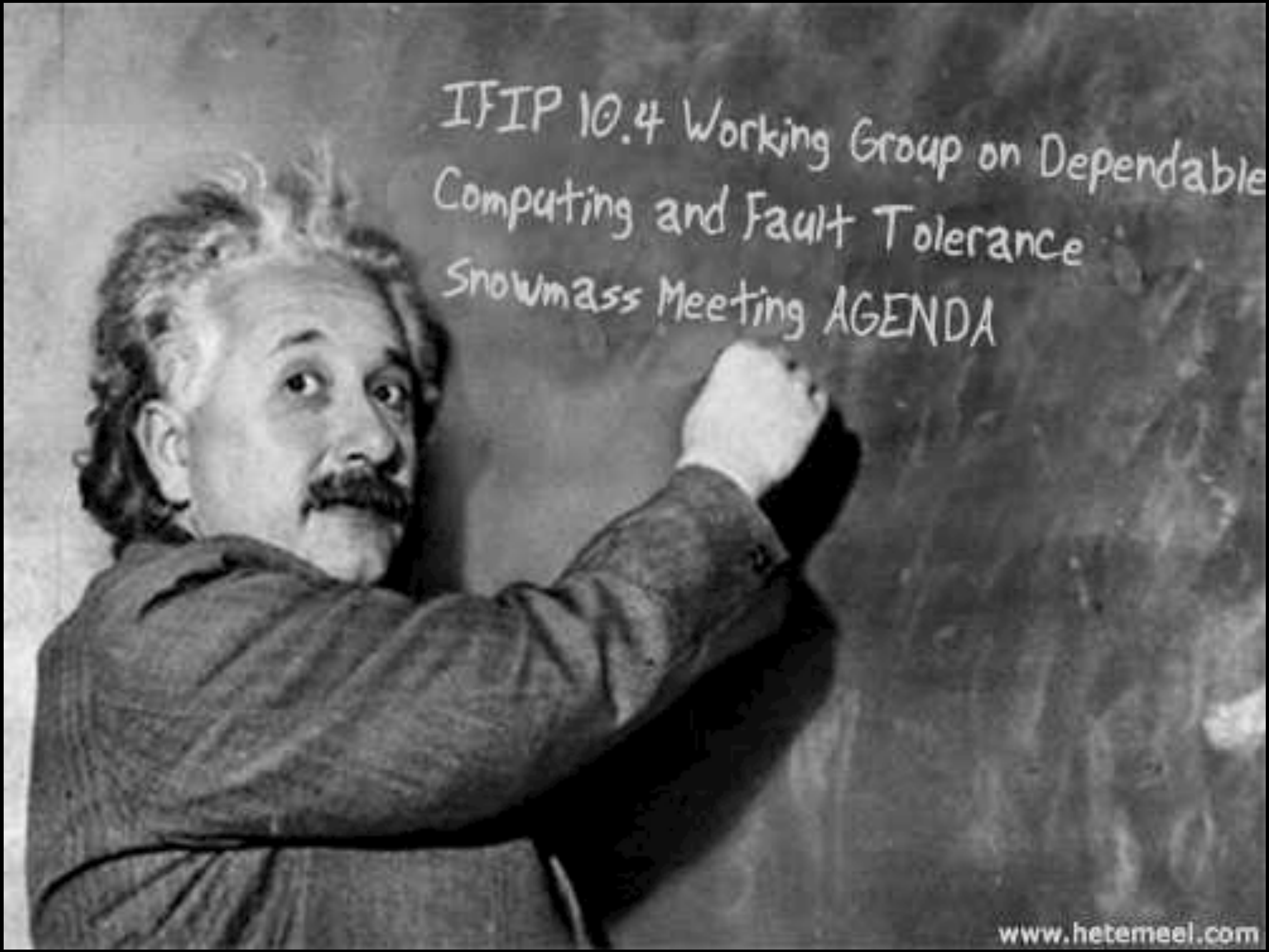
Application of Accident Investigation Notations and Tools

Chuck Howell, howell@mitre.org

14 January 2011

Managing Expectations


IFIP 10.4 Working Group on Dependable
Computing and Fault Tolerance
Snowmass Meeting AGENDA
www.hetemeel.com

You are Here

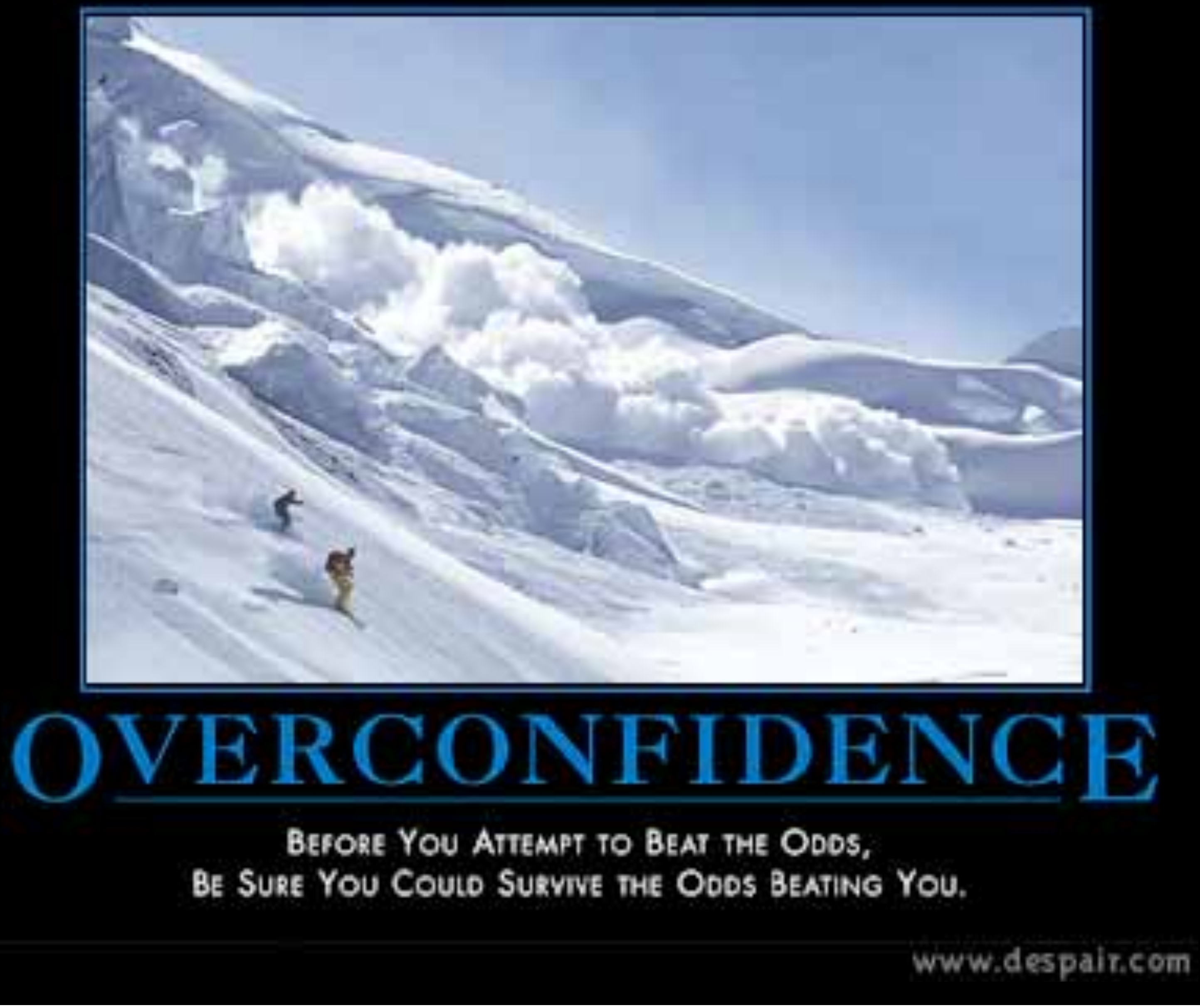
I will Be Good
I will Be Good
I will Be Good
I will Be Good
I will Be Good
I will Be Good
I will Be Good
DUNCE

