Resilience as an Engineered System Property

Does it Make Sense?
What Sense does it Make?

DRAFT WORKING PAPER

Chong Tang, Kevin Sullivan, ...

Abstract

The concept of resilience as a property of engineered systems has garnered considerable attention in recent years. Yet the status of the concept remains unsettled and our ability to specify, realize, and assure resilience properties remains weak. We have conflicting conceptions of the origins of resilience, as either an engineered or organic property. The relationship of resilience to other recognized properties, such as survivability, is unclear. We have numerous but informal and inconsistent definitions of resilience. We have various *mechanisms* that support specific, often narrow notions of resilience. The resilience literature is sparse. We lack resilience specification languages and assurance methods. This paper presents a survey and analysis of work on resilience as a system property, distinct from mechanisms, and assesses the status of the concept and needs for future research and development.

1 Definitions

The International Council on Systems Engineering (INCOSE) defines resilience as "the ability of organizational, hardware and software systems to mitigate the severity and likelihood of failures or losses, to adapt to changing conditions, and to respond appropriately after the fact [**?**]."

2 Related Work

We comprehensively summarize the literature about the definitions of resiliency and related concepts.

Lundberg proposed a systemic resilience model [14]. They think resiliece as a system property, is a contradictory/ trade-off definition of other properties like changeability and robust. So instead of trying to give a simplistic definition, they give a systemic resilience model. It contains six functions: anticipation, monitor- ing, response, recovery, learning, and self-monitoring, as well as four areas: Event-based constraints, Functional Dependencies, Adaptive Capacity and Strategy.

David Woods [27] summaries the label *resilience* as four basic concepts: 1) resilience as rebound from surprise events, no matter the events are anticipated or not; 2) resilience as a synonym for robustness, the ability to absorb perturbations; 3) resilience as graceful extensibility when a system needs to handle almost infinite operating states with finite resources; 4) resilience as sustained adaptability to manage an adaptive system that are layered networks, or a part of layered networks in a large scale. The value

of first two concepts is conventional and have been studying for a long time. The latter two concepts are a rich set. He then argues that in practice, one needs to explicitly point out which one of the four meaning of resilience.

2.1 DoD perspective

The general definition of a resilient system somewhat depends on the discipline and the framework employed for discussion. From Goerger et. al. [1] define the general resiliency in plain English as:

A resilient system is trusted and effective out of the box, can be used in a wide range of contexts, is easily adapted to many others through reconfiguration and/or replacement, and has a graceful and detectable degradation of function.

The perspective of DoD slightly varies though. Their perspective has following key properties: 1) the ability to Repel/Resist/Absorb Disruptions; 2) the ability to recover from disruptions; 3) the ability to adapt to new or changed conditions; 4) and broad utility. Since most systems that DoD cares about is the military equipments, they have some unique characteristics, such as:

- Unknown and Uncertain Environments
- Mobile and Limited Support Structure
- Extreme Conditions
- Agile and Adaptive Adversary
- Changing Natural/Manmade Environments

3 Do we really need Resilience?

Some famous researchers may argue that we don't need resilience at all. They argue that resilience is just another word for survivability that we understand very well. Nevertheless, some other researchers argue that Resilience is a totaly new way to think about safety. Woods [28] explained that in industry, efforts to improve the safety of a system are often dominated by hindsight, say usually drive by events that have happened. It is a nature motivation to make sense and reasoning things already happened. However,

in acdemic institutions, our researches ought to be driven by intellectual, to think about things that might happen in the future. Resilience is such a new way to think about safety. It is not adding a new term to the existing vocabulary, but introducing a completely new vocabulary.

Not like other safety related concepts, resilience allows people to produce success when failure threatens, but not incrementally add some efforts to fix the holes found from the happened failures.

Bibliography

See references...

