Resilience as Graceful Extensibility to Overcome Brittleness[i]

David D. Woods[1]

[1]Department of Integrated Systems Engineering, The Ohio State University

Contact: woods.2@osu.edu

Keywords: Resilience engineering, Brittleness, Saturation, Graceful extensibility

Resilience as Graceful Extensibility

The label "resilience" is used in many ways, as this guide illustrates. For example, some use the label to refer to the ability to rebound from challenges, and others use the label to refer to building more robust systems that absorb a greater range of disrupting events (Woods, 2015). In Resilience Engineering (Hollnagel et al., 2006) the label "resilience" is used to refer to a different kind of adaptive capacity that allow systems to continue to function when challenged by surprises.

In my work, resilience is the opposite of brittleness (Woods, 2006). *Brittleness*, descriptively, is a rapid fall off or collapse of performance that occurs when events push a system beyond its boundaries for handling changing disturbances and variations. Since the word resilience is used in many different ways, a new term was needed to refer to system characteristics that overcome the risk of brittleness-induced failures — Graceful Extensibility.

Graceful Extensibility is the ability of a system to extend its capacity to adapt when surprise events challenge its boundaries (Woods, 2015). All systems have an envelope of performance, or a range of adaptive behavior, due to finite resources and the inherent variability of its environment. Thus, there is a transition zone where systems shift regimes of performance when events push the system to edge of its envelope (e.g., how materials under stress can experience brittle failure; see Baker et al., 1999 and Woods et al. 2008 for analyses of brittleness for complex systems drawing on material science).

Boundary refers to this transition zone where systems shift regimes of performance. This boundary area can be more crisp or blurred, more stable or dynamic, well-modeled or misunderstood. Brittleness and graceful extensibility refer to the behavior of the system as it transitions across this boundary area. Graceful extensibility and brittleness are opposites. The latter is characterized by rapid performance fall off or collapse when events push the system past the boundary of its envelope. The former, graceful extensibility, refers to system's ability to adapt how it works to extend performance past the boundary area into a new regime of performance invoking new resources, responses, relationships, and priorities (for example see Wears et al., 2008 for description

[i] This paper is part of the IRGC Resource Guide on Resilience, available at: https://www.irgc.org/risk-governance/resilience/. Please cite like a book chapter including the following information: IRGC (2016). Resource Guide on Resilience. Lausanne: EPFL International Risk Governance Center. *v29-07-2016*

of how emergency rooms adapt to changing patient loads, in the extreme case following a mass casualty event).

With low graceful extensibility, systems exhaust their ability to respond as challenges grow and cascade. As the ability to continue to respond declines in the face of growing demands, systems with low graceful extensibility risk a sudden collapse in performance. With high graceful extensibility, systems have capabilities to anticipate bottlenecks ahead, to learn about the changing shape of disturbances/challenges prior to acute events, and possess the readiness-to-respond to meet new challenges. As a result, systems with high graceful extensibility are able to continue to meet critical goals and even recognize and seize new opportunities to meet pressing goals. Resilience management builds, sustains, and adjusts graceful extensibility to forestall brittleness-induced failures.

Systems with finite resources in changing environments are always experiencing and stretching to accommodate events that challenge boundaries. No system can escape the constraints of finite resources and changing conditions. All systems, however successful, have boundaries and experience events that fall outside these boundaries. Boundary challenging events are a form of model surprise, not simply a matter of expected frequency or probability. Studies of graceful extensibility then ask: "What do systems draw on to *stretch* to handle surprises?" The properties that contribute to or break down graceful extensibility have emerged from multiple studies of how people in various roles adapt to surprises (e.g., Cook, 2006; Wears et al., 2008; Finkel, 2011; Stephens et al., 2015).

Risk Governance as Control of Brittleness-Induced Failures

From the perspective of graceful extensibility, risk governance addresses how system performance changes when events challenge the limits or boundaries of that system's normal range of adaptive behavior. The location of the boundary of a system's normal range of adaptive behavior is dynamic and uncertain, yet stakeholders' estimate of its performance boundaries easily becomes misplaced and overconfident. In general, systems as designed and operated are more brittle than stakeholders realize (Woods, 2006). However, responsible people in various roles throughout organizations, compensate by anticipating potential bottlenecks and adapting to fill the gaps in order to stretch system performance in the face of smaller and larger surprise events (e.g., Cook, 2006). As a result, it is easy for other perspectives to miss the need for graceful extensibility and, inadvertently, to undercut the resources that produce graceful extensibility when that system adapts to meet production pressures (Woods, 2006).

There are three ways that graceful extensibility breaks down to produce brittle systems: Decompensation, Working at Cross-purposes, and Getting Stuck in Outdated Approaches (Woods and Branlat, 2011). Decompensation occurs when a system exhausts its capacity to deploy and mobilize responses as disturbances cascade. The risk is that the organization's adaptations are too slow and stale to keep pace with the tempo of events. Skill at anticipation offsets this risk.