A Word About This Session and Talk

Some Infrastructure Assurance Challenges

- Thinking and adaptive adversary for some threats
  - Including citizens and users in some cases
  - Can’t assume we can always anticipate creative subtle attacks, limits threat prioritization ROI a bit
- Unknown coupling and dependencies
  - As systems evolve and new ones are connected
- Cascading failures
  - Lessons learned from simple exception mechanisms

Shameless Local Reference


OVERCONFIDENCE
Before You Attempt to Beat the Odds,
Be Sure You Could Survive the Odds Beating You.
www.despair.com

We Resemble This Remark?

And the larger fear looms: We are in the process of building one vast global computer, which could easily become The Legacy System From Hell that holds civilization hostage—the system doesn't really work; it can't be fixed; no one understands it; no one is in charge of it; it can't be lived without; and it gets worse every year.

Stewart Brand, *Written on the Wind*,
Civilization Magazine, November 1998

www.mbe.doe.gov/stratmgt/caib.ppt

CAIB Lessons Learned

January 28, 2004

Developed by:

Major General Kenneth Hess
Major General John Barry
Brigadier General Duane Deal

Presented by:

James N. Hallock, PhD
at the
DOE Senior Leadership Conference

Lesson 1

Well-intentioned people and high-risk organizations can become desensitized to deviations from the norm

– Vaughan's book, The Challenger Launch Decision, called this "***Normalization of Deviance***"

– Board identified this as a major factor in Columbia mishap, much like Challenger disaster

– "Unexpected becomes the expected which becomes the accepted"

– In both Challenger, Columbia: **"The machine was talking to us, but nobody was listening"**

– Small anomalies may be symptomatic of larger problems—failure to address could be disastrous

