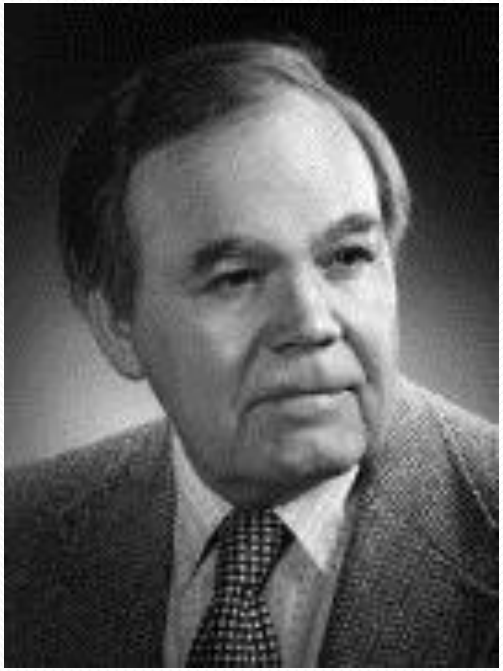
Historical Foundation for Safety Culture and High Reliability Organizations

Douglas M. Minnema, PhD, CHP
U.S. Defense Nuclear Facilities Safety Board

In Memoriam



Herbert J. C. Kouts
1919 - 2008

- Presidentially-appointed Member of U.S. Defense Nuclear Facilities Safety Board, 1989 – 1997
- Member of International Nuclear Safety Advisory Group (INSAG) during preparation of INSAG-1, *Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident*
- Chair of INSAG during preparation of:
  - INSAG-4, *Safety Culture*, 1991.
  - INSAG-7, *The Chernobyl Accident: Updating of INSAG-1*, 1992.
- Received American Nuclear Society's George C. Laurence Award in 2005.
- Received Atomic Energy Commission's E. O. Lawrence Award in 1963.
- Elected to National Academy of Engineering, 1978

