Incident Investigation Based on the STAMP Model

Ioannis M. Dokas

Assistant Professor
Democritus University of Thrace

BDirectors Member
Management Force Group

Incident / Accident Investigation

- **Accident investigation →** Identify the contributing factors of an accident
- **Incident investigation →** Identify potential contributing factors to accidents, **before accidents occur**

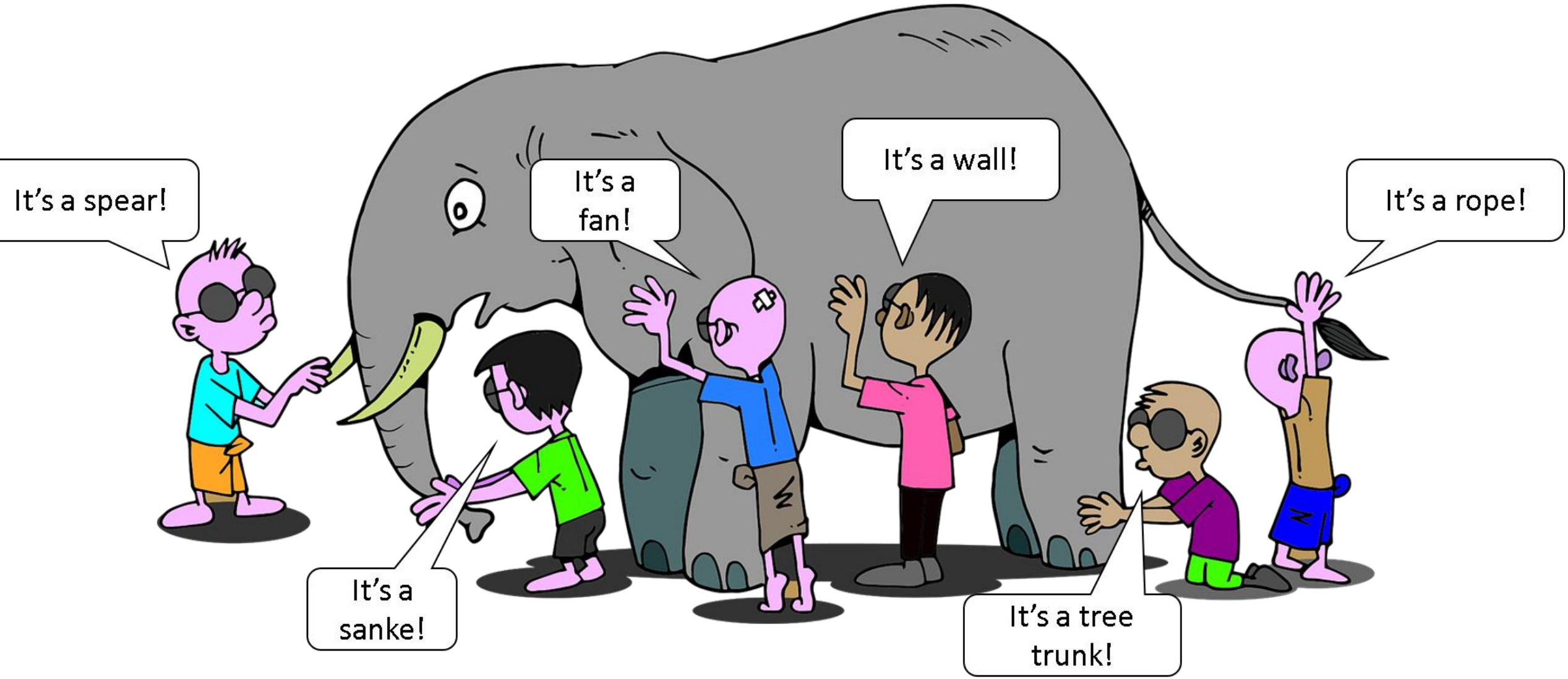
Types of Investigations

- Police / Persecutor Type:
  - To ascertain guilt/blame and to settle legal claims regarding liability for deficient performance
- Safety Engineering Type:
  - Search for causes and preventive measures after accidents
    - Accusatory approach
    - Explanatory approach

Problems

- Investigations not analysing in depth the causes of incident accidents
  - Typically focus on one or two types of causes of an accident
    - Human error
    - Component failure

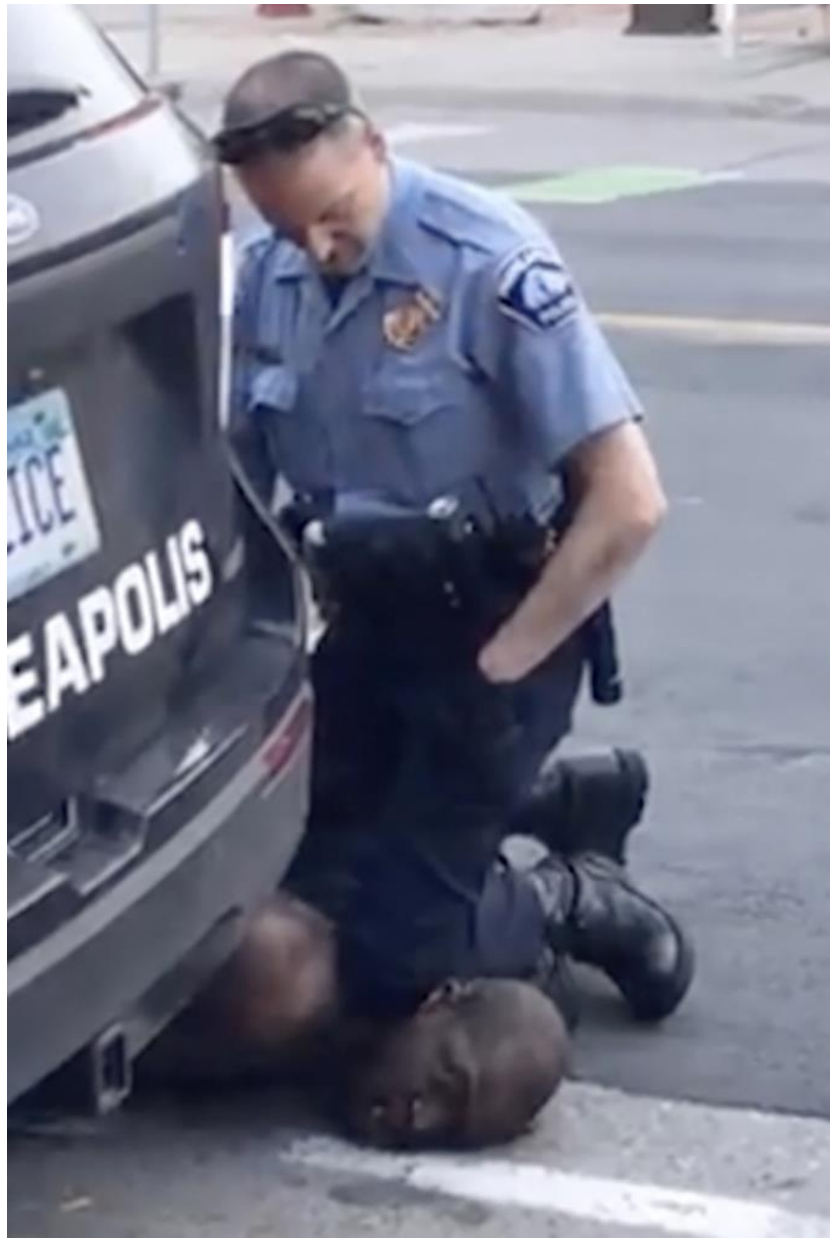
The blind men and the elephant



Therefore

- Results
  - Little knowledge is gained
  - The corrective actions are patches
  - Accidents are repeated
  - Impression that no matter what we do, no matter how much we invest in safety, accidents will emerge


Danger



George Floyd: Minneapolis
Monday, May 25, 2020

Eric Garner: New York City July 17, 2014

Systems Safety (Jerome Lederer)

- ”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,

Systems Safety (Jerome Lederer)

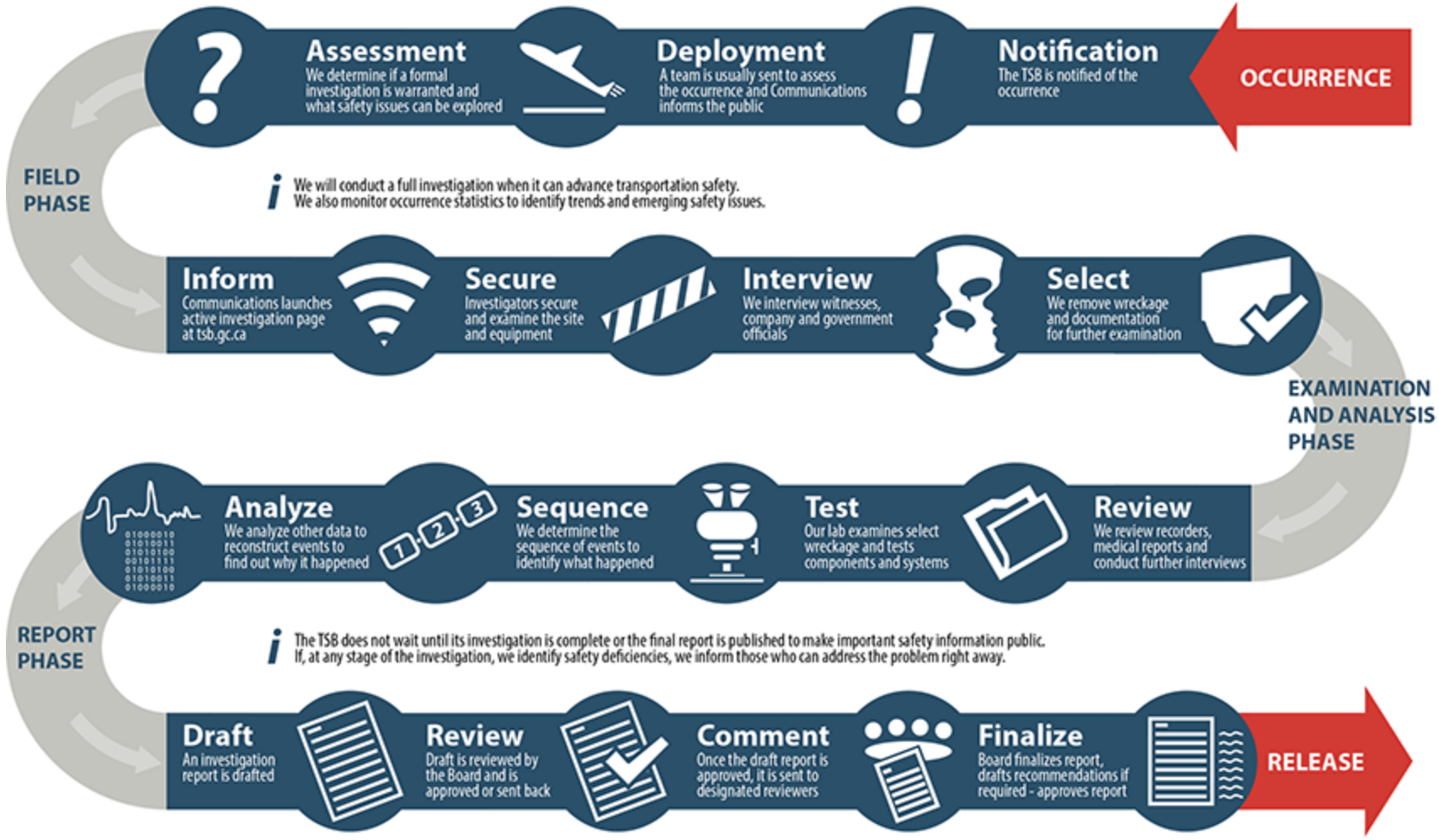
- documentation on the interfaces of industrial and public safety with design and operations,
- the interest and attitude of top management,
- the effects of the legal system on accident investigations and exchange of information,
- the certification of critical workers, political considerations,
- resources, public sentiment and many other non-technical but vital influences on the attainment of an acceptable level of risk control.
- **These non-technical aspects of system safety cannot be ignored**."

