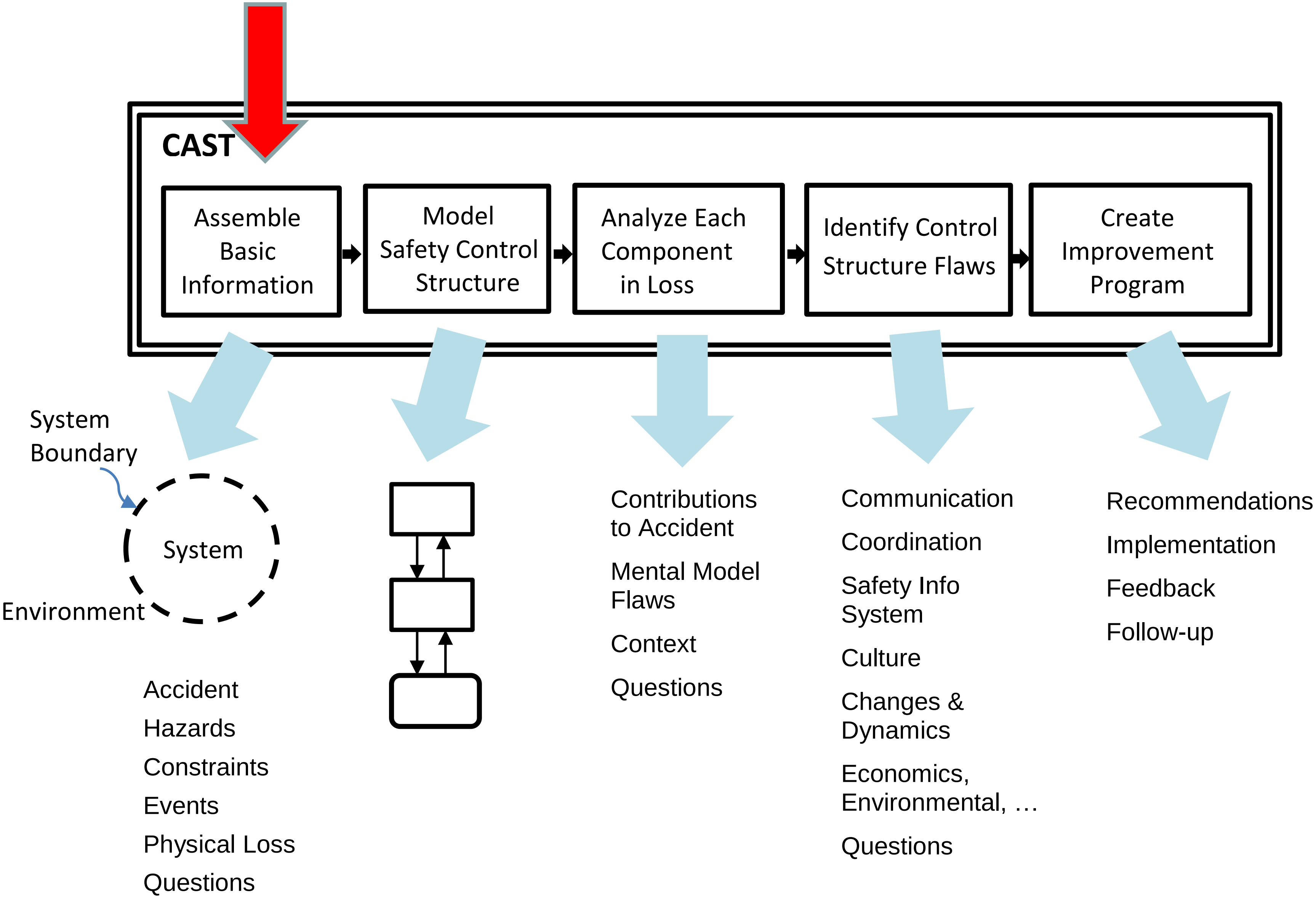
- Aubrey Samost M.D. (large Chicago medical center)
- Meaghan O’Neil (VA medical center)
- Lawrence Wong (U.C. San Diego Medical Center)

What happened?

- Patient admitted to hospital (in Chicago) for a cardiac transplant
- Written orders calls for administration of immunosuppression medication before surgery
- CCU nurse hands off patient to surgical team
- Surgeons start surgery without patient being given immunosuppression medication
- Surgery successful, but patient ventricular function worsens
- Patient placed on ECMO and treated for transplant rejection
- Patient did not survive

Standard “Blame” Approach (RCA)

- CCU nurse did not give immunosuppression medication
- Nurses did not tell surgeon it had not been given
- Surgeon started surgery without patient receiving immunosuppression medication despite executing “timeout” (checklist) before surgery



