Engineering Safety-Critical Systems in the 21st Century

Tom Ferrell, Principal
FAA Consulting, Inc.

A ‘Loose’ Outline

- What is a Safety?
- Safety Levels
- Architecture and Process
- Organizational Focus
- Accident Examples
- Role of the Engineer

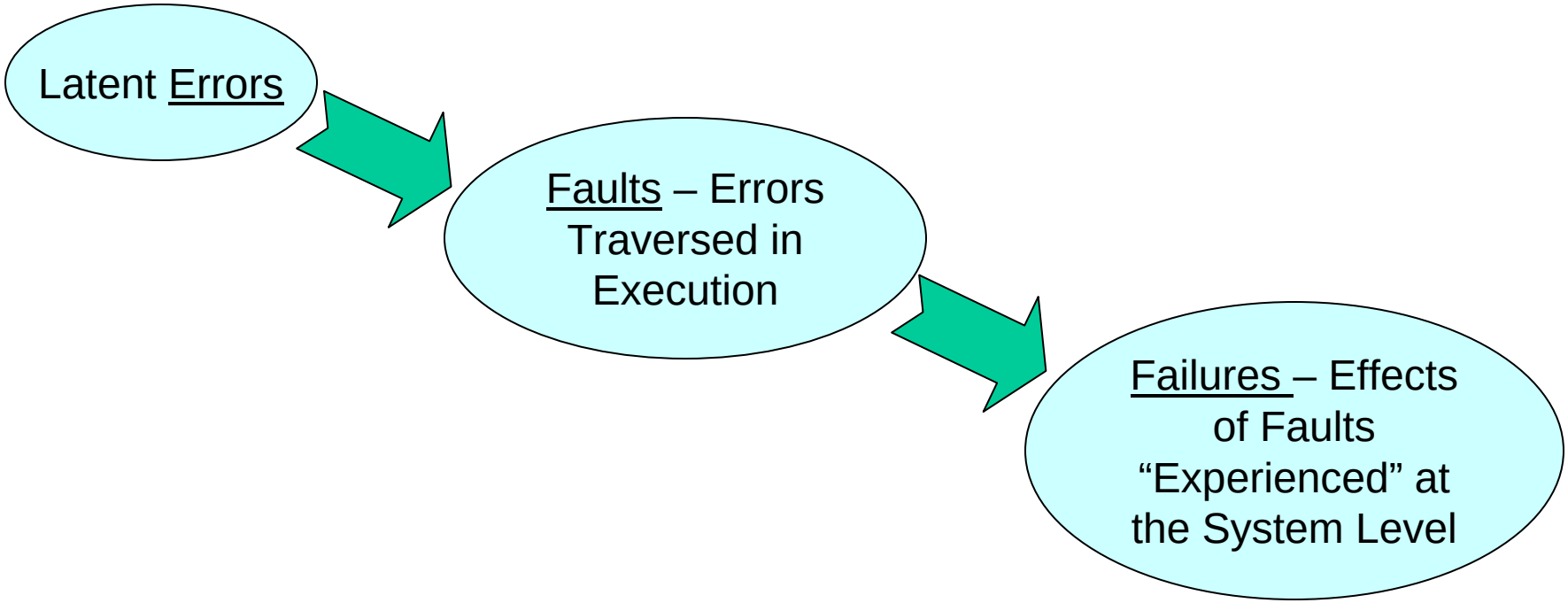
Definition of Safety

- 1. **The state of being safe; freedom from the occurrence of risk of injury, danger, or loss**. 2. The quality of averting or not causing injury, danger or loss. 3. A contrivance or device to prevent injury or avert danger. [Webster's Encyclopedia]
- Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment [MIL-STD-882C and D]
- **Safety is the property of a system that it will not endanger human life or the environment. [Storey, 1996]**
- Safety is freedom from accidents or losses [Leveson, 1995].

Safety, Reliability and Security

- Reliability is a measure of the rate of failures that render the system unusable [Deutsch and Wills]
- Safety is a measure of the absence of failures or conditions that would render the system dangerous
- A system may be reliable but unsafe, and conversely, a system may be safe but not reliable
- Safety depends upon security and reliability in a hierarchical relationship [Neumann]; security depends upon reliability and safety depends upon security.