Investigation Process

- Report the incident
- Form investigation team
- Collect physical evidence
- Interview witnesses
- **Analysis**
- Final report and recommendations

Transportation Safety Board of Canada | Bureau de la sécurité des transports du Canada

TSB investigation process

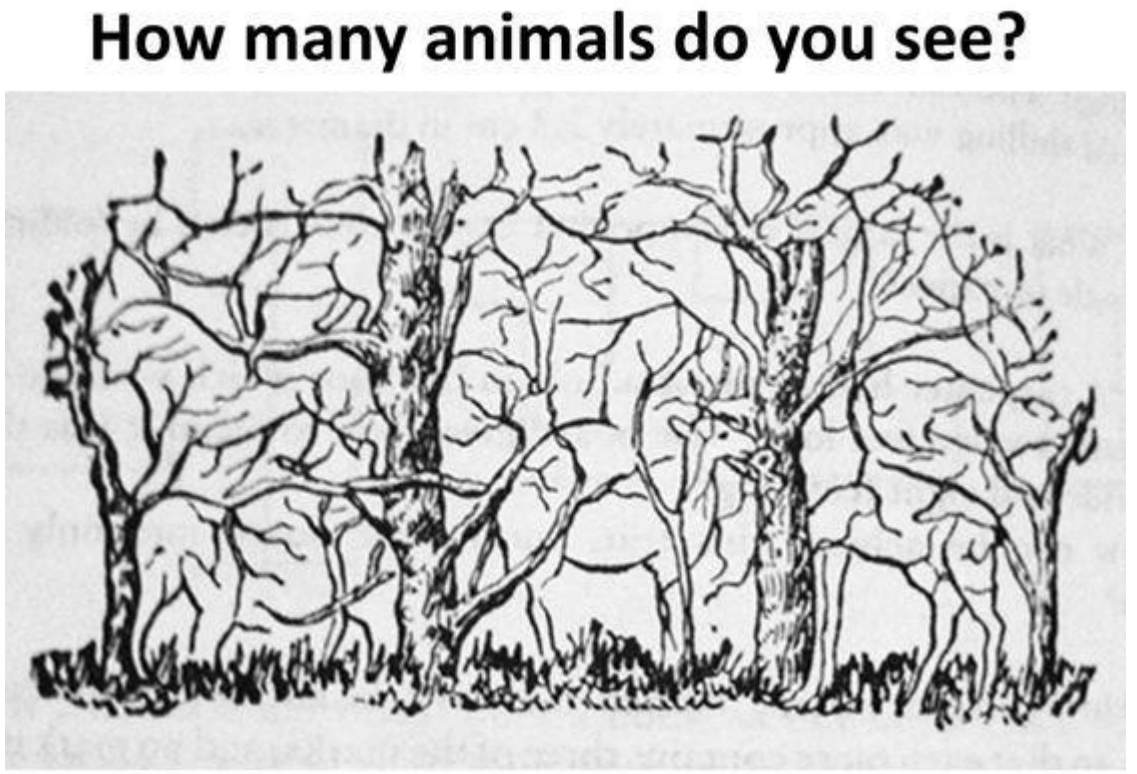


Once the Board approves the final report, it is translated, edited, and then released to the public on the TSB website and through traditional and social media.

Canada

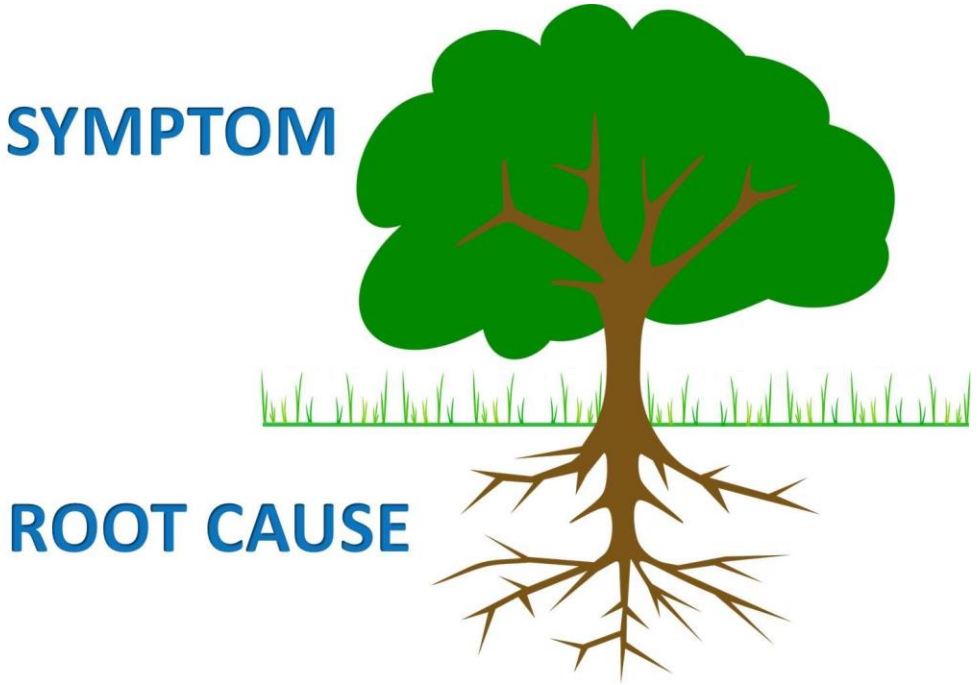
Common Traps in Understanding Accident Causes

- Root cause seduction
- Hindsight bias
- Narrow views of human error
- Focus on blame
- The causes found during an investigation reflect the assumptions of the accident model (What-You-Look-For-Is-What-You-Find Principle)



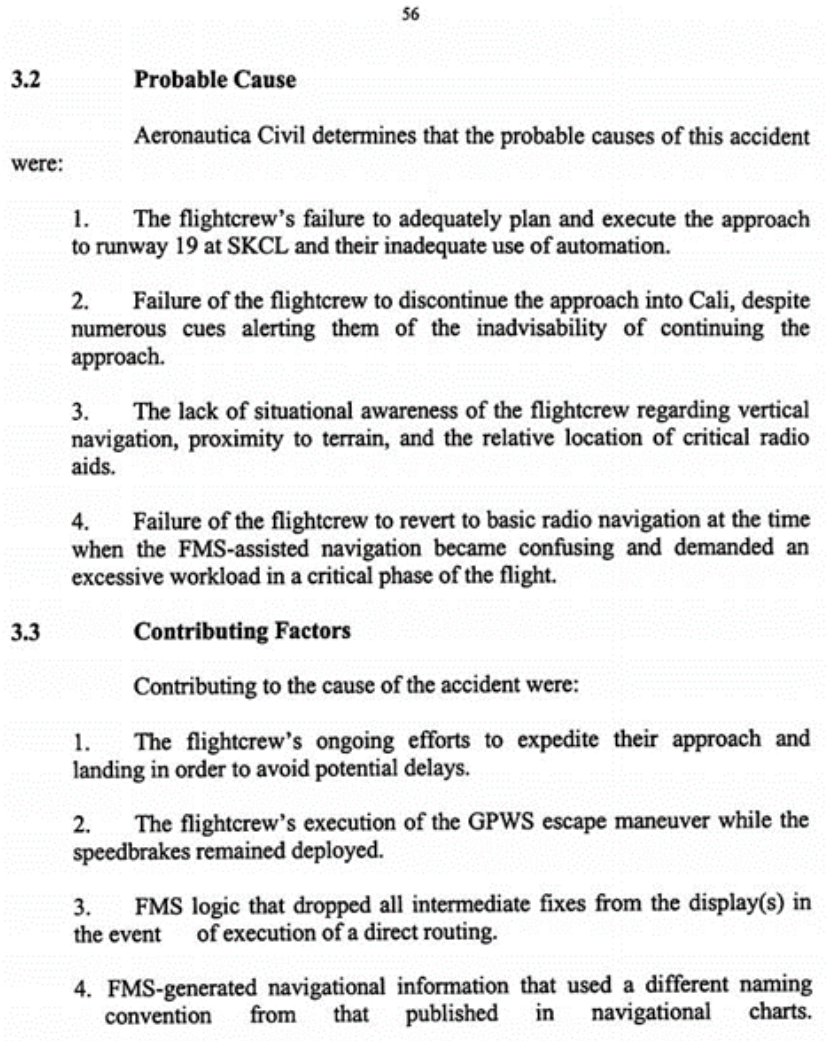
Root Cause Seduction

- We must find THE ROOT CAUSE! → Illusion of control
- Simple analyses
  - Phycological satisfaction - we have the control
  - A root cause → Easy fix
  - The “fix” however is a patch → Accidents occur again
- Almost always there is:
  - Operator “error”
  - Flawed management decision making
  - Flaws in the physical design of equipment
  - Safety culture problems
  - Regulatory deficiencies
- Independence of causal factors is assumed
- Systemic factors are ignored



Cali American Airlines Crash

- December 20, 1995, Boeing 757-200
- 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.



3.2 Probable Cause

Aeronautica Civil determines that the probable causes of this accident were:

1. The flightcrew's failure to adequately plan and execute the approach to runway 19 at SKCL and their inadequate use of automation.

2. Failure of the flightcrew to discontinue the approach into Cali, despite numerous cues alerting them of the inadvisability of continuing the approach.

3. The lack of situational awareness of the flightcrew regarding vertical navigation, proximity to terrain, and the relative location of critical radio aids.

4. Failure of the flightcrew 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 the flight.

3.3 Contributing Factors

Contributing to the cause of the accident were:

1. The flightcrew's ongoing efforts to expedite their approach and landing in order to avoid potential delays.

2. The flightcrew's execution of the GPWS escape maneuver while the speedbrakes remained deployed.

3. FMS logic that dropped all intermediate fixes from the display(s) in the event of execution of a direct routing.

4. FMS-generated navigational information that used a different naming convention from that published in navigational charts.

Hindsight Bias

- Humans understand the causal connections, and everything seems obvious **after the accident/incident**
- As result is psychologically impossible for people to understand **how someone might not have predicted the events beforehand**
- Hindsight bias occurs because, after an accident, it is easy to see where people went wrong and what they should have done or avoided doing
- It is difficult to place ourselves in the minds of those involved who have not had the benefit of seeing the consequences of their actions
- Examples of wordings in reports
  - “he/she should have…,” “he/she could have…,” or “if only he/she would have ….”

Overflow of SO^2 Incident

- **One of the conclusions in the report. “The Board Operator should have noticed the rising fluid levels in the tank.”**
- The operator had turned off the control valve allowing fluid to flow into the tank, and a light came on saying it was closed
- All the other clues that the operator had in the control room showed that the valve had closed, including the flow meter, which showed that no fluid was flowing.
- The high-level alarm in the tank did not sound because it had been broken for 18 months and was never fixed
- There was no indication in the report about whether the operators knew that the alarm was not operational
- Another alarm that was supposed to detect the presence of SO^2 in the air also did not sound until later
- One alarm did sound, but the operators did not trust it as it had been going off spuriously about once a month and had never in the past signaled anything that was actually a problem
- The report writers could not, even after careful study after the release, explain why the valve did not close and the flow meter showed no flow

OSHA Shipyard Accidents - Video Transcript

Examining Fatal Shipyard Accidents - Volume 1

NAR: The scenes you are about to witness depict fatal accidents that occurred while employees were working in shipyards. All identifying references have been removed to protect privacy interests. Please be advised that the depictions may be disturbing and deal with graphic subject matter. (MUSIC)

Accident Examination 1 - Truck Mounted Crane Crushes Rigger - 1 Fatality

Two men were unloading steel beams from a trailer using a truck mounted crane. The outriggers on the crane were fully extended and set. The rigger and his helper walked with each load, controlling it with taglines. The crane operator lifted each load and swung the crane to his right, about 180 degrees and lowered the beams to the ground. During the unloading the foreman approached to talk with the rigger's helper. When the unloading was finished, the crane operator began to put away the rigging and stow the crane. The foreman left but the riggers helper remains standing beside the outrigger. As the operator swung the crane into the stowed position the riggers helper was crushed between the crane cab and the outrigger he was leaning against. (MUSIC)

What went wrong?

The swing radius of the crane was not barricaded to prevent employees from entering a hazardous zone. The crane operator should have kept visual contact with his helpers at all times. An audible signal should be installed on the crane to warn employees of the crane's movement.

