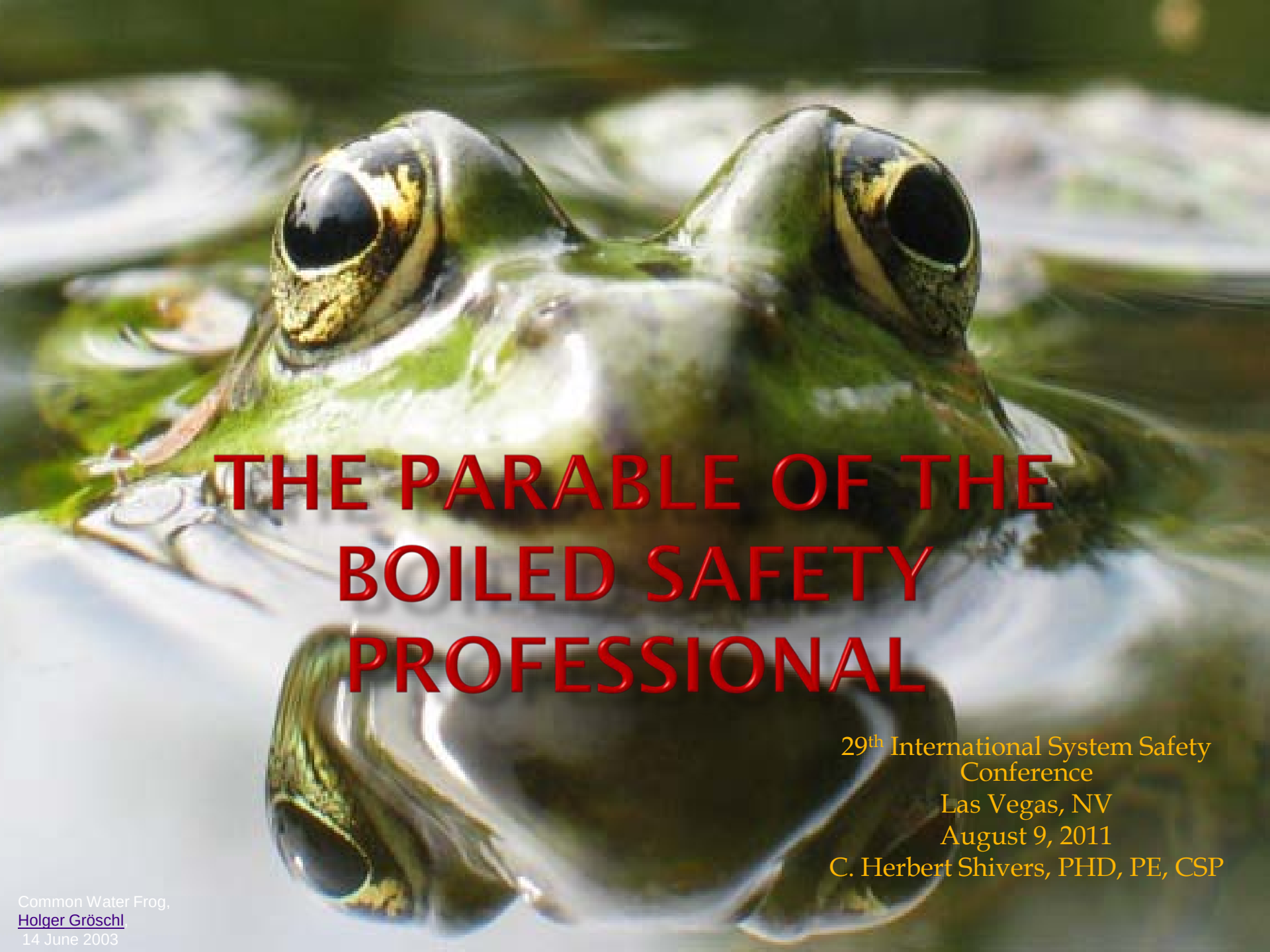
