Hazard Log Information

- System, subsystem, unit
- Description
- Cause(s)
- Possible effects, effect on system
- Category (hazard level −− probability and severity)
- Design constraints
- Corrective or preventative measures, possible safeguards, recommended action
- Operational phase when hazardous
- Responsible group or person for ensuring safeguards provided.
- Tests (verification) to be undertaken to demonstrate safety.
- Other proposed and necessary actions
- Status of hazard resolution process.

Risk and Hazard Level Measurement

- Risk = f (likelihood, severity)
- Impossible to measure risk accurately.
- Instead, use risk assessment:
  - Accuracy of such assessments is controversial.

    > *''To avoid paralysis resulting from waiting for definitive data, we assume we have greater knowledge than scientists actually possess and make decisions based on those assumptions.''*
    >
    > William Ruckleshaus

  - Cannot evaluate probability of very rare events directly.
  - So use models of the interaction of events that can lead to an accident.

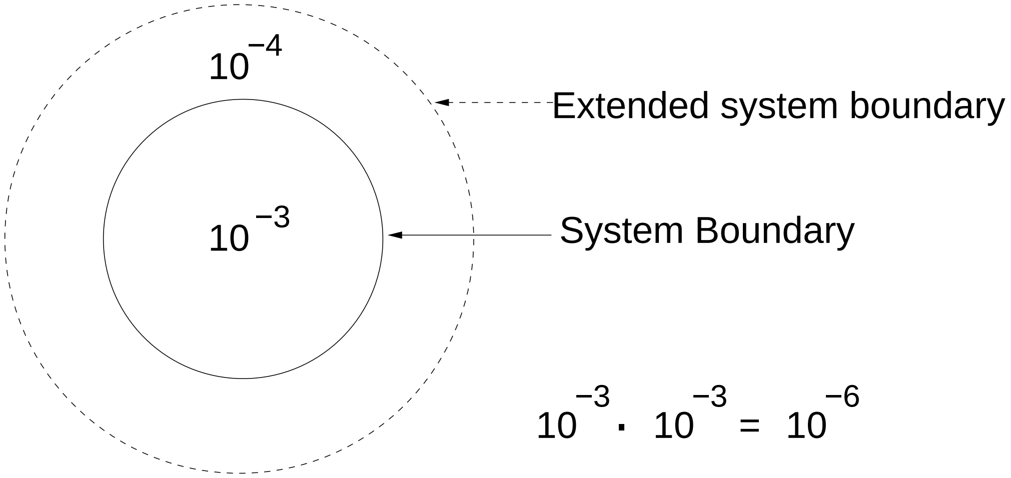
Risk Modeling

- In practice, models only include events that can be measured.
- Most causal factors involved in major accidents are unmeasurable.
- Unmeasurable factors tend to be ignored or forgotten.
- Can we measure software? (what does it mean to measure design?) Human error?

> *Risk assessment data can be like the captured spy;*
> *if you torture it long enough, it will tell you anything*
> *you want to know.*
>
> William Ruckelshaus
> *Risk in a Free Society*

Misinterpreting Risk

Risk assessments can easily be misinterpreted:



$$10^{-3} \cdot 10^{-3} = 10^{-6}$$

Example of unrealistic risk assessment contributing to an accident

Design:

System design included a relief valve opened by an operator to protect against overpressurization. A secondary valve was installed as backup in case the primary valve failed. The operator must know if the first valve did not open so the second valve could be activated.

Events:

The operator commanded the relief valve to open. The open position indicator light and open indicator light both illuminated. The operator, thinking the primary relief valve had opened, did not activate the secondary relief valve. However, the primary valve was NOT open and the system. exploded.

Causal Factors:

Post−accident examination discovered the indicator light circuit was wired to indicate presence of power at the valve, but it did not indicate valve position. Thus, the indicator showed only that the activation button had been pushed, not that the valve had opened.

An extensive quantitative safety analysis of this design had assumed a low probability of simultaneous failure for the two relief valves, but ignored the possibility of design error in the electrical wiring; the probability of design error was not quantifiable. No safety evaluation of the electrical wiring was made; instead confidence was established on the basis of the low probability of coincident failure of the two relief valves.

