



2009

Mini-

Conference



Scott Jackson

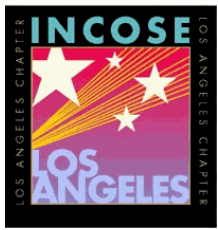
**Adjunct Associate Professor USC Masters Program
in Systems Architecture and Engineering
Instructor in Architecting Resilient Systems
Associate Director of SAE Program
Previously with Boeing
INCOSE Fellow**

**Author *Systems Engineering for Commercial
Aircraft*, Ashgate Publishing Limited, 1997**

**Author: *Architecting Resilient Systems: Accident
Avoidance and Survival and Recovery from
Disruptions* (to be published in 2009 by John Wiley
and Sons)**



Copyright © 2008 John Wiley & Sons, Inc. All rights reserved



2009

Mini-

Conference

USC Viterbi
School of Engineering



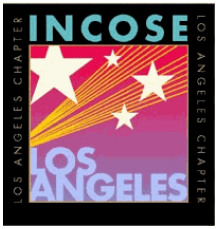
Architecting Resilient Systems: The Fourth Dimension of System Development

INCOSE-LA Mini-conference
February 7, 2009



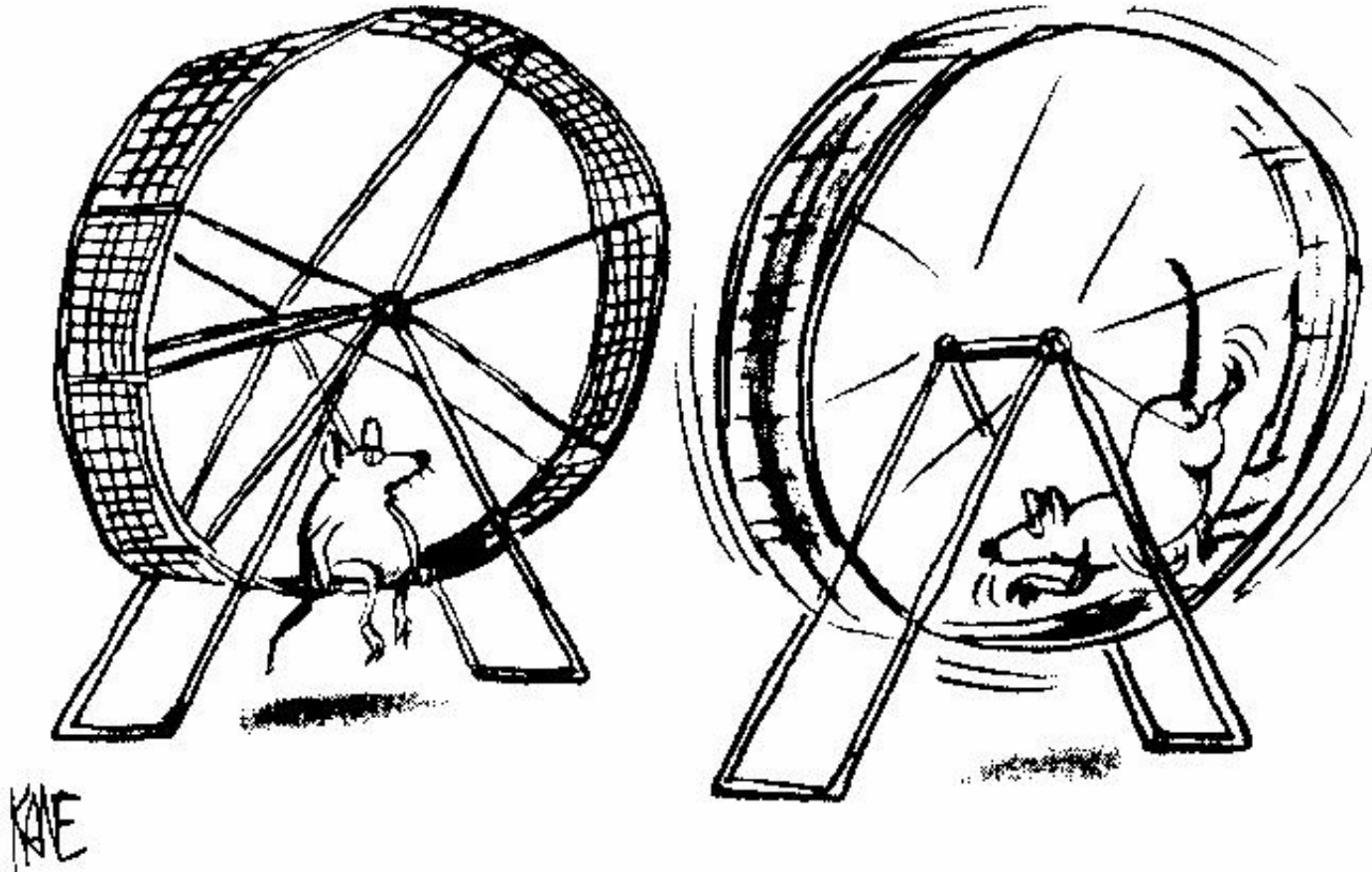
Scott Jackson





2009
Mini-
Conference

An Epiphany



"I had an epiphany."