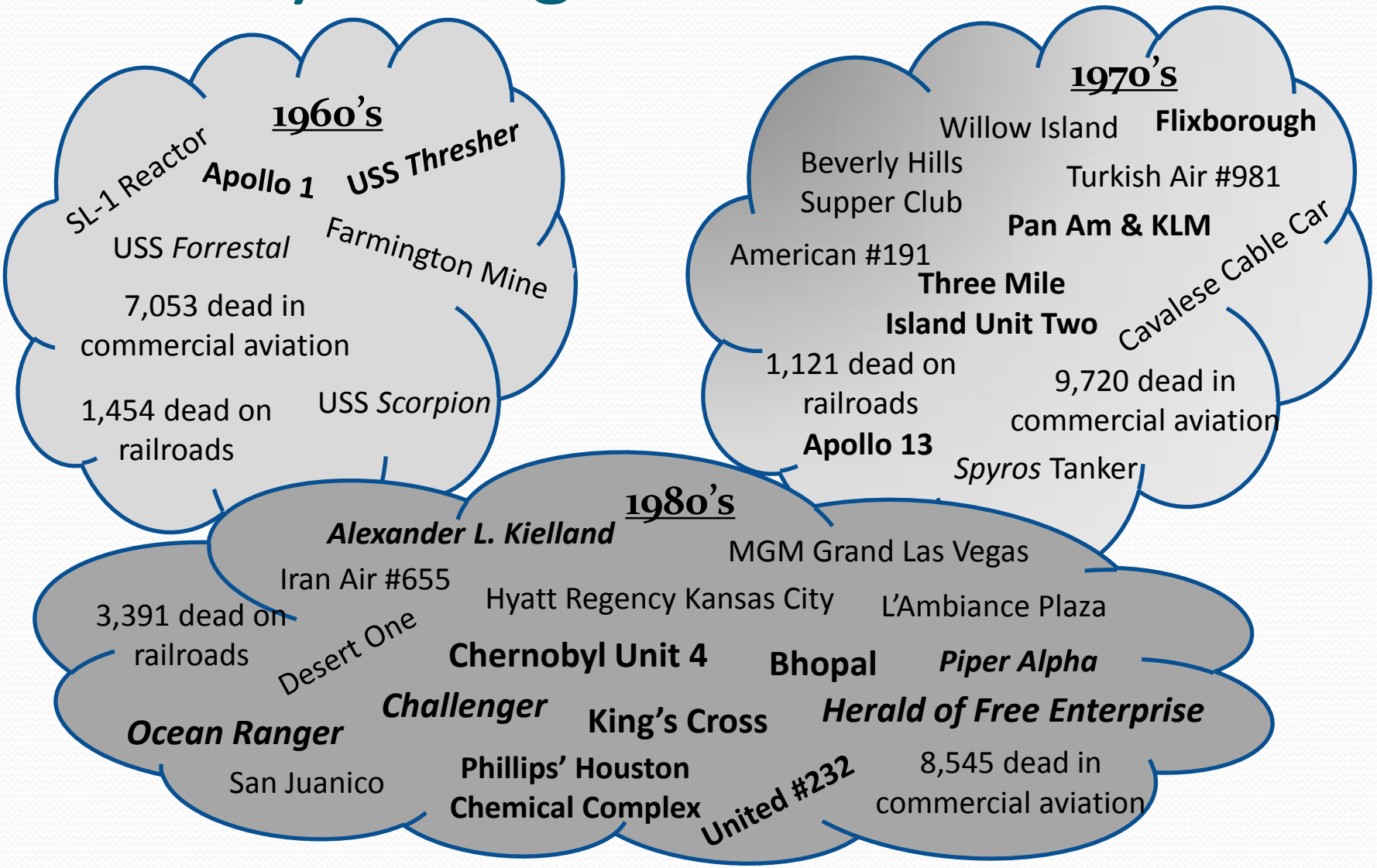
The Value of History

- Conceptual models help us understand how our safety systems work, decisions get made, and accidents occur
- A model's true value comes in its ability to help us identify patterns that are beneficial or detrimental to safety
- Each model has a **history**; it was created to explain a particular set of observations from a particular situation
- When applying models to new situations one should always consider appropriateness by reviewing the **history**

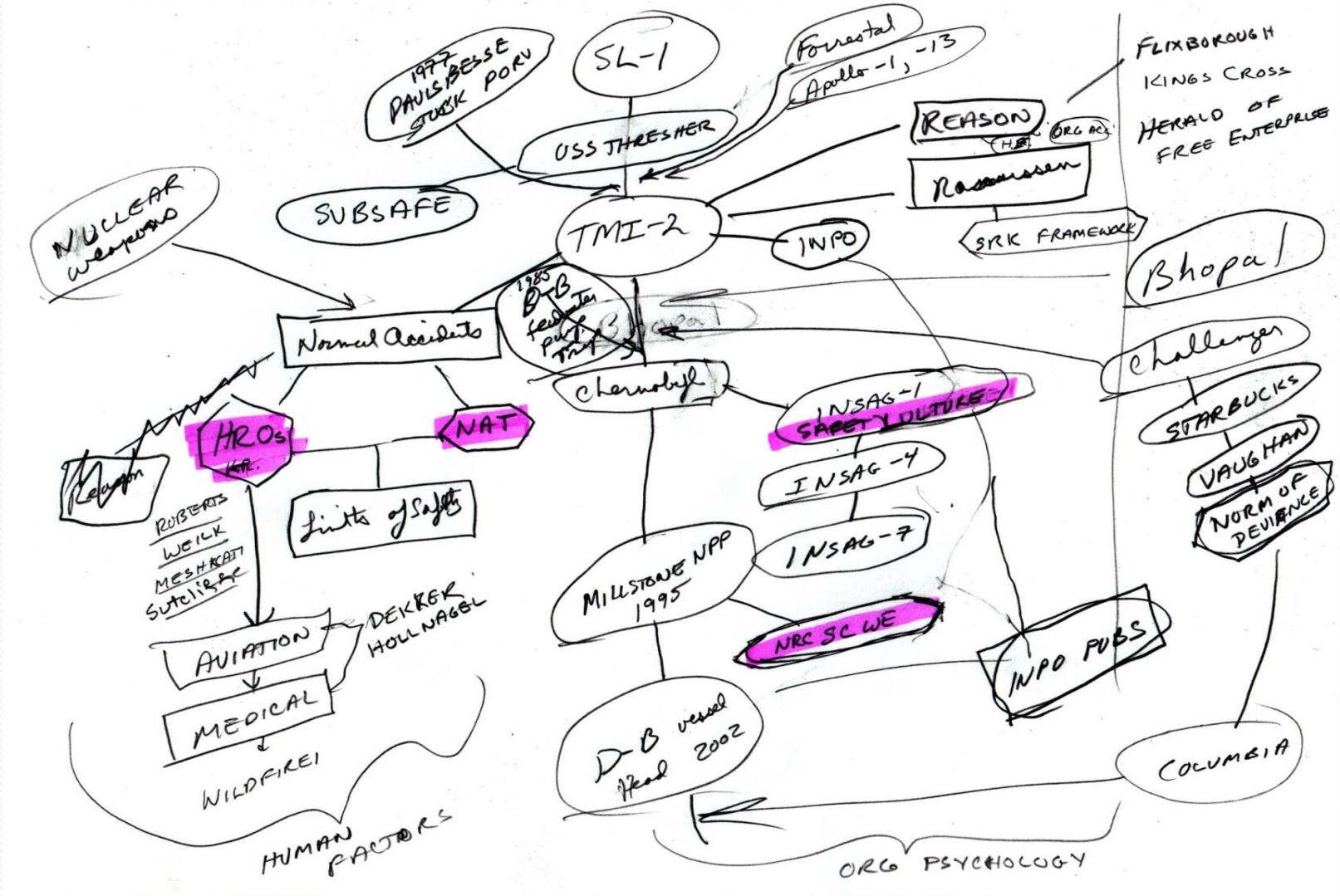
"Essentially, all models are wrong, but some are useful"

