

INCOSE Webinar: Architecting Resilient Systems

Date: 16 Dec 2009

Time: 15:00 UTC (GMT) ; 10:00 EST; 07:00 PST

Presenter: Scott Jackson

General Webinar Details:

<http://www.incose.org/practice/webinars.aspx>

The concept of resilience has reached maturity over the past decade. There is general agreement on the definition of resilience and its attributes. The Resilience Engineering Network (www.resilience-engineering.org) has pioneered this work. Authors, such as Erik Hollnagel and David Woods have written extensively on the subject. The book *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Company, UK, 2006 is one of the first major publications. The IEEE Systems Journal has devoted a whole issue to the subject. The University of Southern California (USC) teaches a graduate course called Architecting Resilient Systems in which the book of the same name by the presenter is used.

The resilience community agrees that resilience architecting (also called resilience engineering) occurs over the three phases of a disruption. In the pre-disruption phase the system should take steps to anticipate the disruption and avoid the disruption, if possible. In the survival phase the system should absorb the disruption so that it can recover in the recovery phase. In the recovery phase the system resumes some degree of its original goals, including the survival of the humans in it.

The nature of disruptions is discussed. Disruptions are the initiating event that may lead to a catastrophic event. Human error is a common source of disruption. However, the resilience of the entire system will determine whether the system is prone to catastrophe. Disruptions may be either external, such as terrorist attacks or natural disasters, or they may be internal, such as human or software errors. The phenomenon in which systems fail when the components function as *designed* is discussed.

Resilience has four primary attributes: capacity, flexibility, tolerance, and inter-element collaboration. This webinar presents approximately 40 *heuristics* for the achievement of these attributes.

Capacity requires that the system be sized to handle the maximum and most likely events, such as terrorist attacks and natural disasters. However, a system cannot depend on capacity alone; the other attributes must be present to handle unpredicted events. Capacity includes *functional redundancy*.

Flexibility requires the system to be able to reorganize. For example, plans must be in place to allow the command and control to shift upwards in the event of a serious disruption, such as a terrorist attack.

Tolerance allows the system to degrade gracefully in the face of an attack. That is, all resources would not become inoperative after the first strike.

One of the most important resilience attributes is inter-element collaboration. This attribute allows all elements of the system to interact and cooperate with each other. The New York Fire Department had excellent collaboration with the police, the military and the power company after the twin tower attacks. On the other hand, the City of New Orleans lacked this attribute after Katrina. This lack of resilience is called brittleness.

In addition to these attributes, a resilient system needs at least two other features: a resilient culture and a serious risk capability. Numerous case studies have shown culture and a lack of attention to risk to be primary causes of brittleness. Although the search for methods to achieve cultural change is still under way, the short term approach is to employ extensive reviews of critical issues. Many brittle systems, for example, Challenger, Chernobyl, etc. have suffered from a lack of a risk process and the will to employ one, this is another critical function. Research has shown that a serious risk process will go far beyond traditional approaches.

In summary, the attributes of resilience are well-defined. Finding the most cost-effective ways to measure them, to incorporate them into a system, and to fund them is the major challenge. The Infrastructure Security Partnership (TISP) (www.tisp.org) on which the presenter serves is moving forward to answer these questions.

To say that resilience is well-defined is not say that the work is finished. There is still much to be learned to accomplish the goals of resilience. Areas of major research include, but are not limited to, the application of resilience in both political and economic environments.

Copyright© John Wiley and Sons, all rights reserved

Scott Jackson is a lecturer at the University of Southern California in the Systems Architecting and Engineering Program where he teaches courses in Architecting Resilient Systems, Systems Engineering Theory and Practice, and Systems Engineering Management. Scott is author of *Systems Engineering for Commercial Aircraft*, published by Ashgate Publishing Limited in 1997. He has also authored many papers for INCOSE, AIAA and IEEE. He is the author of the book *Architecting Resilient Systems: Accident Avoidance and the Survival and Recovery from Disruptions* recently published by John Wiley and Sons, Hoboken, NJ. Within INCOSE Scott is and INCOSE Fellow and the chair of the Resilient Systems Working Group.