Views on Human Error

- Most accident analyses start from a belief that operator error is the cause of most incidents and accidents
- Operators are the cause of 70-90% of accidents
- Bad apple theory

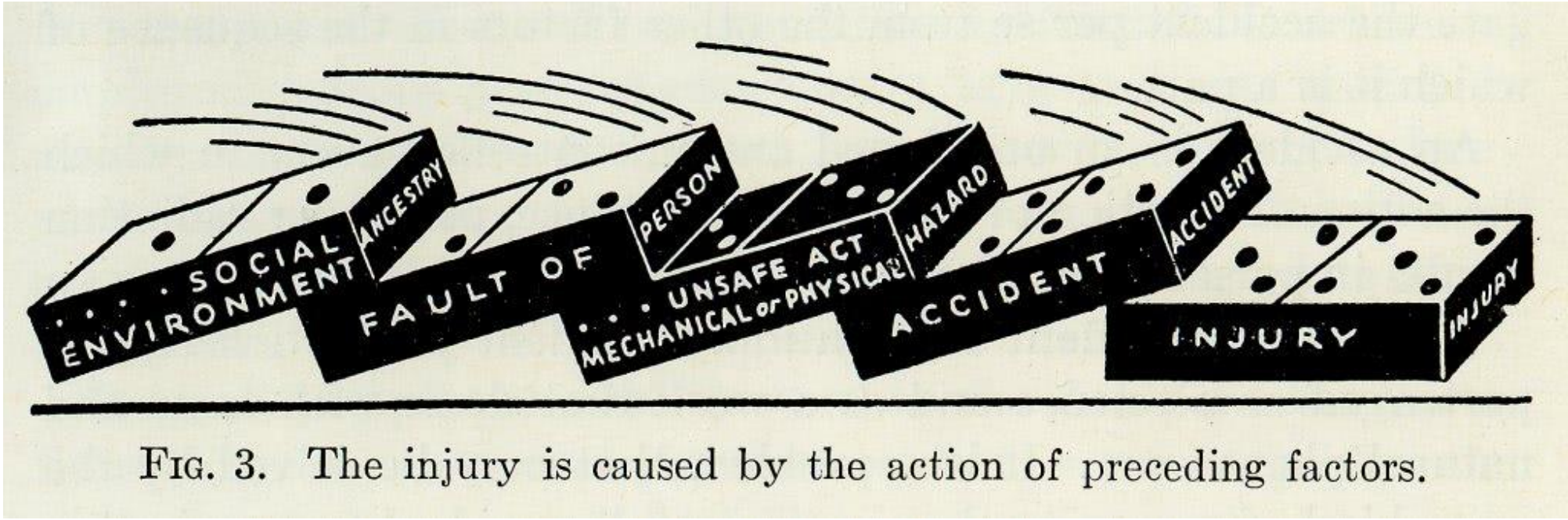


FIG. 3. The injury is caused by the action of preceding factors.

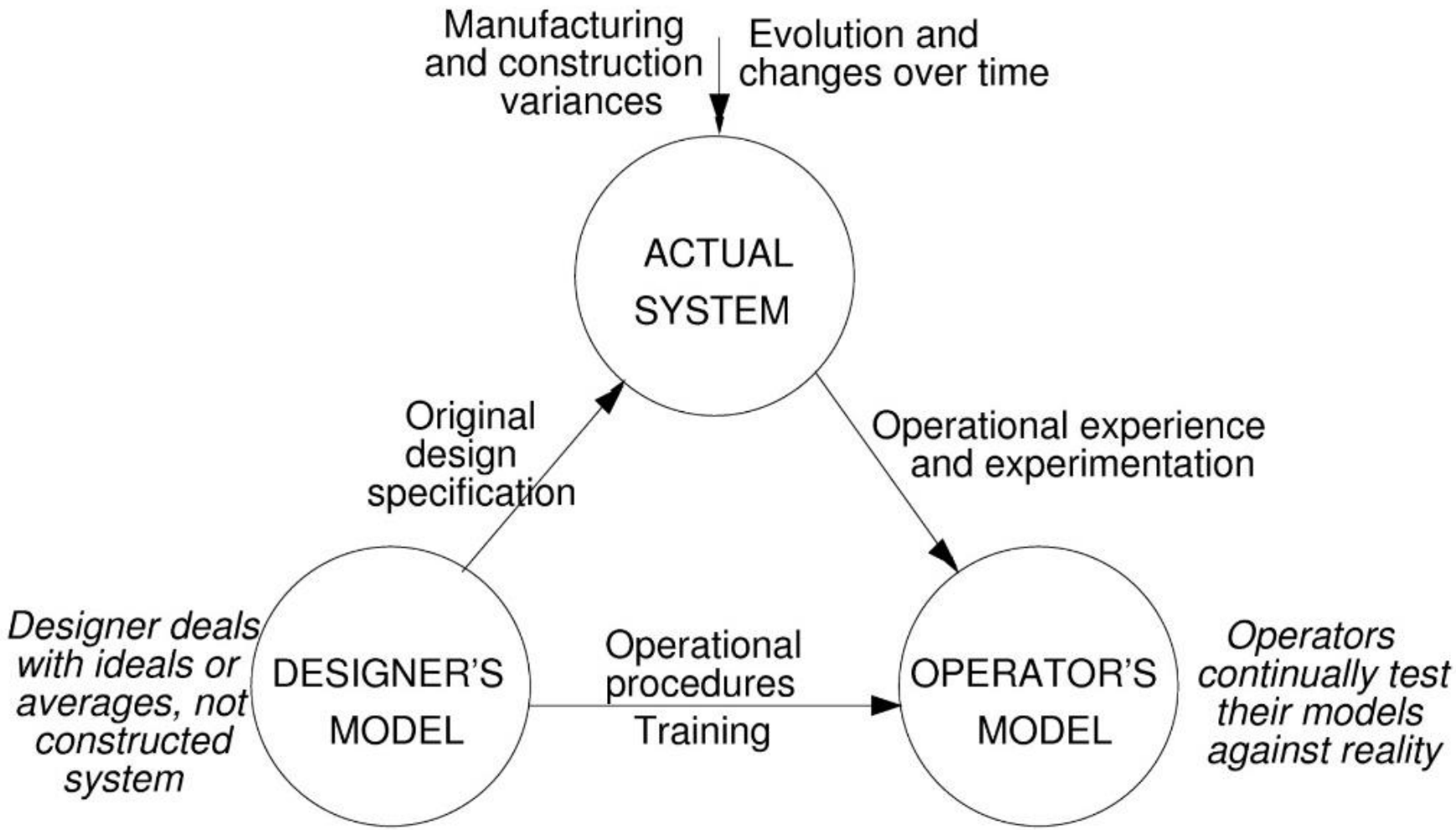
So Do Something About Human Involved

- Suspend, Retrain, Admonish
- Set them aside by putting in more automation
- Constrain their work by creating more rules and procedures
  - which may be impossible or unrealistic to expect them to always follow or which may themselves lead to an accident

Amagasaki Derailment (April 2005)

- 25 minutes before the derailment, Takami had run a red signal, causing the automatic train stop (ATS) to bring the train to a halt.
- The train had also overshot the correct stopping position at an earlier stop at Itami Station, requiring him to back up the train, and resulting in a 90-second delay
- About 4 minutes before the disaster the train passed Tsukaguchi Station at a speed of 120 km/h, the delay had been reduced to 60 seconds
- Investigators speculate that the driver may have been trying to make up this lost time by increasing the train's speed beyond customary limits.
- Furthermore, it is speculated that the driver may have felt stressed because he would have been punished for the two infractions.
- Drivers face financial penalties for lateness as well as being forced into harsh and humiliating retraining programs known as nikkin kyōiku

Violation of Rules and Procedures



Violation of Rules and Procedures

- Operators, if they do not have complete knowledge of the current circumstances and system state, must choose between:

1. Sticking to procedures rigidly when cues suggest they should instead be adapted or modified, or
   - They may be blamed for their inflexibility and applying rules without understanding the current state of the system.
2. Adapting or altering procedures in the face of unanticipated conditions.
   - They will then be blamed for deviations and rule violations

Use of the Official Reporting System

- Fear of reporting
- System being hard to use - hard to locate - website with a clunky interface
- Long time to complete report
- Never see any results or hear anything back and assume the reports are going into a black hole
- Instead report the problem to people who they think can and will do something about it

Role of Humans in Modern Systems

- Not controlling the process directly
- Humans are increasingly supervising automation,
- Software is allowing enormously complex systems to be created, and people find hard to understand them leading to human behavior that under some conditions could be unsafe
- In addition, systems are sometimes designed without using good human-centered and human-factors design principles. The result is that we are designing systems in which operator error is inevitable and then blaming accidents on operator error rather than designer error

Human-Factors Design Principles

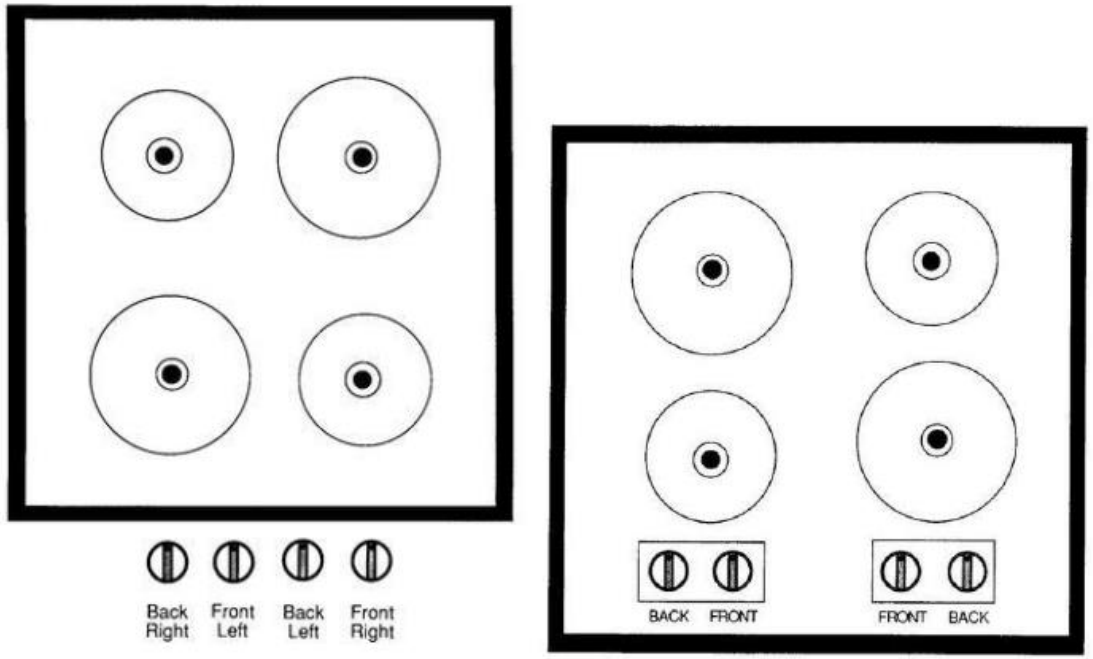


Figure C.1: Two designs of an error-prone stove top (Adapted from Don Norman, The Design of Everyday Things, Basic Books, 2013).

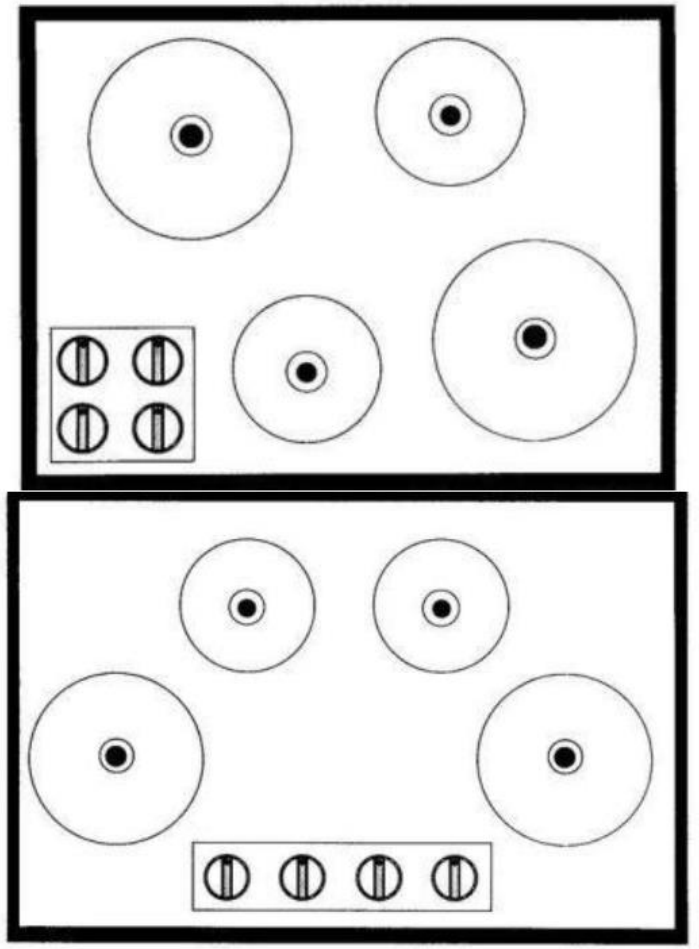


Figure C.2: Less error-prone designs (Adapted from Don Norman, The Design of Everything Things, Basic Books, 2013).