The Therac−25 is another example where unrealistic risk assessment contributed to the losses.

Classic Hazard Level Matrix

SEVERITY

LIKELIHOOD		I Catastrophic	II Critical	III Marginal	IV Negligible
	A Frequent	I−A	II−A	III−A	IV−A
	B Moderate	I−B	II−B	III−B	IV−B
	C Occasional	I−C	II−C	III−C	IV−C
	D Remote	I−D	II−D	III−D	IV−D
	E Unlikely	I−E	II−E	III−E	IV−E
	F Impossible	I−F	II−F	III−F	IV−F

Another Example Hazard Level Matrix

	A Frequent	B Probable	C Occasional	D Remote	E Improbable	F Impossible
Catastrophic I	Design action required to eliminate or control hazard 1	Design action required to eliminate or control hazard 2	Design action required to eliminate or control hazard 3	Hazard must be controlled or hazard probability reduced 4	9	12
Critical II	Design action required to eliminate or control hazard 3	Design action required to eliminate or control hazard 4	Hazard must be controlled or hazard probability reduced 6	Hazard control desirable if cost effective 7	Assume will not occur 12	Impossible occurrence 12
Marginal III	Design action required to eliminate or control hazard 5	Hazard must be controlled or hazard probability reduced 6	Hazard control desirable if cost effective 8	Normally not ve 10	12	12
Negligible IV	10	11	Negligible hazard 12	12	12	12

Hazard Level Assessment

- Not feasible for complex human/computer−controlled systems
  - No way to determine likelihood
  - Almost always involves new designs and new technology
- Severity is often adequate (and can be determined) to plan effort to spend on eliminating or mitigating hazard.
- May be possible to establish qualitative criteria to evaluate potential hazard level to make deployment or technology decisions, but will depend on system.

Example of Qualitative Criteria

AATT Safety Criterion:

The introduction of AATT tools will not degrade safety from the current level.

Hazard level assessment based on:

- Severity of worst possible loss associated with tool
- Likelihood that introduction of tool will reduce current safety level of ATC system.

Example Severity Level

(from a proposed JAA standard)

- Class I: Catastrophic
  - Unsurvivable accident with hull loss.
- Class II: Critical
  - Survivable accident with less than full hull loss; fatalities possible
- Class III: Marginal
  - Equipment loss with possible injuries and no fatalities
- Class IV: Negligible
  - Some loss of efficiency
  - Procedures able to compensate, but controller workload likely to be high until overall system demand reduced.
  - Reportable incident events such as operational errors, pilot deviations, surface vehicle deviation.

Example Likelihood Level

- User tasks and responsibilities

Low:	Insignificant or no change
Medium:	Minor change
High:	Significant change

- Potential for inappropriate human decision making

Low:	Insignificant or no change
Medium:	Minor change
High:	Significant change

- Potential for user distraction or disengagement from primary task

Low:	Insignificant or no change
Medium:	Minor change
High:	Significant change

Example Likelihood Level (2)

- Safety margins

Low:	Insignificant or no change
Medium:	Minor change
High:	Significant change

- Potential for reducing situation awareness

Low:	Insignificant or no change
Medium:	Minor change
High:	Significant change

- Skills currently used and those necessary to backup and monitor new decision support tools

Low:	Insignificant or no change
Medium:	Minor change
High:	Significant change

- Introduction of new failure modes and hazard causes

Low:	New tools have same function and failure modes as system components they are replacing
Medium:	Introduced but well understood and effective mitigation measures can be designed
High:	Introduced and cannot be classified under medium

- Effect of software on current system hazard mitigation measures

Low:	Cannot render ineffective
High:	Can render ineffective

- Need for new system hazard mitigation measures

Low:	Potential software errors will not require
High:	Potential software errors could require

Causality

- Accident causes are often oversimplified:

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

- Larger organizational and economic factors?