– System effects take years to develop and cause failures

2003

Another View of Normalization of Deviance

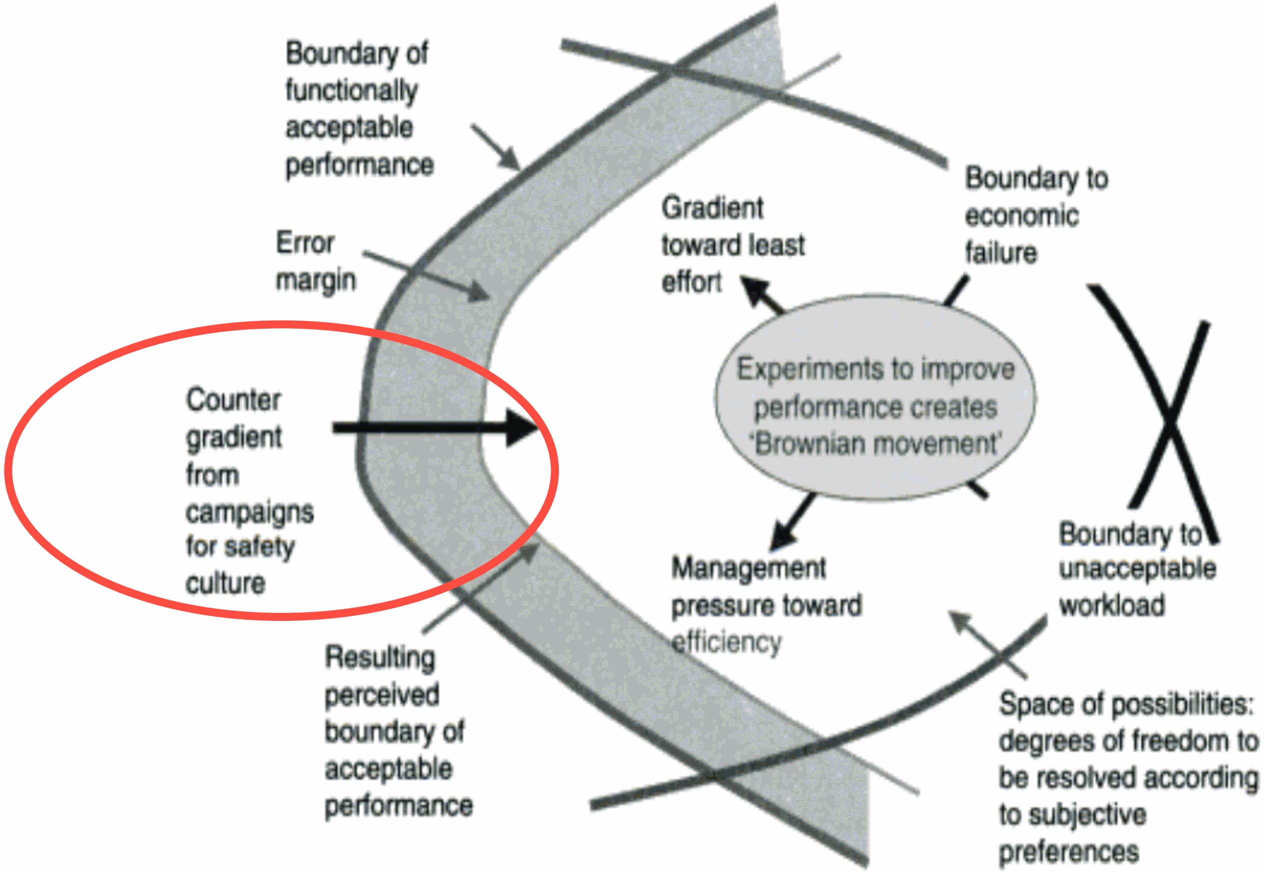

Boundary of functionally acceptable performance
Error margin
Counter gradient from campaigns for safety culture
Resulting perceived boundary of acceptable performance
Gradient toward least effort
Experiments to improve performance creates 'Brownian movement'
Management pressure toward efficiency
Boundary to economic failure
Boundary to unacceptable workload
Space of possibilities: degrees of freedom to be resolved according to subjective preferences

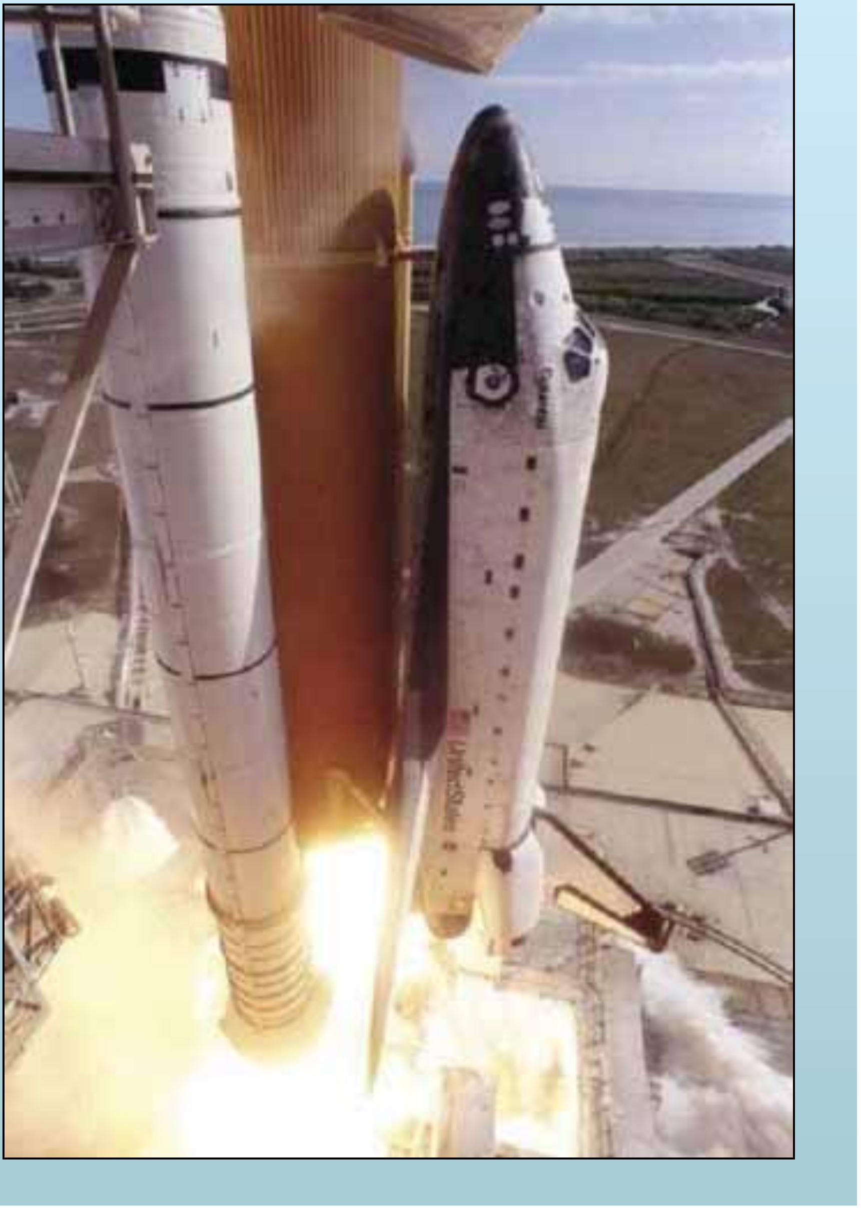
FIGURE 1 Rasmussen's "drift to disaster" diagram (redrawn). The safe envelope is in the middle; the drift is to the left, where disaster lurks.