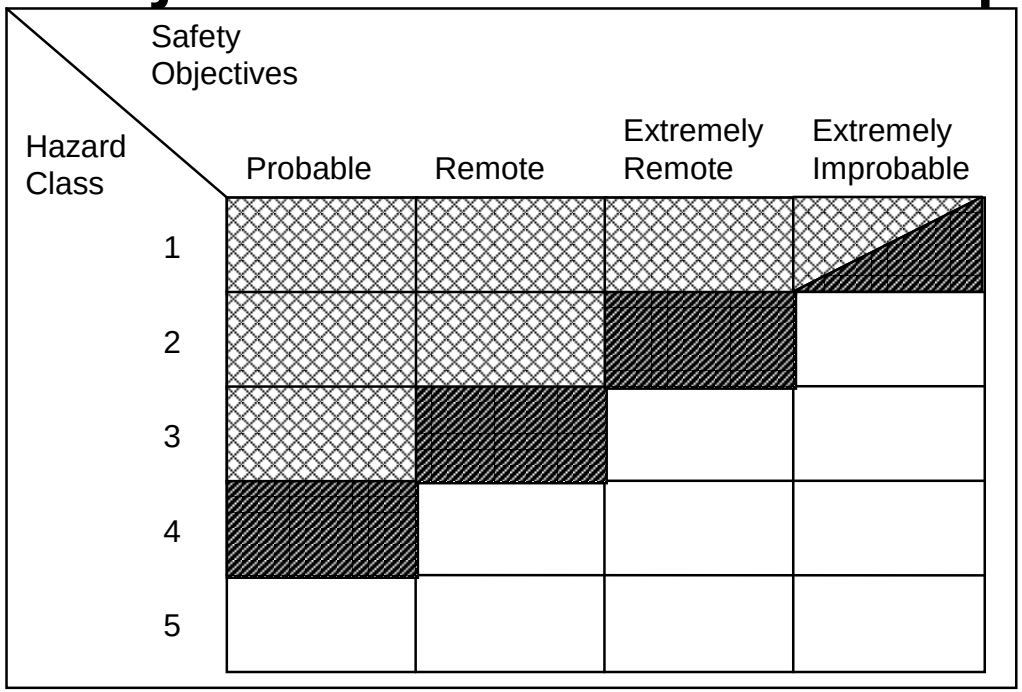
The Semantics of Software Safety



The Philosophy of Safety Levels

- Measurement of safety property involves how severe and how frequent are the dangers –
  - Criteria of severity is derived from system safety assessment
  - Criteria of frequency namely, extremely improbable, improbable and probable
- System Safety Assessment is a means to identify and control hazardous consequences to be within acceptable risk: “As Low As Reasonably Practicable” (ALARP)