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

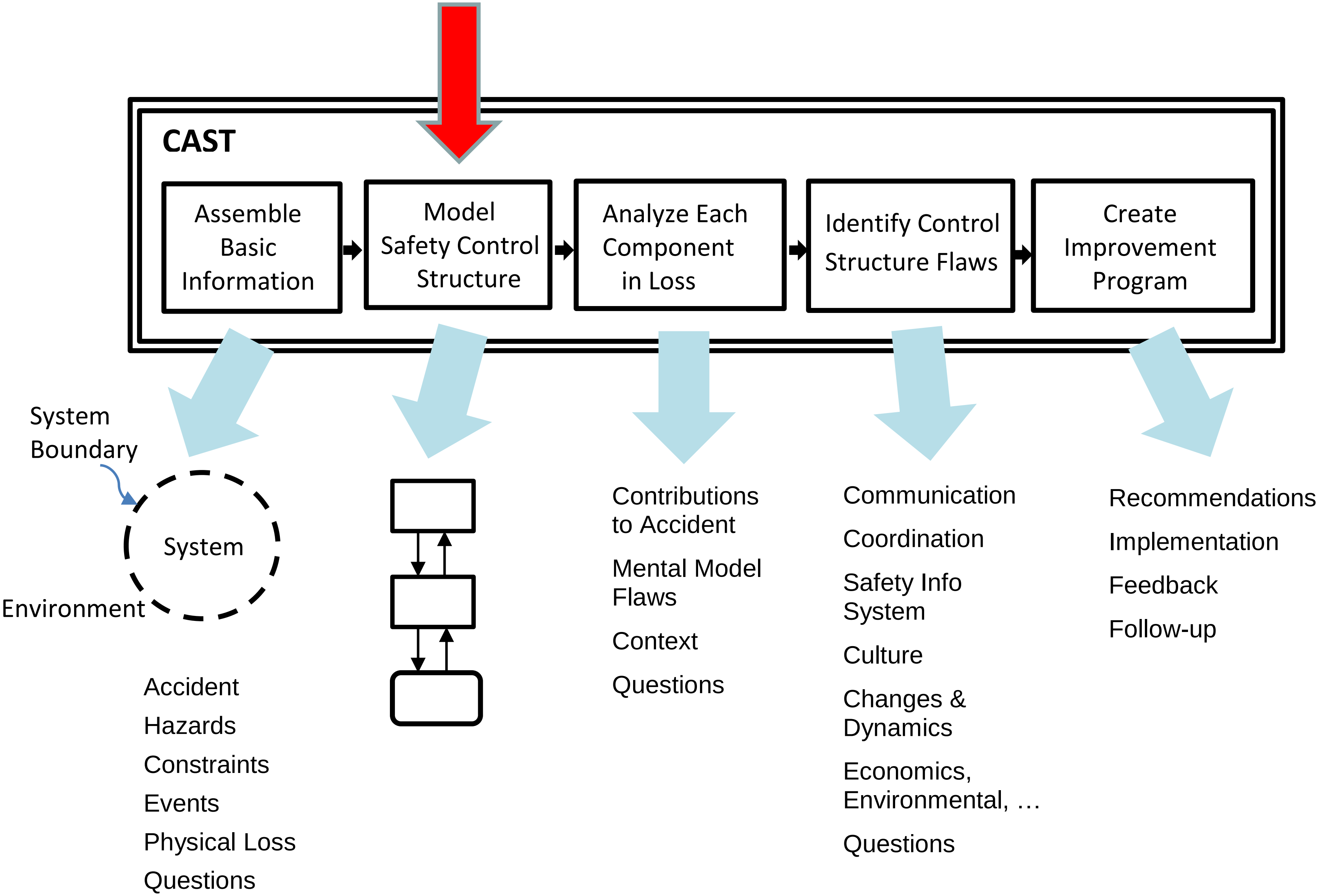
Implementation

Feedback

Follow-up

Systems Approach: CAST

- **Adverse Event**: Patient experiences rejection of transplant
- **Hazard**: Patient not getting proper pre-surgical medication
- Goal is to determine why the controls in place were not effective and how to improve them for the future



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, …

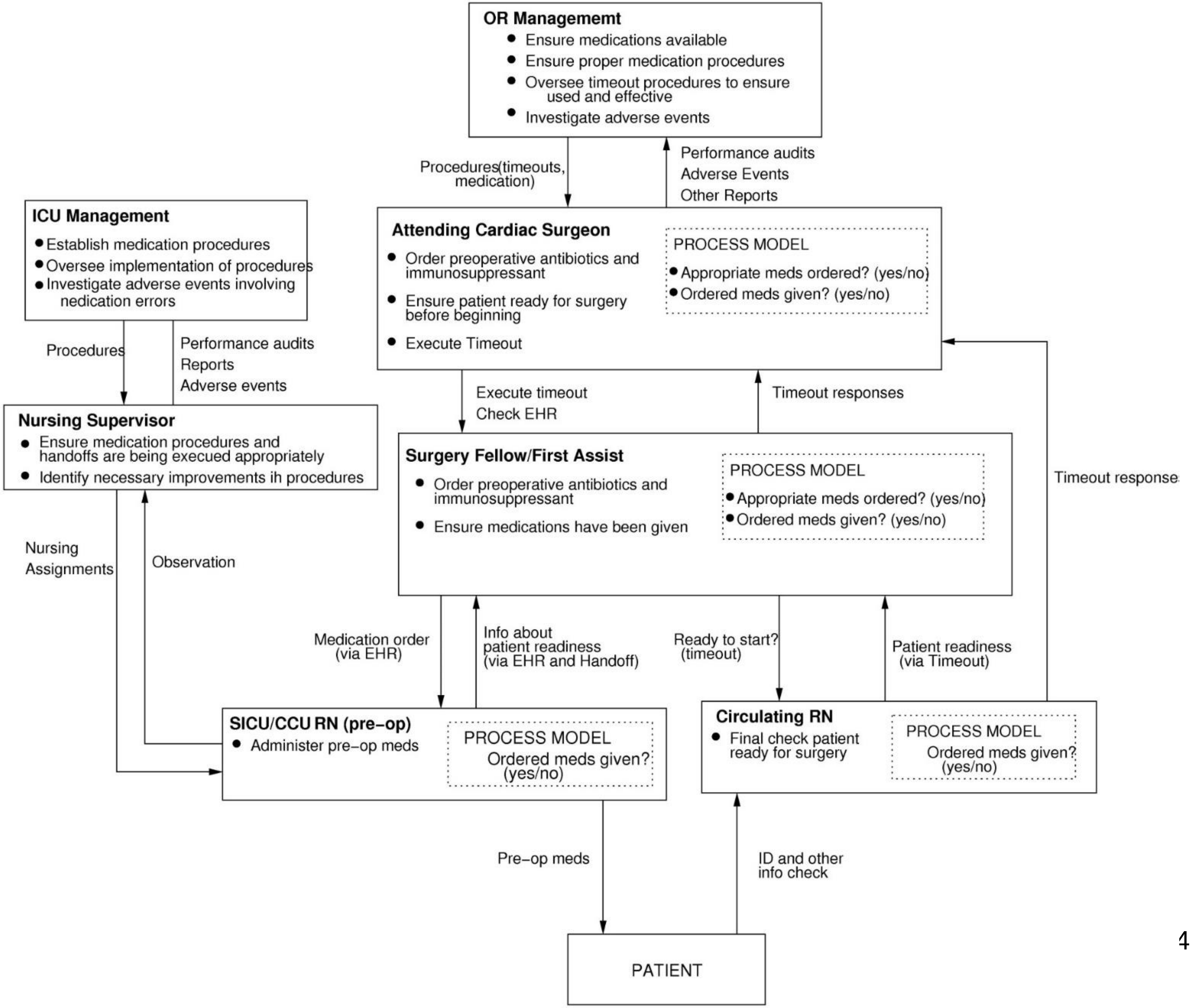
Questions

Recommendations

Implementation

Feedback

Follow-up



OR Managememt

- Ensure medications available
- Ensure proper medication procedures
- Oversee timeout procedures to ensure used and effective
- Investigate adverse events

Procedures(timeouts, medication)

Performance audits
Adverse Events
Other Reports

ICU Management

- Establish medication procedures
- Oversee implementation of procedures
- Investigate adverse events involving nedication errors

Procedures

Performance audits
Reports
Adverse events

Attending Cardiac Surgeon

- Order preoperative antibiotics and immunosuppressant
- Ensure patient ready for surgery before beginning
- Execute Timeout

PROCESS MODEL

- Appropriate meds ordered? (yes/no)
- Ordered meds given? (yes/no)