Normalization of Deviance

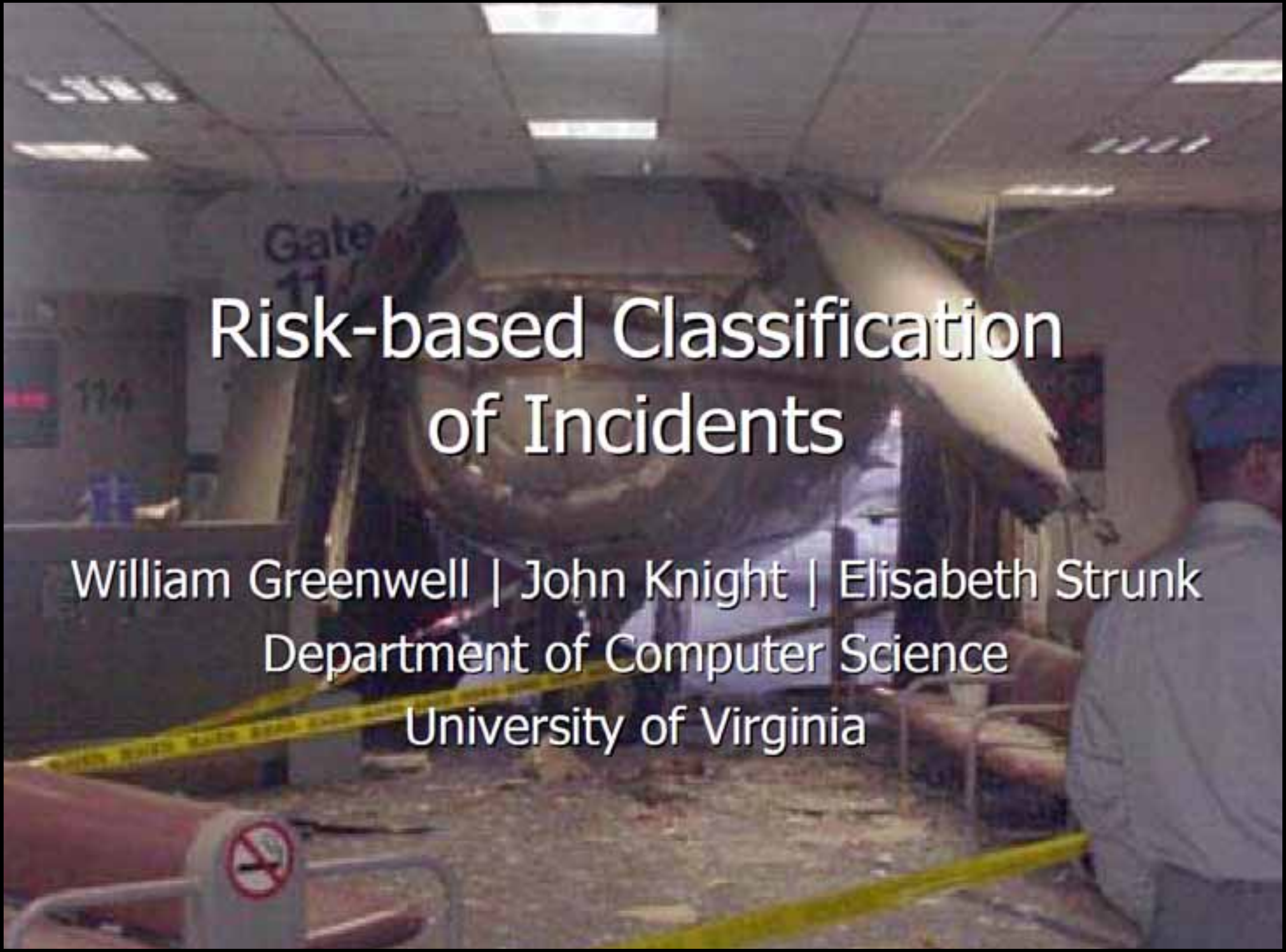
- **After 113 shuttle missions, foam shedding, debris impacts, and TPS tile damage came to be regarded as only a routine maintenance concern**

"…No debris shall emanate from the critical zone of the External Tank on the launch pad or during ascent…"

Ground System Specification Book – Shuttle Design Requirements



Greenwell at UVA: Pandora, 1 of 4



Risk-based Classification of Incidents

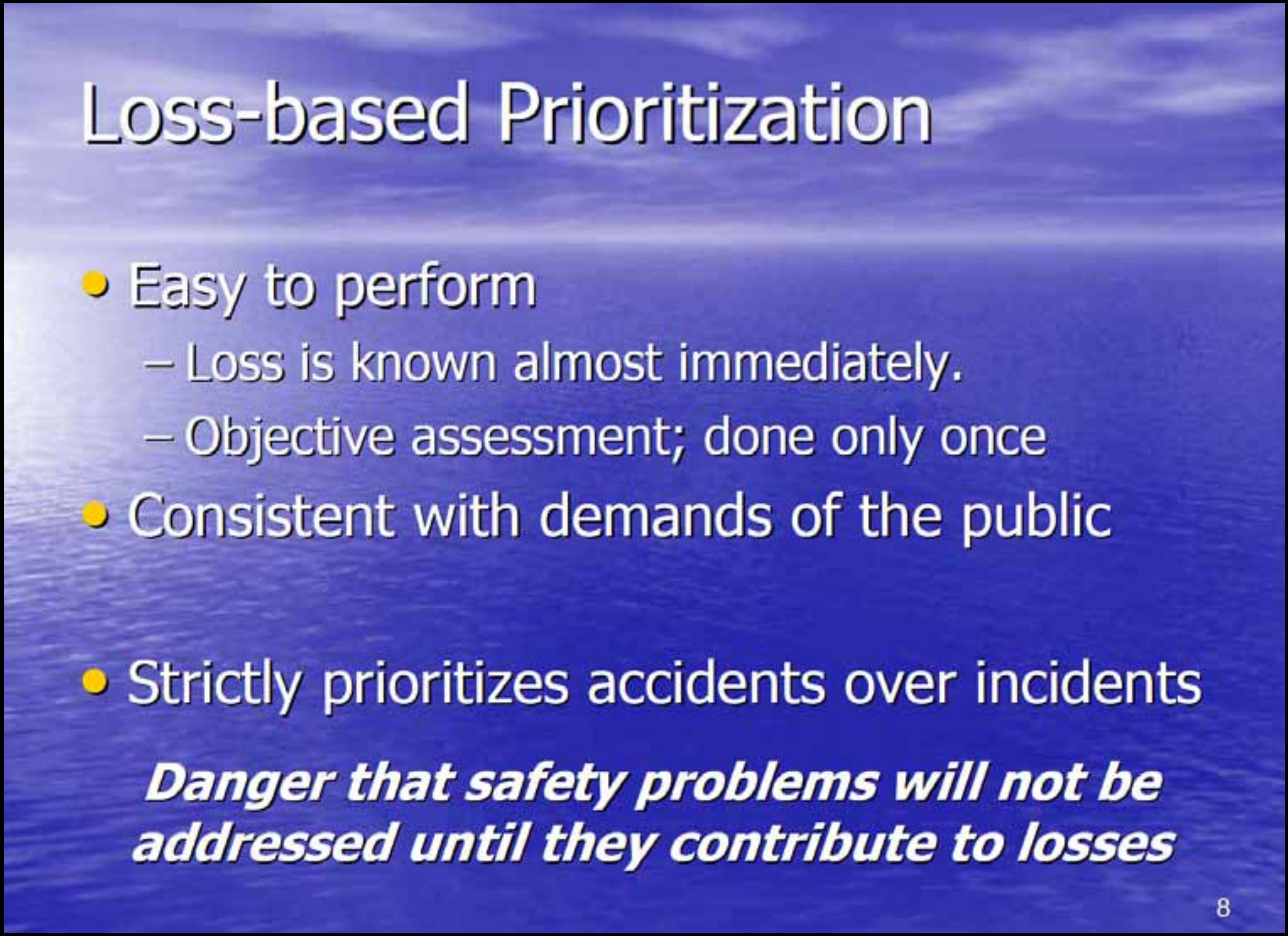
William Greenwell | John Knight | Elisabeth Strunk