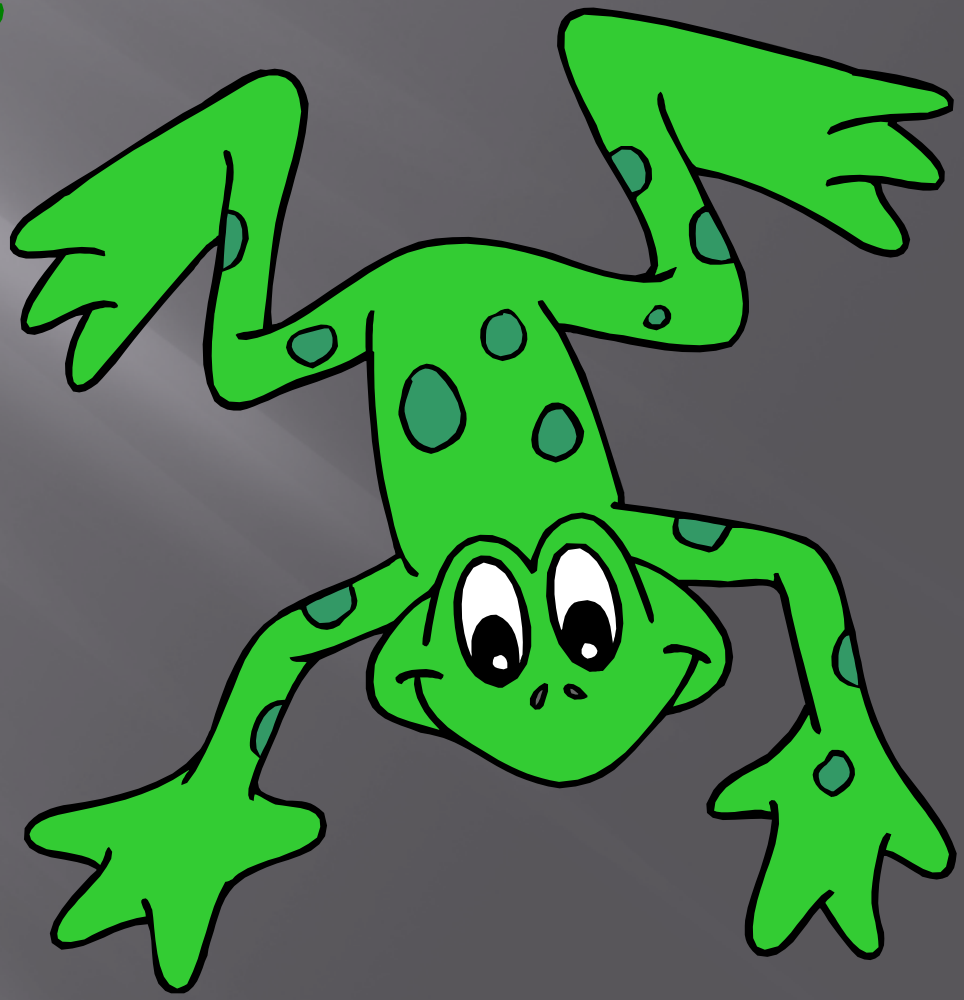