Execute timeout
Check EHR

Timeout responses

Nursing Supervisor

- Ensure medication procedures and handoffs are being execued appropriately
- Identify necessary improvements ih procedures

Surgery Fellow/First Assist

- Order preoperative antibiotics and immunosuppressant
- Ensure medications have been given

PROCESS MODEL

- Appropriate meds ordered? (yes/no)
- Ordered meds given? (yes/no)

Timeout response

Nursing Assignments

Observation

Medication order (via EHR)

Info about patient readiness (via EHR and Handoff)

Ready to start? (timeout)

Patient readiness (via Timeout)

SICU/CCU RN (pre-op)

- Administer pre-op meds

PROCESS MODEL
Ordered meds given? (yes/no)

Circulating RN

- Final check patient ready for surgery

PROCESS MODEL
Ordered meds given? (yes/no)

Pre-op meds

ID and other info check

PATIENT

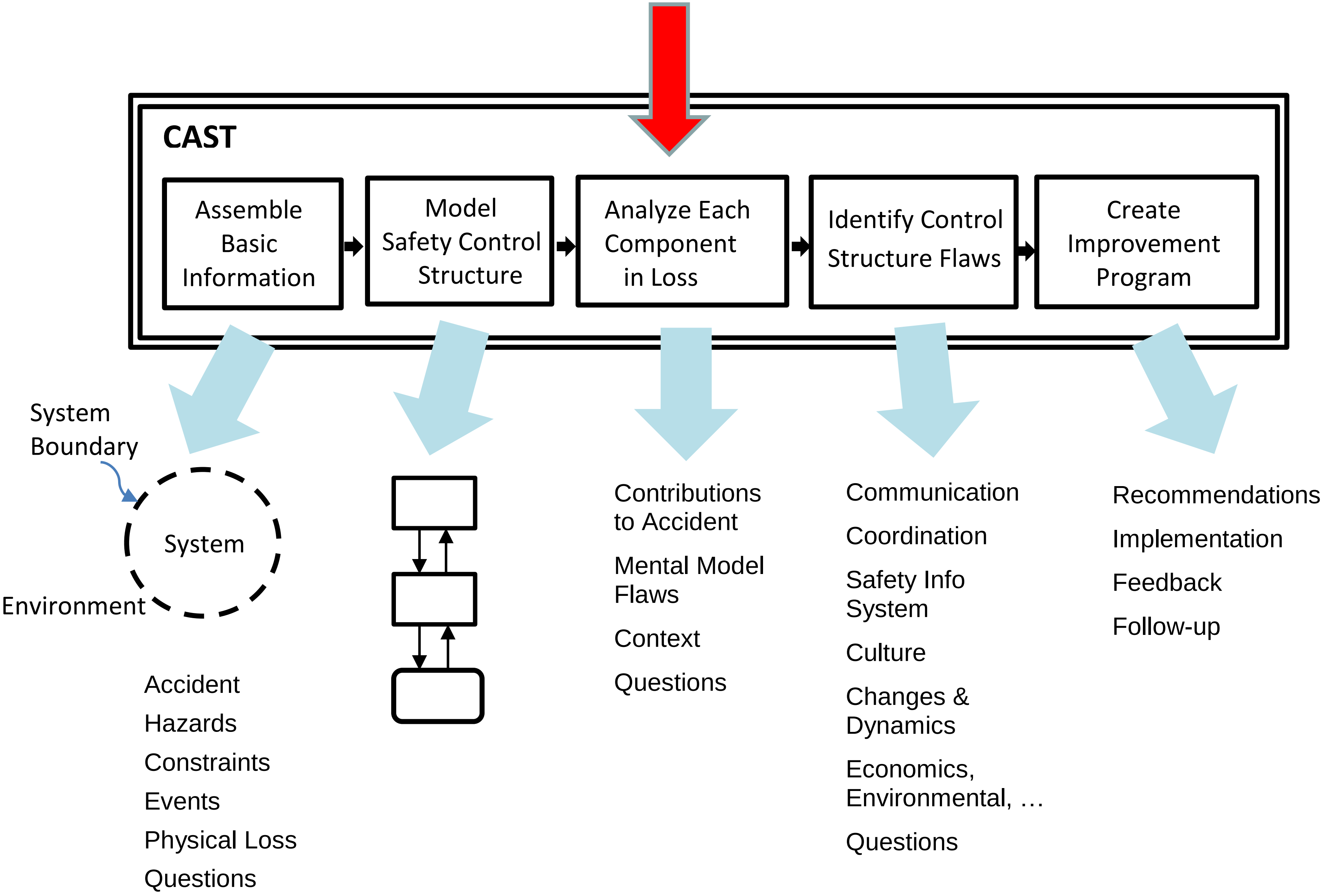
Controls to Ensure Proper Medication Given

- Written order sets, EHR (Electronic Health Record)
- Handoff of patient to surgical team
- Surgical timeout (checklist)
- Other OR checks (e.g., circulating nurse, surgical fellow, attending physician)

None of these was successful in this case

To understand why, need to look at individual behavior, operation of structural controls, and safety control structure design (SMS)

- Everyone involved had incorrect process models
- Lots of missing feedback paths
- Controls and control structure as designed were not effective



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

Cardiac Care Unit (CCU) Nurse

Safety Responsibilities:

- Administer pre-operative medications
- Report concerns about patient to the surgical team

Role in Adverse Event:

- Did not give pre-operative immunosuppression
- Did not tell surgical staff that patient had not received the medication

Why?

Process Model Flaws	Questions
Not aware she needed to give the immunosuppression	*How was she supposed to know? Why didn't she?*

Contextual Factors	
Several years since had done transplants so not aware of requirements for that operation [note a **change**]. Checklists will not help here.	*Who was responsible for training on changes in duties? Were there management of change procedures defined and used?*
Not adequately trained for CCU	*Why not? Who is responsible for this?*
Antibiotics were as part of preoperative order set but floor nurses do not give them; they are given in the OR. Could have created confusion about who was responsible for giving immunosuppression	
Order in the EHR does not specify who is responsible for carrying out the order	

Circulating RN (Operating Room Nurse)

Safety Responsibilities:

- Final check that patient is ready for surgery

Role in Adverse Event:

- Did not stop surgery from proceeding despite patient not having received immunosuppression

Why?

Process Model Flaws	**Questions**
Believed patient had received immunosuppression	*How was she supposed to know? Why did she think it had been given?*

Contextual Factors	Questions
Nobody mentioned a concern during timeout	
On order screen of EHR there is no record of whether an order has been acknowledged or carried out	
Preoperative timeout checklist is a generic checklist, so it does not explicitly ask about pre-operative immunosuppression. Tradeoffs between large number of things on checklist vs. fewer but more likely to be executed.	