Department of Computer Science

University of Virginia

http://www.cs.virginia.edu/~wsg6p/research.html

Greenwell at UVA: Pandora, 2 of 4



Loss-based Prioritization

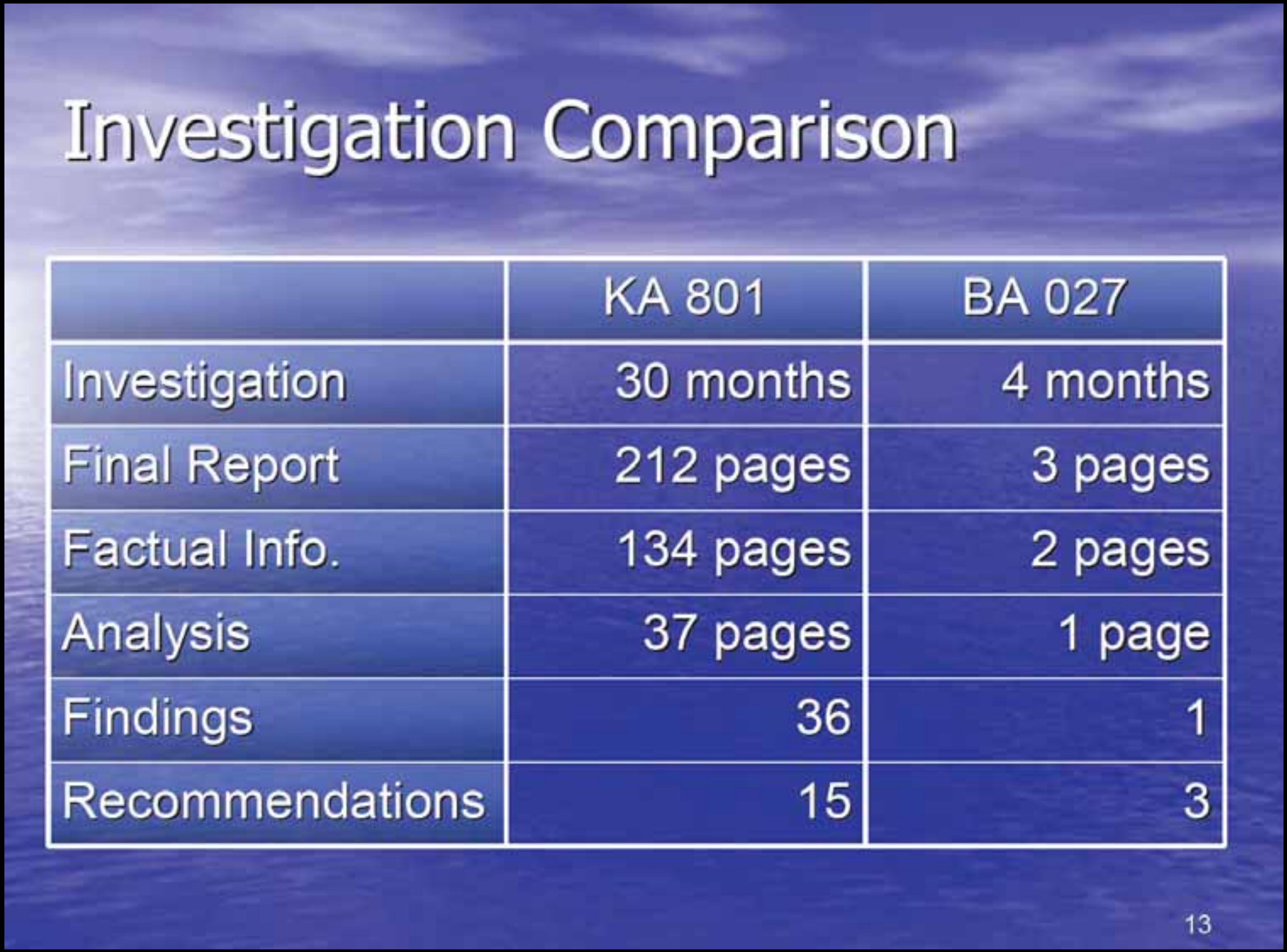
- Easy to perform
  - Loss is known almost immediately.
  - Objective assessment; done only once
- Consistent with demands of the public

- Strictly prioritizes accidents over incidents

Danger that safety problems will not be addressed until they contribute to losses