Hazard Classification / Safety Objectives Relationship



Risk Acceptance Cases

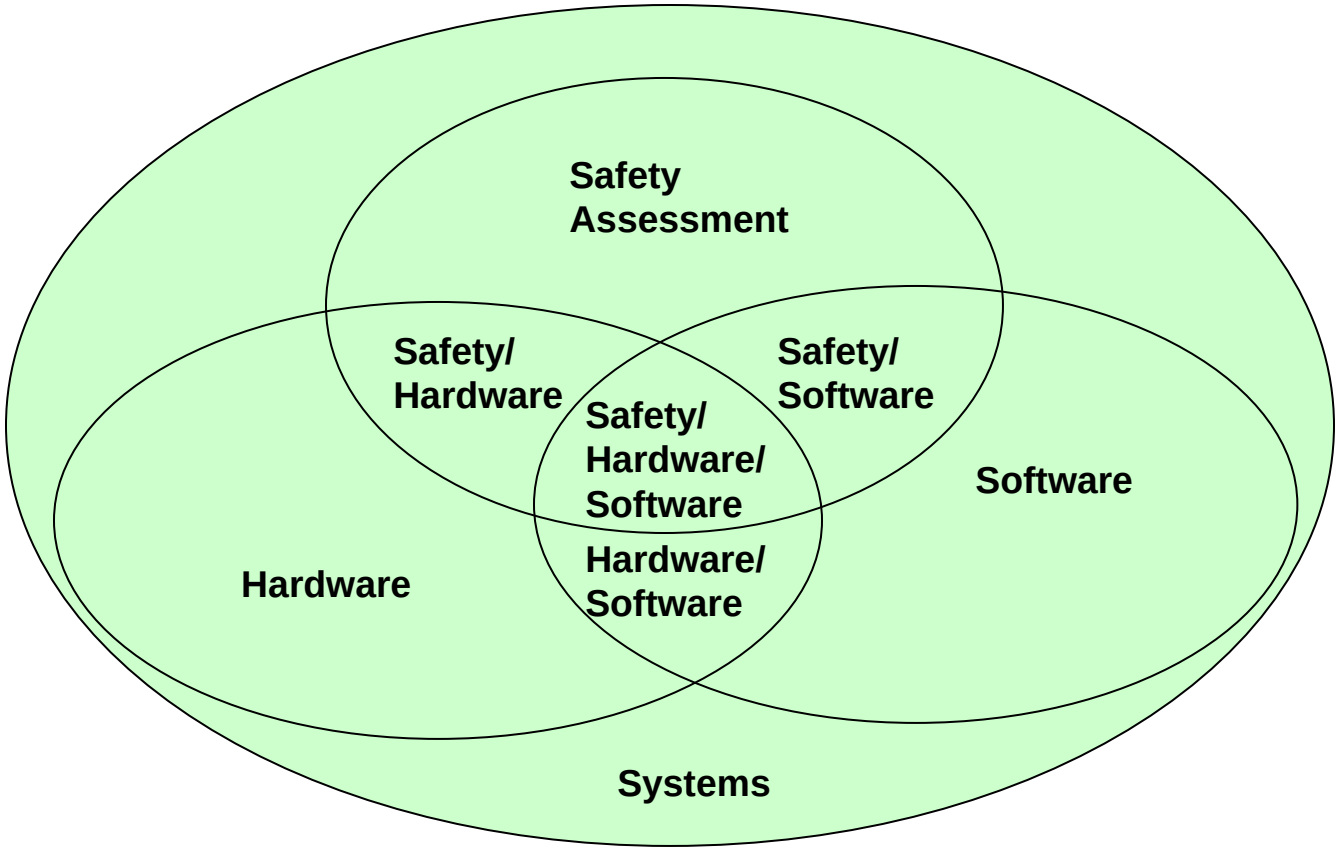
Unacceptable

Acceptable with Review

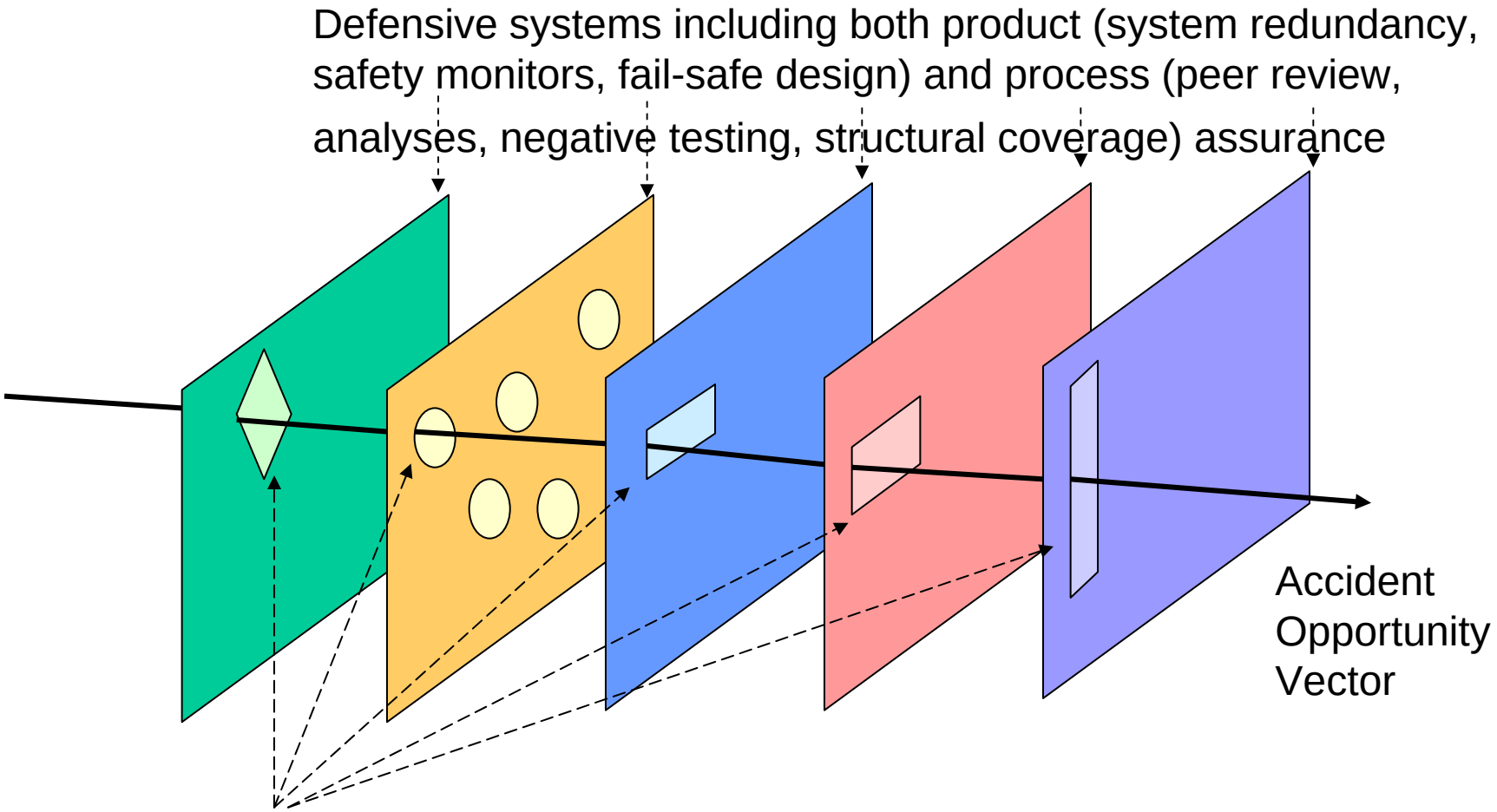
Acceptable

Acceptable with Review - Unacceptable with Single Point Failures and Common-Cause Failures