Working at Cross-purposes is the inability to coordinate different groups at different echelons as goals conflict (Dietz et al., 2003). As a result of miscoordination, the groups work at cross-purposes. Each group works hard to achieve their local goals for their scope of responsibility, but these activities make it more difficult for other groups to meet the responsibilities of their roles or undermine the global goals that all groups recognize. In other words, the different roles act in ways that are locally adaptive, but globally maladaptive (see Stephens et al., 2015 for a case in hospitals). Skill at synchronizing over multiple roles and levels offsets this risk.

Getting Stuck in Outdated Approaches refers to a breakdown in how systems learn to revise models, strategies, and tactics as changes occur and new evidence arrives. The key is the ability to revise models as new evidence accumulates *before* experiencing collapse or failure events—proactive learning. However, organizations can rationalize away evidence that contradicts current models and plans especially in complex systems under production/resource pressures. As a result, previous approaches can become rigid even as information builds that the world is changing and that the usual approaches are not producing desired results. The Columbia Space Shuttle accident is a vivid example of discounting evidence under productions pressure even though the indicators showed the system was operating well outside of its boundaries (e.g., Woods, 2005). Skill at proactive learning offsets this risk.

Instruments for Resilience Management

The key evidence about the difference between resilient and brittle systems comes from studies of cases where graceful extensibility developed to compensate for increasing brittleness and from studies of cases where graceful extensibility was reduced, undermined, or exhausted leading to failures (Cook, 2006; Finkel, 2011; Stephen et al., 2015). The empirical base of cases is growing and provides information for organizations to enhance their Resilience Management approaches.

Techniques to build the resilience of critical digital infrastructure have emerged (e.g., Allspaw, 2012; Robbins et al., 2012). These organizations, against conventional wisdom, 'embrace' small failures — even during important periods of operations — because they recognize that edge of the envelope events will continue to arise regardless of efforts to better plan ahead and utilize more automation. These events at the edge provide crucial information and learning opportunities. These events reveal and highlight what skills and tools provide graceful extensibility: the abilities to recognize anomalies, coordinate across roles, intervene to block potential cascades, decide which infrastructure functions are key to preserve, and prepare to recover operations, all quickly. Plus, shortly after the anomaly is resolved, extensive blameless post-mortem learning methods are used to revise how infrastructure is managed. The learning process develops general skills needed for future anomalies, because the organization knows the next anomaly they experience is likely to be quite different from the last anomaly they faced.

Measurements and Indicators of Graceful Extensibility

All systems have boundaries, or a range of adaptive behavior, whose location is uncertain and continually changing. All systems face surprises that challenge their boundaries and create the risk of brittleness-induced failures. Saturation occurs when the system is no longer able to respond to keep pace with changing demands, disturbances, and challenges (e.g., Cook, 2006). Saturation is dangerous, for example, the risk of the decompensation rises as the response capability of the system becomes saturated (hence, why avoiding saturation is a basic goal in control engineering techniques).

This means that all systems need mechanisms that can come into play to provide sufficient graceful extensibility to *control the risk of saturation*. The risk of saturation provides a general control parameter to manage the risk of failures due to brittleness (Fariadian et al., 2016). No matter what is to be controlled or managed, and no matter how well that is controlled or managed, things can and will change. When that change or new challenge occurs, some capacity has to be there to draw on to adjust to the change or challenge — otherwise the system is too brittle and the risk of collapse in performance on an important dimension is too high.

This quick overview of the basics of the emerging Theory of Graceful Extensibility highlights what is the fundamental capacity to be measured. It is the risk of saturating that system's *capacity to maneuver* as new events occur. Saturation refers to how much of the system's capacity to maneuver has been used up to handle ongoing events which then reduces what remains available to handle future events. As a system nears saturation, it has exhausted its ability to handle upcoming events — it is at the brittle breaking point (Woods & Branlat, 2011).

Understanding what capabilities and resources produce graceful extensibility leads to new descriptions of critical measurable and actionable concepts. Examples include:

> *Saturation*: When responses to current demands exhaust a unit's range of adaptive behavior or capacity for maneuver.
>
> *Risk of saturation*: Contrast of remaining range of adaptive behavior or capacity for maneuver to what is needed to handle ongoing and upcoming demands.
>
> *Brittleness*: Insufficient graceful extensibility to manage the risk of saturation (as a new more actionable operational definition).

These and related concepts are leading to new control engineering approaches to measuring and managing the risk of failures due to brittleness for complex systems (e.g., Doyle and Csete, 2011; Fariadian et al., 2016).

Annotated Bibliography

Allspaw, J. (2012). Fault injection in production: Making the case for resilience testing. *ACM Queue*, 10(8), 30-35. doi: 10.1145/2346916.2353017.
Illustration of resilience management for critical digital infrastructure.

