



Mission Success Starts with Safety

**19th International System Safety Conference
Huntsville, Alabama
September 11, 2001**

**Michael A. Greenfield, Ph.D.
Deputy Associate Administrator
Office of Safety and Mission Assurance**

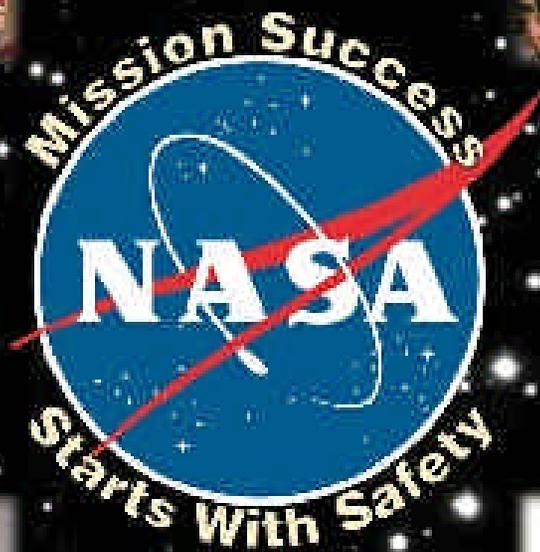
*Protecting the Public, Astronauts and Pilots, the NASA Workforce, and
High-Value Equipment and Property*



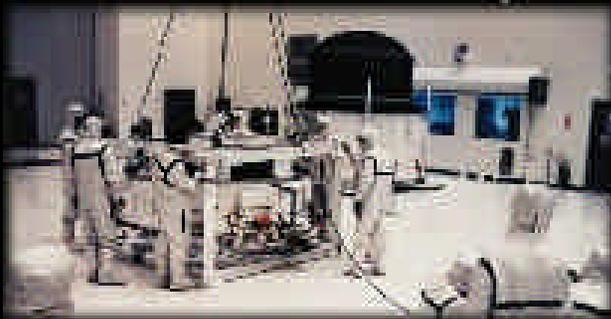
Public



Astronauts and Pilots



<http://www.hq.nasa.gov/safety>



NASA Workforce



High-Value Equipment and Property



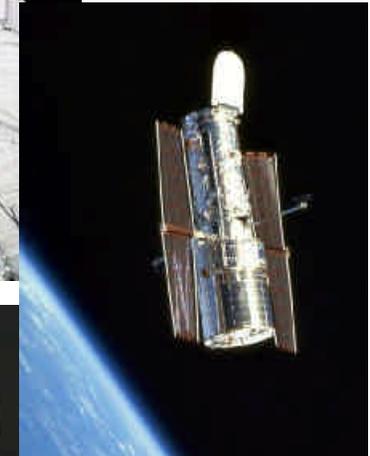
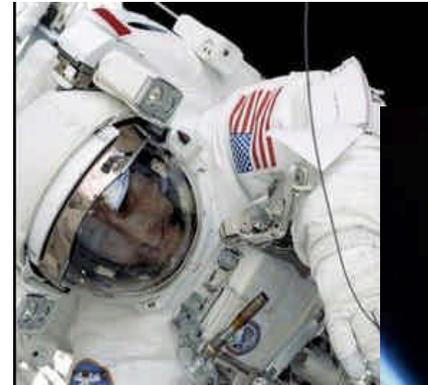
Overview

- **There's a lot at stake**
- **Theory behind incidents and accidents**
 - H. W. Heinrich
 - James Reason
 - Charles Perrow
- **NASA's "Risky Business"**
- **A new approach -- "Design for Safety"**
- **Summary**



There's a Lot at Stake

- Human life
- One-of-a-kind hardware
- Scientific knowledge
- International cooperation in space



An accident could have unbelievable consequences.