Surgery Fellow/First Assist

Safety Responsibilities:

- Order preoperative antibiotics and immunosuppression
- Ensure medications have been given

Role in Adverse Event:

- Did not ensure medications had been given

Why?

Process Model Flaws	Questions
Ordered immunosuppression so believed patient had received it.	*How was he supposed to know? Why didn't he?*

Contextual Factors	Questions
On screen of EHR, there is no record of whether an order has been acknowledged and carried out. To see this, requires leaving EHR screen and going to eMAR (medication administration record) but even that does not clearly show that order given but not carried out. Have to be clearly looking for it to find it and no reason for Surgical Team or Circulating Nurse to suspect medication had not been given.	
Patients come from CCU where surgical team knows and trusts nurses so don't feel need to check up on their work. These nurses specialize in cardiac patients so surgical team) assumes they should be very familiar with pre-operative medications.	

Attending Cardiac Surgeon

Safety Responsibilities:

- Order pre-operative antibiotics and immunosuppression
- Ensure patient is ready for surgery before beginning
- Execute timeout

Role in Adverse Event:

- Began surgery without patient receiving prophylactic immunosuppression

Why?

Process Model Flaws	**Questions**
Assumed surgery fellow had ordered immunosuppression and checked it was given	*How was he supposed to know whether it had been given?*

Contextual Factors	
Trusted surgical fellow	
Executed the timeout that was provided by management	*Why was timeout designed the way it was?*
Everyone highly trained and had always performed their duties responsibly	

Nursing Supervisor

Safety Responsibilities:

- Ensure medication procedures and handoffs are being executed appropriately and that staff know them
- Identify necessary improvements in procedures

Role in Adverse Event:

- Assigned inappropriate nursing staff to CCU
- Did not ensure that proper training and procedures being executed

Why?

Process Model Flaws	**Questions**
Not aware medication errors were occurring	*How was she supposed to know? Why didn't she?*

Contextual Factors	**Questions**
Budget had been cut and could not always find cardiac qualified CCU nurses	Had she complained about this?
???	

OR Administration

Safety Responsibilities:

- Ensure medications available
- Ensure proper medication procedures
- Oversee timeout procedures to ensure used and effective
- Investigate adverse events (RCA)

Role in Adverse Event:

- Did not establish safe procedures
- Allowed inappropriate timeout procedures for transplants
- RCA did not identify systemic factors in previous incidents

Why?

Process Model Flaws	Questions
Thought timeout was appropriate, procedures were adequate, RCA appropriate	

Contextual Factors	Questions
We found several medication errors that were never investigated thoroughly but had same or very similar causes (instead stopped with blaming medical staff)	
Tradeoffs between cost and safety permeated decisions (including staffing levels, personnel training, equipment inventory)	
Complete turnover of management team, different specialties, different styles. Came from hospital that specialized in cardiac transplants. No plan to move from rarely doing transplants to one that specialized in them.	

CCU Administration

Safety Responsibilities:

- Ensure safe practices in CCU
- Maintain staffing levels and training
- Establish safe medication procedures

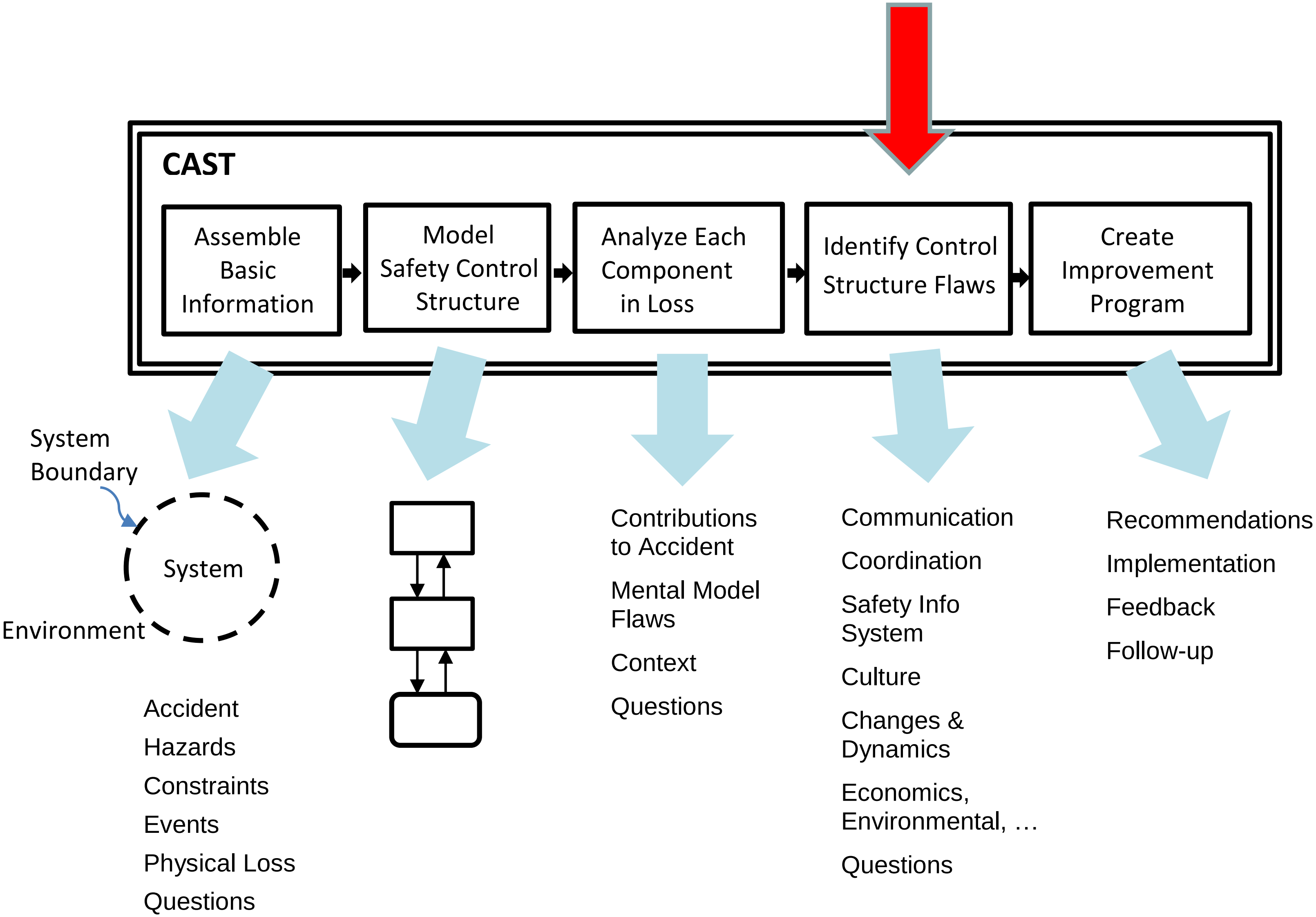
Role in Adverse Event:

- Did not establish safe, standardized medication procedure for preoperative immunosuppression

Why?