3.1 Useful URLs

1. Four primary attributes of Resilience: capacity, flexibility, tolerance, and inter-element collaboration
   (a) `http://www.incose.org/newsevents/currentevents/2014/10/23/webinar-15-00-utc-architecting-resilient-systems`
2. `http://www.incose.org/docs/default-source/wgcharters/resilient-systems.pdf?sfvrsn=6`
3. `http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=C359CF09E0E785A43C91C0A doi=10.1.1.169.9384&rep=rep1&type=pdf`

3.2 Books

- INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities

3.3 Slides

- `http://www.slideshare.net/JR_Ruault/sociotechnical-systems-resilience`
- `http://www.slideshare.net/SERENEWorkshop/presentations`

References

[1] S. R. Goerger, A. M. Madni, and O. J. Eslinger, "Engineered resilient systems: A DoD perspective," *Procedia Computer Science*, vol. 28, no. Cser, pp. 865–872, 2014.

[2] A. Azadeh, V. Salehi, B. Ashjari, and M. Saberi, "Performance evaluation of integrated resilience engineering factors by data envelopment analysis: The case of a petrochemical plant," *Process Safety and Environmental Protection*, vol. 92, no. 3, pp. 231–241, 2014.

[3] J. Bergström, R. van Winsen, and E. Henriqson, "On the rationale of resilience in the domain of safety: A literature review," *Reliability Engineering & System Safety*, vol. 141, pp. 131–141, 2015.

[4] D. Bodeau, R. Graubart, J. Picciotto, and R. McQuaid, *Cyber Resiliency Engineering Framework*, 2012, no. September.

[5] O. Diez and A. Silva, "Resilience of cloud computing in critical systems," *Quality and Reliability Engineering International*, vol. 30, no. 3, pp. 397–412, 2014.

[6] J. Fitzgerald, P. G. Larsen, K. Pierce, M. Verhoef, and S. Wolff, "Collaborative modelling and co-simulation in the development of dependable embedded systems," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6396 LNCS, pp. 12–26, 2010.

[7] S. Flood and J. Schechtman, "Ocean & Coastal Management The rise of resilience : Evolution of a new concept in coastal planning in Ireland and the US," *Ocean and Coastal Management*, vol. 102, no. January 2002, pp. 19–31, 2014.

[8] C. Guariniello and D. DeLaurentis, "Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks through Interdependency Analysis," *Procedia Computer Science*, vol. 28, no. Cser, pp. 720–727, 2014.

[9] M. Bellare and P. Rogaway, *The exact security of digital signatures-How to sign with RSA and Rabin*, 1996.

[10] J.-C. Laprie, "From dependability to resilience," *38th Annual IEEE/IFIP International Conference On Dependable Systems and Networks*, p. Fast abstracts, 2008.

[11] N. Leveson, N. Dulac, D. Zipkin, J. Cutcher-Gershenfeld, J. Carroll, and B. Barrett, "Engineering Resilience into Safety-Critical Systems," *In Resilience Engineering: Concepts And Precepts*, pp. 95–123, 2006.

[12] M. Liu and D. Hutchison, "Towards Resilient Networks Using Situation Awareness," *PGNet2011*, 2011.

[13] T. Lu, J. Zhao, L. Zhao, Y. Li, and X. Zhang, "Towards a Framework for Assuring Cyber Physical System Security," vol. 9, no. 3, pp. 25–40, 2015.

[14] J. Lundberg and B. J. Johansson, "Systemic resilience model," *Reliability Engineering & System Safety*, vol. 141, pp. 22–32, 2015.

[15] A. M. Madni and S. Jackson, "Towards a conceptual framework for resilience engineering," *IEEE Systems Journal*, vol. 3, no. 2, pp. 181–191, 2009.

[16] A. M. Madni and M. Sievers, "Systems Integration: Key Perspectives, Experiences, and Challenges," *Systems Engineering*, vol. 14, no. 3, pp. 305–326, 2011.