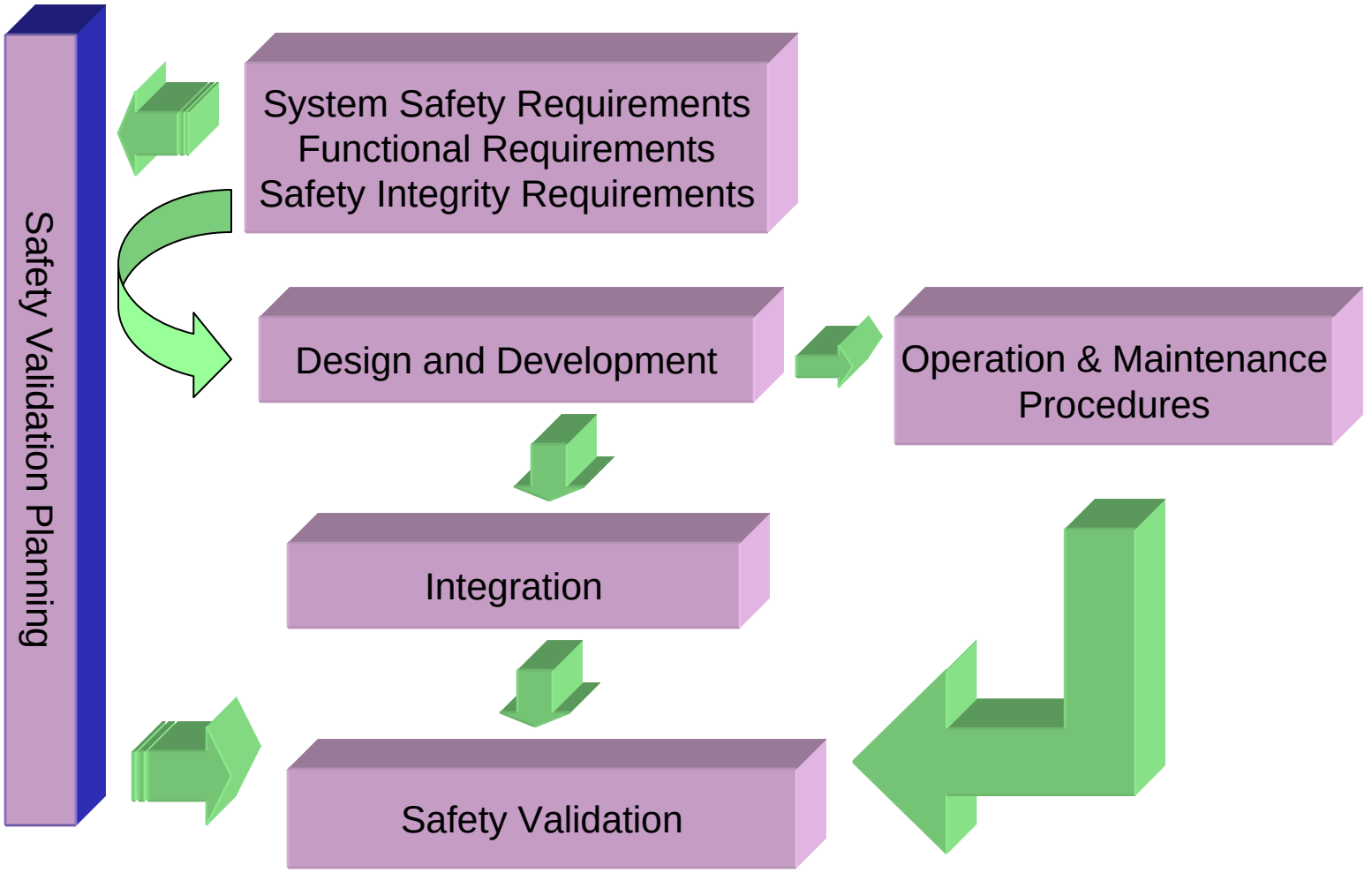
Relationships between Safety, HW & SW



Reason's Model: Safety is Everyone's Responsibility



Safety-driven Engineering



Tools and Techniques

Functional Hazard Assessment
(May be accomplished using HAZOP)