Process Model Flaws	Questions
Believed staff knew how to order and administer all medications	

Contextual Factors	
Separate management silos for surgery and intensive care complicate communications between the two departments	



CAST

Assemble Basic Information → Model Safety Control Structure → Analyze Each Component in Loss → Identify Control Structure Flaws → Create Improvement Program

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

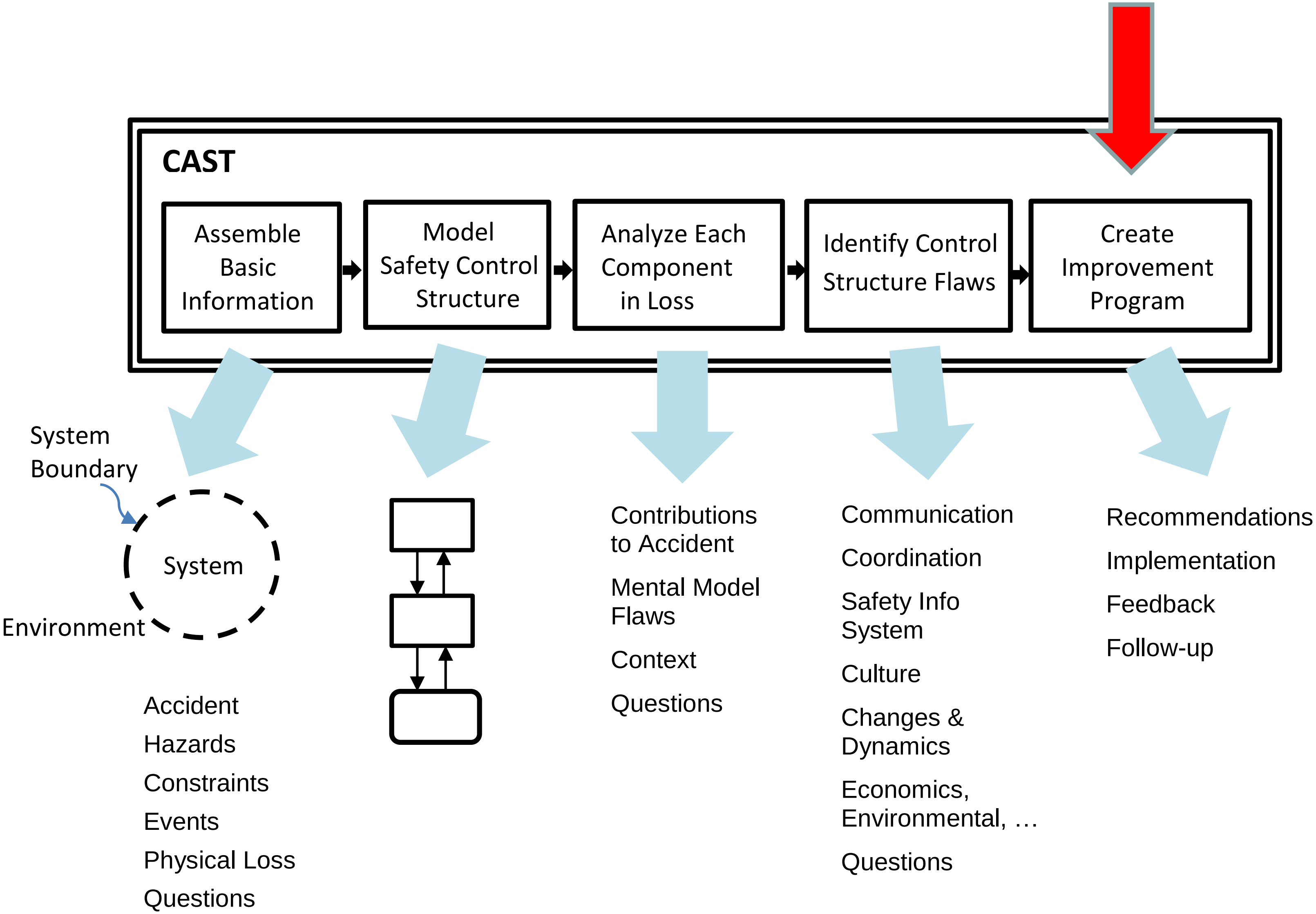
Recommendations
Implementation
Feedback
Follow-up

Flaws in Interactions Among Components

- Safety Information System: EHR (Electronic Health Record)
  - Poor layout, doesn’t provide clear instructions from physicians or provide clear feedback about carrying out of orders
  - Order set used to decrease chance of OR team forgetting to place important orders
  - But order sets introduce confusion because contain orders to be filled by CCU nurses as well as orders carried out by surgical team in OR
  - Time assigned to each order but no mention of who is responsible.
  - For common surgeries, everyone knows their role. But heart transplant here was less common and had not been done for a long time. So confusion about who was to do what

- Communication and Coordination
  - **Handoff** when surgical team picks up patient to transfer to OR
    - Nursing staff were to communicate any concerns and surgical team can ask questions.
    - No formal structure in handoff, so important info may not be shared.
    - In this case, nurses had no concerns as they were unaware they were supposed to provide immunosuppression medication.
  - **Timeout (checklist)**
    - No question about preoperative immunosuppression, only asked about antibiotics.
    - Some questions irrelevant, e.g., wrong site surgery
    - Trying to keep it short to encourage compliance
    - In aviation, found shorter was more likely to encourage compliance
    - Did not have different lists but tried to use one for all types of surgeries
  - Communication difficulties between departments (autonomous silos between divisions in hospital), missing feedback channels

- Safety Culture
  - “Bad apple” theory
- Confusion about responsibilities
  - Accidents often in interfaces between departments
- Dynamics and Changes over Time