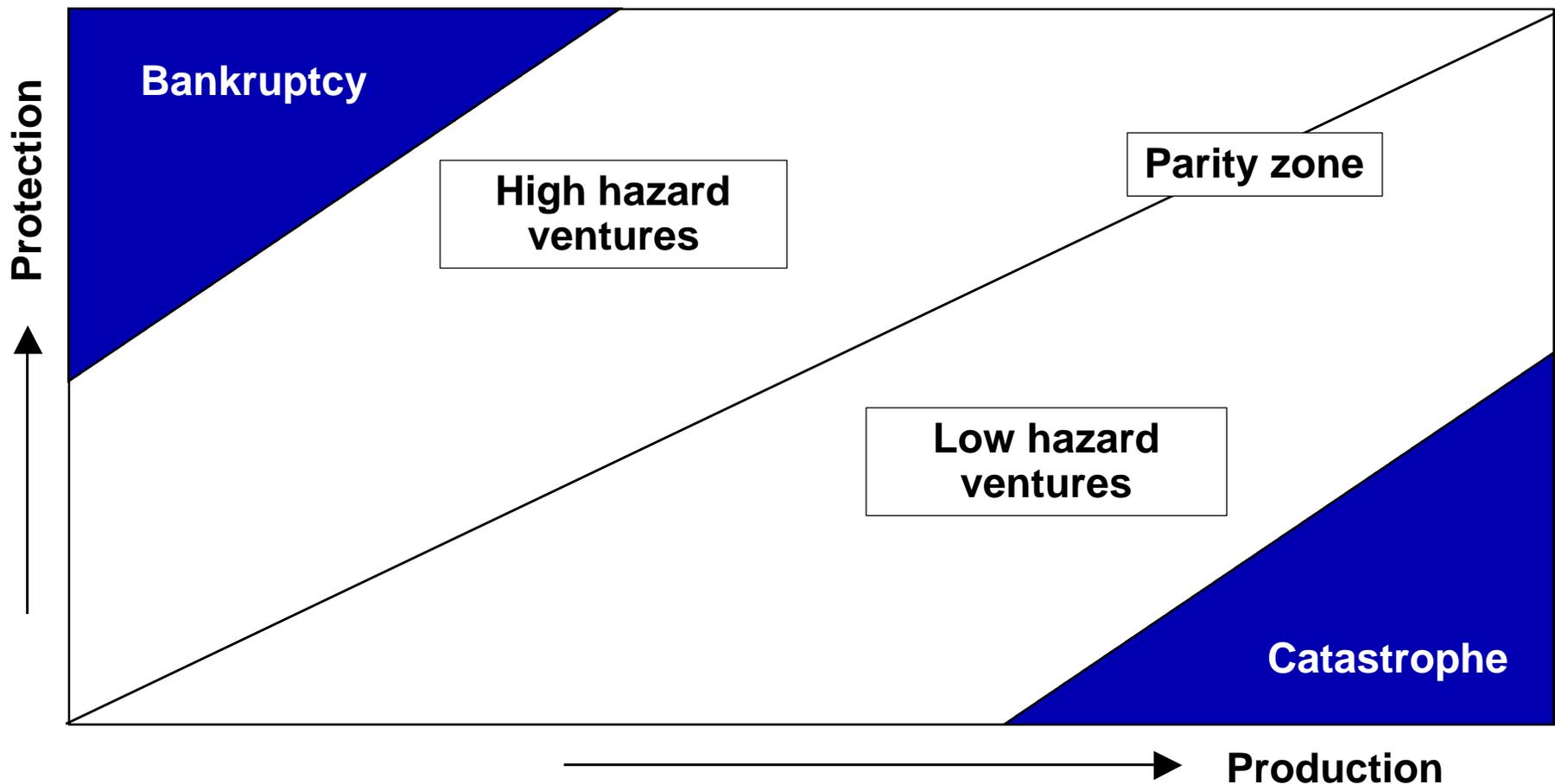


“If eternal vigilance is the price of liberty,
then chronic unease is the price of
safety.”

- James Reason, “Managing the Risk of Organizational Accidents”