Issues in Causality

- Filtering and subjectivity in accident reports
- Root cause seduction
  - Idea of a singular cause is satisfying to our desire for certainty and control.
  - Leads to fixing symptoms
- The "fixing" orientation
  - Well understood causes given more attention

    Component failure
    Operator error
  - Tend to look for linear cause−effect relationships
  - Makes it easier to select corrective actions (a "fix")

NASA Procedures and Guidelines: NPG 8621 Draft 1

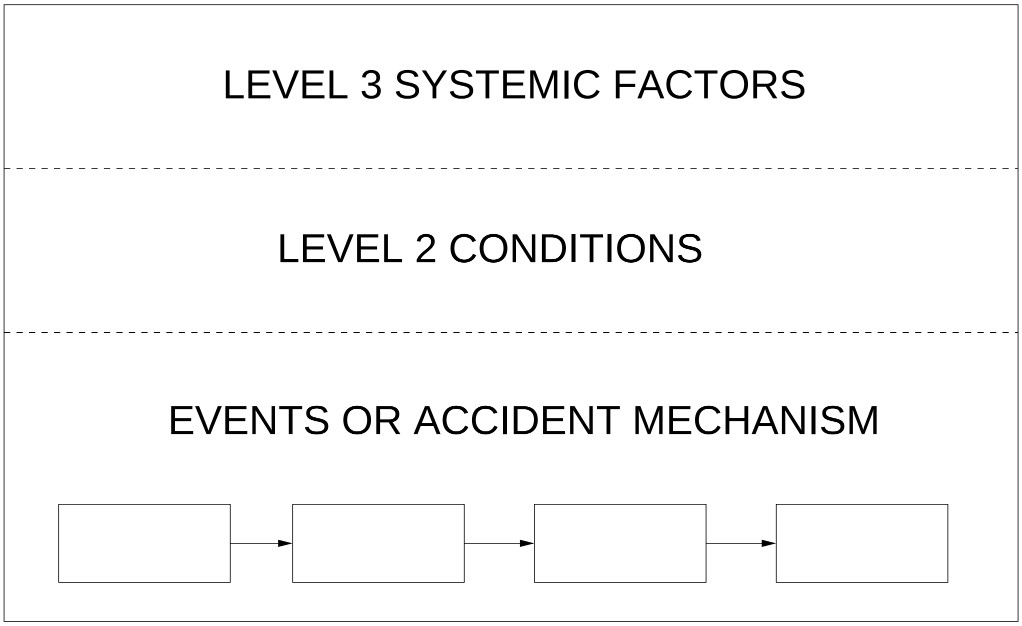
Root Cause:

"Along a chain of events leading to a mishap, the first causal action or failure to act that could have been controlled systematically either by policy/practice/procedure or individual adherence to policy/practice/procedure."

Contributing Cause:

"A factor, event, or circumstance that led directly or indirectly to the dominant root cause, or which contributed to the severity of the mishap."