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

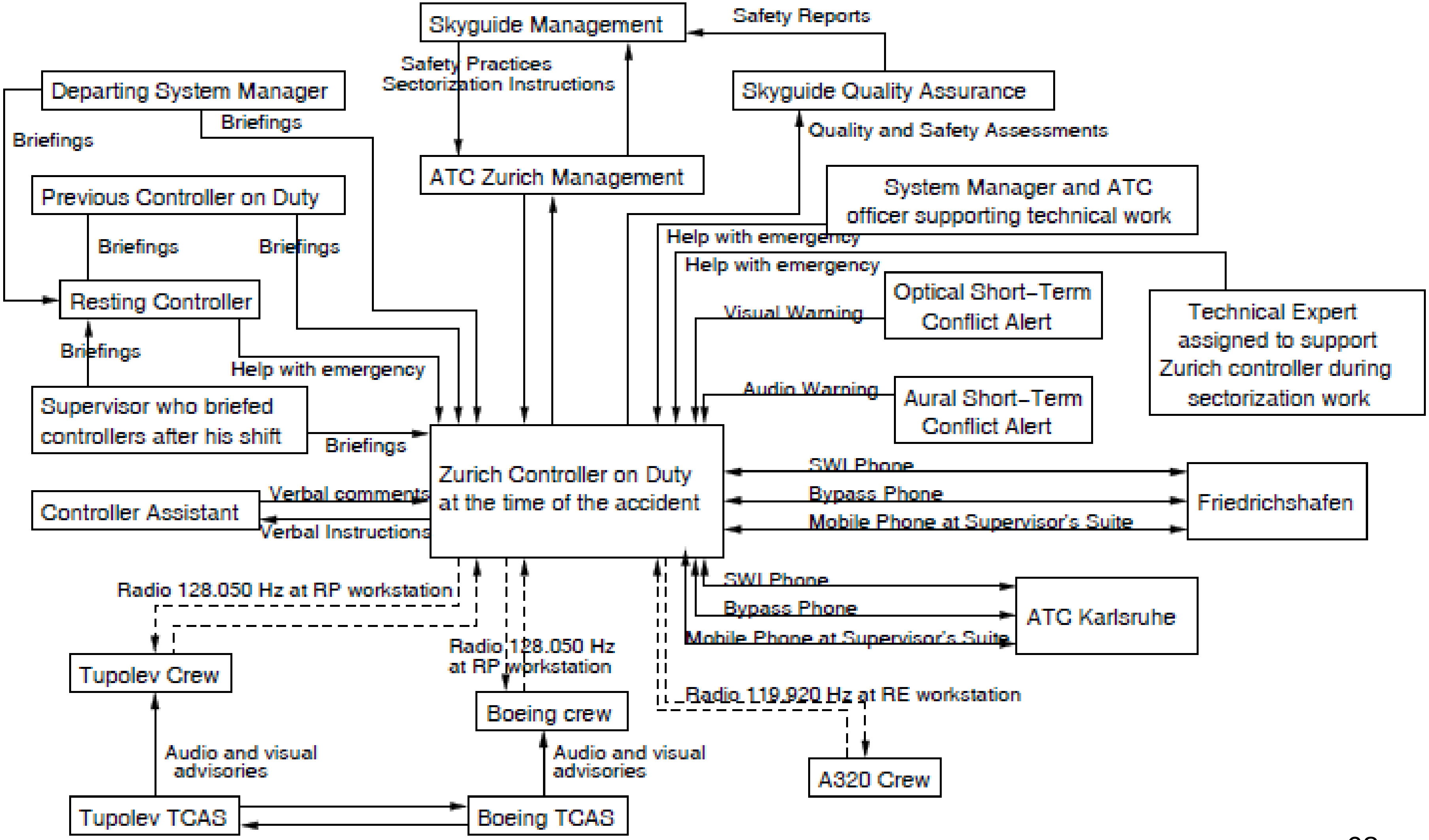
Feedback

Follow-up

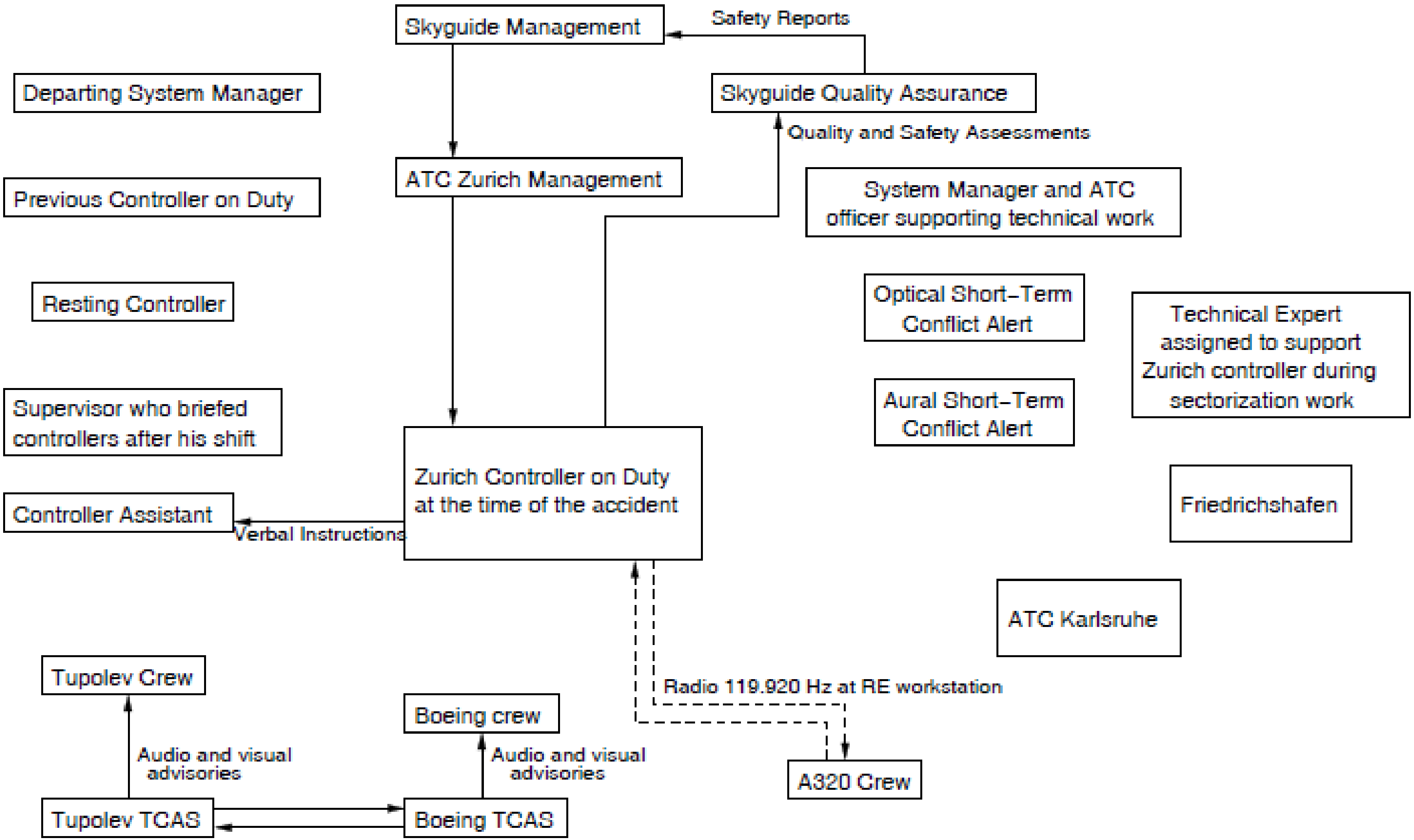
Standard “Blame” Approach (RCA)

