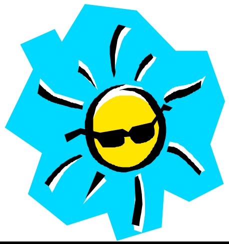
Normal Accident Theory

The Changing Face of NASA and Aerospace
Hagerstown, Maryland

November 17, 1998

Dr. Michael A. Greenfield
Deputy Associate Administrator
Office of Safety and Mission Assurance

Life 101



A Day in Your Life

→ You have an important decision meeting downtown.

→ Your spouse has already left. Unfortunately he/she left the glass coffee pot on a lit burner and it cracked.

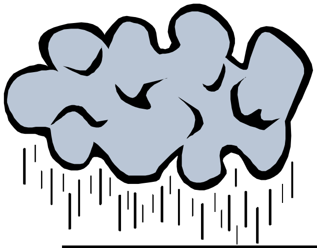
→ You desperately need your coffee so you rummage around for an old drip coffee pot.

→ You pace back and forth waiting for the water to boil while watching the clock. After a quick cup you dash out the door.

→ You get in your car only to realize that you left your car and apartment keys inside the house.

→ That's okay. You keep a spare house key hidden outside for just such emergencies.

Source: Charles Perrow, Normal Accidents: Living with High-Risk Technologies, 1984.



Not a Good Day at That

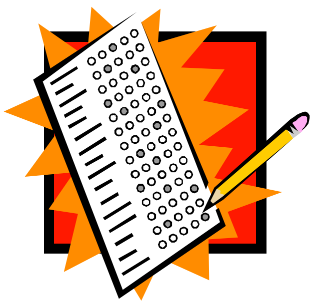
- → Then you remember that you gave your spare key to a friend. *(failed redundant pathway)*
- → There's always the neighbor's car. He doesn't drive much. You ask to borrow his car. He says his generator went out a week earlier. *(failed backup system)*
- → Well, there is always the bus. But, the neighbor informs you that the bus drivers are on strike. *(unavailable work around)*
- → You call a cab but none can be had because of the bus strike. *(tightly coupled events)*
- → You give up and call in saying you can't make the meeting.
- → Your input is not effectively argued by your representative and the wrong decision is made.

Perrow, Ibid,

A Quiz

What was the primary cause of this mission failure?

1. Human error *(leaving heat under the pot or forgetting the keys)*
2. Mechanical failure *(neighbor's car generator)*
3. The environment *(bus strike and taxi overload)*
4. Design of the system (*a door that allows you to lock yourself out or lack of taxi surge capability)*
5. Procedures used *(warming coffee in a glass pot; allowing only normal time to leave the house)*
6. Schedule expectations (*meeting at set time and place*)



What is the correct answer?

The Answer

☑ All of the above

Life is a complex system.

What Characterizes a Complex System?

- A complex system exhibits complex interactions when it has:
  - Unfamiliar, unplanned, or unexpected sequences which are not visible or not immediately comprehensible
  - Design features such as branching, feedback loops
  - Opportunities for failures to jump across subsystem boundaries.

- A complex system is tightly coupled when it has:
  - Time-dependent processes which cannot wait
  - Rigidly ordered processes (as in sequence A must follow B)
  - Only one path to a successful outcome
  - Very little slack (requiring precise quantities of specific resources for successful operation).

Perrow, Ibid.

Subsystem Linkage and Interaction

The mission is simple--provide critical data at a meeting.

→In our daily world we plan and think things through.

The activity is straightforward--have some coffee, get in the car, drive to the meeting, provide input.

→One could expect keys to be linked to using the car.

But a cracked coffeepot to using the car? Taxi alternative to a bus contract dispute? Neighbor's car not available that day?

***These interactions were not in our design*.**

Welcome to the Normal Accident Environment

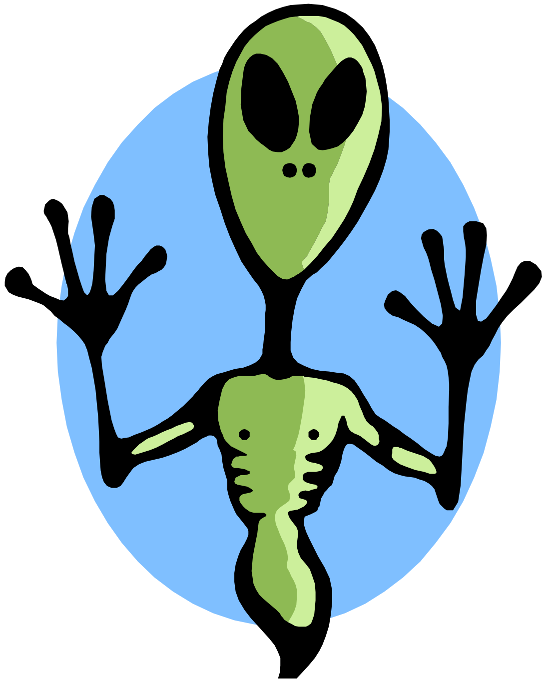
- → Failure in one part (material, human, or organization) may coincide with the failure of an entirely different part. This *unforeseeable combination* can cause cascading failures of other parts.
- → In complex systems these possible combinations are practically limitless.
- → System "unravelings" have an intelligence of their own: they expose hidden connections, neutralize redundancies, bypass firewalls, and exploit chance circumstances for which no engineer could reasonably plan.
- → Cascading failures can accelerate out of control, confounding human operators and denying them a chance for recovery.