http://www.cs.virginia.edu/~wsg6p/research.html

Greenwell at UVA: Pandora, 3 of 4



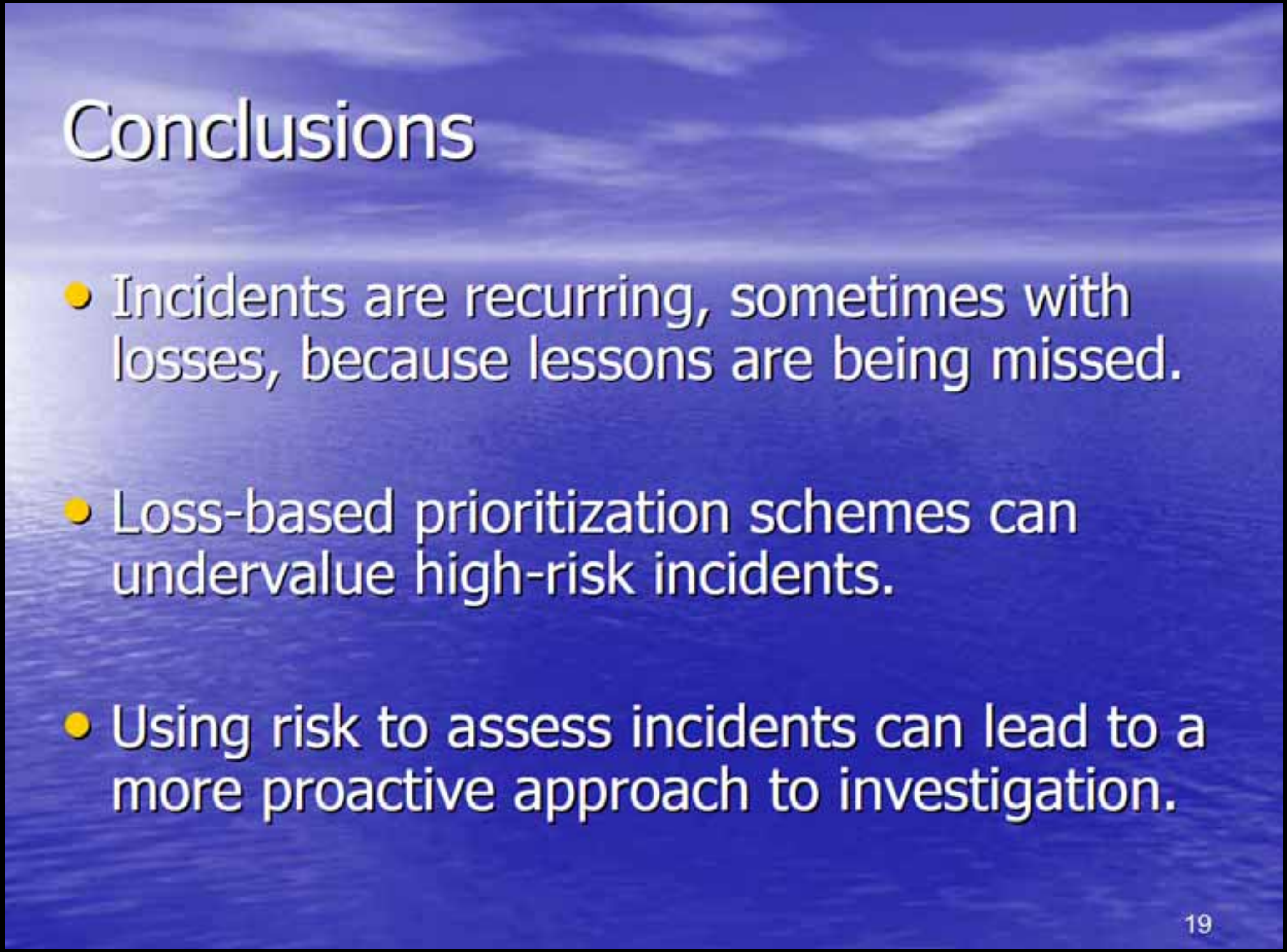
Investigation Comparison

	KA 801	BA 027
Investigation	30 months	4 months
Final Report	212 pages	3 pages
Factual Info.	134 pages	2 pages
Analysis	37 pages	1 page
Findings	36	1
Recommendations	15	3

13

http://www.cs.virginia.edu/~wsg6p/research.html

Greenwell at UVA: Pandora, 4 of 4



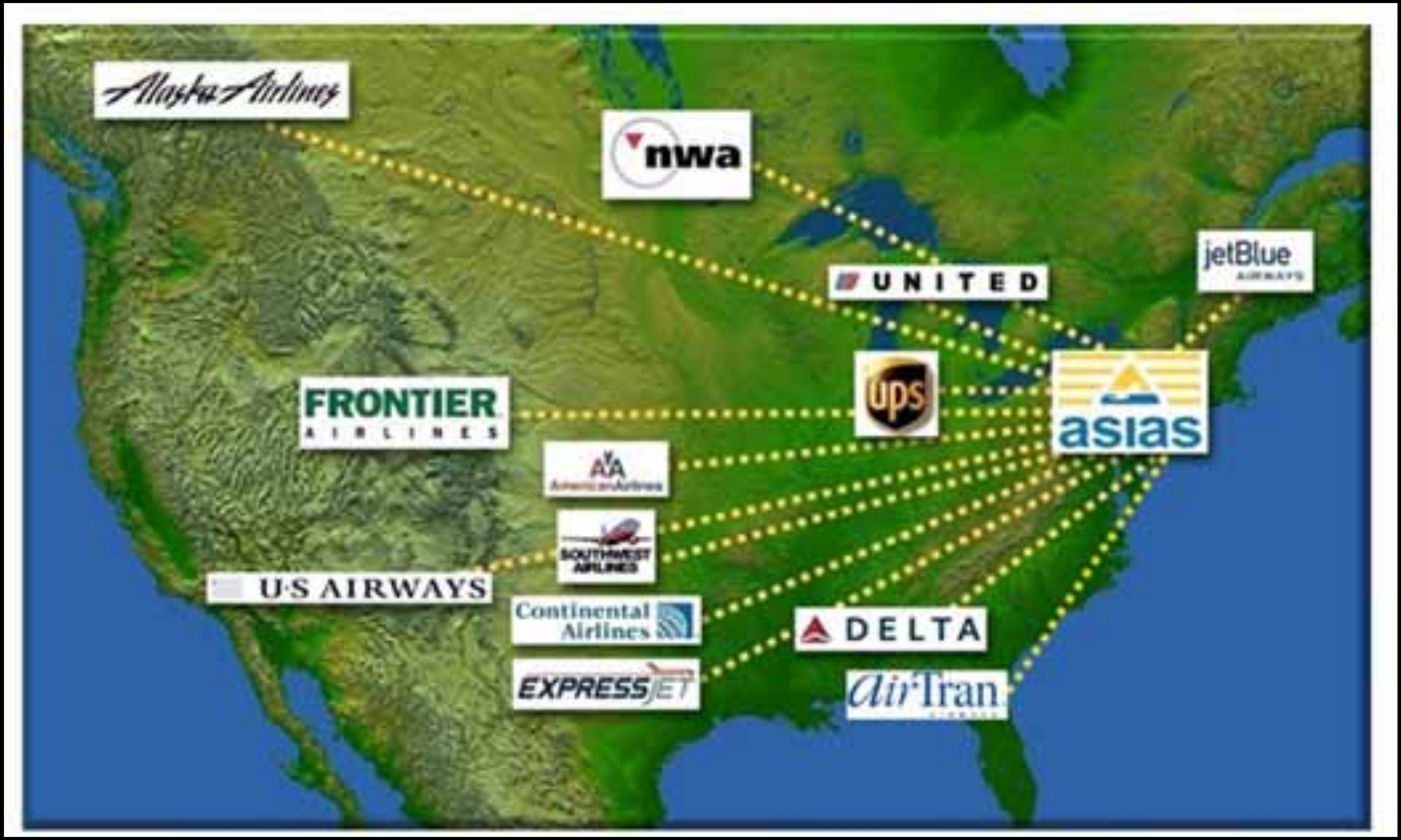
Conclusions

- Incidents are recurring, sometimes with losses, because lessons are being missed.
- Loss-based prioritization schemes can undervalue high-risk incidents.
- Using risk to assess incidents can lead to a more proactive approach to investigation.