Fault Tree Analysis
Dependence diagram
Markov Analysis

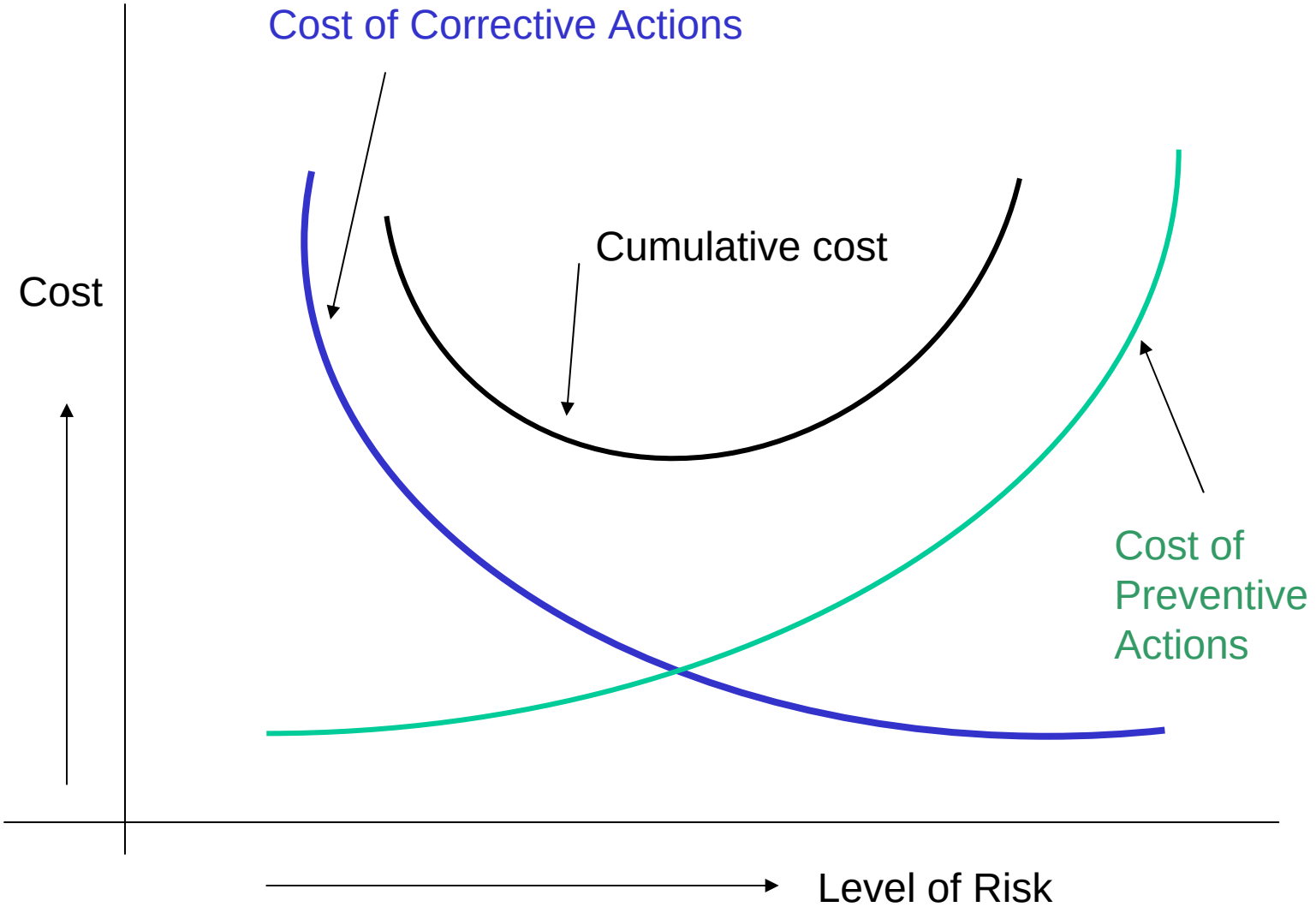
Failure Modes and
Effects Analysis
&
Failure Modes
Effects and Criticality Analysis