THE PARABLE OF THE BOILED SAFETY PROFESSIONAL

29th International System Safety Conference
Las Vegas, NV
August 9, 2011
C. Herbert Shivers, PHD, PE, CSP

Common Water Frog,
Holger Gröschl
14 June 2003

The Parable of the Boiled Frog



Phrases related to the idea

- “Latent conditions,” James Reason
- “Drift to Failure,” Sydney Dekker
- “Normalization of deviance,” Diane Vaughan
- Reason also said, “If eternal vigilance is the price of liberty, then chronic unease is the price of safety.”

Drift to Failure

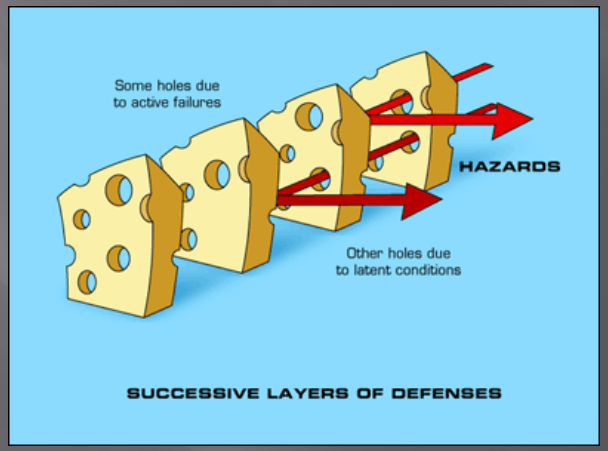
- Dekker - … "drift to failure" is the greatest risk to today's safe socio-technical systems.
- "Drifting to failure" is a metaphor for the slow, incremental movement of systems operations toward (and eventually across) the boundaries of their safety envelope .
- People within the system do not recognize the drift because of decisions made with incomplete knowledge in the face of competition, scarcity, etc.

Background

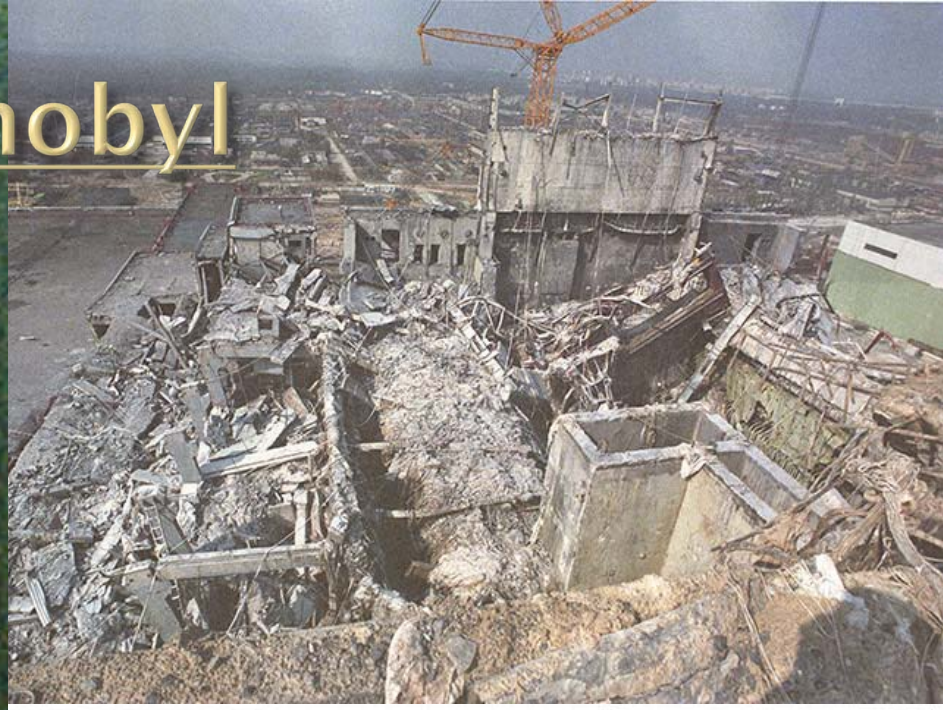
- How do we know that we are drifting toward failure? What data or metrics exist that we can rely on to make sure that we avoid making the decisions or doing the things that take us along that path to failure?
- Do we rely on doing the best we can and serendipity to get us there?
- Serendipity might help us, we certainly should not base a strategy on it.
- Is there a model for measuring this drift? Do we need such a model?

Determining Drift

- In the spirit of Reason's Swiss Cheese model, what happens when we make decisions regarding our design and engineering rigor ?
- Do we make the holes in the cheese larger, shift the position or alignment of the holes, or create more holes, or make the holes smaller or fewer?
- We need to focus on decreasing the total amount of permeability in the barrier rather than the alignment.
- We shall focus on the "dark side" of Swiss Cheese hole alignment for purposes of this discussion, that is, things that go wrong.