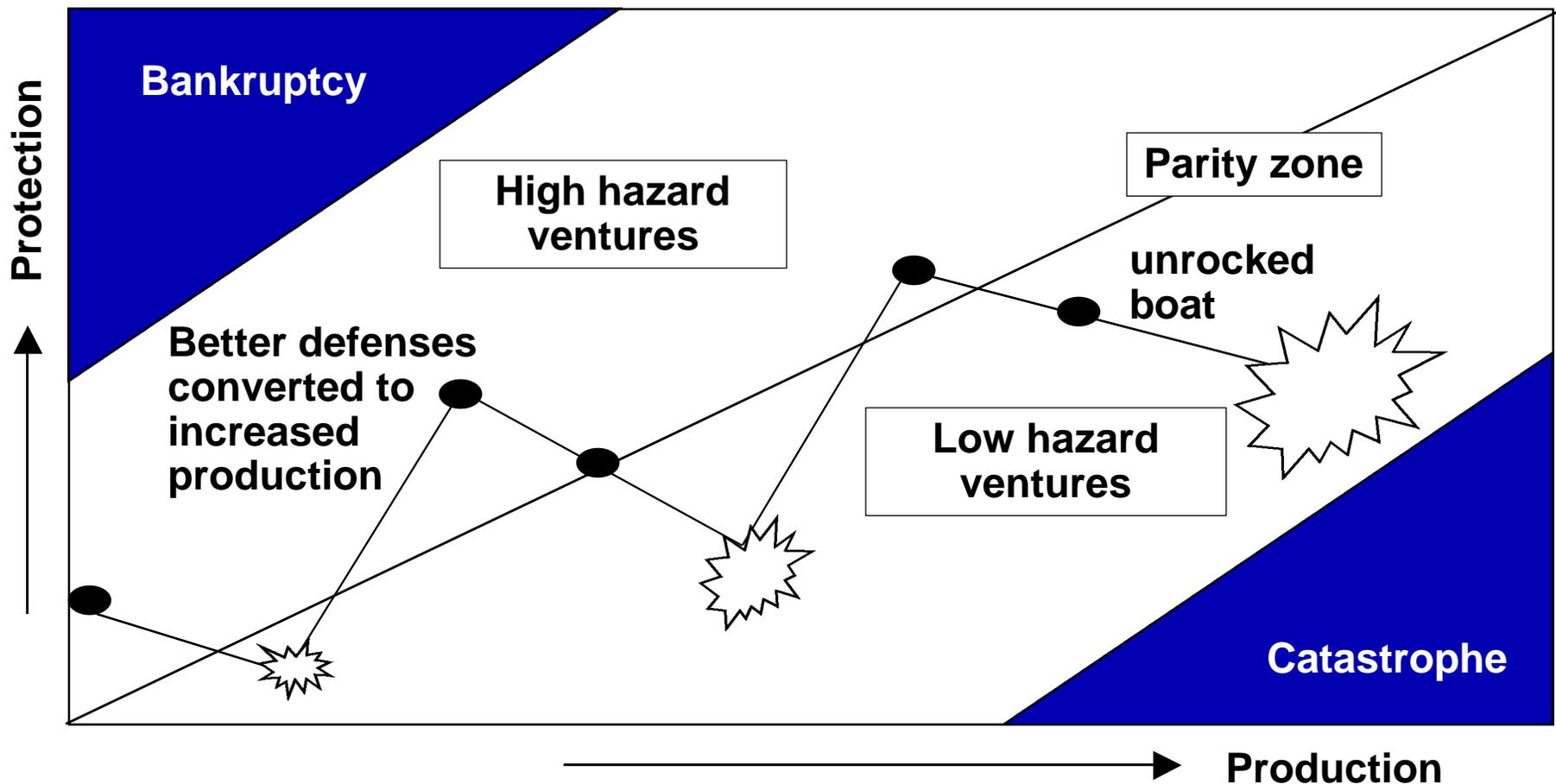


The Relationship between Production and Protection





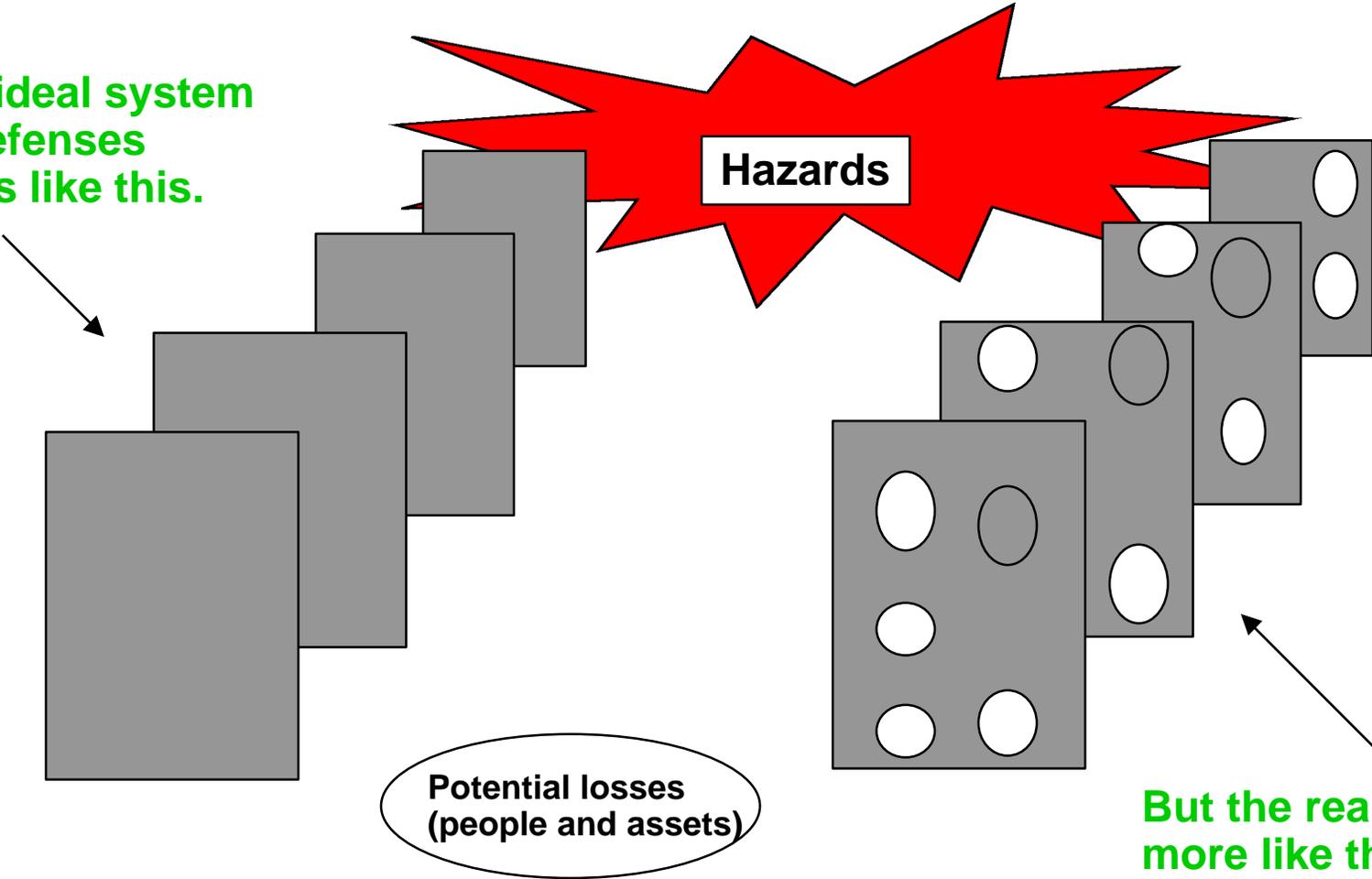
The Relationship between Production and Protection