Hierarchical Models

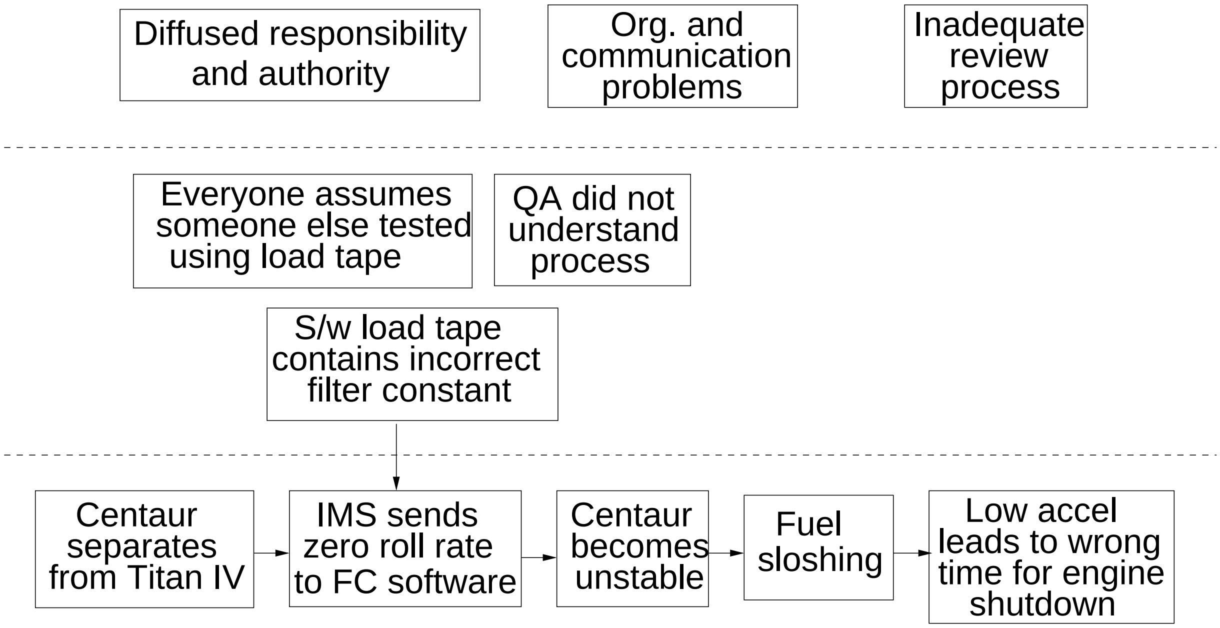


LEVEL 3 SYSTEMIC FACTORS

LEVEL 2 CONDITIONS

EVENTS OR ACCIDENT MECHANISM

Hierarchical Analysis Example



Diffused responsibility and authority

Org. and communication problems

Inadequate review process

Everyone assumes someone else tested using load tape

QA did not understand process

S/w load tape contains incorrect filter constant

Centaur separates from Titan IV

IMS sends zero roll rate to FC software

Centaur becomes unstable

Fuel sloshing

Low accel leads to wrong time for engine shutdown

Systemic Factors in (Software−Related) Accidents

1. Flaws in the Safety Culture

Safety Culture: The general attitude and approach to safety reflected by those who participate in an industry or organization, including management, workers, and government regulators

- Underestimating or not understanding software risks
- Overconfidence and complacency
- Assuming risk decreases over time
- Ignoring warning signs
- Inadequate emphasis on risk management
- Incorrect prioritization of changes to automation
- Slow understanding of problems in human−automation mismatch
- Overrelying on redundancy and protection systems
- Unrealistic risk assessment

Systemic Factors (con’t)

2. Organizational Structure and Communication
   - Diffusion of responsibility and authority
   - Limited communication channels and poor information flow

3. Technical Activities
   - Flawed review process
   - Inadequate specifications and requirements validation
   - Flawed or inadequate analysis of software functions
   - Violation of basic safety engineering practices in digital components
   - Inadequate system engineering
   - Lack of defensive programming
   - Software reuse without appropriate safety analysis

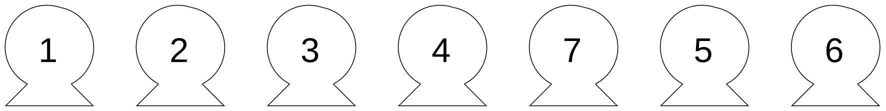
Systemic Factors (con’t)

- Inadequate system safety engineering
- Unnecessary complexity and software functions
- Test and simulation environment does not match operations
- Deficiencies in safety−related information collection and use
- Operational personnel not understanding automation
- Inadequate design of feedback to operators
- Inadequate cognitive engineering

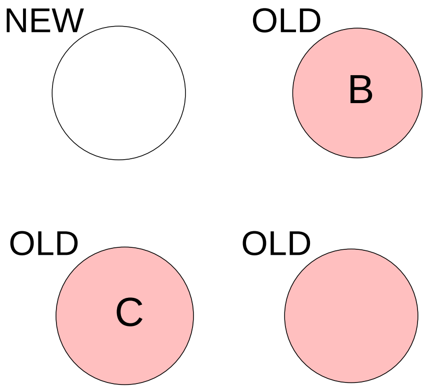
Do Operators Cause Most Accidents?