Chernobyl

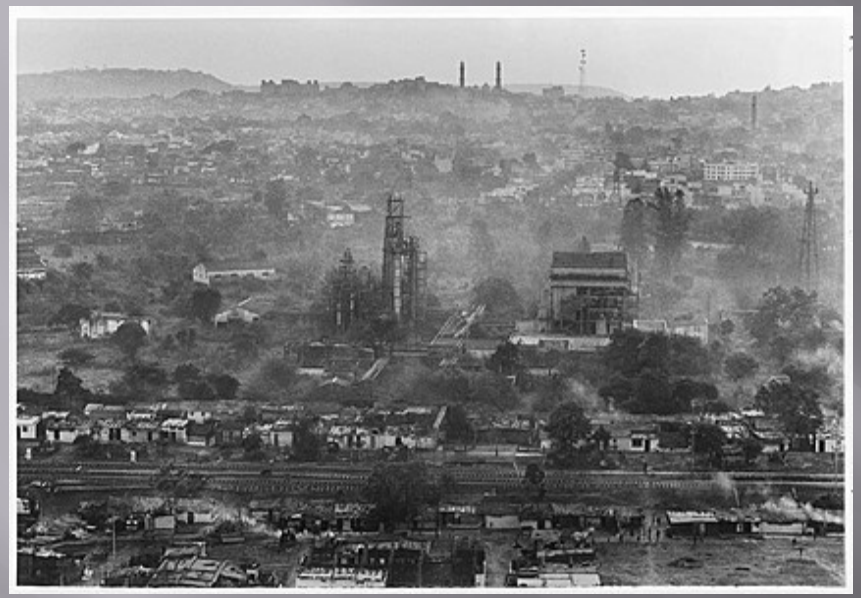


DC-10 Cargo Door System

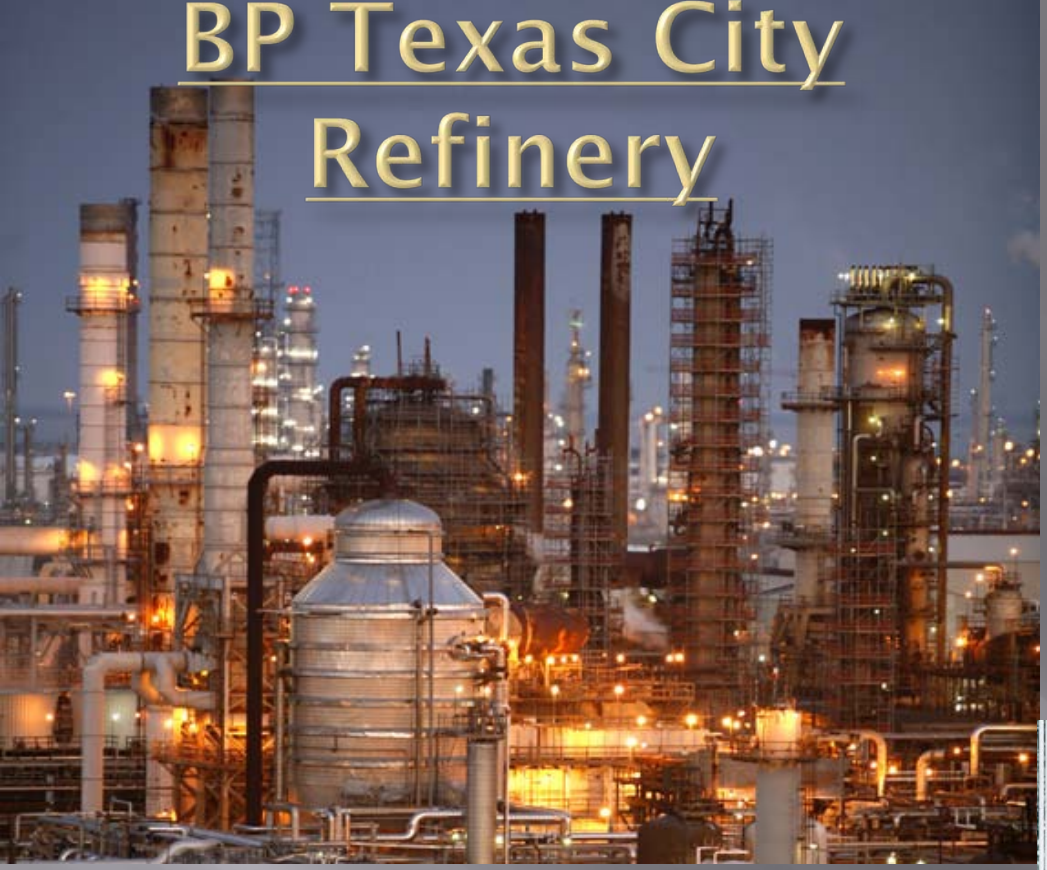
By strange coincidence, a few weeks before the Paris crash, British solicitor Bernard Engler photographed the commanding sight of a Turkish Airlines DC-10 at Heathrow Airport. He would later become actively involved in the litigation.
BERNARD ENGLER