Focus on Blame

- *Blame is a legal or moral concept, not an engineering one*
- Reduce learning from accidents and impedes preventing future ones.
  - (For example those involved point finger at everyone else and searching for someone else to blame)
- Search for causes devolves to identifying the immediate actors in the event chain, usually the human operators or low-level managers, who obviously participated in the events and have no way to deflect attention onto others.
- No complete picture of what caused the accident

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

Figure 5: Two opposing views of accident explanation

Inappropriate Accident Causality Models

- Linear /chain of events
- Epidemiological
- Systemic

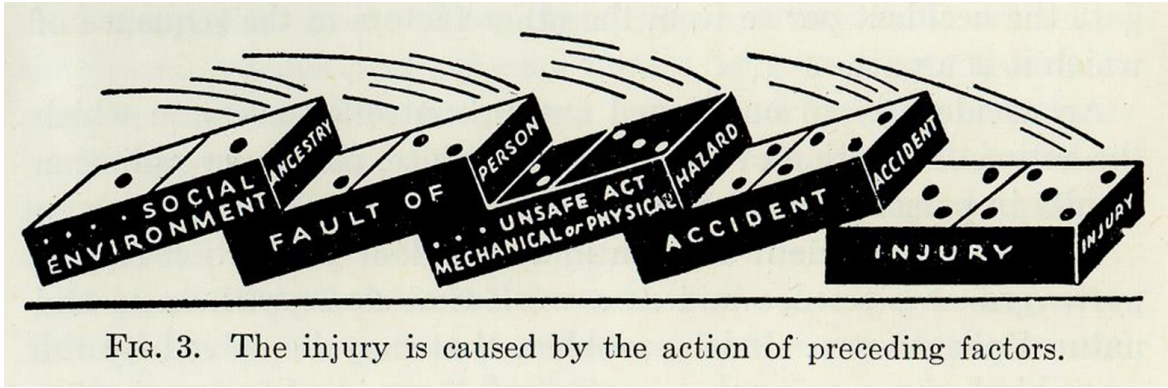
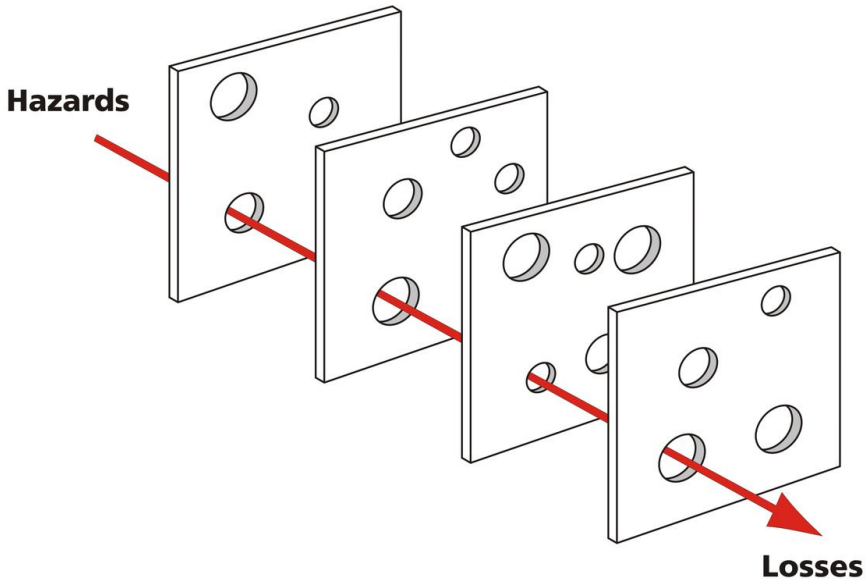
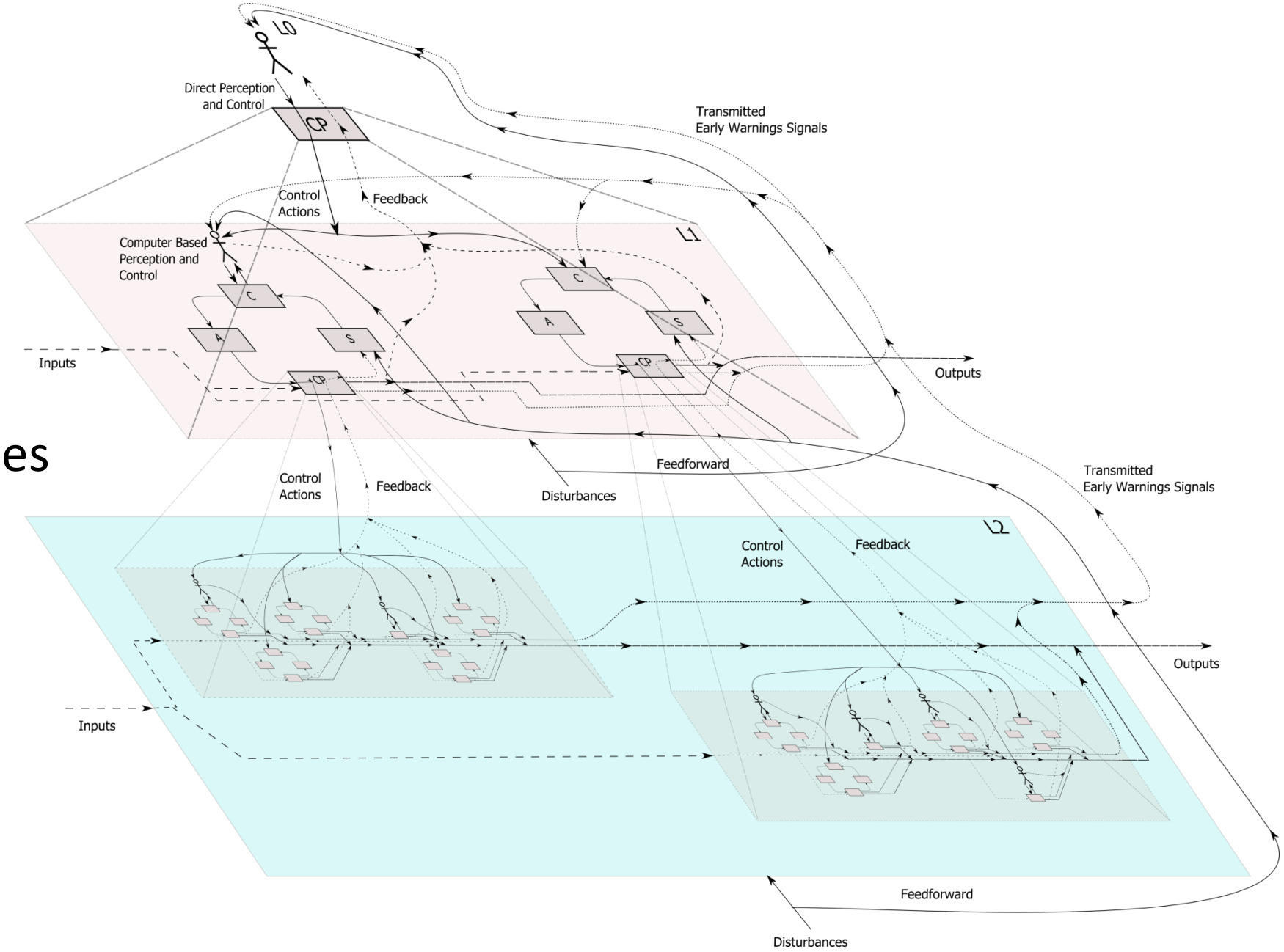


FIG. 3. The injury is caused by the action of preceding factors.

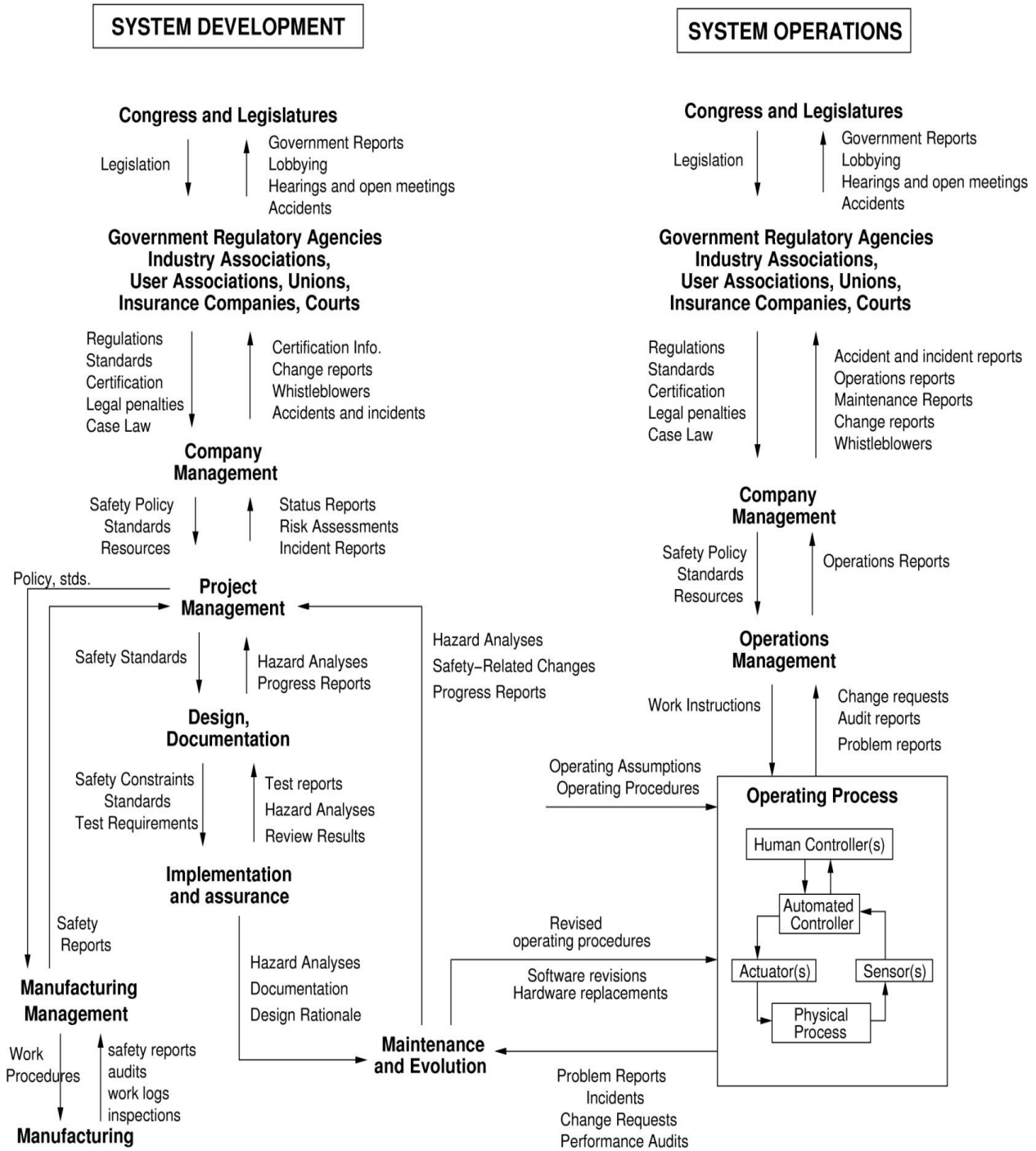


STAMP

- Systems Theoretic Approach
  - Hierarchy
  - Emergent Properties
  - Information and Control



Hierarchy


SYSTEM DEVELOPMENT
Congress and Legislatures
Legislation
Government Reports
Lobbying
Hearings and open meetings
Accidents
Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts
Regulations
Standards
Certification
Legal penalties
Case Law
Certification Info.
Change reports
Whistleblowers
Accidents and incidents
Company
Management
Safety Policy
Standards
Resources
Status Reports
Risk Assessments
Incident Reports
Policy, stds.
Project
Management
Safety Standards
Hazard Analyses
Progress Reports
Design,
Documentation
Safety Constraints
Standards
Test Requirements
Test reports
Hazard Analyses
Review Results
Implementation
and assurance
Safety
Reports
Manufacturing
Management
Work
Procedures
safety reports
audits
work logs
inspections
Manufacturing
Hazard Analyses
Documentation
Design Rationale
Maintenance
and Evolution
Hazard Analyses
Safety–Related Changes
Progress Reports
SYSTEM OPERATIONS
Congress and Legislatures
Legislation
Government Reports
Lobbying
Hearings and open meetings
Accidents
Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts
Regulations
Standards
Certification
Legal penalties
Case Law
Accident and incident reports
Operations reports
Maintenance Reports
Change reports
Whistleblowers
Company
Management
Safety Policy
Standards
Resources
Operations Reports
Operations
Management
Work Instructions
Change requests
Audit reports
Problem reports
Operating Assumptions
Operating Procedures
Operating Process
Human Controller(s)
Automated
Controller
Actuator(s)
Sensor(s)
Physical
Process
Revised
operating procedures
Software revisions
Hardware replacements
Problem Reports
Incidents
Change Requests
Performance Audits