***Accidents are inevitable* -- "*normal*."**

Perrow, Ibid.

The NASA Way

What should we do to protect against accidents or mission failure?



High Reliability Approach

- → Safety is the primary organizational objective.
- → Redundancy enhances safety: duplication and overlap can make “a reliable system out of unreliable parts.”
- → Decentralized decision-making permits prompt and flexible field-level responses to surprises.
- → A “culture of reliability” enhances safety by encouraging uniform action by operators. Strict organizational structure is in place.
- → Continuous operations, training, and simulations create and maintain a high level of system reliability.
- → Trial and error learning from accidents can be effective, and can be supplemented by anticipation and simulations.

Accidents can be prevented through good organizational design and management.

Source: Scott D. Sagan, The Limits of Safety, 1993, p. 46.

It’s Not Always Smooth Sailing

Normal Accidents - The Reality

- → Safety is one of a number of competing objectives.
- → Redundancy often causes accidents. It increases interactive complexity and opaqueness and encourages risk-taking.
- → Organizational contradiction: decentralization is needed for complexity and time dependent decisions, but centralization is needed for tightly coupled systems.
- → A "Culture of Reliability" is weakened by diluted accountability.
- → Organizations cannot train for unimagined, highly dangerous, or politically unpalatable operations.
- → Denial of responsibility, faulty reporting, and reconstruction of history cripples learning efforts.

Accidents are inevitable in complex and tightly coupled systems.

Sagan, Ibid.

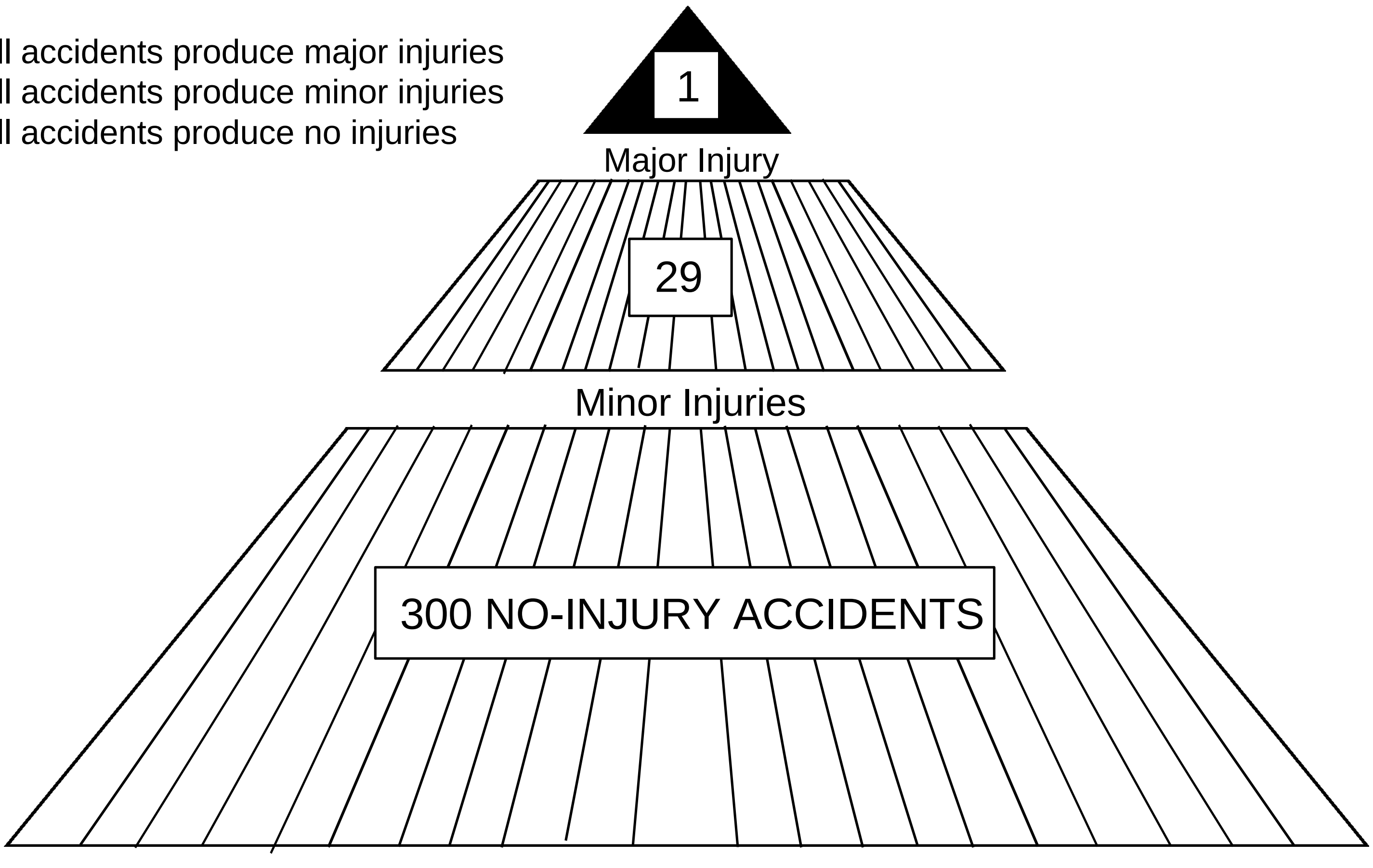
What Are We Doing?