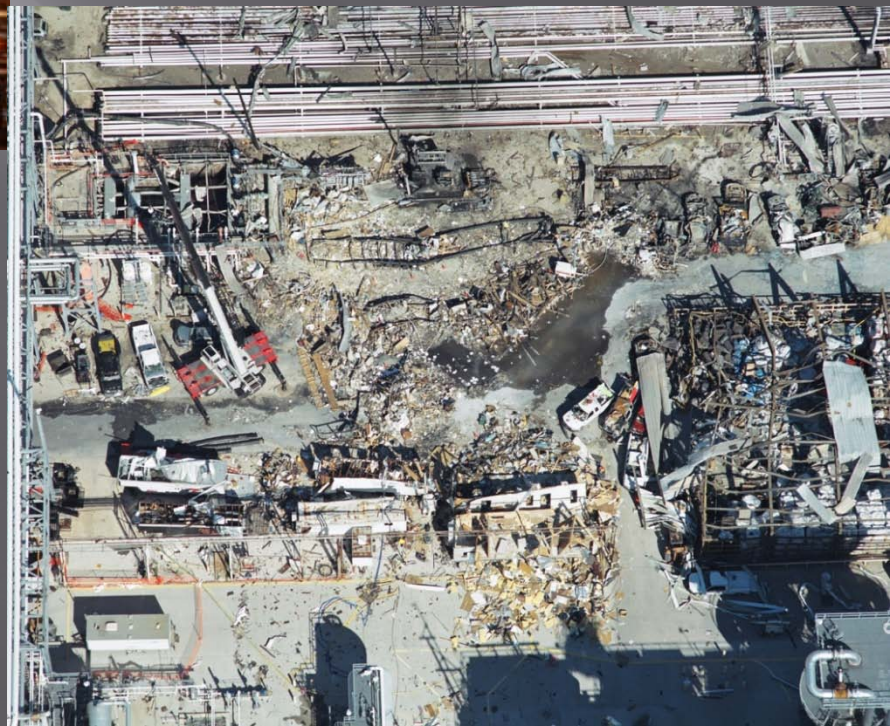
This section of fuselage was the largest remaining section of the plane. JAMES ANDANSON/SYGMA

Bhopal



BP Texas City Refinery





The USS Thresher

TWA 800 In-Flight Breakup

Soyuz-11 Depressurization

Minneapolis Bridge Collapse

The Valero Refinery Fire

X-31 Mishap

Design Considerations

- Consider environmental effects on a process, especially when environmental changes are intermittent or cyclic rather than constant.
- Calculate actual energy releases possible within a system to be realistic when estimating safety margins.
- Include 'damage control' capability into the system where mass and other considerations allow.
- Complex systems can defeat attempts to ensure comprehensive human understanding of designs.
- Eliminate common cause failures through proper design for failure tolerance and appropriate analysis of accident scenarios.
- Provide sufficient resources (funding, education, expertise) for a proper design review.
- Develop controls that detect and correct latent conditions in unused equipment or facilities.
- Isolate sources where high energy release potential exists, to contain component or assembly failures from initiating a chain reaction leading to system failure.
- Design intent can be inadequately communicated or misinterpreted as the design progresses through its life cycle.
- Products in the concept phase of the project life cycle should account for the effects of age and include a means to later analyze the system's integrity.