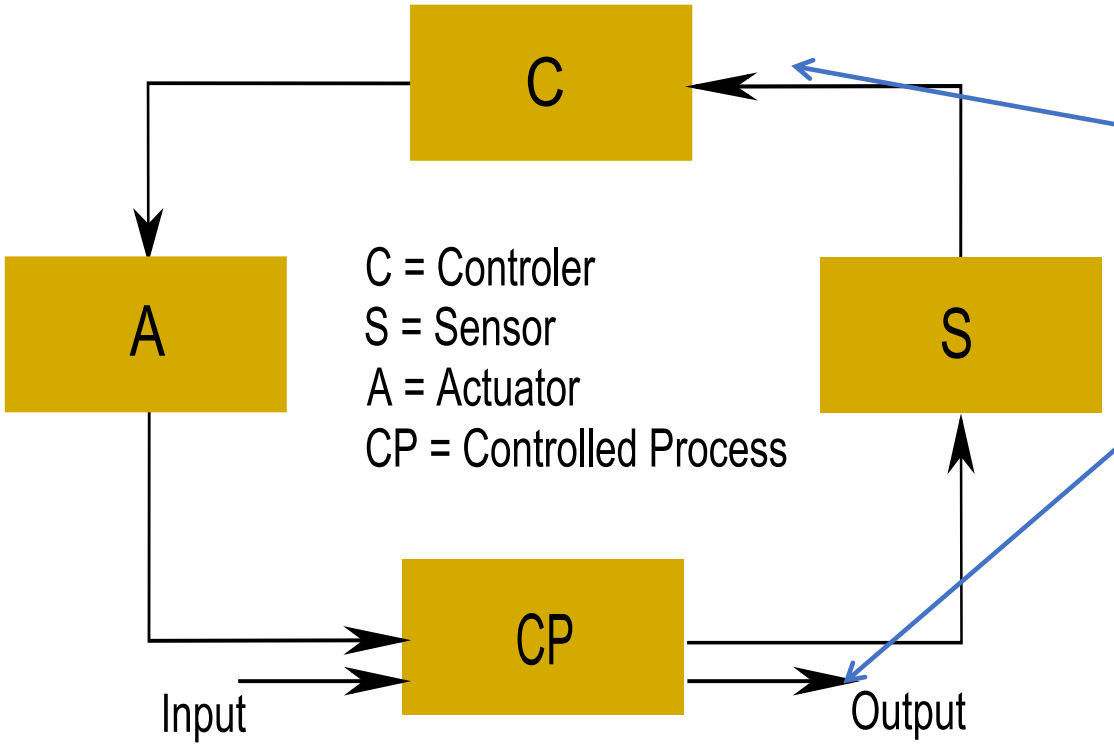
Emergent Properties

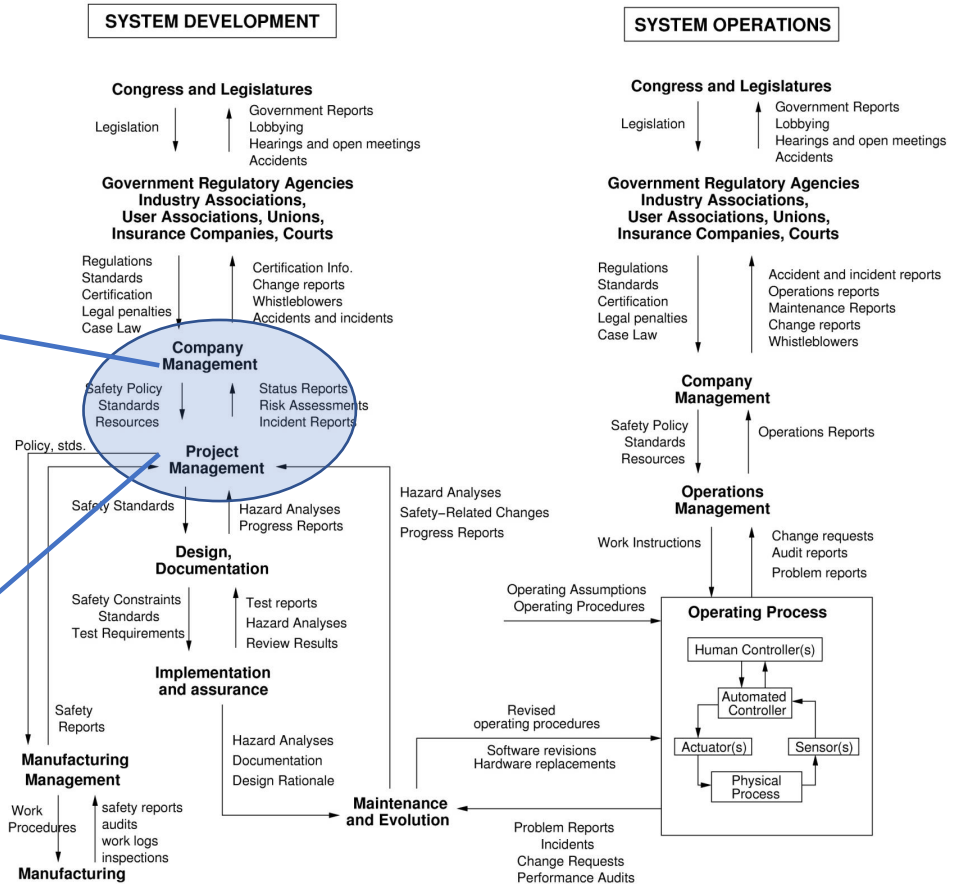
- Comfort vs Strength

Emergent Properties

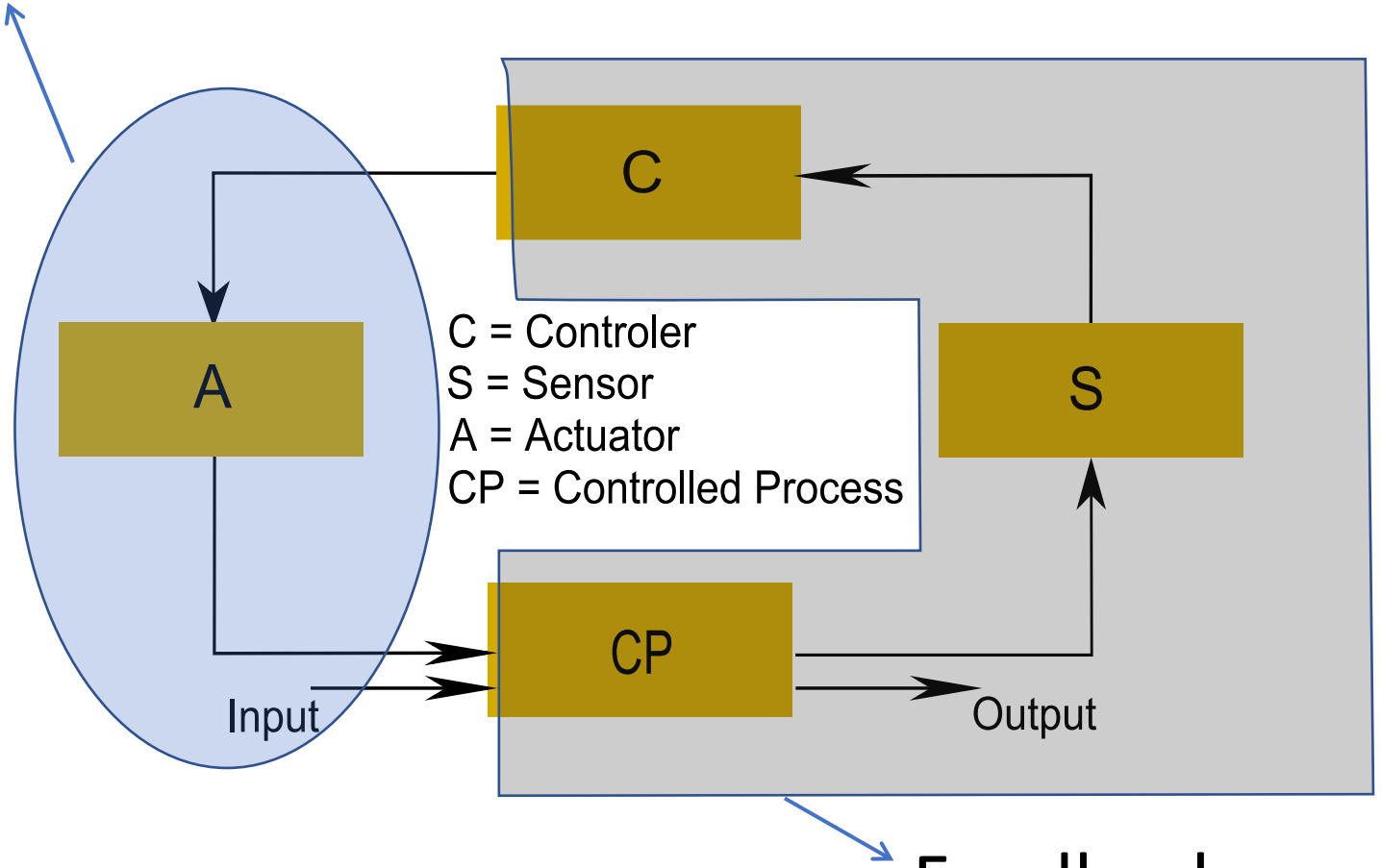
- Comfort vs Strength

Information and Control



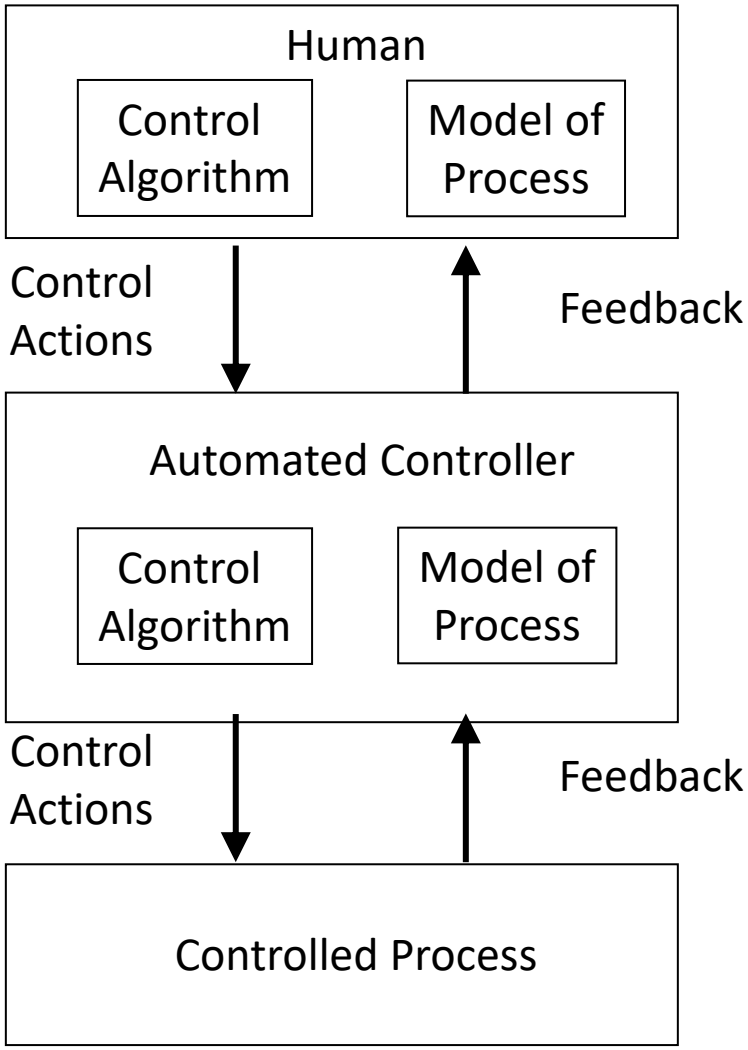


- Control actions

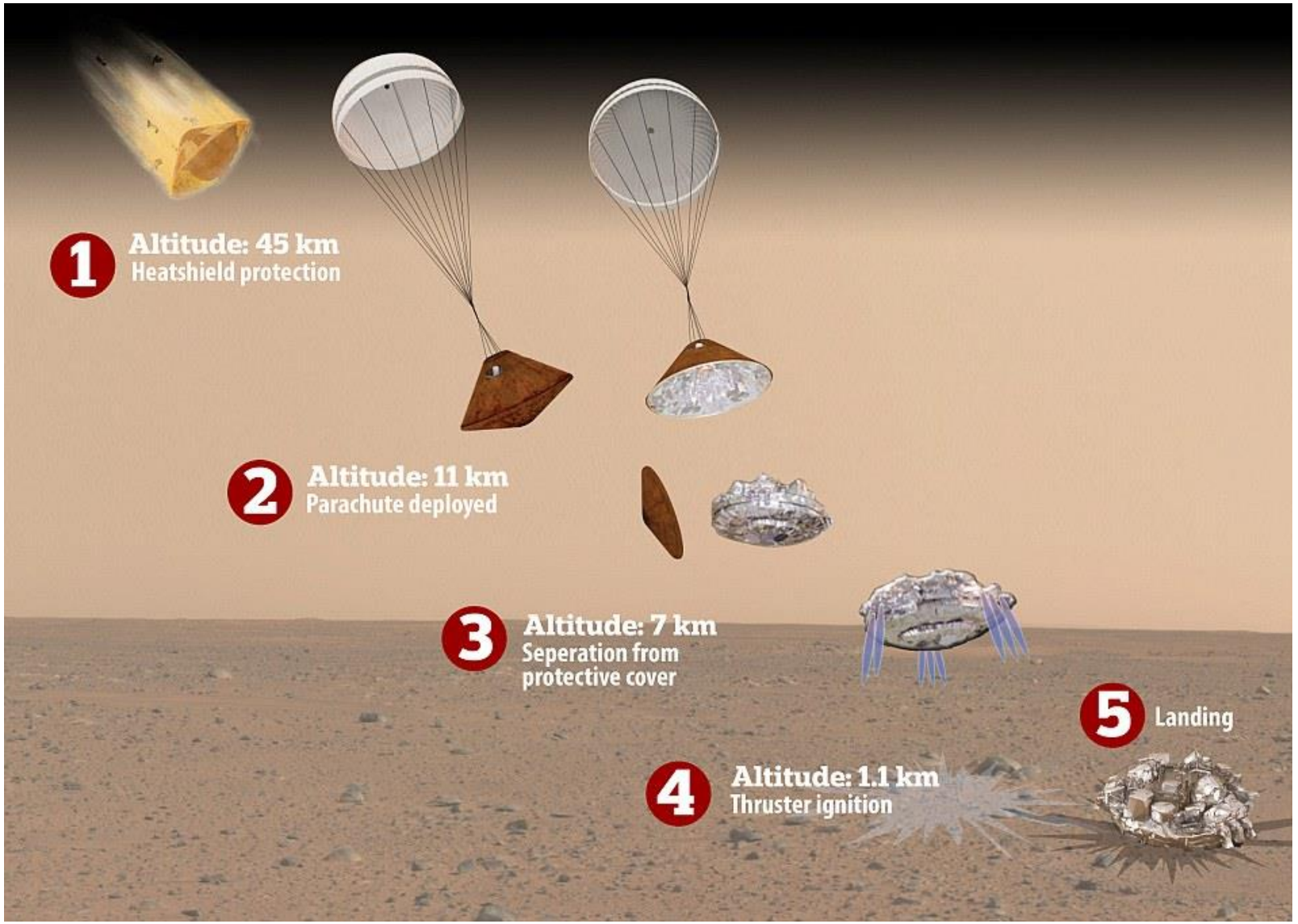


- Feedback

Process Models

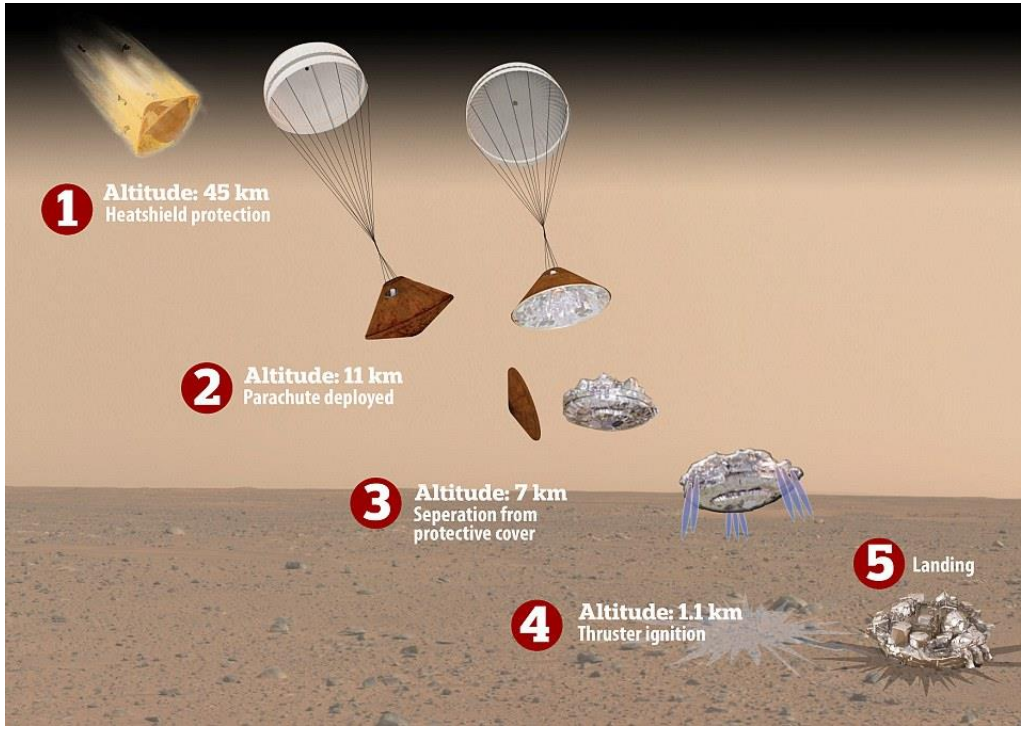


ESA Schiaparelli Lander (October 2016)



Schiaparelli Lander (October 2016)

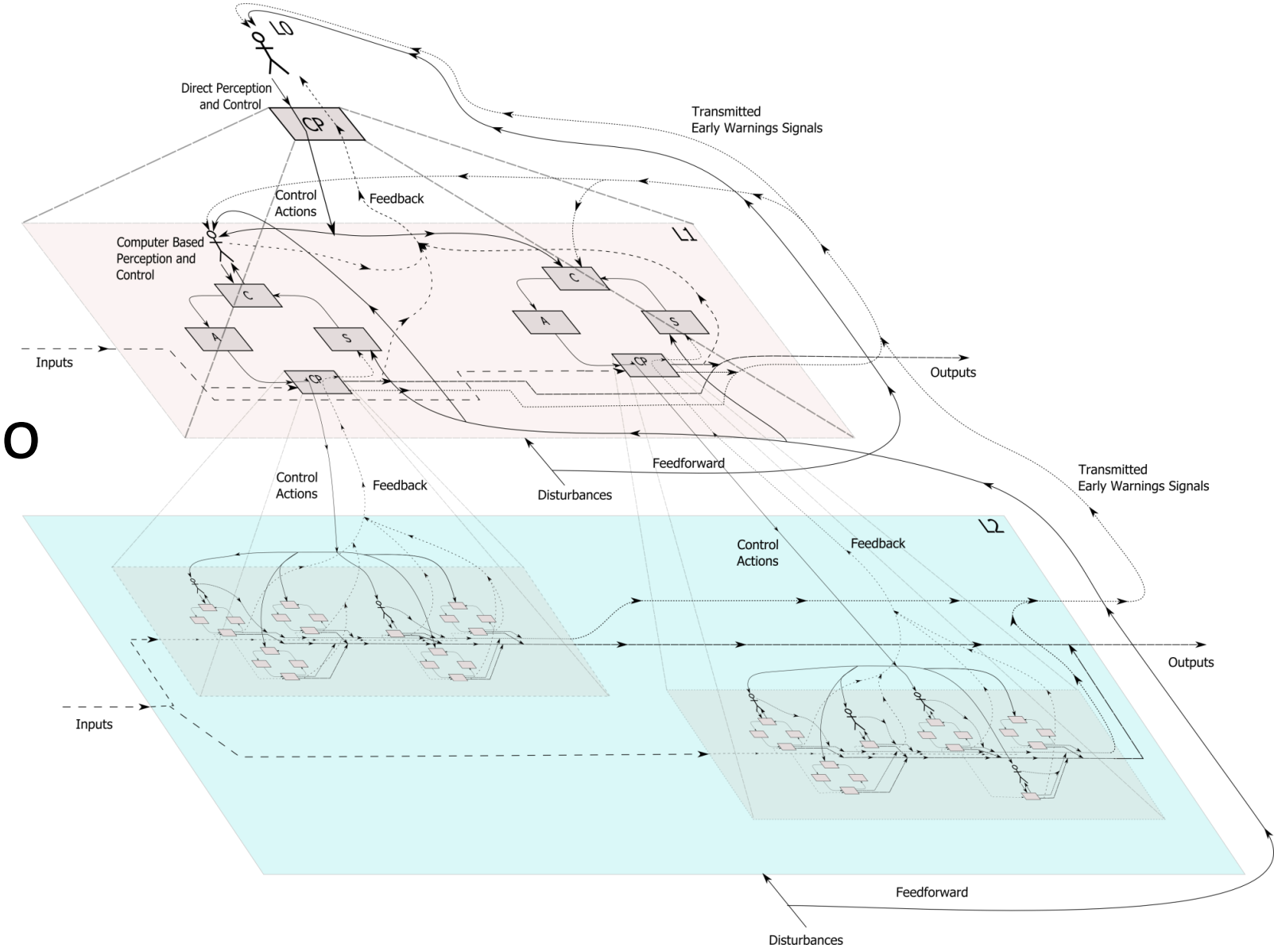
- Atmospheric entry occurred normally,
- Parachute deployed at 12 km and 1,730 km/h
- Heat shield released at 7.8 km
- However, the lander's inertial measurement unit, which measures rotation, became saturated for about one second. This saturation, coupled with data from the navigation computer, generated an altitude reading that was negative, or below ground level