Defenses are Never Perfect

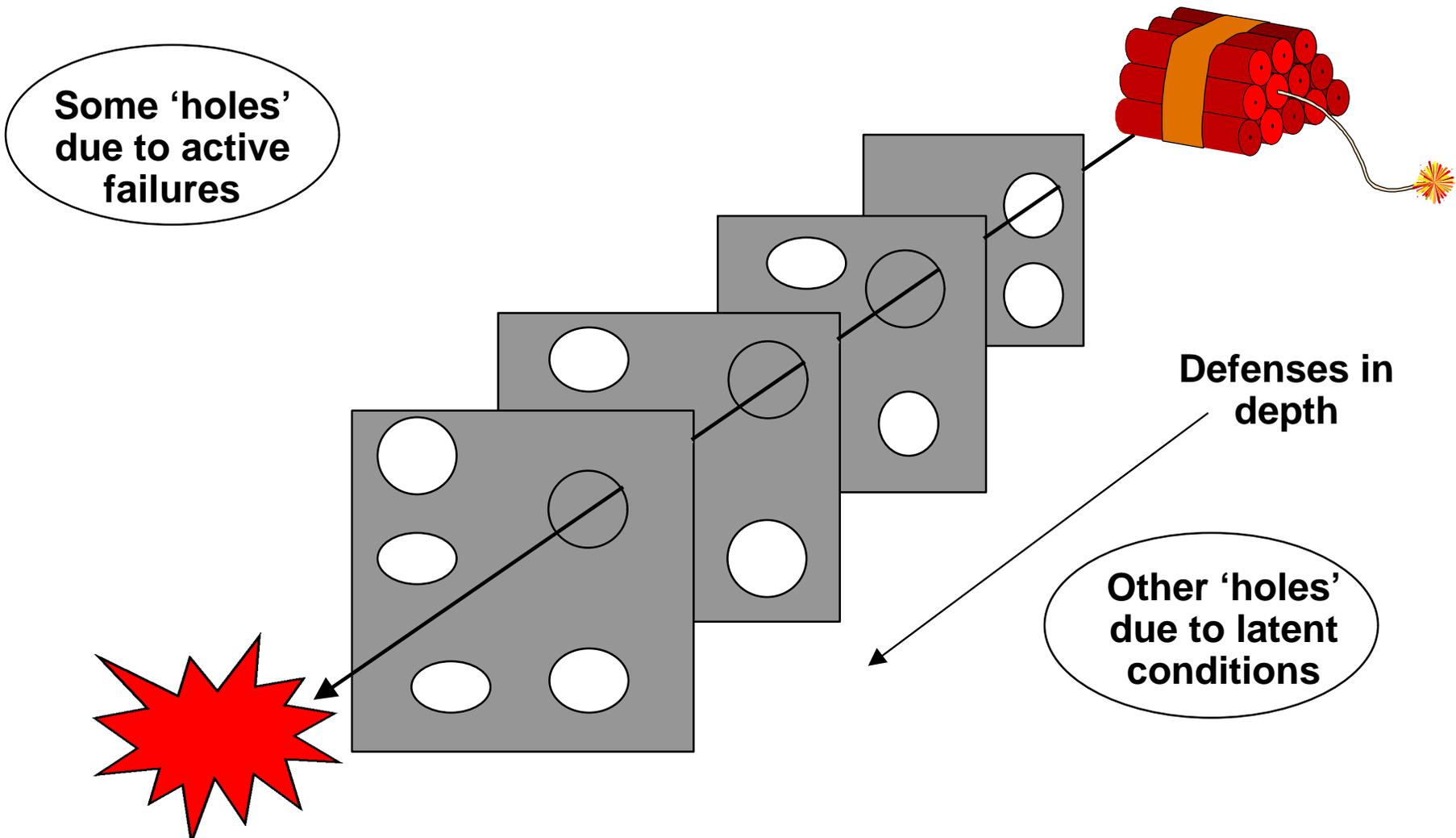
Our ideal system of defenses looks like this.



But the reality is more like this.