Bush, S.F., Hershey, J., & Vosburgh, K. (1999), Brittle system analysis, http://arxiv.org/pdf/cs/9904016.pdf.
Tools to assess brittleness of systems in general based on material science concepts and measures.

Cook, R.I. (2006). Being bumpable: Consequences of resource saturation and near-saturation for cognitive demands on ICU practitioners. In D.D. Woods & E. Hollnagel, *Joint Cognitive Systems: Patterns in Cognitive Systems Engineering*. (p. 23–35). Boca Raton, FL: Taylor & Francis/CRC Press.
Example study of how people adapt to control the risk of saturation in critical care medicine.

Dietz, T., Ostrom, E., & Stern, P.C. (2003). The struggle to govern the commons. *Science*, 302(5652), 1907.
Fundamental results on how human systems overcome the risk of working at cross purposes — locally adaptive behavior that is globally maladaptive.

Doyle, J. C., & Csete, M.E. (2011). Architecture, Constraints, and Behavior, *Proceedings of the National Academy of Sciences USA*, 108, Sup 3: 15624-15630.
Non-mathematical explanation of general properties of complex layered networks that manage risk of brittleness.

Fariadian, A.B., Annaswamy, A.M., & Woods, D.D. (2016). Towards A Resilient Control Architecture: A Demonstration of Bumpless Re-Engagement Following an Anomaly in Flight Control. *Proceedings of the International Symposium on Sustainable Systems and Technologies* (ISSN 2329-9169). Jun-Ki Choi and Annick Anctil, co-editors, Sustainable Conoscente Network, ISSSTNetwork@gmail.com.
Example of a new control algorithm to enhance graceful extensibility in an aviation case.

Finkel, M. (2011). *On Flexibility: Recovery from Technological and Doctrinal Surprise on the Battlefield*. Stanford Security Studies.
Contrasts match cases of resilience in action versus brittleness in action from military history.

Robbins, J., Allspaw, J., Krishnan, K., & Limoncelli, T. (2012). Resilience Engineering: Learning to embrace failure. *Communications of the ACM*, 55(11), 40-47. doi: 10.1145/2366316.2366331
Illustration of resilience management for critical digital infrastructure.

Stephens, R.J., Woods, D.D., & Patterson, E.S. (2015). Patient Boarding in the Emergency Department as a Symptom of Complexity-Induced Risks. In R.L. Wears, E. Hollnagel, J. Braithwaite, (Eds.), *Resilience in Everyday Clinical Work* (pp. 129-144), Farnham, UK: Ashgate.
Example study of how different units in a hospital adapt to control the risk of saturation even when it sometimes constricts the adaptive capacity for other parts of the hospital system.

Wears, R.L., Perry, S.J., Anders, S., & Woods, D.D. (2008). Resilience in the Emergency Department. In E. Hollnagel, C. Nemeth and S. W. A. Dekker, eds., *Resilience Engineering Perspectives 1: Remaining sensitive to the possibility of failure*. Ashgate, Aldershot, UK, pp. 193-209.
General patterns of resilience-in-action are evident in how Emergency Rooms adapt to changing patient loads.

Woods, D.D. (2005). Creating Foresight: Lessons for Resilience from Columbia. In W. H. Starbuck and M. Farjoun (eds.), *Organization at the Limit: NASA and the Columbia Disaster*. pp. 289--308. Malden, MA: Blackwell.
The Columbia Space Shuttle accident is an example of brittleness-induced failure.

Woods, D.D. (2006). Essential Characteristics of Resilience for Organizations. In E. Hollnagel, D.D. Woods and N. Leveson, eds., *Resilience Engineering: Concepts and Precepts*. Ashgate, Aldershot, UK, pp. 21-34.
Resilience as the opposite of brittleness, results from studies of resilience-in-action, and how systems manage or mismanage fundamental trade-offs.

Woods, D.D. (2015). Four Concepts for Resilience and their Implications for Systems Safety in the Face of Complexity. *Reliability Engineering and System Safety*, 141, 5-9. doi:10.1016/j.ress.2015.03.018.
Introduces graceful extensibility and contrasts this with other uses of the label resilience.

Woods, D.D., & Branlat, M. (2011). How Adaptive Systems Fail. In E. Hollnagel, Paries, J., Woods, D.D., and Wreathall, J., Eds., *Resilience Engineering in Practice* (pp. 127-143), Aldershot, UK: Ashgate.
Introduces the three basic forms of breakdown in adaptive systems and illustrates them in the context of urban firefighting.

Woods, D.D., & Wreathall, J. (2008). Stress-Strain Plot as a Basis for Assessing System Resilience. In E. Hollnagel, C. Nemeth and S. W. A. Dekker, eds., *Resilience Engineering Perspectives 1: Remaining sensitive to the possibility of failure*. Ashgate, Aldershot, UK, pp. 145-161.
A new form of adaptive landscape that builds on key concepts from material science to model the varieties of adaptive capacity of complex adaptive systems.