- Data may be biased and incomplete
- Positive actions usually not recorded
- Blame may be based on premise that operators can overcome every emergency
- Operators often have to intervene at the limits.
- Hindsight is always 20/20
- Separating operator error from design error is difficult and perhaps impossible.

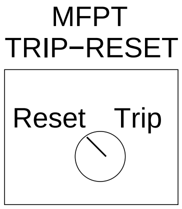
Example accidents from chemical plants:



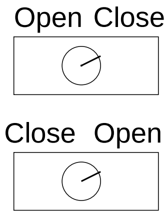
Operator told to fix pump 7.



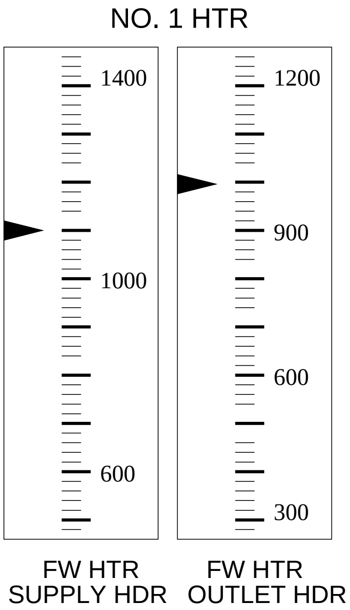
Operator told to replace crystallizer A



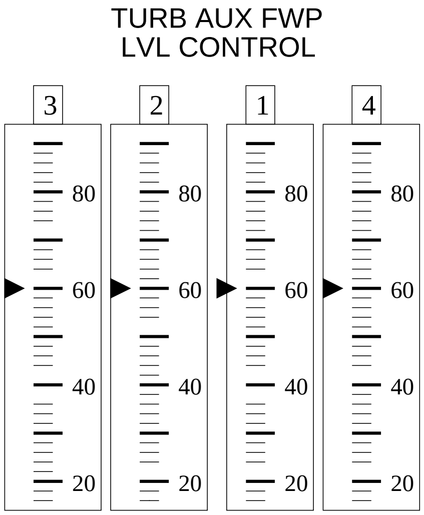
a. Note reversal of trip−reset positions



b. Another Inconsistency



c. Heater pressure gauges. A hurried operator under stress might believe the outlet pressure is higher than the supply, even though it is lower.



d. A strange way to count.

A−320 accident while landing at Warsaw:

Blamed on pilots for landing too fast.

Was it that simple?

- Pilots told to expect windshear. In response, landed faster than normal to give aircraft extra stability and lift.
  - Meteorological information out of date −− no windshear by time pilots landed.
  - Polish government's meteorologist supposedly in toilet at time of landing.
- Thin film of water on runway that had not been cleared.
  - Wheels aquaplaned, skimming surface, without gaining enough rotary speed to tell computer braking systems that aircraft was landing.
  - Computers refused to allow pilots to use aircraft's braking systems. So did not work until too late.
- Still would not have been catastrophic if had not built a high bank at end of runway.
  - Aircraft crashed into bank and broke up.

Blaming pilots turns attention away from:

- Why pilots were given out−of−date weather information
- Design of computer−based braking system
  - Ignored pilots commands
  - Pilots not able to apply braking systems manually
  - Who has final authority?
- Why allowed to land with water on runway
- Why decision made to build a bank at end of runway

Human Error vs. Computer Error

- Automation does not eliminate human error or remove humans from systems.

- It simply moves them to other functions

  - Design and programming
  - High−level supervisory control and decision making
  - Maintenance

  where increased system complexity and reliance on indirect information makes decision−making process more difficult.

Mixing Humans and Computers

- Automated systems on aircraft have eliminated some types of human error and created some new ones.

- Human skill levels and required knowledge may go up.

- Correct partnership and allocation of tasks is difficult

  Who has the final authority?

Why Not Simply Replace Humans with Computers?

> *Computers do not produce new sorts of errors. They merely provide new and easier opportunities for making the old errors.*
>
> *Trevor Kletz, "Wise After the Event"*

- Not all conditions (or the correct way to deal with them) are foreseeable.