When Everything Lines Up Just Right, the Consequences Can Be Devastating





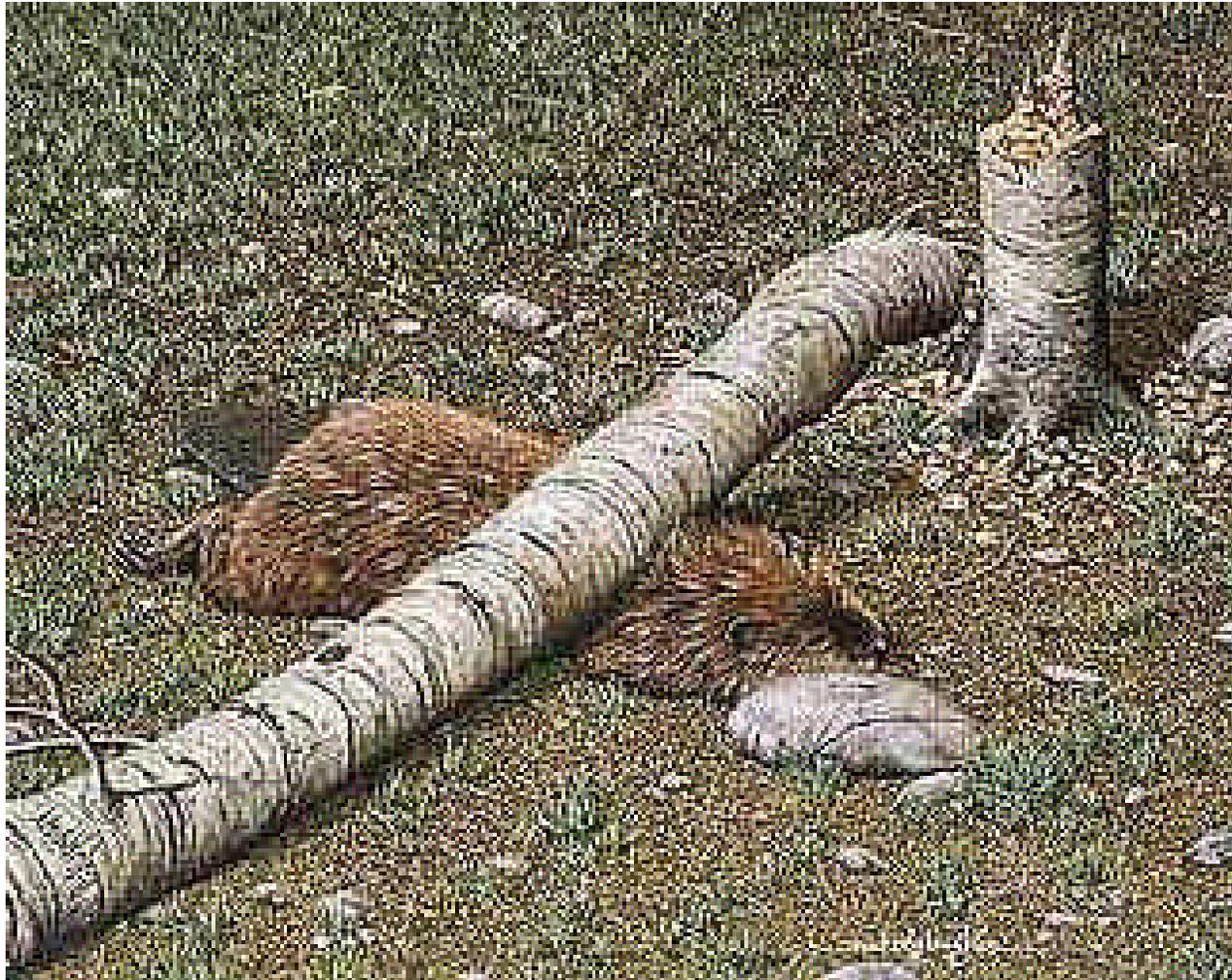
The Risky Environment of Aeronautics and Space Provides Distinct Challenges

- 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.”