- George E. P. Box

History of Organizational Accidents



The Graphic Version of History



The Foundational Decade 1960-1969

- January 3, 1961: Prototype SL-1 reactor explodes in Idaho; all three operators killed.
  - Investigation determined *what* happened
  - No satisfactory answer has ever been found for *why*
- April 4, 1963: Nuclear submarine *USS Thresher* sinks in North Atlantic with all hands. 129 killed.
  - Investigation determined probable *what* and *why*
  - **Resulted in the birth of the SUBSAFE program**
- January 27, 1967: *Apollo-1* suffers flash fire during dress rehearsal on launch pad; 3 astronauts killed.
  - Investigation determined *what* and probable *why*
  - "No single person bears all of the responsibility … It happened because many people made the mistake of failing to recognize a hazardous situation." – Senate Committee Report

The Formative Decade 1970-1979

- April 13, 1970: Inflight explosion in damaged oxygen tank leaves Apollo-13 command module crippled; 3 astronauts survive.
  - Oxygen tank damage occurred during testing, years before flight
  - **Strong leadership, competence, improvisation, and teamwork overcome many latent conditions to enable a safe return to earth**
- March 3, 1974: Turkish Air Flight 981 crashes near Paris; 346 dead.
  - Improperly secured cargo door opened in flight, causing explosive decompression and severing control cables
- June 1, 1974: Chemical plant explodes in Flixborough, UK, decimating local community; 26 dead, 86 injured.
  - "Hasty modification" of improvised bypass pipe in process line
- J. Reason later refers to these accidents: "maintenance errors … are not just isolated causes… they are themselves consequences of upstream organizational factors" (Managing the Risks of Organizational Accidents)

The Formative Decade (cont.)

- March 27, 1977: Two Boeing 747 aircraft collide in fog on runway at Los Rodeos Airport, Tenerife; 583 dead.
  - Pure organizational accident; no significant technical failures, but a combination of many latent conditions
- 1978: Barry A. Turner publishes Man-Made Disasters based on a study of accidents and disasters in Britain over 11 year period
  - Credited by Reason as one of the "intellectual origins" of the organizational model approach to safety management
- April 27, 1978: Hyperbolic cooling tower collapses during construction in West Virginia; 51 dead.
  - Believed to be largest construction accident in American history
  - Schedule pressures led to number of safety lapses
- October 12, 1978: Tanker ship *Spyros* explodes in Singapore during maintenance activities in shipyard; 76 dead.
  - Inquiry concluded that normal safety practices had been ignored