- → Agency's Safety Initiative (ASI) reinforces the importance of safety at all levels in the organization.
- → Redundancy is no longer the automatic answer. Risk management planning provides alternate approaches.
- → Program responsibility has been moved to the Centers. They are most capable to determine the appropriate level of centralized decision-making.
- → Government's move from oversight to insight places accountability where it belongs.
- → ASI is committed to non-retribution incident reporting.

A new thrust in the analysis of close calls and mishaps provides insight into the unplanned and unimaginable.

The Foundation of a Major Injury

00.3% of all accidents produce major injuries
08.8% of all accidents produce minor injuries
90.9% of all accidents produce no injuries



Source: H. W. Heinrich, Industrial Accident Prevention, 1950, p. 24.

Understanding Complexity

→ Accident investigators generally focus on:

→Operator error

→Faulty system design

→Mechanical Failure

→Procedures

→Inadequate training

→Environment (including management organization)

→ Many times there is a tendency to cite “operator error” alone as the cause of an accident.

Closer scrutiny generally points to more complex interactions.

Is It Really “Operator Error?”

- → Operator receives anomalous data and must respond.
  - → Alternative A is used if something is terribly wrong or quite unusual.
  - → Alternative B is used when the situation has occurred before and is not all that serious.
- → Operator chooses Alternative B, the “de minimis” solution. To do it, steps 1, 2, 3 are performed. After step 1 certain things are supposed to happen and they do. The same with 2 and 3.
- → All data confirm the decision. The world is congruent with the operator’s belief. But wrong!
- → Unsuspected interactions involved in Alternative B lead to system failure.
- → Operator is ill-prepared to respond to the unforeseen failure.

Close-Call Initiative

The Premise:

→ Analysis of close-calls, incidents, and mishaps can be effective in identifying unforeseen complex interactions if the proper attention is applied.

→ Root causes of potential major accidents can be uncovered through careful analysis.

→ Proper corrective actions for the prevention of future accidents can be then developed.

It is essential to use incidents to gain insight into interactive complexity.

Human Factors Program Elements

1. Collect and analyze data on “close-call” incidents.

   Major accidents can be avoided by understanding near-misses and eliminating the root cause.

2. Develop corrective actions against the identified root causes by applying human factors engineering.
3. Implement a system to provide human performance audits of critical processes -- process FMEA.
4. Organizational surveys for operator feedback.
5. Stress designs that limit system complexity and coupling.

In Summary

- → NASA nominally works with the theory that accidents can be prevented through good organizational design and management.
- → Normal accident theory suggests that in complex, tightly coupled systems, accidents are inevitable.
- → There are many activities underway to strengthen our safety posture.
- → NASA's new thrust in the analysis of close-calls provides insight into the unplanned and unimaginable.

To defend against normal accidents, we must understand the complex interactions of our programs, analyze close-calls and mishaps to determine root causes, and USE this knowledge to improve programs and operations.

Read All About It

- → H. W. Heinrich, “Industrial Accident Prevention: A Scientific Approach” (1950).
- → William Langewiesche, “The Lessons of ValuJet 592,“ The Atlantic Monthly; March 1998; Volume 281, No. 3; pages 81 - 98.
- → Charles Perrow, “Normal Accidents: Living with High-Risk Technologies” (1984).
- → Scott D. Sagan, “The Limits of Safety: Organizations, Accidents, and Nuclear Weapons” (1993).