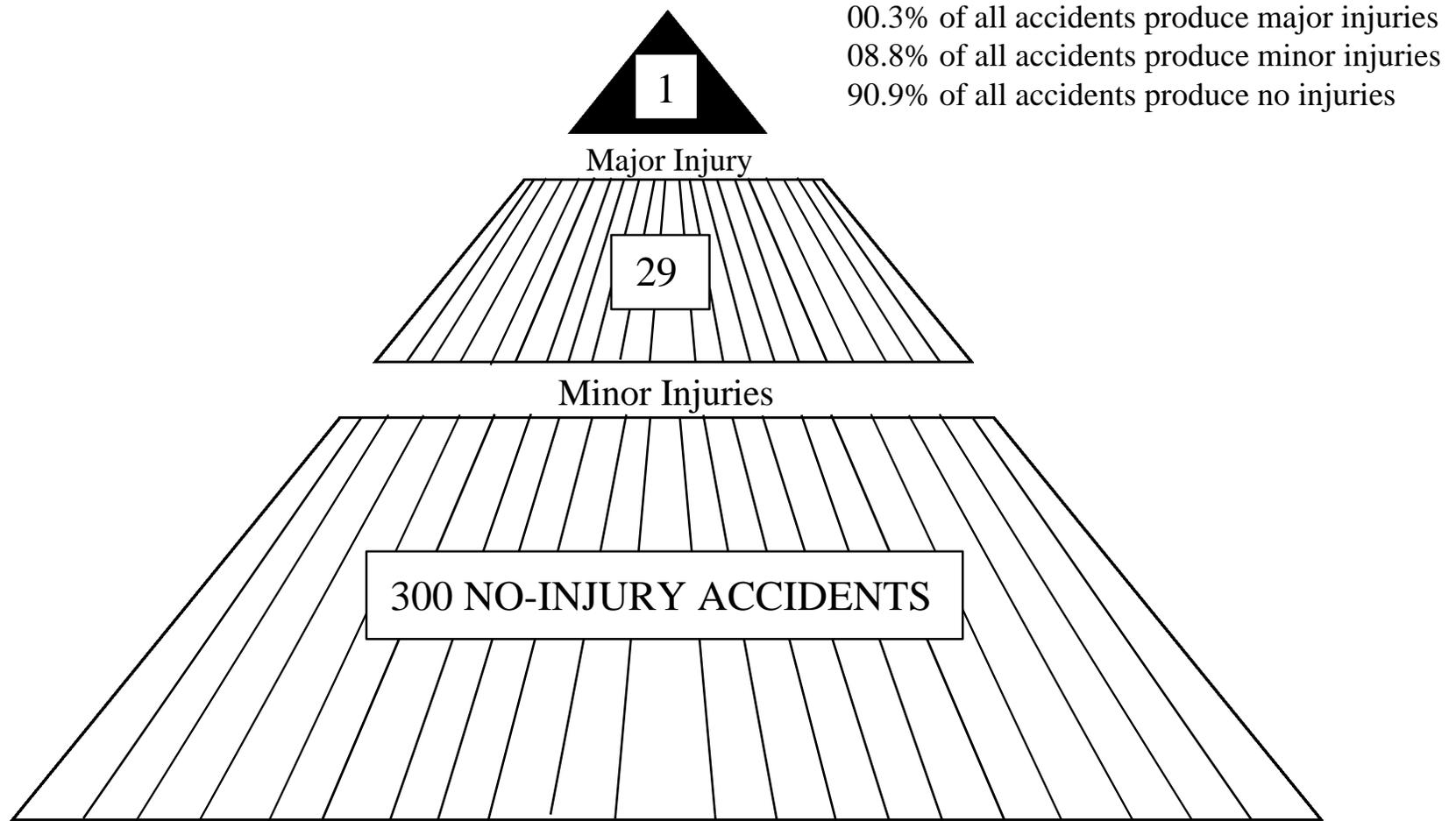
Even Routine Tasks Have Some Risk*



*Note: No beavers were harmed in making this chart.

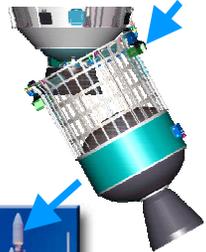


Incidents and Close Calls Provide an Indication and Warning of Vulnerability





Some Examples

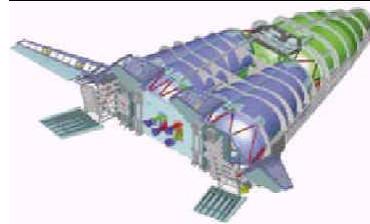


Connector Separation Failure

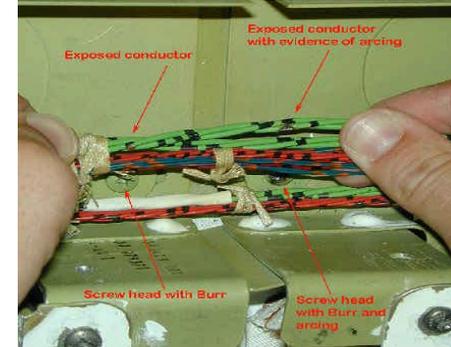


Titan IV

April 99, Inertial Upper Stage



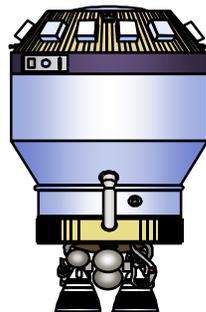
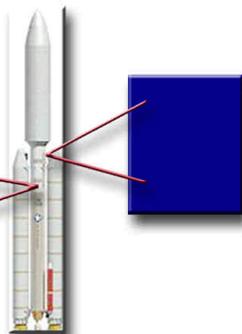
X33 LH2 Tank Test Failure



STS-93 AC1 short



Aug 98, Titan IV Wiring Short



Centaur

April 99, Wrong Roll Rate Filter



SSME Test Engine Failure (Tape Contamination)



STS-93 SSME Coolant Tube Damage



Today's Safety Challenges

- **Today's Challenge**
 - **Increased mission complexity is needed to meet ambitious goals**
 - **Safety critical interactions increase as the complexity of highly integrated systems increases**
 - **Increased resource constraints**
 - **Attrition and retirements are removing a generation of experience from the ranks of managers, engineers, and operators**
 - **Hardware platforms are often out-lasting their designers**
 - **Pressure to “do more with less”**
 - **Faster, Better, Cheaper**
 - **Increased expectations: the safety bar raises every year**



A Systems Approach is Needed

- **Traditional Methods can not handle system complexity**
 - **System de-coupled => only components and subsystems addressed**
 - **Static, rule-based, deterministic process**
 - **Design phase: does not address dynamic and probabilistic nature of the world**
 - **Operations: depends on humans to reason and react to the unexpected**
 - **Risk not explicit in trade space: generally external to the main processes**
 - **Knowledge resides in people**
- **But, safety is a system characteristic:**
 - **Dependent on the frailty of components, subsystems, software, interactions, organizations, and human behavior**
 - **Continuously variable throughout the entire life-cycle**



Design for Safety

“Design for Safety” is the technology component of the Agency’s response to these challenges.