2009

Mini-

Conference

The Beginning



- Paté-Cornell, Elisabeth,
“Organizational Aspects of
Engineering Safety: The Case
of Offshore Platforms,”
Science, December 1990





2009

Mini-

Conference

A Definition

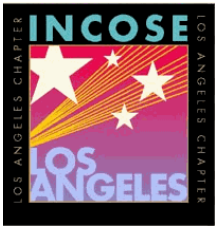


- The ability to anticipate a disruption and prevent something bad from happening – avoidance
- The ability to prevent something from getting worse – survival
- The ability to recover from something bad once it has happened – recovery

Westrum

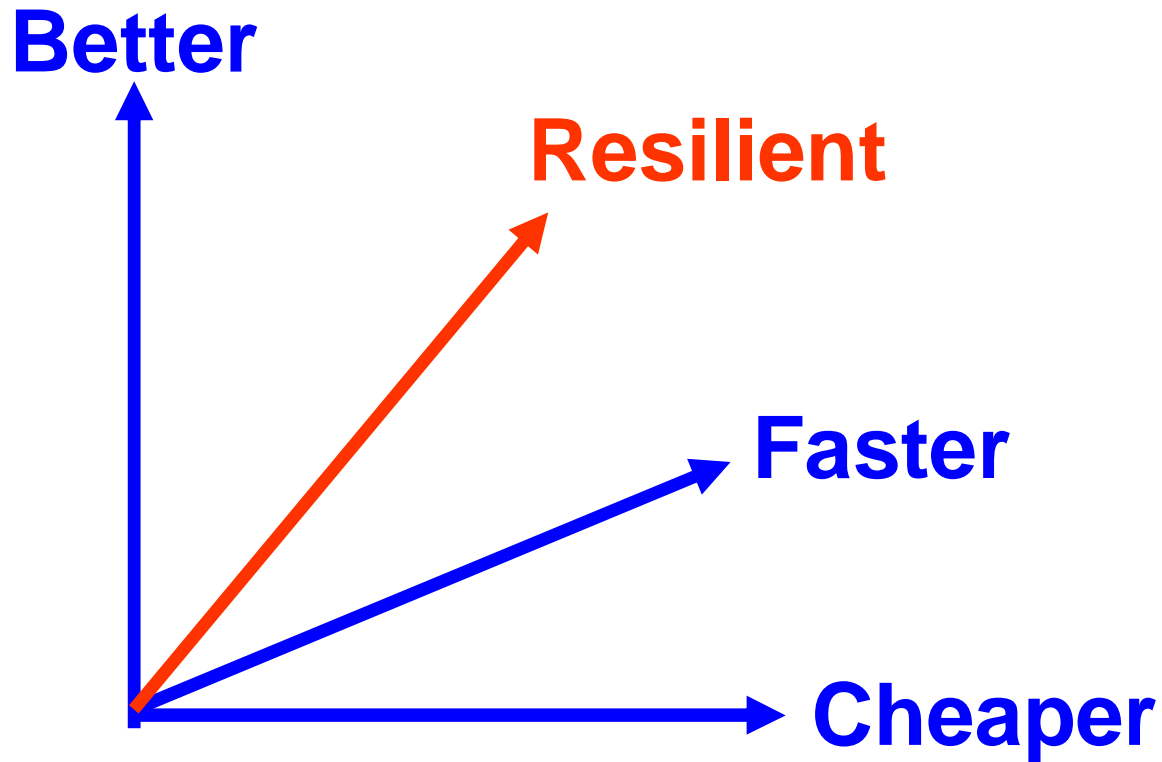
Note: According to Westrum, a system only needs two of these three abilities to be resilient.