The First Seminal Event

- March 28, 1979: Stuck pressure relief valve leads to core meltdown at Three Mile Island Unit 2 NPP; No fatalities.
  - Minor technical issues initiated event, but numerous latent conditions interfered with attempts at response and recovery

This event:

- Nearly leads to collapse of nuclear power industry in USA
- Drives industry to create Institute of Nuclear Power Operations
- Forces Nuclear Regulatory Commission to restructure its system
- Motivates Charles Perrow to write Normal Accidents (1984)
- Motivates James Reason to write Human Error (1990)
- Inspires Jens Rasmussen's Skill-Rule-Knowledge framework
- Indirectly leads to studies by Karlene Roberts, Karl Weick, et al, resulting in **High Reliability Organizations**, Sensemaking, etc.
- Indirectly leads to Scott Sagan's study, The Limits of Safety (1993)

The Nurturing Decade 1980-1989

- March 27, 1980: Offshore platform *Alexander L. Kielland* capsizes during storm in the North Sea; 123 dead.
  - Improper construction and inadequate emergency preparedness
- July 17, 1981: Elevated walkways collapse at the Hyatt Regency Hotel in Kansas City, MO; 111 dead.
  - Deviations from design during construction were not analyzed
- February 15, 1982: Offshore drilling rig *Ocean Ranger* capsizes during storm in Atlantic Ocean; 84 dead.
  - Inadequate training for operations and emergencies
- December 3, 1984: Massive chemical release from pesticide plant at Bhopal, India; estimated 3800 – 16,000 dead.
  - Large number of latent conditions and plant deficiencies

The Nurturing Decade (cont.)

- January 28, 1986: Space Shuttle *Challenger* destroyed in deflagration over Atlantic shortly after launch; 7 dead.
  - O-ring failure due to cold launch temperatures vents hot gases onto external fuel tank; coldest shuttle launch on record
  - Inspires Richard Feynman to write "Personal observations on the reliability of the Shuttle" in which he discusses NASA personnel's perceptions of risk and reliability (Appendix F to Presidential Commission's report on the accident)
  - Inspires William Starbuck to write "Challenger: Fine-tuning the odds until something breaks" in 1987
  - Following Starbuck, Diane Vaughan is inspired to study the launch decision and writes The Challenger Launch Decision (1997) in which she defines the "normalization of deviance"

The Second Seminal Event

- April 26, 1986: Unit 4 at the Chernobyl Nuclear Power Plant in Ukraine explodes during tests; 31 acute deaths.
  - Operators conducted residual power test during routine shutdown, numerous procedural violations and safety systems were bypassed
  - Accident had global impacts in social, political, and industrial spheres

This event:

- Nearly leads to global collapse of the nuclear power industry
- Inspires the IAEA's International Nuclear Safety Advisory Group (INSAG) to coin the phrase **"Nuclear Safety Culture"** while trying to understand the organizational aspects of the accident
- Inspires INPO to issue a series of guidance documents on leadership, professionalism, and organizational topics related to safety culture
- Inspires the creation of the World Association of Nuclear Operators (WANO), an INPO-like organization

The Nurturing Continues

- March 6, 1987: The *Herald of Free Enterprise* capsizes shortly after leaving port in the English Channel; 193 dead.
  - Organizational weaknesses resulted in bow doors not being closed and the ship not being trimmed properly prior to departure
- November 18, 1987: Fire erupted in the King's Cross St. Pancras Tube Station in London, UK; 31 dead.
  - Attitudes towards possibility of fire were "lax," and the hazard had been underestimated by both facility and emergency personnel
- July 6, 1988: Oil platform *Piper Alpha* explodes and burns in the North Sea; 167 dead.
  - Production continued during major maintenance and upgrades; inadequate control of out-of-service systems led to major gas leak
  - **Led to UK's adoption of Offshore Installations (Safety Case) Regulations in 1992**

The Nurturing Continues (cont.)