- This caused the premature release of the parachute and back shell. The braking thrusters then fired for about three seconds rather than the expected 30 seconds
- Followed by the activation of ground systems as if the vehicle had already landed. In reality, it was still at an altitude of 3.7 km



Polluted by the IMU data, the **lander's computer apparently thought it had either already landed or was just about to land**. The parachute system was released, the braking thrusters were fired only briefly, and the on-ground systems were activated

Safety Based on STAMP

- Emergent property of systems
- Control problem
- Feedback loop → “Lego brick”
- SAFETY ≠ RELIABILITY



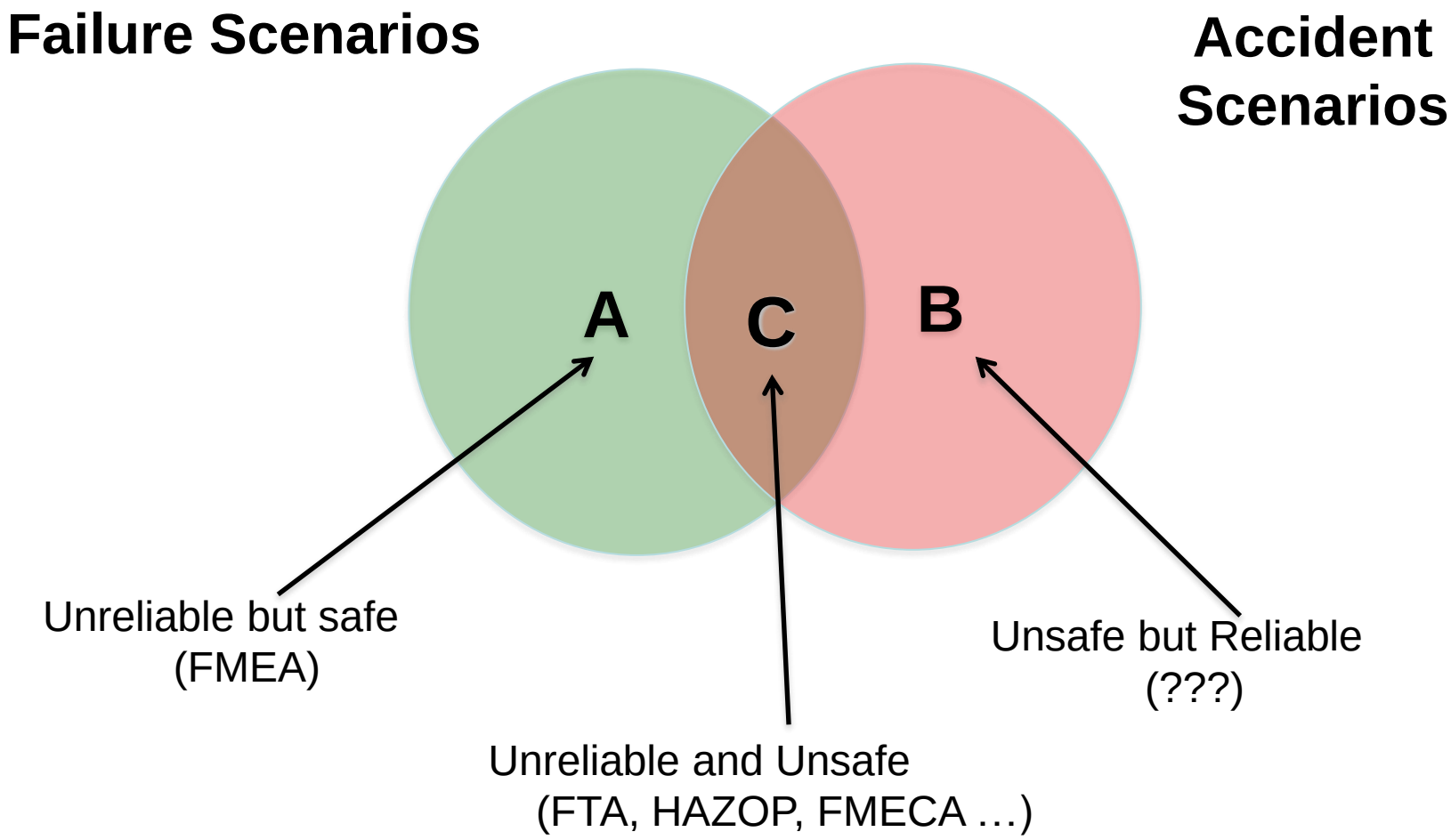
Is it Safe?