2009
Mini-
Conference

The Fourth Dimension of System Development





2009

Mini-

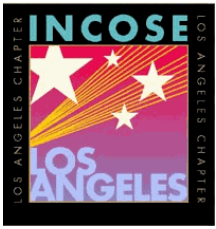
Conference

Types of Systems



- **General** – any type of human-made or human-operated system or system in which there is human intervention
- **Specific**
 - Technological systems
 - Human-intensive systems¹
 - Technological systems with human interfaces
 - Infrastructure systems
 - The infrastructure system that surrounds a technological system
 - Systems of systems
 - Socio-ecological systems
 - ¹Human-intensive systems, as defined here, may include some hardware and software components, for example, hospitals





2009
Mini-
Conference

Types of Disruptions

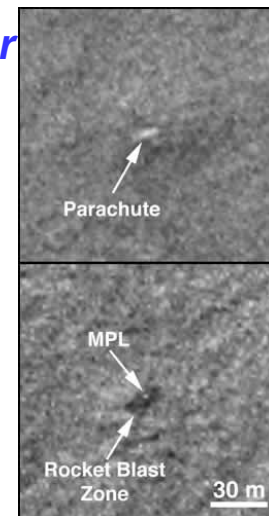


- **Type A – A disruption of input**
 - An unexpected or unknown (to the designer) phenomenon
 - Twin towers attack
 - Tacoma Narrows bridge
 - A change in environment
 - Katrina
 - The Robert Scott expedition
- **Type B – A degradation in function, capability or capacity**
 - Software error
 - Human error (in the system)
 - Nagoya
 - Metrolink 111
 - Component failure
 - Challenger
 - Interaction Between Components
 - Helios 522
 - Mars Polar Lander



Airbus 320

Mars Polar Lander





2009

Mini-

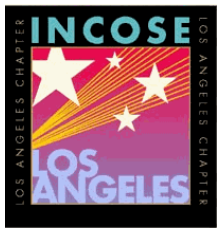
Conference

Case No. 1: Apollo 13



- **Background – Explosion in oxygen tank caused loss of power in command module. Crew survived by moving into lunar module.**
- **Type of System: Technological system (space craft) with human components (the crew). Including ground station this is a system of systems.**
- **Type of disruption: Type B – loss of function (power loss)**
- **Inter-component collaboration: Excellent**
- **communications with ground**
- **Capacity: Good, second module**
- **Flexibility: Excellent**
- **Tolerance: Excellent due to decision making and ability to reorganize (move to second module)**





2009
Mini-
Conference

Some Resilience Aspects of Apollo 13



Disruption: Type B - Systemic	
Flexibility	Excellent
Inter-element collaboration	Mixed (deficient to excellent)
Decision Making	Excellent
Reliability	Deficient
Safety Process	Deficient
Risk Management	Deficient
Capacity	Excellent
Tolerance	Excellent





2009

Mini- Case No. 2: Metrolink 111

Conference



- **On September 12, 2008 a Metrolink commuter train collided with a freight train in Chatsworth near Los Angeles. There were 25 fatalities and many injuries.**
- **Disruption – type B – Systemic**
 - Official disruption – Engineer was sending text messages
 - Alternative disruption – Failure of signal
- **Capacity – deficient – no redundancy, single track, single engineer**
- **Flexibility – deficient – no method to shift control**
- **Tolerance – deficient – No method to anticipate on-coming train or perform corrective action**
- **Inter-element collaboration – deficient – no timely communication with Metrolink**





2009
Mini-
Conference

Some Resilience Aspects of Metrolink 111



Disruption: Type B – Systemic	
Capacity	Deficient
Flexibility	Deficient
Tolerance	Deficient
Inter-element collaboration	Deficient





2009

Mini-

Conference

The Systems Approach



- Identification of the elements of a system
- Division of elements into smaller elements
- Grouping of elements
- Identification of the boundary of a system
- Identification of the function of each element
- Identification of the interactions among the elements
- Definition of the system's environment
- Identification of emergent characteristics of a system

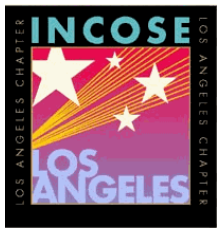
Holistic (non-reductionist) methodologies

- Focus on system as a whole
- Interaction between the elements
- Extensive use of laws, principles, heuristics, culture, risk and other factors

Analytical (reductionist) methodologies

- Focus on elements
- Based on verifiable, traceable requirements





2009

Mini-

Conference

Capacity Heuristics



- *The absorption heuristic – the ability to sustain a disruption (Woods)*
- *The functional redundancy heuristic – There should exist an alternative method to perform each critical function that does not rely on the same physical systems (Madni)*
- *The physical redundancy heuristic – Physical redundancy should exist wherever possible (Richards)*
- *The margin heuristic – The system should have adequate margin to absorb disruptions (Woods)*
- *The context spanning heuristic - The system should be designed to both the worst case and most likely scenarios (Madni)*