Common Cause Analyses
(Includes Zonal and Particular Risks Analyses

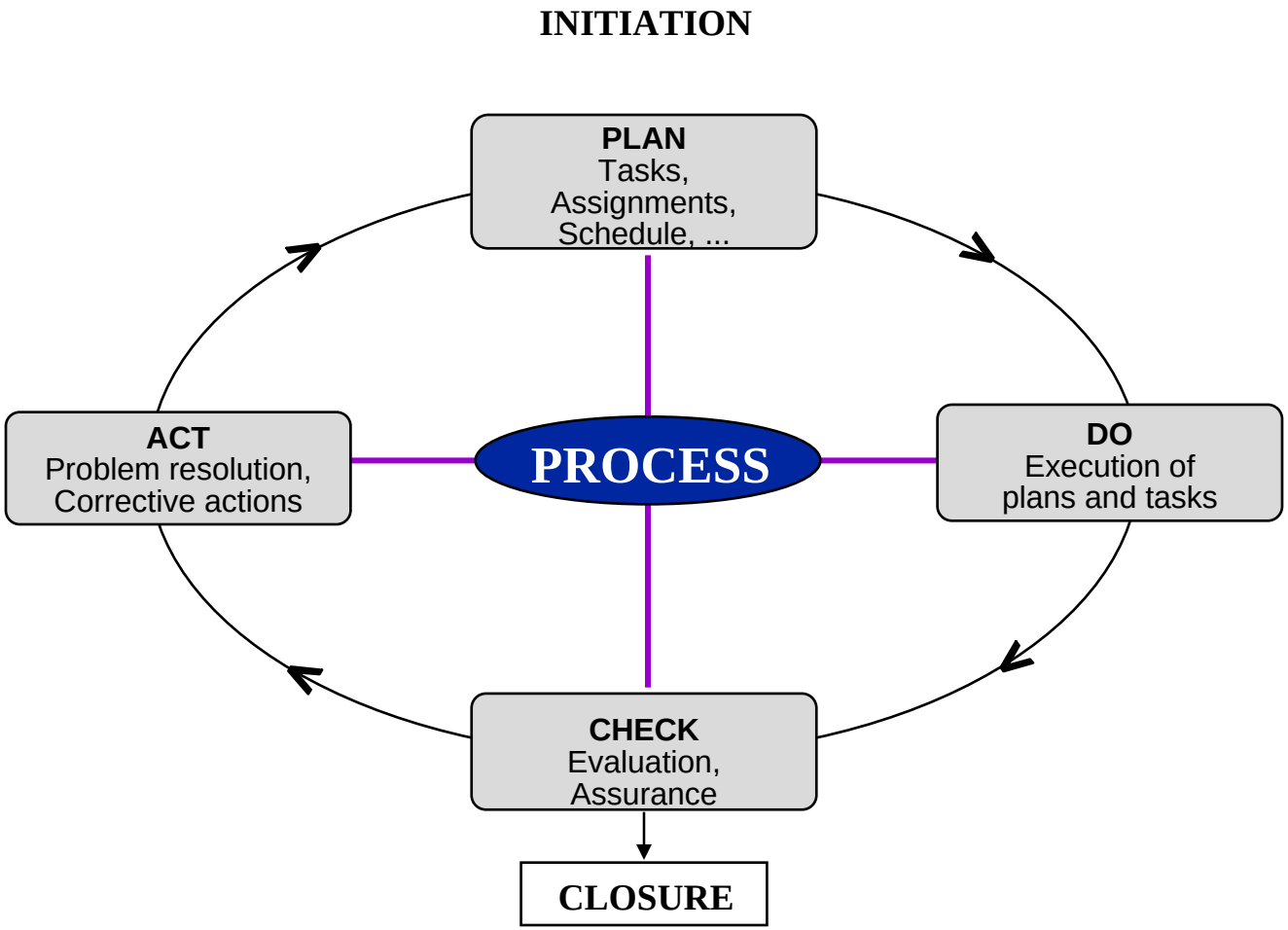
Architecture, Safety and Cost

- Architecture that can mitigate system level concerns may allow you to reduce the criticality of the article which in turn saves money.
- Architectural mitigations include:
  - Partitioning
  - Wrappers
  - Safety monitors
  - Backup and redundancy

Balance Between Risk and Cost

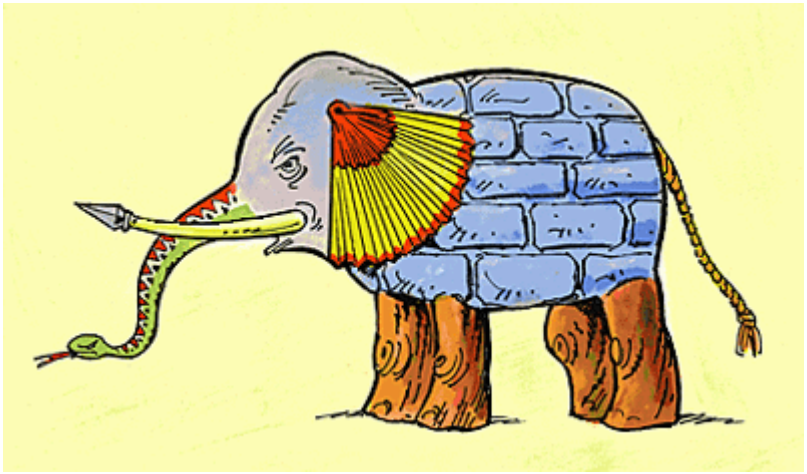


Closed Loop Engineering



The Reductionism Problem

Misunderstood technical requirements or work assignments can result in unintended results



Assurance methods must be capable of demonstrating that no such misunderstanding has taken place

The Human Side of Safety

Engineering design with large safety margins lead to higher costs.

Organizational desire to lower costs result in shrinking safety margins.