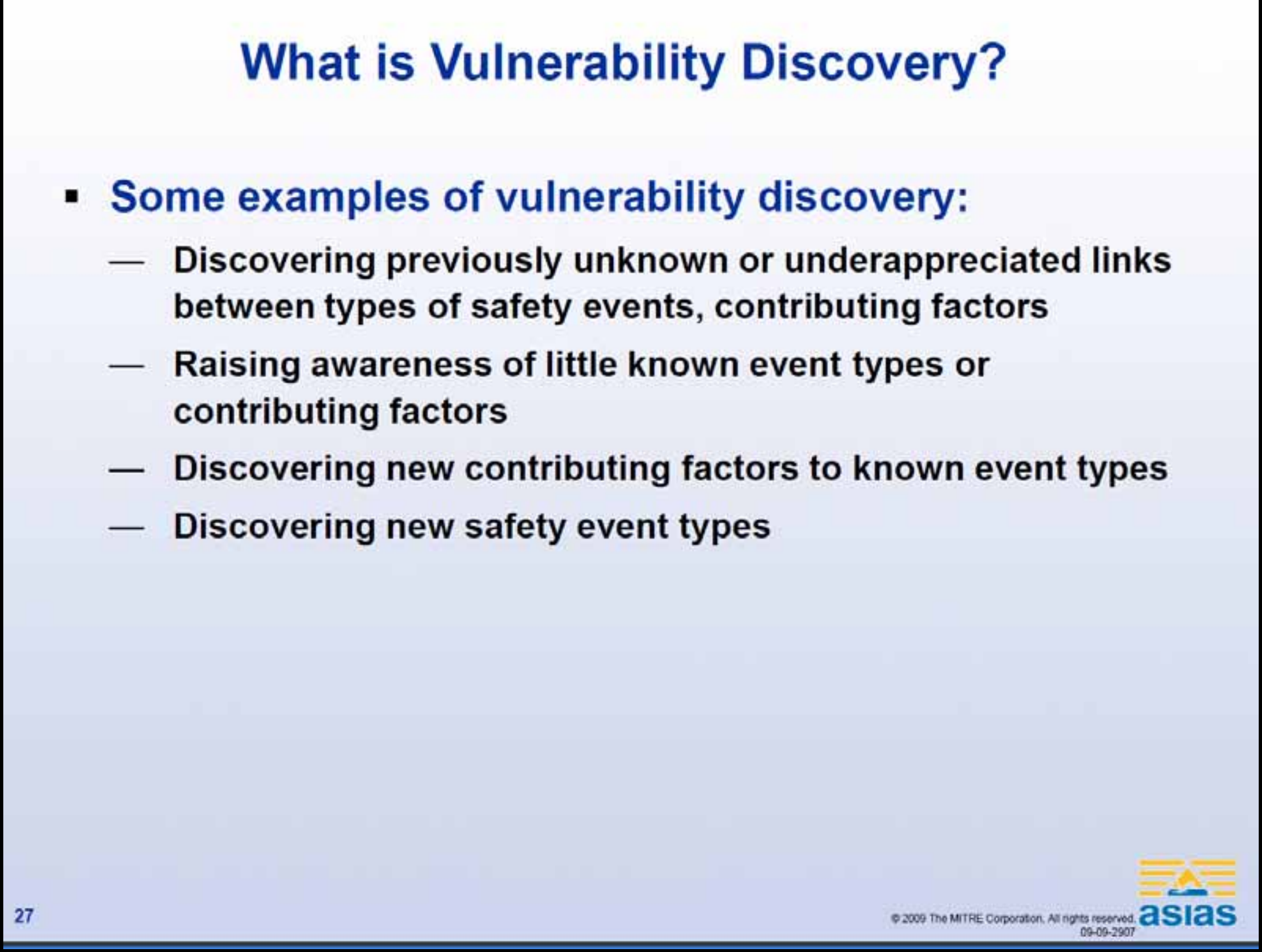
19

http://www.cs.virginia.edu/~wsg6p/research.html

ASIAS:
Aviation Safety Information Analysis and Sharing



ASIAS Listening to the Data



What is Vulnerability Discovery?

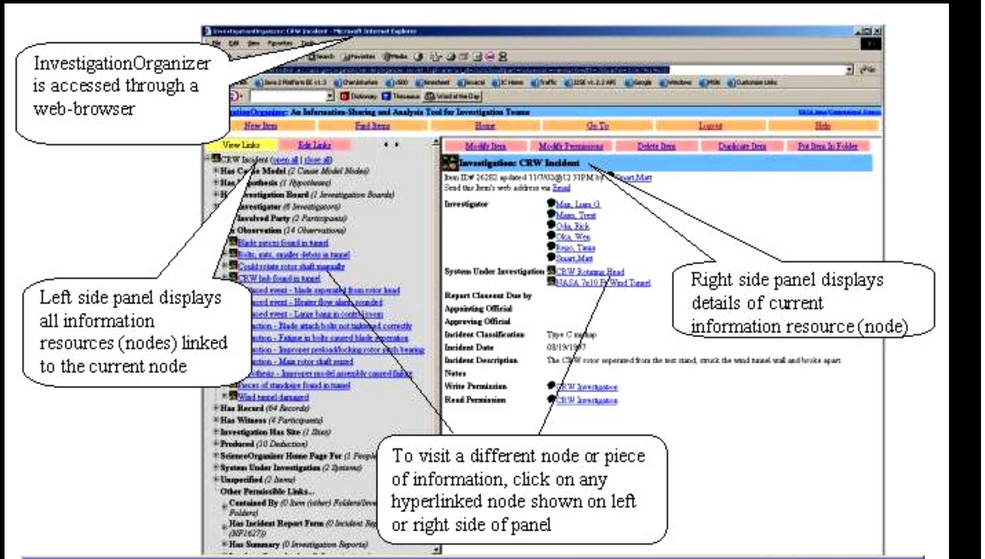
- Some examples of vulnerability discovery:
  - — Discovering previously unknown or underappreciated links between types of safety events, contributing factors
  - — Raising awareness of little known event types or contributing factors
  - — Discovering new contributing factors to known event types
  - — Discovering new safety event types