[17] R. Neches and A. M. Madni, "Towards Affordably Adaptable and Effective Systems," *Systems Engineering*, vol. 14, no. 3, pp. 305–326, 2011.

[18] R. M. Pietravalle and D. M. Lanz, "Resiliency Research Snapshot," 2011.

[19] M. G. Richards, D. E. Hastings, D. H. Rhodes, and A. L. Weigel, "Defining Survivability for Engineering Systems," *Conference on Systems Engineering Research*, pp. 1–12, 2007.

[20] A. W. Righi, T. A. Saurin, and P. Wachs, "A systematic literature review of resilience engineering: Research areas and A research agenda proposal," *Reliability Engineering & System Safety*, vol. 141, pp. 142–152, 2015.

[21] C. Rochas, T. Kuzecova, and F. Romagnoli, "The concept of the system resilience within the infrastructure dimension: application to a Latvian case," *Journal of Cleaner Production*, vol. 88, pp. 358–368, 2014.

[22] G. a. Shirali, I. Mohammadfam, and V. Ebrahimipour, "A new method for quantitative assessment of resilience engineering by PCA and NT approach: A case study in a process industry," *Reliability Engineering and System Safety*, vol. 119, pp. 88–94, 2013.

[23] M. Sievers and A. M. Madni, "A Flexible Contracts Approach to System Resiliency," pp. 1002–1007, 2014.

[24] Stockholm Resilience Centre, "What is resilience?" Tech. Rep., 2014.

[25] C. Systems, "Resilient Cyberphysical Systems," no. December 2012, pp. 2012–2013, 2014.

[26] Various, "System Resilience at Extreme Scale White Paper," *Computer*, 2009.

[27] D. Woods, "Four Concepts for resilience and the Implications for the Future of Resilience Engineering," *Reliability Engineering & System Safety*, vol. 141, pp. 5–9, 2015.

[28] D. D. Woods, "Prologue: Resilience Engineering Concepts," *Resilience Engineering: Concepts and Precepts*, pp. 1–6, 2006.

[29] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward resilient security in wireless sensor networks," *Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp. 34–45, 2005.

[30] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Bas, "Resilient Control of Cyber-Physical Systems against Denial-of-Service Attacks.pdf," pp. 0–5, 2013.

[31] E. Hollnagel, D. D. Woods, and N. Leveson, Eds., *Resilience Engineering: Concepts And Precepts*. Ashgate Pub Co, 9 2006.

[32] J. Knight, E. Strunk, and K. Sullivan, "Towards a rigorous definition of information system survivability," *Proceedings DARPA Information Survivability Conference and Exposition*, vol. 1, 2003.

[33] S. R. Centre, "Resilience dictionary," http://www.stockholmresilience.org/21/research/what-is-resilience/resilience-dictionary.html, 2015, [Online; accessed 29-August-2015].

[34] D. J. Bodeau, R. D. Graubart, and E. R. Laderman, "Cyber resiliency engineering overview of the architectural assessment process," *Procedia Computer Science*, vol. 28, pp. 838 – 847, 2014, 2014 Conference on Systems Engineering Research.

[35] O. Erol, D. Henry, and B. Sauser, "Exploring resilience measurement methodologies," *INCOSE International Symposium*, vol. 20, no. 1, pp. 302–322, jul 2010.

[36] S. Sheard, "A framework for system resilience discussions," *INCOSE International Symposium*, vol. 18, no. 1, pp. 1243–1257, jun 2008.

[37] S. Jackson, "A multidisciplinary framework for resilence to disasters and disruptions," *J. Integr. Des. Process Sci.*, vol. 11, no. 2, pp. 91–108, Apr. 2007.

[38] ——, "System resilience: Capabilities, culture and infrastructure," *INCOSE International Symposium*, vol. 17, no. 1, pp. 885–899, jun 2007.

[39] N. Suri and G. Cabri, *Adaptive, Dynamic, and Resilient Systems (Mobile Services and Systems)*. Auerbach Publications, 2014.