Recently renamed

“Engineering for Complex Systems”



Engineering for Complex Systems

Vision

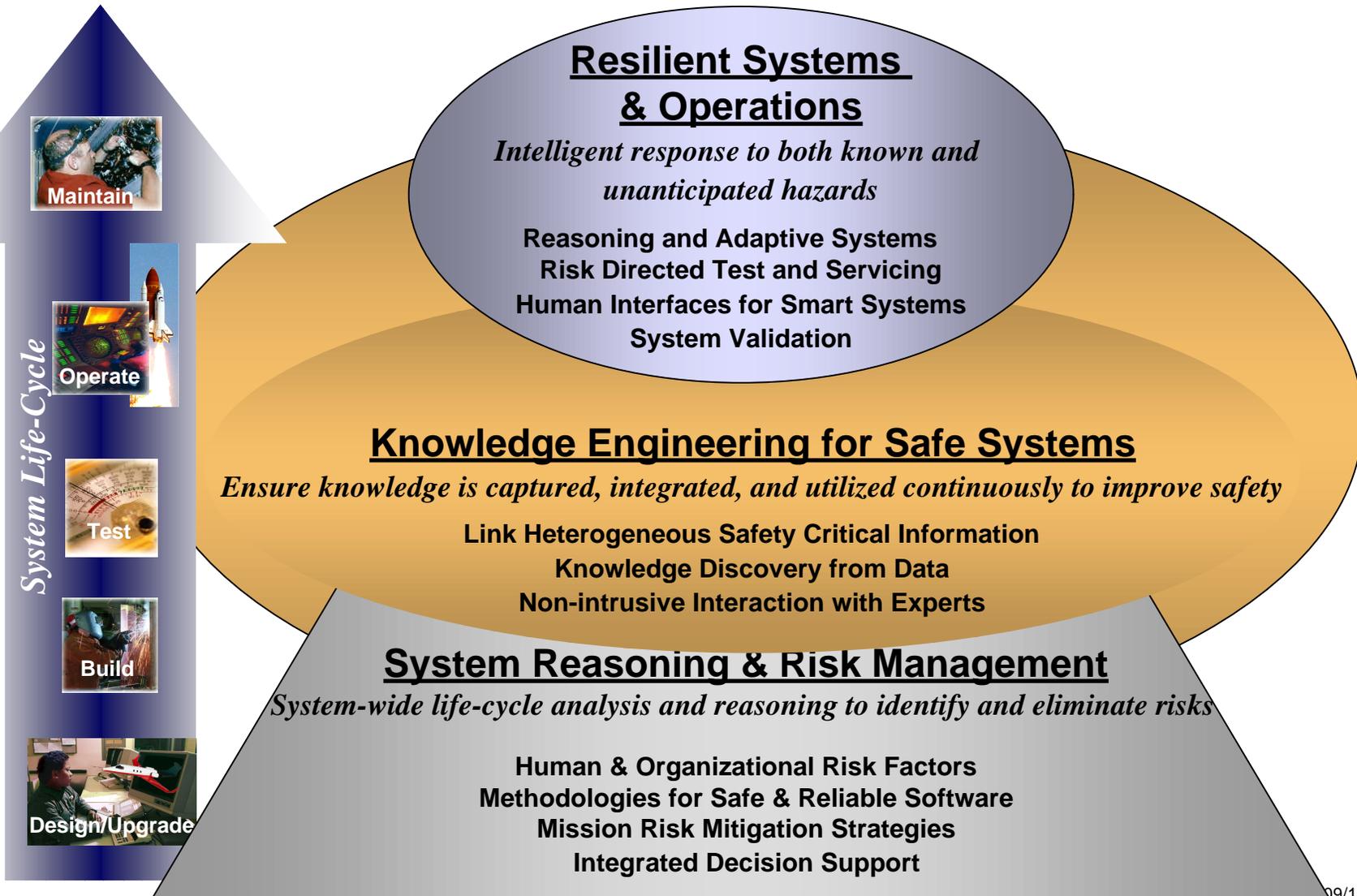
- Achieve ultra-high levels of safety and mission success by fundamentally advancing NASA's system life-cycle approach through the infusion of advanced information technologies.

Goals

- Develop advanced information science and technology methods to quantitatively assess risk and to enhance existing processes to continuously mitigate risk.
- Tailor, mature, and infuse this technology into all NASA Enterprise development processes.

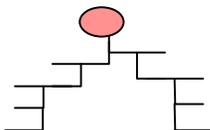
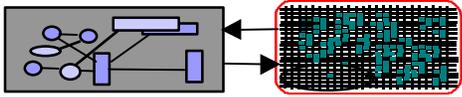
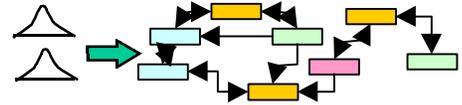
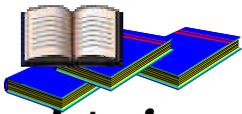
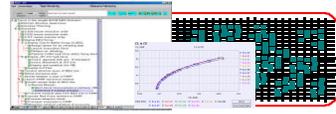
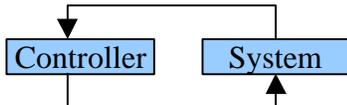
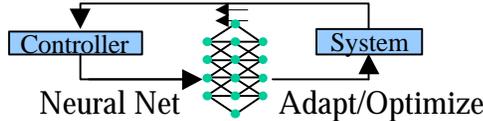
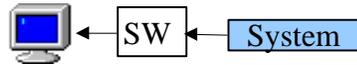
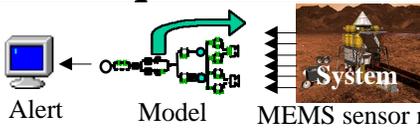