Is it Safe?

Safety Based on STAMP

- Contributing factors to accidents: The divergence between the image of the system state based on the process models of controllers and the system states in reality
- Enforcement of unsafe control actions
- Appropriate control actions correctly enforced but not executed

SAFETY ≠ RELIABILITY

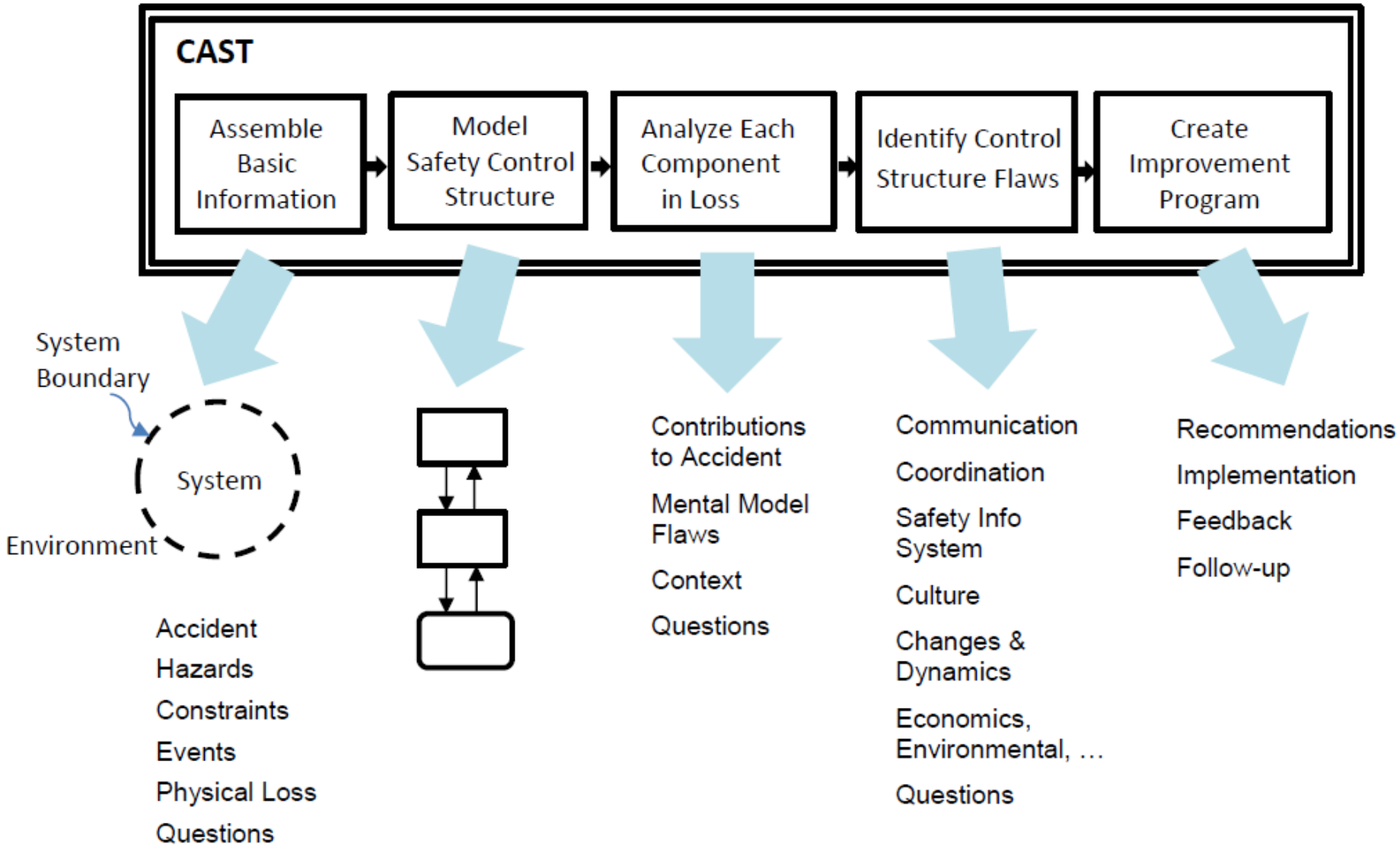


Operator Error: Systems View

- To understand human error, look at the system
- All behavior affected by context (system) in which it occurs
- System designs can make human error inevitable
- To do something about operator error, look at:
  - Unintuitive equipment and system designs
  - Usefulness of procedures
  - Existence of goal conflicts and production pressures

Human error is a symptom of the system and its design

CAST (Causal Analysis based on System Theory)



Tagarades Landfill Fire, Thessaloniki Greece 2006

Date	Time	Events
1/9/2004	-	A fire broke out on a slope which was successfully extinguished. There have been several fire incidents around the area where that fire occurred were reported during the periof 1/9/2004 to 17/6/2006
17/06/2006	-	Small fire incident at a slope 200 meters away from the working front
-	-	Reconstruction works near the cell
14/07/2006	06:00 am	Landslide of 150.000 m3 of waste + soil cover
14/07/2006	06:00 am	Wastes from the landslide entered the leachate collection pool causing violent overflow of leachate and a rupture on the NW side of the leachate pool. The leachate leak was estimated at 5.000 m3.
14/07/2006	09:30 am	Fire in the waste body at the center of the landslide
14/07/2006	09:40 am	Call at the fire department. Emergency response plan in effect
14/07/2006	10:00 am	The rupture in the leachate pool restored
14/07/2006	12:00	Fire spread in an area of 100 acres.
14/07/2006	afternoon	Fire retained within the area of the landslide
15/07/2006	-	Enforcement of the Fire extinguishing plan / Final fire extinguishing
27/07/2006	-	Fire extinguished

Tagarades Landfill Fire, Thessaloniki Greece 2006

- System Hazard 1: Uncontrolled release of waste
  - SC: Tilt limits during the configuration of the waste cell must not be exceeded
  - SC: The static balance of the waste cell must be maintained within acceptable levels
- System Hazard 2: Release of toxic substances into the atmosphere
  - SC: Personnel and the community near the landfill should not be exposed to various chemicals
- System Hazard 3: Release of leachate on uninsulated ground
  - SC: Leachate must always be withing the controlled limits of the leachate control system

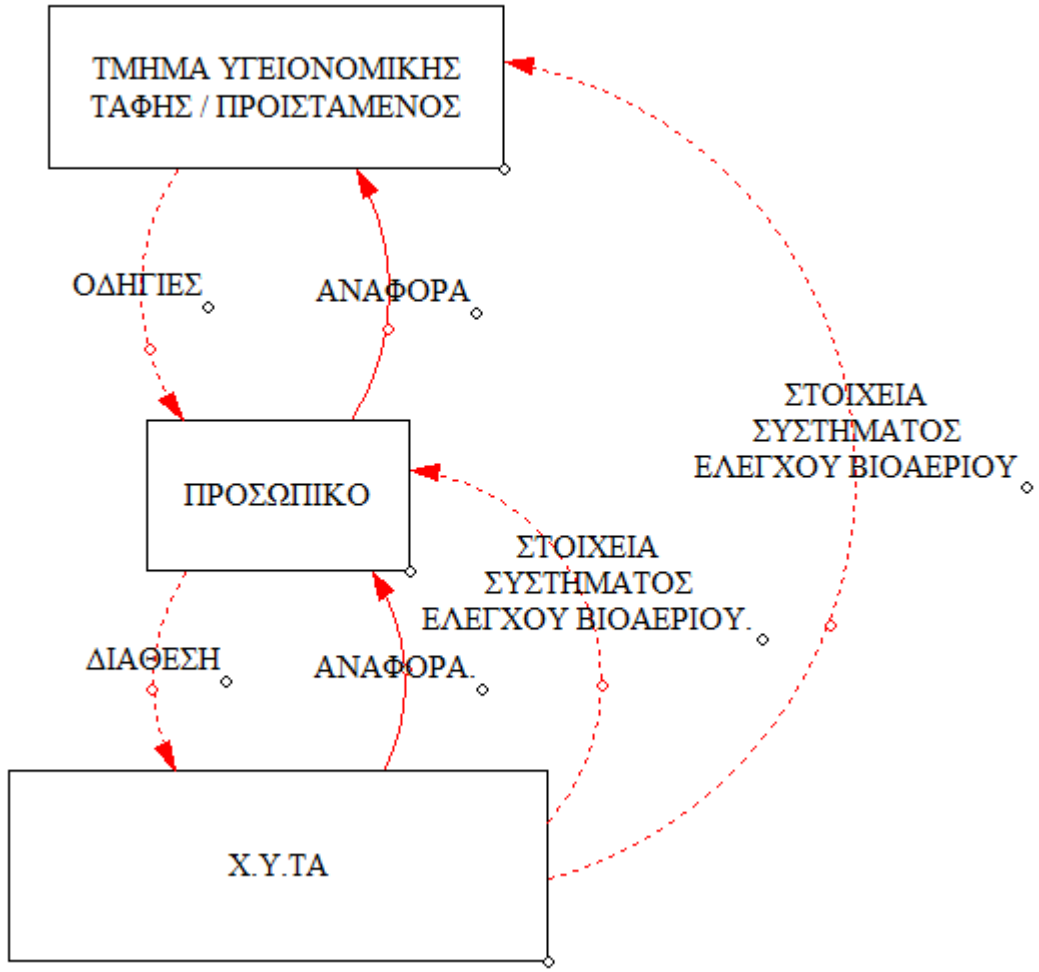
Physical System – Failures / Dysfunctional Interactions

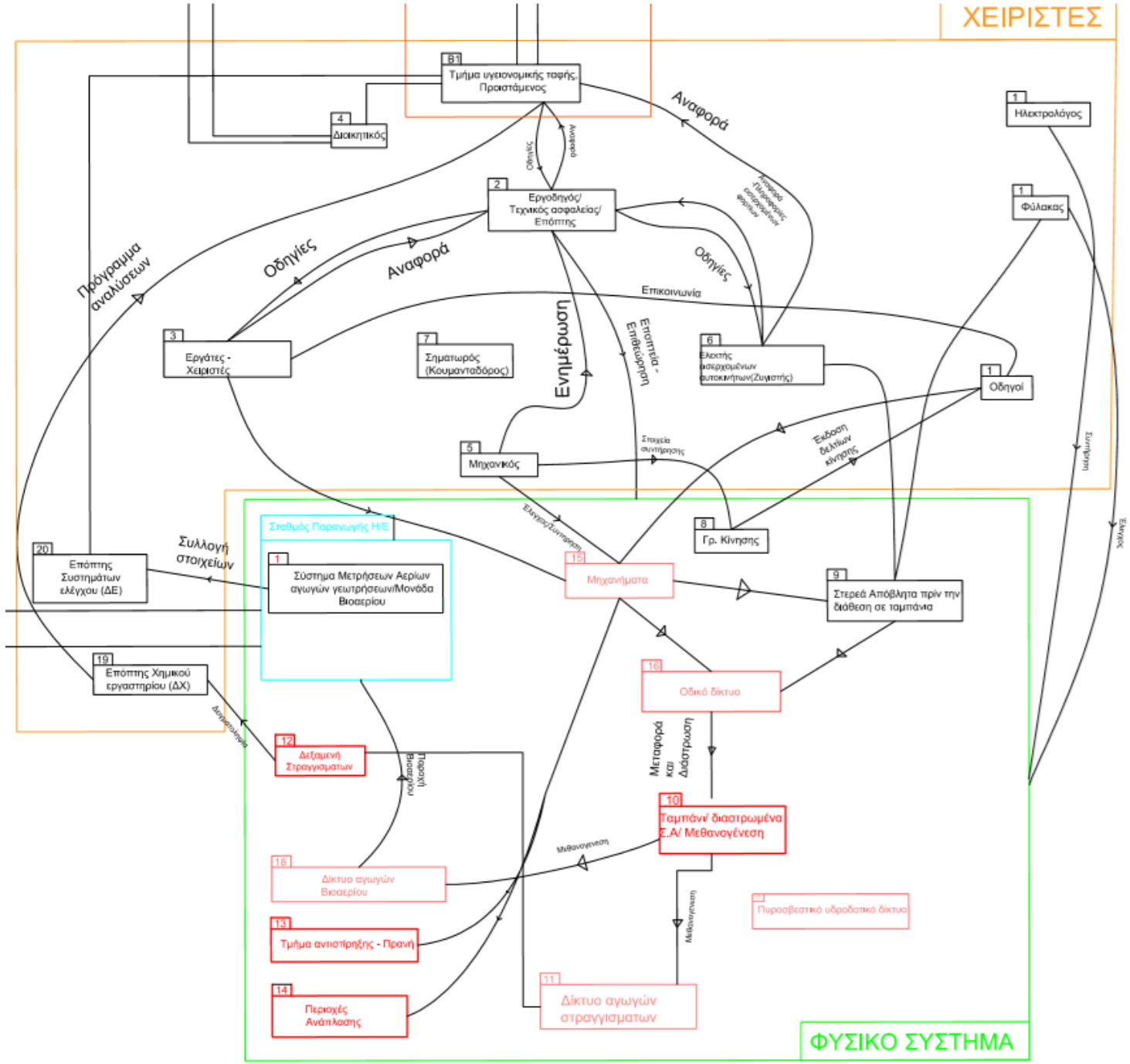
- Waste cell (slope, height, width decomposition)
- Daily operations (Trucks , Dozers, Daily cover, etc)
- Leachate collection system
- Gas collection and monitoring system
- Road network
- Fire extinguish network
- Water drainage system network
- Slope of cell
- Differential settlement due to decomposition, subsurface fire
- Distance between cell and leachate collection pond.
- Shoring system to support the cell