2009

Mini-

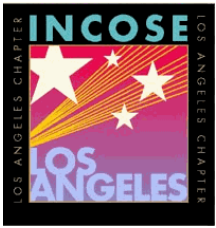
Conference

Flexibility Heuristics



- *The reorganization heuristic - The system should be able to restructure itself in response to disruptions or the anticipation of disruptions (Woods)*
- *The human backup heuristic - Humans should be able to backup the automated system when there is a change in context the automated system cannot handle and there is time for human intervention (Madni)*
- *The human-in-the-loop heuristic – Humans should be elements of the system when there is a need for human cognition (Madni)*
- *The diversity heuristic – There should be diversity within systems (Resilience Alliance)*
- *The human-in-control heuristic – The human operator should be in command (Billings)*





2009

Mini-

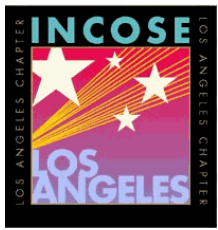
Conference

Flexibility Heuristics (cont'd)



- *The predictability heuristic – Automated systems should behave predictably and allow human over-ride. (Billings)*
- *The inspectability heuristic – The system should enable humans to take actions when needed without making unsubstantiated assumptions. (Madni)*
- *The simplicity heuristic – Automated systems should be simple to train, to learn, and to operate. (Billings)*
- *The complexity avoidance heuristic – Complexity should only reflect the complexity demanded by the system functionality. (Madni)*
- *The reparability heuristic - The system should be repairable. (Richards)*
 - *The loose coupling heuristic – The organizational system should allow for flexibility in organizational processes and decisions.*





2009

Mini-

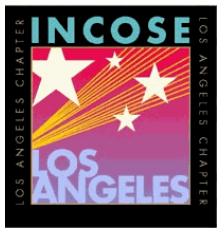
Conference

Tolerance Heuristics



- *The graceful degradation heuristic – The system should degrade gradually when exposed to a disruption. (Woods)*
- *The drift correction heuristic – Drift towards brittleness should be detected and corrected. (Woods)*
- *The neutral state heuristic – The system should be put into neutral if possible. (Madni)*
- *The automatic function heuristic – Functions should be automatic only if there is a good reason for doing so. (Billings)*
- *The organizational decision-making heuristic - Organizational decision-making should be monitored.*





2009

Mini-

Conference

Tolerance Heuristics (cont'd)



- *The organizational planning heuristic – Notice signs that call into question organizational plans, models and routines.*
- *The mobility heuristic – The system should be able to avoid a threat by moving. (Richards)*
- *The prevention heuristic – The system should be able to suppress future potential disruptions. (Richards)*
- *The retaliation heuristic – The system should be able to retaliate to a disruption. (Richards)*
- *The concealment heuristic – The system should attempt to conceal itself against potential threats.*





2009

Mini- Tolerance Heuristics (p. 3)

Conference



- *The deterrence heuristic – The system should attempt to deter hostile threats from attacking. (Richards)*
- *The regroup heuristic – The system should be able to restructure itself after a disruption to recover some degree of functionality and performance. (Raveh)*





2009

Mini-

Conference

Inter-element Collaboration Heuristics



- *The informed operator heuristic – The human operator should be informed. (Billings)*
- *The hidden interaction heuristic – Avoid hidden interactions. (Woods)*
- *The knowledge between nodes heuristic – Maximize knowledge between nodes. (Billings)*
- *The human monitoring heuristic – The automated system should be able to monitor the human operator. (Billings)*
- *The automated system monitoring heuristic - The human operator should be able to monitor the automated systems. (Billings)*





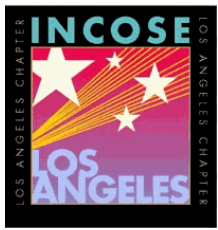
2009
Mini-
Conference

Inter-element Collaboration Heuristics (cont'd)



- *The intent awareness heuristic – Each element of the system should have knowledge of the others' intent and should back up each other when called on. (Madni and Billings)*
- *The inter-element impediment heuristic – There should be no impediments to inter-element collaborations. (Jackson)*





2009

Mini-

Conference

Conclusions



- Causes of catastrophes are beyond the domains of traditional reliability, safety and other reductionist approaches
- Disruptions (e.g., human error) are not the cause of catastrophes; they simply initiate it
- A system can be architected to create resilience
- The primary aspects of resilience are adaptability, risk and culture
- Resilience architecting requires both analytical and holistic approaches