Test Considerations

- Design engineers must test critical components versus worst case off-nominal events to uncover single-point failures.
- Aggressively test critical hardware/software systems in nominal and off-nominal operational regimes to flush out latent design defects and test assumptions.

Analysis Considerations

- Prove a system is safe. Actual system performance is indifferent to human assumptions.
- Use a systematic approach and technical expertise appropriate to the task.
- Rigorously apply analyses and properly interpret the results.
- Conduct and verify hazard analyses to determine where and how hazards might arise.
- Encourage and reward hazard identification beyond any checklist used for inspection.
- Hazard analysts may be more challenged to deduce or discover failure modes overlooked during design than by quantifying risk inherent to known scenarios.

Configuration Management Considerations

- Exercise quality control in the design process and over the design products.
- Assess and evaluate adverse impact to systems when replacing components or removing portions of the system from design. Ensure the changes do not compromise safety, system efficiency, and system life cycle.
- Assess all the impacts to the original design when modifying, especially when use has changed and the design is well into its expected life.
- Ensure effective communication and rigorous configuration management, even with operationally mature programs and projects.

Risk Management Considerations

- Consider both the likelihood and consequence of risk – even a very unlikely event could jeopardize mission success and crew safety.
- Plan for contingencies, understand systems well enough that teams can react to and handle unplanned contingencies as well.
- Review decisions to 'mothball' a system and, if sections must remain, render them inert (incapable of energy release).
- Continue questioning initial assumptions about operations, equipment, and facilities.
- Sustaining rigorous maintenance and quality checks underscores recognition that failure modes cannot always be identified at the time of a product's inception.
- Maintain the level of rigor required to effectively understand and manage program risks.

Project Management Considerations

- Schedule is an important element of any program, but when it becomes the big driver, leaders must ensure they understand the risks to performance and safety, and mitigate appropriately.
- We must not let schedule define our test program, but rather, let it be defined by risk and technical performance … allow for the chance that we may need another test before we "go operational."
- All project team members must fully understand and implement program processes and procedures.

Conclusion

- Common and unique issues contribute to system failures. This paper has merely touched on the concept of drift to failure as a cautionary message. What, then, is the point?
- The point is James Reason's chronic unease as the price of safety.
- So what should be the focus of our chronic unease?
- Managers and leaders, design team members, fabricators and assemblers, analysis and assurance personnel, and others associated with operating and maintaining systems, need to pay attention to identify the manifestation of individual and collective behaviors that might indicate slips in rigor or focus or decisions that might eat away at safety margins as our system drifts to failure.
- Corrections to drift made during design and development phases may efficiently prevent or mitigate drift problems occurring in the operational phase.

References

- James Reason, Managing the Risks of Organizational Accidents, Ashgate, Burlington, VT, 1997.
- "Drift to Failure," Sydney Dekker (pp. 82-92) in "Resilience Engineering: Chronicling the Emergence of Confused Consensus in Resilience Engineering: Concepts and Precepts," Hollnagel, Woods and Leveson, Ashgate, Burlington, VT, 2006.
- Diane Vaughan, "The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA," the University of Chicago Press, Chicago, 1996.
- Hollnagel, Woods and Leveson, Resilience Engineering: Chronicling the Emergence of Confused Consensus in Resilience Engineering: Concepts and Precepts," Ashgate, Burlington, VT, 2006.
- Carl Metzger, book Review for Merton and Barber, "The Travels and Adventures of Serendipity," in Professional Safety Magazine, April 2011, pp.14-15.
- NASA Systems Failures Archive, http://pbma.nasa.gov/index.php?fuseaction=pbma.archive