- July 19, 1989: Catastrophic failure of tail engine results in crash landing of United flight 232 at Sioux City, IA; 111 dead, **185 survived.**
  - Engine failure results in loss of all flight controls while at cruise altitude; situation was believed to be unrecoverable
  - **Pilots maintained control with improvised techniques, flew 44 minutes to airport; high survival rate due to these actions**
- October 23, 1989: Explosions and fire at the Phillips' Houston Chemical Complex in Texas; 23 dead.
  - Improperly connected valve operated in reverse of intent during maintenance operations
  - **Led to OSHA's issuance of the Process Safety Management Regulations in 1993**

Organizational Accidents

So what are the features of organizational accidents?

- Traditionally viewed as accidents due to "human error;" physical evidence doesn't provide satisfying explanation
- Post-accident investigations usually reveal:
  - multiple process breakdowns in various elements of organization existed prior to the accident
  - Significant differences between "work as imagined" and "work as performed" at multiple levels in organization
  - Lack of awareness or acceptance of deviation by supervision
  - Failure to recognize safety significance of actions prior to accident
  - Failure of feedback and improvement processes to detect and/or correct process breakdowns
- These are failures to aggressively and consistently ensure that safety systems are in place and functioning properly
- These are latent conditions in the organization's culture

Culture and Accidents

- Any organization will have a number of cultural traits that may not support or prioritize safety as a value
- This is normal and expected; many of those traits support other organizational needs
- Organizations have processes in place to balance cultural traits that do not support safety with those that do
- After accident, it is often found that those processes have failed, allowing one aspect of culture to dominate
- The investigator's challenge is to align physical evidence with cultural artifacts to identify latent cultural conditions
- Neither technical investigation nor culture assessment alone can or will provide adequate explanation of accident

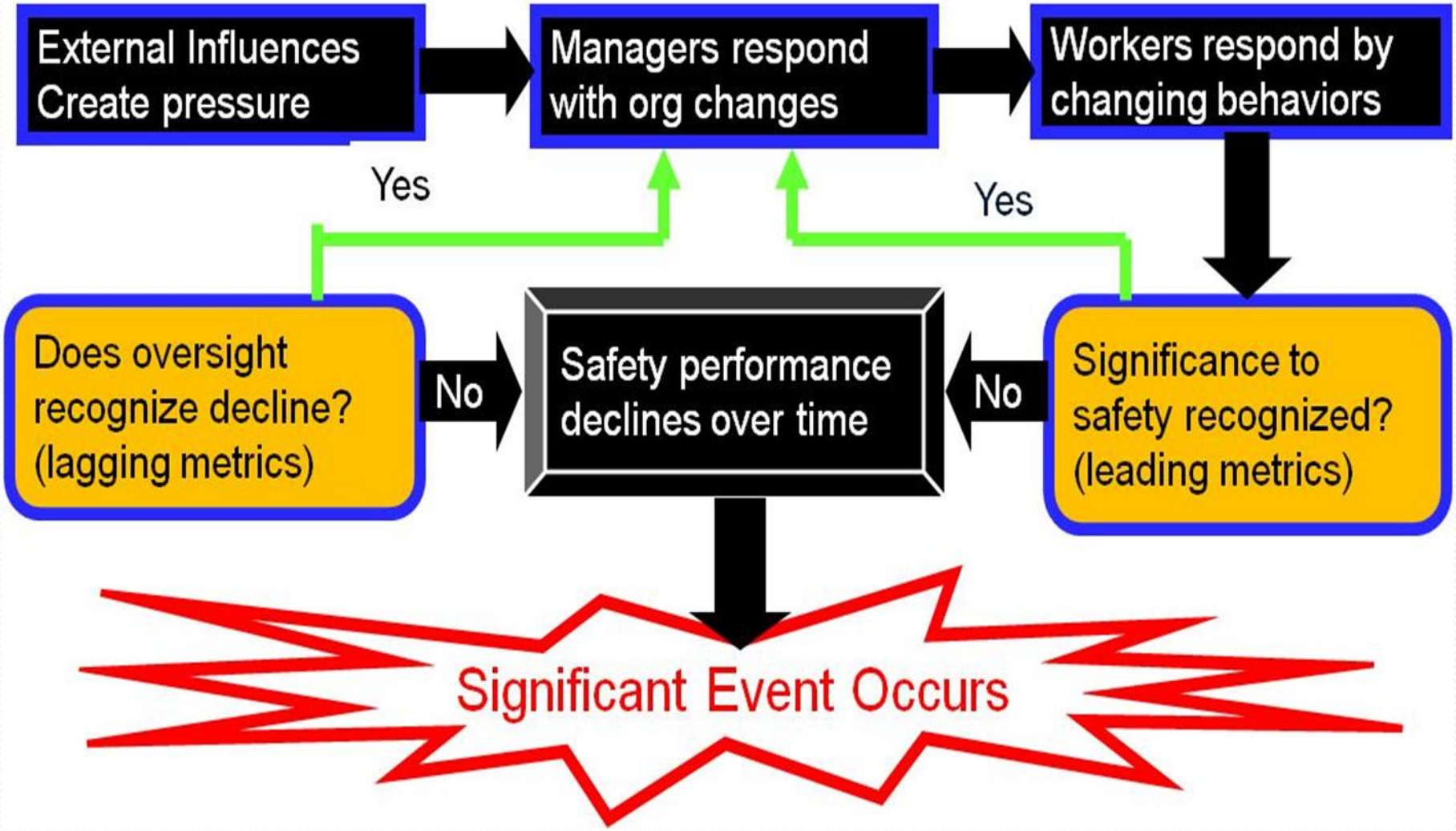
So what can we learn?