- Even those that can be predicted are programmed by error−prone human beings.

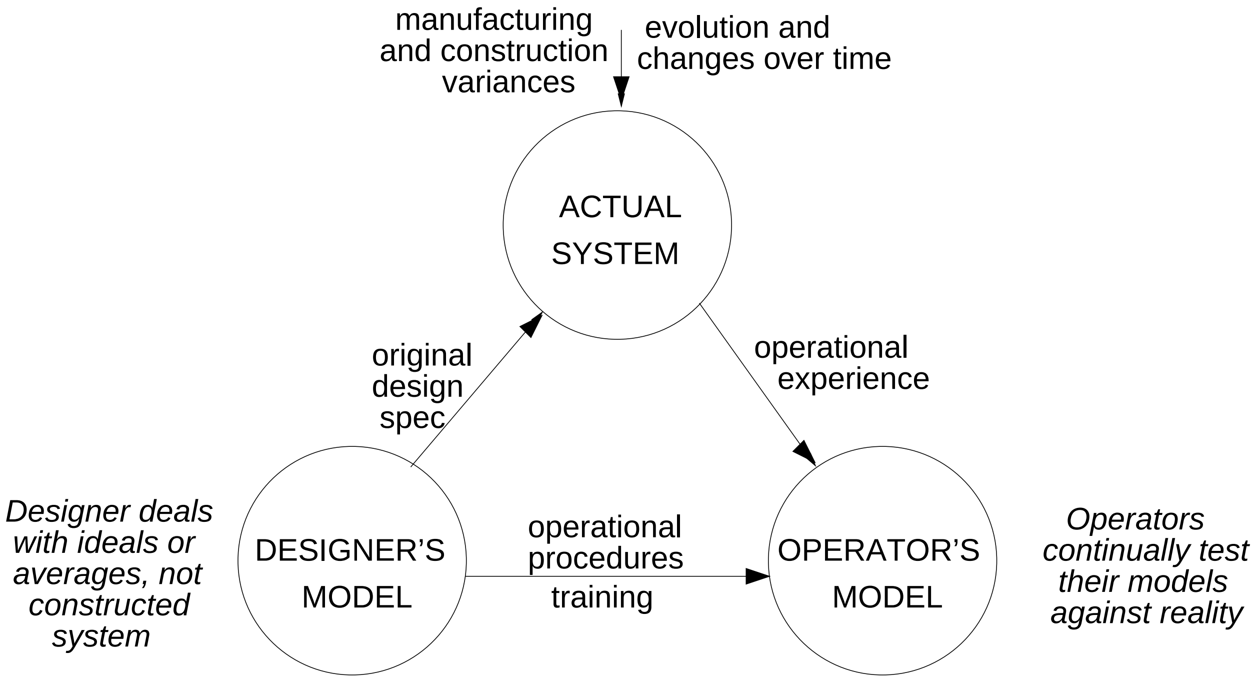
Designers Make Mistakes Too

- Many of same limitations of human operators are characteristic of designers:
  - Difficulty in assessing probabilities of rare events.
  - Bias against considering side effects.
  - Tendency to overlook contingencies.
  - Limited capacity to comprehend complex relationships.
  - Propensity to control complexity by concentrating only on a few aspects of the system.

Advantages of Humans

- Human operators are adaptable and flexible.
  - Able to adapt both goals and means to achieve them.
  - Able to use problem solving and creativity to cope with unusual and unforeseen situations.
  - Can exercise judgement.
- Humans are unsurpassed in
  - Recognizing patterns.
  - Making associative leaps.
  - Operating in ill−structured, ambiguous situations
- Human error is the inevitable side effect of this flexibility and adaptability.

Mental Models


manufacturing and construction variances
evolution and changes over time
ACTUAL SYSTEM
original design spec
operational experience
Designer deals with ideals or averages, not constructed system
DESIGNER'S MODEL
operational procedures
training
OPERATOR'S MODEL
Operators continually test their models against reality

System changes and so must operator's model