Engineering for Complex Systems Major Thrust Areas





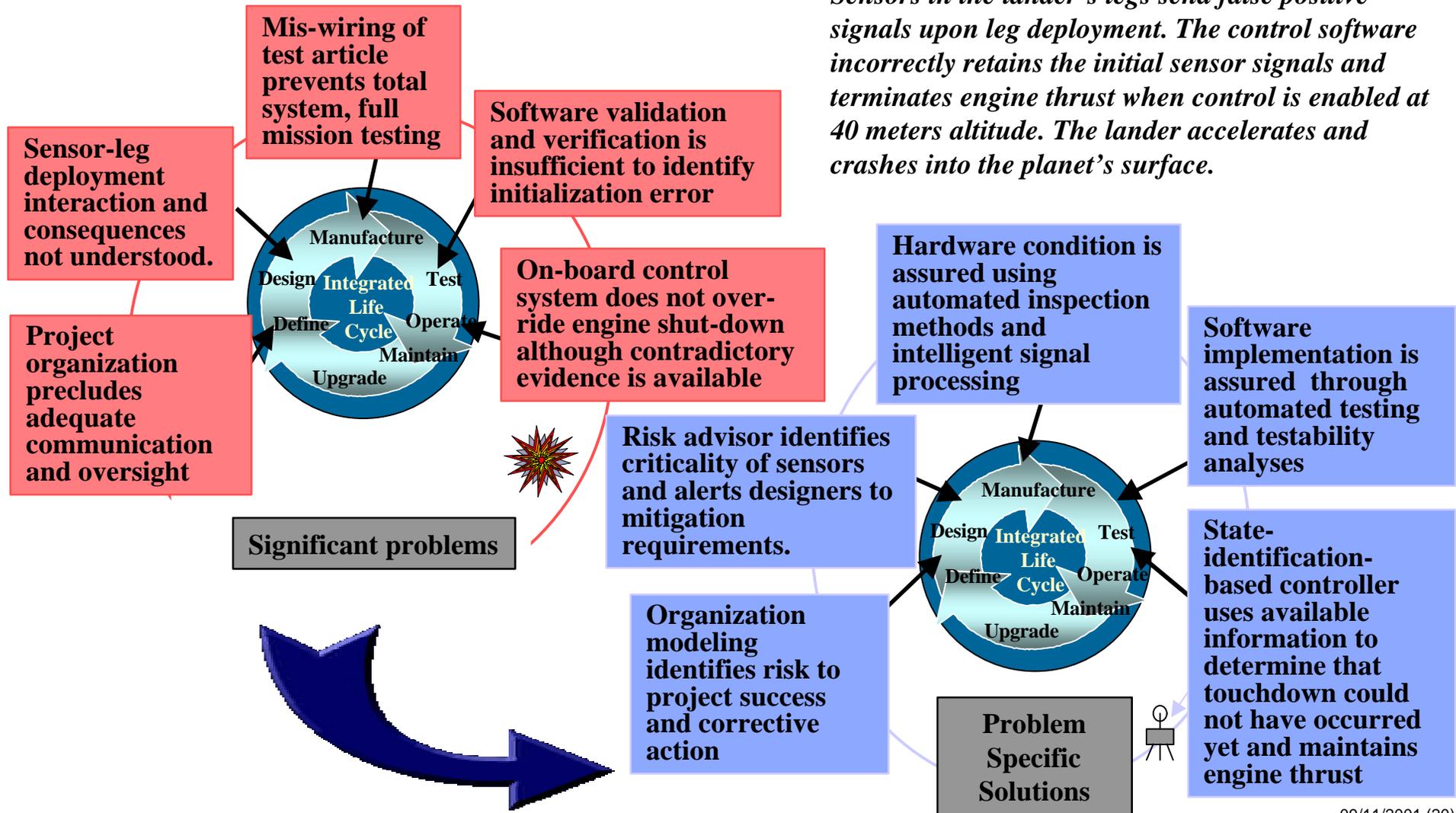
Engineering for Complex Systems Envisioned Improvements

	Current	ECS
Risk ID & Analysis	 <i>Static, sporadic, subjective</i>	 <i>Dynamic, systematic, model-based</i>
Org. Risk Factors	 <i>Heuristic, qualitative</i>	 <i>Model-based, quantitative</i>
Knowledge	 <i>Incomplete, inaccessible</i>	 <i>Extensive, mapped, mined, active</i>
Robust Control	 <i>Brittle, manual</i>	 <i>Adaptive, autonomous</i>
Health Monitoring	 <i>Fixed threshold alert</i>	 <i>Reasoned capability diagnosis</i>



Case Study: Mars Polar Lander

Sensors in the lander's legs send false positive signals upon leg deployment. The control software incorrectly retains the initial sensor signals and terminates engine thrust when control is enabled at 40 meters altitude. The lander accelerates and crashes into the planet's surface.





In Summary

- **Although theory suggests that accidents are inevitable in complex, tightly coupled systems--NASA believes that engineering, organizational design, and management can prevent all accidents.**
- **Accordingly-- we're attacking the potential for accidents by:**
 - **Analyzing incidents and close-calls to obtain insight into the unexpected, the unplanned, and the unimaginable.**
 - **Employing classic System Safety and Risk Management to prevent, find, eliminate, and control hazards.**
 - **Using advanced information technologies (Design for Safety) to enable designers, operators, and the systems themselves to be knowledgeable enough to prove the theory wrong.**