- CCU nurse did not give immunosuppression medication
- Nurses did not tell surgeon it had not been given
- Surgeon started surgery without patient receiving immunosuppression medication despite executing “timeout” (checklist) before surgery

Communication Links Theoretically in Place in Uberlingen Accident


Skyguide Management
Safety Reports
Safety Practices
Sectorization Instructions
Skyguide Quality Assurance
Departing System Manager
Briefings
Briefings
Quality and Safety Assessments
ATC Zurich Management
Previous Controller on Duty
System Manager and ATC officer supporting technical work
Help with emergency
Briefings
Briefings
Help with emergency
Resting Controller
Optical Short–Term Conflict Alert
Visual Warning
Technical Expert assigned to support Zurich controller during sectorization work
Briefings
Help with emergency
Audio Warning
Aural Short–Term Conflict Alert
Supervisor who briefed controllers after his shift
Briefings
Zurich Controller on Duty at the time of the accident
SWI Phone
Bypass Phone
Mobile Phone at Supervisor's Suite
Friedrichshafen
Controller Assistant
Verbal comments
Verbal Instructions
Radio 128.050 Hz at RP workstation
SWI Phone
Bypass Phone
Mobile Phone at Supervisor's Suite
ATC Karlsruhe
Tupolev Crew
Radio 128.050 Hz at RP workstation
Radio 119.920 Hz at RE workstation
Boeing crew
Audio and visual advisories
Audio and visual advisories
A320 Crew
Tupolev TCAS
Boeing TCAS

Communication Links Actually in Place

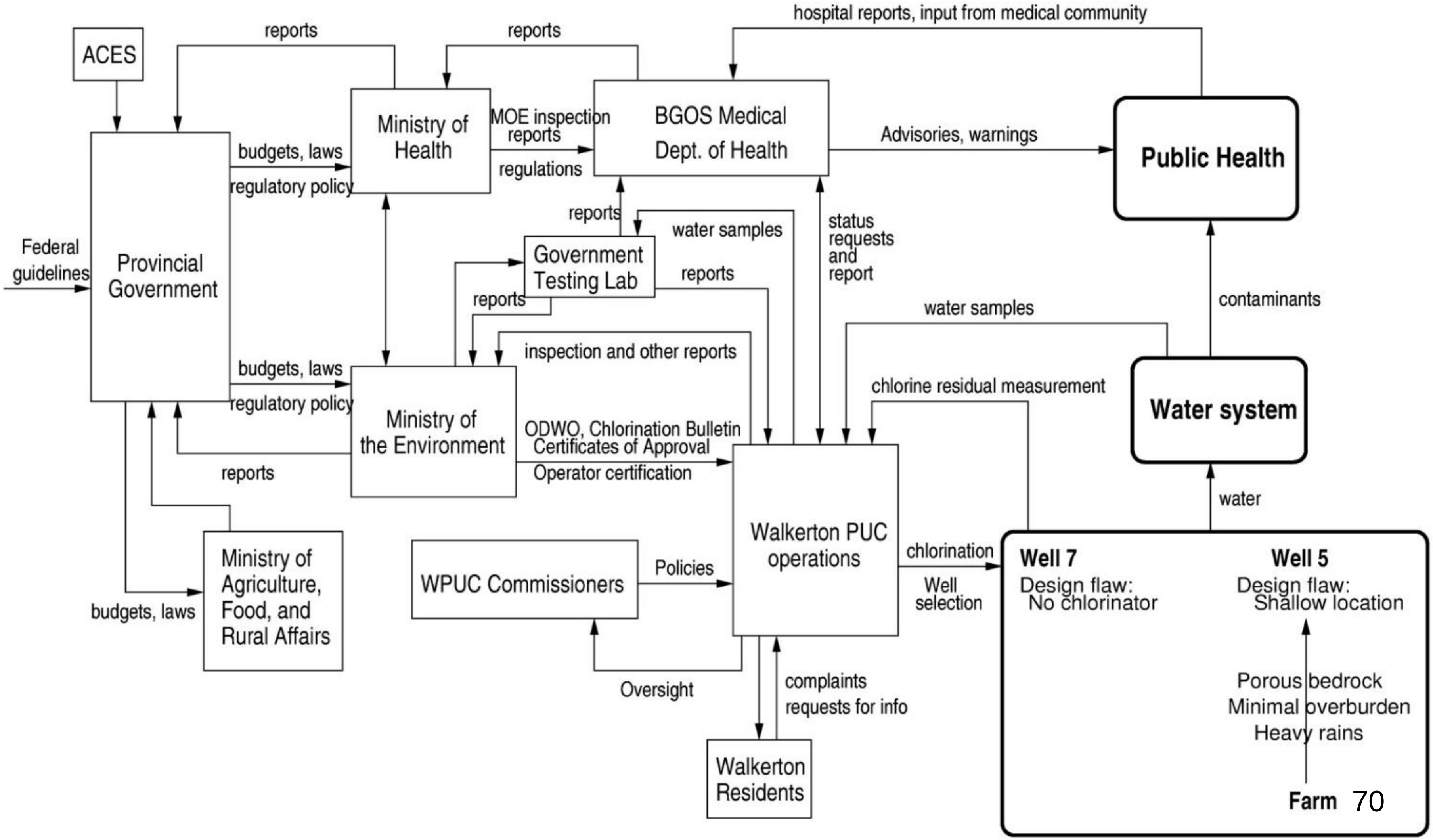

Skyguide Management
Safety Reports
Departing System Manager
Skyguide Quality Assurance
Quality and Safety Assessments
ATC Zurich Management
Previous Controller on Duty
System Manager and ATC officer supporting technical work
Resting Controller
Optical Short-Term Conflict Alert
Technical Expert assigned to support Zurich controller during sectorization work
Supervisor who briefed controllers after his shift
Aural Short-Term Conflict Alert
Zurich Controller on Duty at the time of the accident
Controller Assistant
Verbal Instructions
Friedrichshafen
ATC Karlsruhe
Radio 119.920 Hz at RE workstation
Tupolev Crew
Boeing crew
Audio and visual advisories
Audio and visual advisories
A320 Crew
Tupolev TCAS
Boeing TCAS