Accident Investigation Tools and Notations

- Working back from an incident or accident to root causes can be extremely expensive and complex
  - Millions of $s, years of effort
  - Consequences of false positive and negative findings
  - Tools and notations have evolved to help manage the data, do “book keeping” and structural checks, and communicate complicated findings
- Screenshots of a few follow, but the key ideas are that they are intended to support a collaborative team working backwards from a rare event through a complex, subtle, and incomplete sea of data to root causes: investigation and diagnosis

Examples of Tools

- Aviation and Industrial accident investigations have begun to use investigation tools and notations
- Support for managing
  - multiple hypotheses,
  - lots of data that are incomplete, inconsistent, of uncertain relevance
- Underlying rigor in notation that allows machine checking of completeness and consistency of causal chains
- Some evidence that tools and notations help



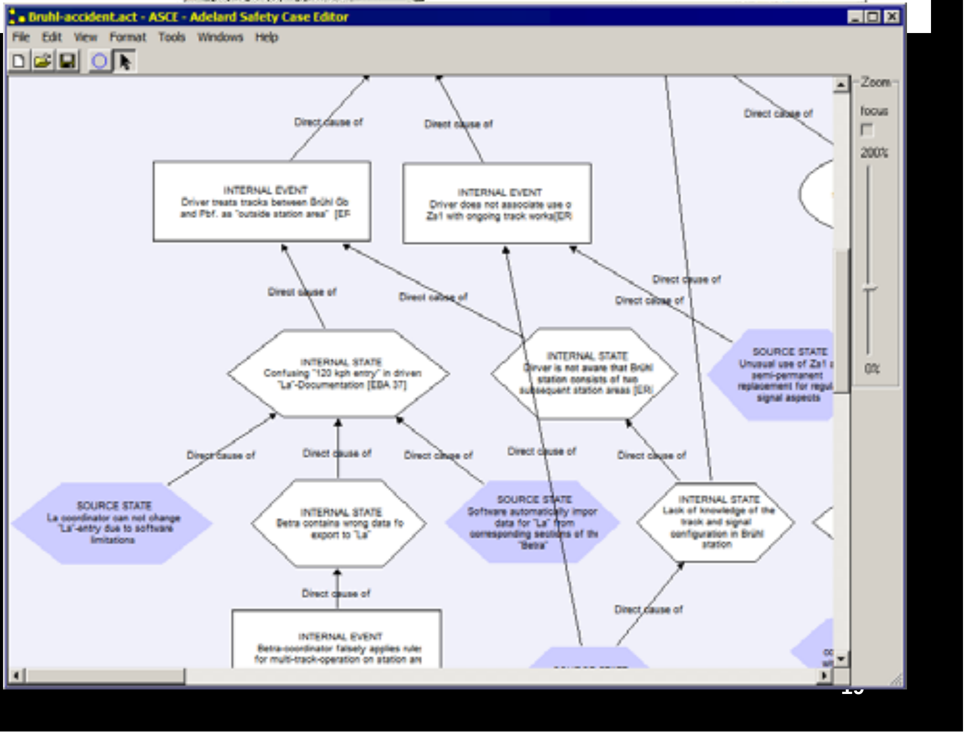
InvestigationOrganizer is accessed through a web-browser

Left side panel displays all information resources (nodes) linked to the current node

Right side panel displays details of current information resource (node)

To visit a different node or piece of information, click on any hyperlinked node shown on left or right side of panel

Investigation: CRW Incident
Investigator
System Under Investigation
Has Summary (0 Investigation Reports)



Bruhl-accident.act - ASCE - Adelard Safety Case Editor
File
Edit
View
Format
Tools
Windows
Help
Zoom
focus
200%
0%
Direct cause of
INTERNAL EVENT Driver treats tracks between Brühl Gb and Pbf. as "outside station area" [EF
INTERNAL EVENT Driver does not associate use o Za1 with ongoing track works[ER
INTERNAL STATE Confusing "120 kph entry" in driven "La"-Documentation [EBA 37]
INTERNAL STATE Driver is not aware that Brühl station consists of two subsequent station areas [ER]
SOURCE STATE Unusual use of Za1 semi-permanent replacement for regul signal aspects
SOURCE STATE La coordinator can not change "La"-entry due to software limitations
INTERNAL STATE Betra contains wrong data fo export to "La"
SOURCE STATE Software automatically impor data for "La" from corresponding sections of th "Betra"
INTERNAL STATE Lack of knowledge of the track and signal configuration in Brühl station
INTERNAL EVENT Betra-coordinator falsely applies rule for multi-track-operation on station are

Many Notations and Tools

- STAMP, Leveson et al. MIT
- Why-Because-Analysis, Ladkin, Bielefeld U.
- Investigation Organizer, NASA
- Rasmussen Investigation Framework, Hurecon
- Structured Occurrence Nets, Randell
- Pandora, Greenwell, UVA
- Etc…

- Plus model based diagnostics, instrumentation and monitoring for diagnosis,…

Some Questions to be Resolved

- How can accident investigation tools and techniques be married to analytics that suggest *possible* subtle issues?
  - E.g., Indications and Warnings from ASIAS
- What additional instrumentation and monitoring is needed or will be especially high ROI?
- Do these approaches work for “Bright Spots” and support a “Positive Deviance” approach to finding islands of infrastructure resilience vs. looking for subtle flaws?

Limits of Tools and Techniques

They're teaching a new way of plowing over at the Grange tonight - you going?

Naw - I already don't plow as good as I know how...

**"Knowing is not enough, we must apply.
Willing is not enough, we must do."** Goethe