Conception and building of the system

System Operation

System Maintenance

Remember – There is Another Cost of Safety

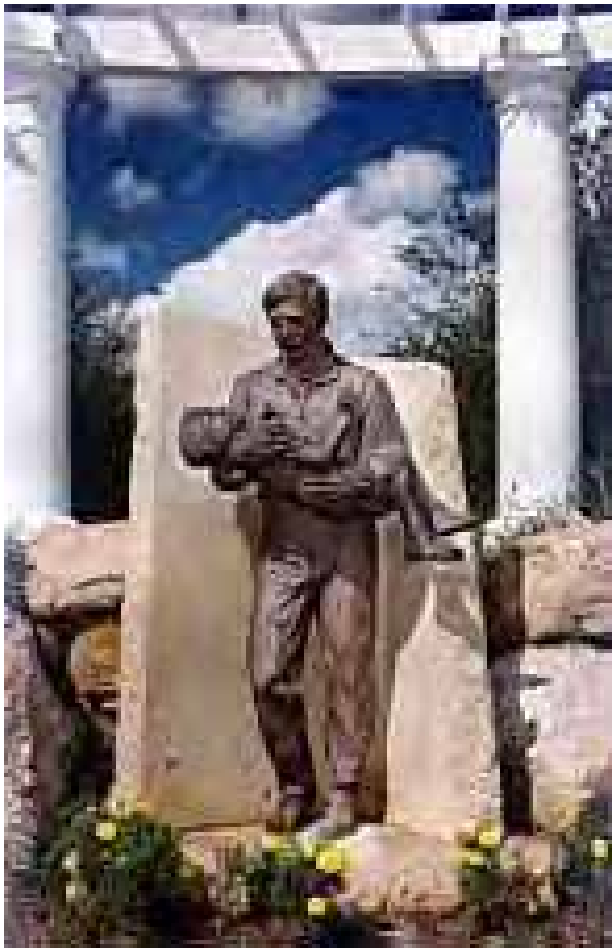
- End User Effects
  - Fatality
  - Injury
  - Permanent Disability
- Repair/Replacement of property destroyed
- Time/money spent in accident investigation process
- Litigation costs
- Others
  - Public Relations
  - Recruiting/Retention
  - Future Business

Aeroperu 603 Revisited

- So was Aeroperu due only to bad maintenance practices?
- Think about:
  - Human Interface Design
  - Overall Aircraft Design
  - Overall Airspace System Design
- Next few slides highlight other accidents where engineering played a direct role

UA Flight 232

- July 19, 1989
- DC-10
- 112 fatalities out of 229 onboard
- Lost number 2 engine, when the #2 engine blew, it took out the #2 accessory drive section, which took out the hydraulics for the #2 system. And some 70 pieces of shrapnel penetrated the horizontal stabilizer and severed the #1 line and the #3 line, No controllability, no braking power. An amazing performance from the pilot saved many lives.



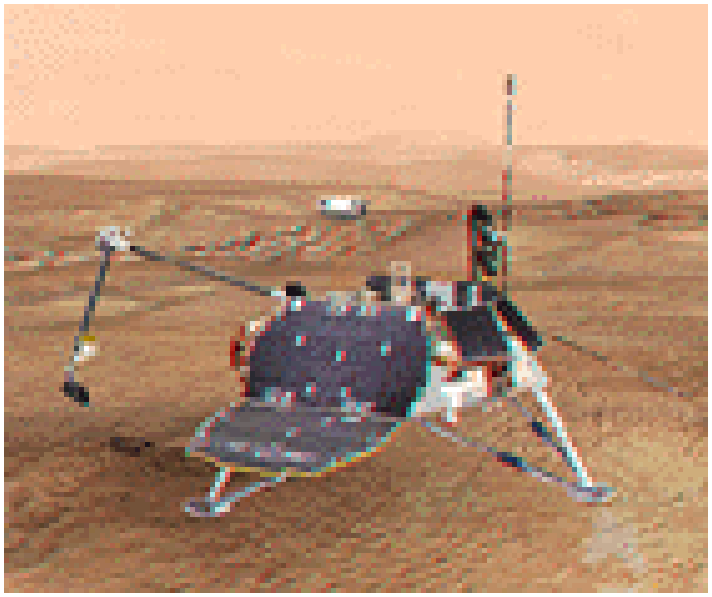
TWA-800

- TWA-800 crashed July 17, 1997 off Long Island.
- Investigation was hampered by the need for underwater recovery operations and numerous conflicting eye witness reports.
- Debris field examination coupled with extensive forensics isolated location of initial mid-air breakup.
- Center fuel tank explosion due to hot fuel and unanticipated ignition source

The investigation of TWA-800 included the most extensive aircraft reconstruction to date.

Mars Polar Lander

- Launched on January 3, 1999. Lost on December 3, 1999
- Tremendous loss of opportunity to know more about Mars.
- Loss of tax dollars.
- An error occurred while processing a directive.
- The error was found to be in the unit conversion between subsystems built by different contractors.