Proximal Events

EVENTS	QUESTIONS
Having wastes buried in the cell for approximately 20 years CO_2 and CH_4 will be produced. As result subsurface fires can occur due to spontaneous combustion. In fact several fires occurred in a slope of the cell since 2004	– Tagarades landfill was equipped with gas monitoring system. Was that system capable of measuring the parameters (temperature, CO) to indicate problems such as subsurface fires? – Were there any differences in the data collected from the gas monitoring system from 2004 to 2006 when the accident occurred?
There were reports indicating the occurrence of differential settlements in the cell body indicating the possibility of subsurface fire	– Based on that information what was the response of the system?
Several fires reported from 2004 to2006	- How these fires were put out? Soil cover is one effective approach to put out a fire in landfill. Was this approach utilized to take out the reported fires?

Model of the Safety Control Structure




ΧΕΙΡΙΣΤΕΣ
Τμήμα υγειονομικής ταφής, Προιστάμενος
Διοικητικός
Εργοδηγός/ Τεχνικός ασφαλείας/ Επόπτης
Εργάτες - Χειριστές
Σηματωρός (Κουμανταδόρος)
Μηχανικός
Ελεκτής εισερχομένων αυτοκινήτων(Ζυγιστής)
Γρ. Κίνησης
Ηλεκτρολάγος
Φύλακας
Οδηγοί
Αναφορά
Οδηγίες
Πρόγραμμα αναλύσεων
Επικοινωνία
Ενημέρωση
Εποπτεία - Επιθεώρηση
Στοιχεία συντήρησης
Έκδοση δελτίων κίνησης
Συντήρηση
Έλεγχος
Συλλογή στοιχείων
Σταθμός Παραγωγής Η/Ε
Επόπτης Συστημάτων ελέγχου (ΔΕ)
Σύστημα Μετρήσεων Αερίων αγωγών γεωτρήσεων/Μονάδα Βιοαερίου
Επόπτης Χημικού εργαστηρίου (ΔΧ)
Μηχανήματα
Στερεά Απόβλητα πριν την διάθεση σε ταμπάνα
Οδικό δίκτυο
Μεταφορά και Διάστρωση
Ταμπάνι/ διαστρωμένα Σ.Α/ Μεθανογένεση
Δεξαμενή Στραγγισματων
Παραγωγή Βιοαερίου
Μεθανογένεση
Δίκτυο αγωγών Βιοαερίου
Τμήμα αντιστήριξης - Πρανή
Περιοχές Ανάπλασης
Δίκτυο αγωγών στραγγισματων
Πυροσβεστικό υδροδοτικό δίκτυο
ΦΥΣΙΚΟ ΣΥΣΤΗΜΑ

Analyse Each Component - Landfill Manager

Responsibilities

- Responsible for the normal daily operations of the landfill
- Monitors and enforces the task of landfill operations in daily bases. All personnel report to him abnormal conditions
- Provide periodic reports to the Municipality and provides data
- Responsible for the conditions of the equipment and personnel
- Responsible in cooperation/coordination with the Municipality for the provision of proper equipment and materials for the daily operations
- Reports to the Municipality any issue related to operational problems of the landfill.
- Fills the daily log of the landfill

Safety related responsibilities

- Management of risks during daily operations
  - Related to the accident
    - Waste layering in alignment to the statics study
    - Availability of PPE

Unsafe Control Actions

- Layering of wastes despite reports of static problems
- Fire department was not called at 6.00 am right after the landslide but at 9.40am 10 mins after the fire broke out

Why? (Contextual Factors Affecting the Unsafe Control)

Static problems were known to the management

- Where these problems shared with the municipality?
- If yes, then what was the response of the Municipality
- If there was no response, why?

Why? (Contextual Factors Affecting the Unsafe Control)

At the top of the cell where the landslide took place topsoil cover operations were carried out

- Typically hazard analysis studies precede the operations. Was a hazard analysis study for this work?
- Did that study identify as potential hazard the landslide of the cell?
- If yes, were any interventions carried out to prevent this hazard?

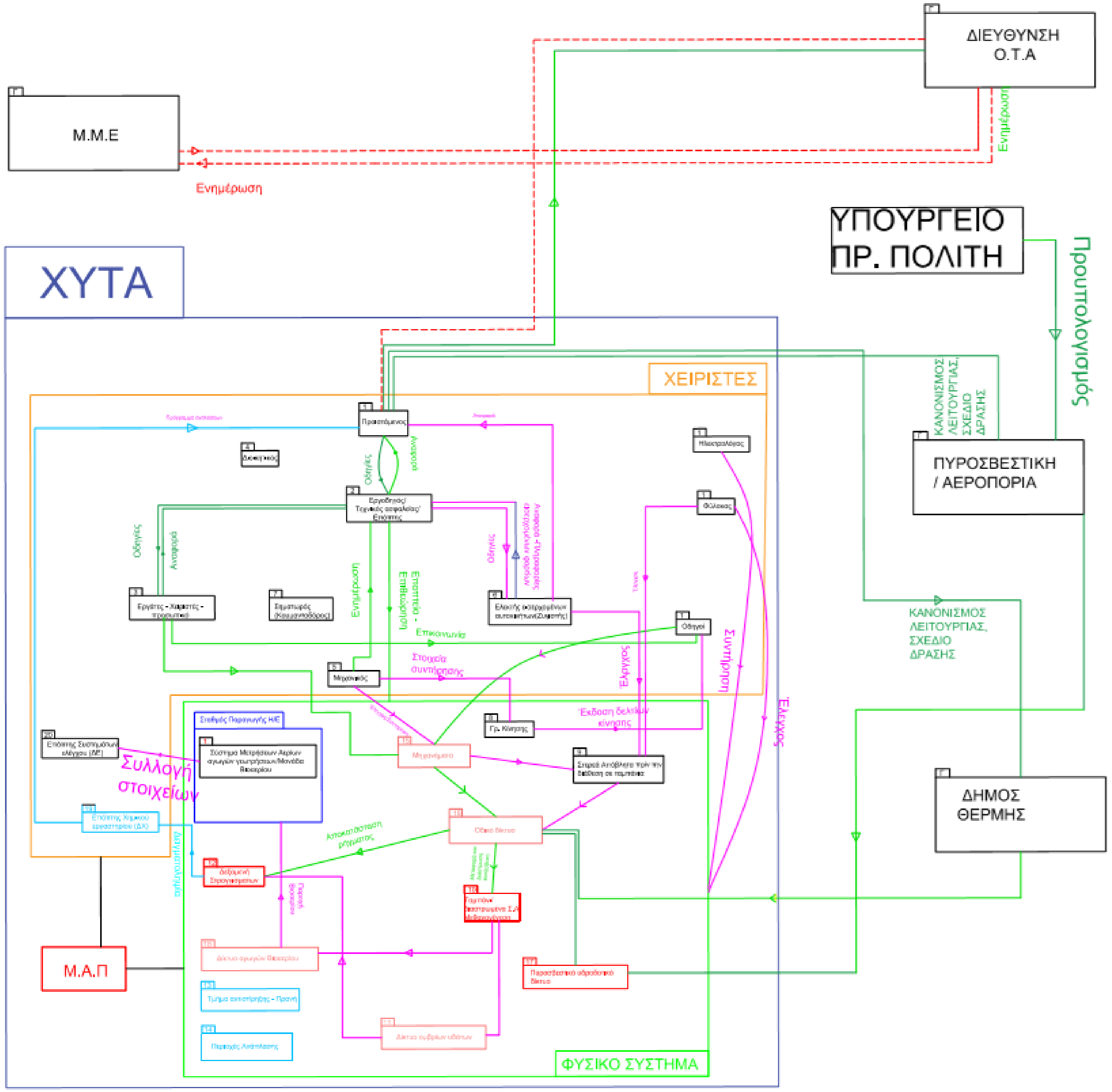
Why? (Contextual Factors Affecting the Unsafe Control)

The operation of the landfill stretched beyond its designed lifetime. Due to the continued operation and the settlement of the waste mass over time it had inefficient shoring support in its north face

- Why the site exceeded its lifetime for so long?
- Was any study of the unintended consequences of stretching the lifetime of the landfill for so many years?
- Where reports made by the personnel and manager of the landfill to the Municipality for that problem?
- What was the response of the Municipality?

Process Model Flaws

- The call to the fire department was made 3h and 40 mins after the landslide, when the fire broke out
  - It is known to those who work in landfills that the sudden inflow of oxygen to a waste mass with wastes buried for many years can cause fire due to existence of CH_4
  - Was it known to the landfill personnel and the manager or not?
  - If they knew it why they didn’t call the fire department in advance to be proactive?



ΔΙΕΥΘΥΝΣΗ Ο.Τ.Α
Μ.Μ.Ε
Ενημέρωση
Ενημέρωση
ΥΠΟΥΡΓΕΙΟ ΠΡ. ΠΟΛΙΤΗ
Πρωτόκολλο
ΧΥΤΑ
ΧΕΙΡΙΣΤΕΣ
ΚΑΝΟΝΙΣΜΟΣ ΛΕΙΤΟΥΡΓΙΑΣ, ΣΧΕΔΙΟ ΔΡΑΣΗΣ
ΠΥΡΟΣΒΕΣΤΙΚΗ / ΑΕΡΟΠΟΡΙΑ
ΚΑΝΟΝΙΣΜΟΣ ΛΕΙΤΟΥΡΓΙΑΣ, ΣΧΕΔΙΟ ΔΡΑΣΗΣ
ΔΗΜΟΣ ΘΕΡΜΗΣ
Ενημέρωση
Επιτήρηση - Επιθεώρηση
Επικοινωνία
Στοιχεία συντήρησης
Έκδοση δελτίων κίνησης
Έλεγχος
Συντήρηση
Έλεγχος
Συλλογή στοιχείων
Αποκατάσταση ρήγματος
Μ.Α.Π
ΦΥΣΙΚΟ ΣΥΣΤΗΜΑ

Analyzing the Control Structure as a Whole

- Operation beyond its design lifetime
- The Prefecture was looking for a new landfill site since 1981 why the new site delayed since 2007 to operate?
  - Not in my back-yard culture?
  - Social arrest?
  - Unwilling politicians to go ahead with the operation of the new landfill?
  - Delays of bureaucratic or legal nature?
- Tagarades landfill has not expanded over the years to accept more waste
  - Expropriation of adjacent land was not used as a tool to expand the landfill (political cost?)
  - Economic resources low to rent additional land and expand the landfill?

Analyzing the Control Structure as a Whole

- Dysfunctional interactions and decision-making process for the new supplies
- Dysfunctional interactions between the technical service department with the landfill operations department
- Dysfunctional interactions for preparedness between Landfill, Municipality, Fire department in case of emergency
- Safety Culture (Many warnings, no effective response) (investigations of previous incidents ?)

Recommendations

- Monitoring systems capable of identifying subsurface fires
- Programs for preparedness to disasters
- Effective protocols of information and control between Landfill manager and Municipality
- Coordination/Collaboration between the landfill and technical service department of the municipality
- Effective protocols for acquiring supplies
- Hazard analysis for operations in landfill
- Effective early warning system at a municipality and prefecture level

Thank you!

Dr. Ioannis M. Dokas

Email: idokas@civil.duth.gr