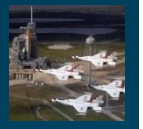
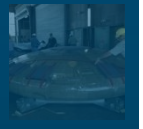
National Aeronautics and Space Administration








The Case for Safety

The North Sea Piper Alpha Disaster

Senior Management ViTS Meeting

May 2013

Terry Wilcutt
Chief, Safety and Mission Assurance

Tom Whitmeyer
Deputy Chief, Safety and Mission Assurance

This and previous presentations are archived at
nsc.nasa.gov/articles/SFCS

The Risk-Informed Safety Case (RISC)

- Program/project SMA has operated under paradigm of assurance (audit, inspection, oversight, insight). Good, but more can be done.

- New flight systems developed by NASA and under Space Act Agreements can benefit from a systems safety approach that *uses evidence to establish safety goals and a minimum threshold of safety*—the RISC.
- As a system matures, the initially-established minimum threshold of safety can and should move toward a full realization of safety goals—a "prove it's safe enough" approach.
- A 1988 mishap in the petroleum industry inspired change toward a similar paradigm—called "process safety" today…

WHAT HAPPENED and WHY

July 6, 1988, Piper Oilfield, North Sea: As shifts changed and the night crew aboard Alpha Piper assumed duties for the evening, one of the platform's two condensate pumps failed. The crew worked to resolve the issue before platform production was affected. But unknown to the night shift, the failure occurred just hours after a critical pressure safety valve had just been removed from the other condensate pump system and was temporarily replaced with a hand tightened blind flange. As the night crew turned on the alternate condensate pump system, the blind flange failed under the high pressure, resulting in a chain reaction of explosions and failures across Piper Alpha that killed 167 workers in the deadliest offshore oil industry disaster to date.

Proximate Cause: condensate leak following Lock Out/Tag Out (LOTO) procedure failure

- Safety permit system allowed simultaneous tasks on system interfaces (safety valve and blind flange)
- No central way to control maintenance on the system or know the detailed status of critical components.

Drilling platform design: new gas production module

- The original modular design separated hazardous areas.
- 1978: Gas Compression Module (GCM) was built next to Piper Alpha's control room; the effects on safe operation were not understood.
- GCM fire drove control room evacuation and decapitated emergency response communication;
- Crew was blocked from lifeboat escape by fire and retreated to living quarters to await orders that never came; they died there or jumped into the sea. 59 of 226 were rescued and lived.

Organizational Culture: maintain oil and gas flow, cut short-term costs

- Understaffed and inexperienced crew under production pressure; shortcuts and workarounds to the permit-to-work system were normal. Failed to learn from 1987 LOTO fatality.
- Minimal inspections; little attempt to identify systemic issues.

AFTERMATH

- 1990: **Public Inquiry into the Piper Alpha Disaster** by Lord Cullen made 106 historic recommendations, all adopted by government regulators and the UK oil industry. The key recommendation: a requirement to submit a safety case to the UK Health and Safety Executive.
- Since 1992, the owner/operator of every fixed and mobile installation operating in UK waters must demonstrate that safety management systems are in place, risks are identified and reduced to as low as reasonably practical (ALARP), management controls on the system are in place, and provisions for temporary safe refuge as well as safe evacuation and rescue are in place. As major changes are made to the system, the safety case must be updated.

Is the Safety Case Effective? Necessary?

- History tells us that, like other control measures, a safety case is only as good as the commitment made to its preparation and implementation. A poor quality safety case was found causal to the 2006 RAF Nimrod crash, killing all 14 crew members. See our case study "Safe Anyway" for details.
- NASA embraces system safety assessment in NPR 8715.3C, NASA General Safety Program Requirements. Tools such as hazard analysis, failure mode and effects analysis, and probabilistic risk assessment have provided assurance to a great degree. But a performance-based approach can identify risks at the entry level, at the very assumptions which underpin traditional assurance methods. The RISC is such a holistic approach.

INFORM YOURSELF

- **Risk-Informed Safety Case:**
  "A risk-informed safety case is a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is or will be adequately safe for a given application in a given environment. This is accomplished by addressing each of the operational safety objectives that have been negotiated for the system, including articulation of a roadmap for the achievement of safety objectives that are applicable to later phases of the system life cycle.
- The term 'risk-informed' is used to emphasize that a determination of adequate safety is the result of a deliberative decision making process that necessarily entails an assessment of risks and tries to achieve a balance between the system's safety performance and its performance in other areas."
- Download the NASA System Safety Handbook and learn more!