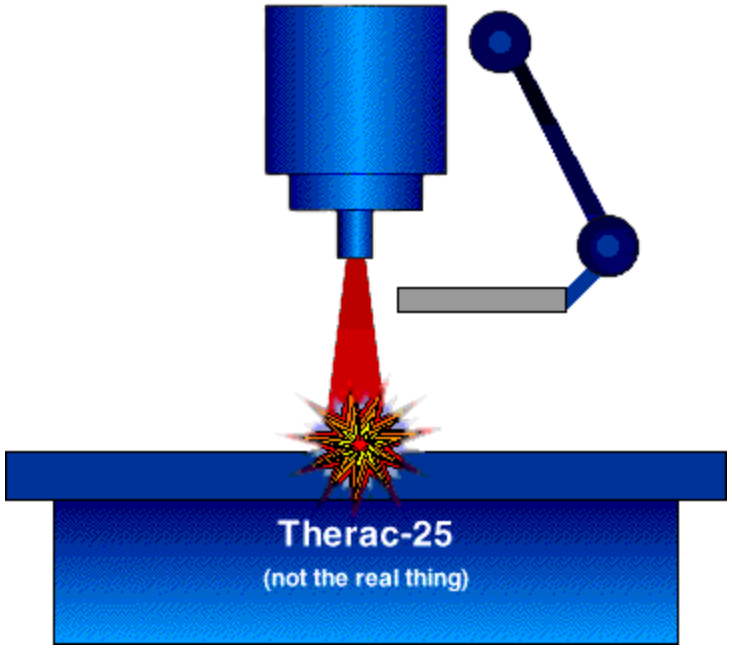


Osprey

- The V-22 Osprey crashed four times during the development and early field trials.
- Three of the four crashes have been traced to design or assembly flaws:
  - Incorrect wiring
  - Engine nacelle design
  - Common point of hydraulic flow coupled with a software design error
- The V-22 illustrates numerous problems associated with not designing for availability, reliability, and maintainability.

Therac-25

- Multiple radiation overdoses including:
  - Kennestone Regional Oncology Center, June 1985 Ontario Cancer Foundation, July 1985
  - Yakima Valley Memorial Hospital, December 1985 and February 1987
  - East Texas Cancer Center March and April 1986
- Primary Causes
  - Software errors
  - Poor software engineering
  - Reliance on poorly built software for interlocking operation
  - Attempts to correct particular design errors rather than putting safeguards



Three-Mile Island Accident

- March 28, 1979
- Partial core meltdown in Unit 2 (a pressurized water reactor manufactured by Babcock & Wilcox) of the Three Mile Island Nuclear Generating Station in Pennsylvania
- Release of up to 481 PBq (13 million curies) of radioactive gases
- Due to inadequate training and industrial design errors (human factors) relating to ambiguous control room indicators in the power plant's user interface
- Accident resulted in enhancements in training, safety procedures, emergency operation, and oversight

Concorde

- The crash on July 25, 2000 represented the 19th tire burst incident in which the aircraft sustained damage beyond the tire itself.
- The crash appears to be the eight incident in which a tire burst was precipitated by **Foreign Object Debris (FOD).**
- NTSB recommendations dating back to 1979 had been ignored by the DGAC, the French equivalent of the FAA.
- Arguably an organizational accident.

The Space Shuttle Challenger Disaster

- An O-ring failing to seal on the Challenger Space Shuttle in 1989 was only a trigger for the disaster.
- Numerous other failures, mostly organizational led to the decision to launch.
- This decision was made over the objections of senior engineers at both Morton Thiokol and Rockwell International.
- Post-event analysis demonstrated conclusively that numerous, basic safeguards failed.

More Examples of Organizational Failures

- **Apollo 13** – maintenance-initiated failure saved by the crew skills.
- **Bhopal** – botched maintenance, improvised bypass pipes, inoperable refrigeration plant, lack of cleaning of pipes etc.
- **Clapham Junction** commuter train accident and collision- failed signals caused by rewiring practices of reusing the insulation tape or not using the tape at all.
- **American Airlines Flight 191**(DC-10), Chicago O'Hare- maintenance practices recommended by McDonnell Douglas were overridden by AA by what was thought to be a more efficient practice for working on the engine pylon.

Safety Culture and the Engineer

- Engineers need to recognize that the engineering discipline is basically a form of social engineering.
- The consequences of engineering decisions must be considered throughout development process.
- Engineering ALWAYS involves tradeoffs – inherent conflict of interest.
- Engineers MUST proactively promote safety including:
  - Substantiating their decisions with technical data
  - Educating their organization and management on potential consequences of engineering/management decisions
  - Working to build a safety conscious organization through ongoing education/mentoring
  - Always maintain a questioning attitude – safety is NEVER automatic!
  - BE WILLING TO TAKE A STAND!

Engineering Ethics

- When you are faced with making a determination as to whether something is good enough answer four fundamental questions:

1. Would I be willing to defend my position in a court of law including answering whether what I am accepting represents best practice in industry?
2. Would I be able to stand up to the questioning of a determined ’60 Minutes’ reporter doing an exposé story on the latest death-inducing system failure?
3. Will I be able to sleep at night after signing for this data?
4. AND – Would I be willing to expose my wife/husband, children or parents to this system?