Improve the Balancing of Priorities

- **Organizations and people profit from taking risks**
- This is normal and should be anticipated
- Do we understand the magnitude and nature of the risk?
- Are we using our resources based on our true priorities?
- Are we monitoring the absolute values and relative trends between safety and mission resources?
- Do our relative trends reflect where priorities our lay?
- Are our safety and mission resources changing consistently?

"Real progress on safety can be made by understanding how people create safety, and understanding how … safety can break down in resource-limited systems."
- Sydney Dekker

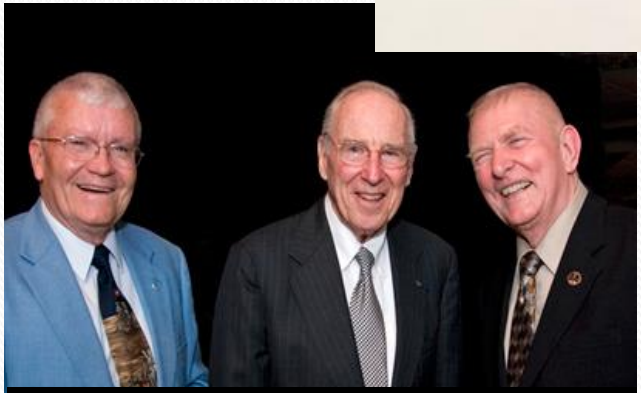
Watch for Declining Performance



Recognize Importance of Leaders

Naohiro Masuda
Plant Manager,
Fukushima Daini

Captain Chesley Sullenberger and crew, US Airways #1549



Fred Haise, Jim Lovell, and Gene Kranz, Apollo 13

Captains Dennis Fitch and Al Haynes, United #232

Recognize Importance of Leaders (cont.)

- There are "successful failures" from which we can learn about the role of leaders
- There were no procedures, guides, or experience to rely on
- Survival came down to a fundamental understanding of the systems and a refusal to accept failure
- The leaders made the difference
- **Safety culture is the artifact of the *values* of the leaders**
- **Are we properly selecting and preparing our leaders for conducting high-risk operations?**

"Failure is not an option!"

– Gene Kranz, NASA

Final Thoughts

Myth buster: Organizational accidents are not rare or extraordinary events; they occur all the time.
It is the spectrum of possible consequences that makes some appear to be extraordinary.

- Individual culpability tends to be a small contributor to workplace accidents – organizations are responsible
- Most workplace "individual accidents" disclose latent conditions, but they are not always recognized
- An accident's consequences are based on probability and chance; they are not predestined by the triggering event
- Essentially every workplace accident has some features of organizational accidents
- **All accidents are organizational learning opportunities**