

About Resilience Engineering ...

Erik Hollnagel, David Woods and Nancy Leveson, Organizers
International Symposium on Resilience Engineering,
Soderoping Sweden
October 20-25, 2004

From Symposium Material

Safety is a system property that emerges from a conglomerate of components, subsystems, software, organizations, human behavior, and their interactions. Over the last 20-30 years the accumulation of major mishaps and case studies have made it clear that organizations must revise their handling of processes and capabilities to address not only technical but also human and organizational risk factors. Numerous strategic case studies and accident analyses have pointed to the need to monitor and manage risk continuously throughout the life cycle of a system, and in particular to find ways of maintain a balance between safety and the often considerable pressures to meet production and efficiency goals (just think of NASA).

The traditional fields of practice, such as risk analysis and probabilistic safety assessment (PSA), have been unable of provide the much needed solutions. There are several reasons for this, the most important probably being that they are firmly rooted in oversimplified accident models. Insights from research on failures in complex systems, organizational contributors to risk, and human performance have made it clear that safety is an emergent rather than resultant property of a system, which means that it cannot be predicted by considering only the constituent parts of the system. Safety is something a system does, rather than something a system has. This means that we must try to understand how a system can actively ensure that things do not get out of hand and that control is not lost. Systems should be made resilient, rather than reliable. It is not enough that they are reliable so that the failure probability is acceptably low; they must also be resilient and have the ability to recover from irregular variations, disruptions and a degradation of expected working conditions.

We boldly postulate a new field that appropriately may be called Resilience Engineering. Fortunately, many of the essential constituents of resilience engineering are already at hand. Since the beginning of the 1990s there has been a growing evolution of the principles for organizational resilience and in the understanding of the factors that determine human and organizational performance. As a result, there is an appreciable basis for how to incorporate human and organizational risk in life cycle systems engineering tools and how to build knowledge management tools that proactively capture how human and organizational factors affect risk."

Resilience engineering stands for the view that failure is the flip side of the adaptations necessary to cope with the complexity of the real world, rather than a breakdown or malfunctioning as such. The performance of individuals and organizations must always adjust to the current conditions and because resources and time are finite such adjustments are always approximate. Success has been ascribed to the ability of organizations, groups and individuals to anticipate the changing shape of risk before failures and harm occur. Failure is simply the absence, temporary or permanent, of that ability. The initial steps in developing a practice of Resilience Engineering must therefore focus on the following critical components:

1. Ways to analyze, measure and monitor the resilience of organizations in their operating environment.
2. Tools and methods to improve an organization's resilience vis-à-vis the environment.
3. Techniques to model and predict the short- and long-term effects of change and decisions on risk.