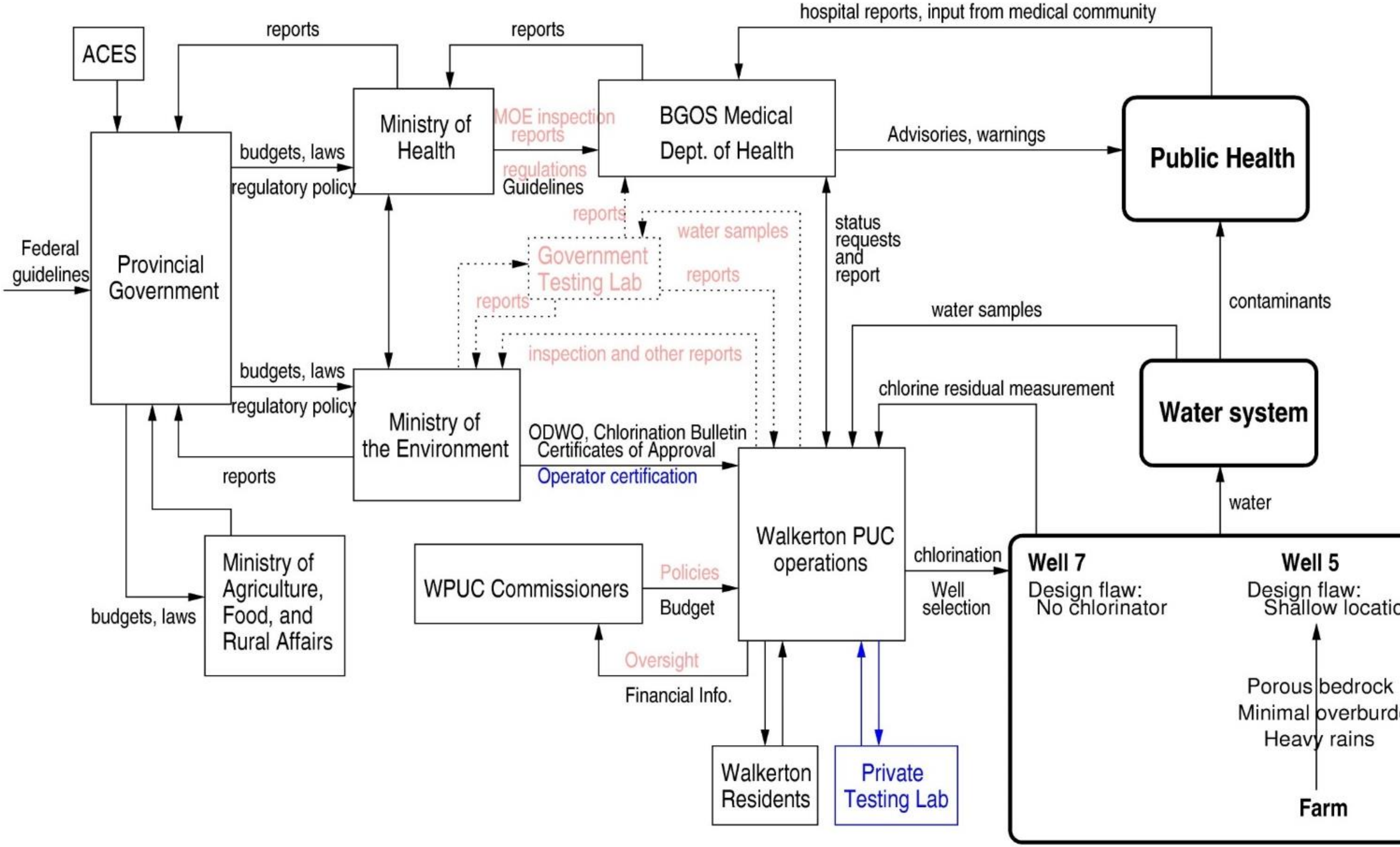
System Hazard: Public is exposed to E. coli or other health–related contaminants through drinking water.

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

Provincial Government

budgets, laws

regulatory policy

Federal guidelines

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 selection

Well 7

Design flaw: No chlorinator

Well 5

Design flaw: Shallow locatio

Ministry of Agriculture, Food, and Rural Affairs

budgets, laws

WPUC Commissioners

Policies

Budget

Oversight

Financial Info.

Porous bedrock

Minimal overburd

Heavy rains

Farm

Walkerton Residents

Private Testing Lab

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 <u>not</u> 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.

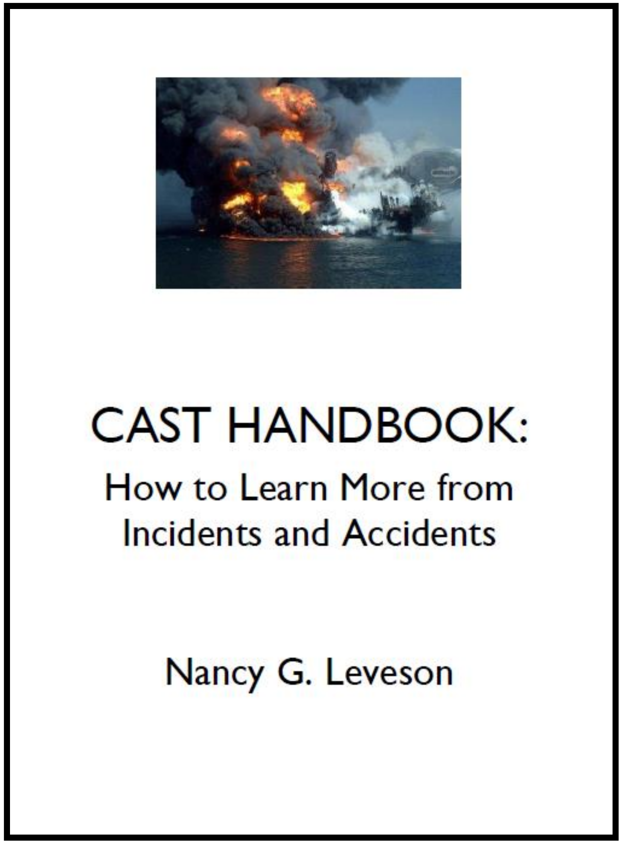
Discussion

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

More Information

- http://psas.scripts.mit.edu (papers, presentations from conferences, tutorial slides, examples, etc.)



CAST HANDBOOK:

How to Learn More from
Incidents and Accidents

Nancy G. Leveson

Free download:
http://sunnyday.mit.edu/CAST-Handbook.pdf