Robustness and Reconfigurability – Key Concepts to Build Resilience

Hans Rudolf Heinimann[i]*

Keywords: Robustness, reconfigurability, resilience, organisational mindfulness

*Corresponding author: hans.heinimann@frs.ethz.ch

Introduction

Urbanization is an aggregation process that fosters the emergence of urban clusters where much of the world population resides, and where the magnitude of human activities prevails. Several phenomena characterise this process (Heinimann & Hartfield, 2017), in particular (1) the continuously increasing density of infrastructure assets per unit of area, (2) the flows of goods, services, information and people, borne by layered infrastructure networks that are enabling a different type of flows continue to expand dramatically, and (3) cities of today represent a nascent skeleton of cybernetic organism (cyborg) entities that constitute an interdependent mosaic of advanced infrastructure systems, enabling technologies, green spaces and social systems. Additionally, “smart technology” policies, such as “smart cities”, “smart nation” emerged, adding cyber-components to our physical infrastructure, which will amplify the cyborg trend significantly. A considerable amount of human design and development activities is still relying on certainty assumptions, while risk management – emerging in the 1950s to cope with large-scale impacts technologies in case of failure – introduced a systematic approach to cope with uncertainties. The above trends result in higher levels of complexity, which is going along with emergent behaviour and ambiguous or even unexpected behaviour that we are not able to explain with historical data. Resilience management is extending risk management to cope with ambiguous, unexpected events.

This development trend is facing some fundamental challenges. First, expected damages due to disruptions will increase because the value at risk has grown. Second, climate change is changing the uncertainties of environmental states, which will undermine the very assumptions used to design existing interdependent engineering systems. Third, the coupling strength between and within the infrastructure, organisational and user systems continues to grow and may result in regime shifts that foster system disruptions that were never experienced before and that cannot be explained with observational data of the past.

Risk management developed methods and tools to assess and manage portfolios of uncertain events (Keller & Modarres, 2005). The underlying assumption is that the process of generating those uncertain events is staying the same in time and that it is possible to characterise both frequency and consequence with the methods of extreme value statistics. Complex systems might demonstrate emerging behaviour and disruptions, which means that the process that this is generating those

---

[i] Future Resilient Systems, Singapore-ETH Centre, Singapore

Suggested citation: Heinimann, H. R. (2018). Robustness and reconfigurability – Key concepts to build resilience. In Trump, B. D., Florin, M.-V., & Linkov, I. (Eds.). *IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems.* Lausanne, CH: EPFL International Risk Governance Center. Available on irgc.epfl.ch and irgc.org.

events is changing in time, which makes the methods of risk management questionable. This calls for a new approach, which is focusing on robustness and resilience. Robustness refers to design characteristics of the system, aiming to provide reliable performance for a set of requirements, despite changes in the environment or within the systems after the system has entered service; it is a strategy to bring uncertainty and ambiguity into the design process. Resilience refers to the:

> *biophysical capacity of a system to resist within acceptable limits of degradation, to re-stabilising is crucial functions, to rebuild functionality up to a sufficient level of performance, and to reconfigure its flows of services and the underlying physical structures. This biophysical capacity is coupled with the cognitive ability to perceive the state of the system and its environment, to understand its significance and meaning, to retrieve purposeful courses of actions, to release the most meaningful action and to learn and to adapt (adapted from Heinimann & Hatfield, 2017).*

The purpose of this contribution is to provide a framework for how resilience-based management augments traditional risk-based management approaches, and to discuss strategies how to build resilience. It explores first the essence of ambiguous and unexpected system states, triggered by complexity properties, which is the primary rationale why there is a need for resilience-based management. It then explores three strategies that have the potential to build resilience effectively.

Beyond risk management – Coping with complexity

The quality of available knowledge of infrastructure system behaviour under different endogenous and exogenous conditions is the crucial issue (Figure 1, x-axis). Many engineering approaches, for example those identifying optimal solutions with mathematical methods, rely on certainty assumptions; that is, they assume complete knowledge of the system and the environment. The introduction of uncertainty enables the relaxation of those assumptions with expectation values, which are the product of probability times some metrics of consequences. Probabilistic risk analysis, which is the backbone of risk management since the 1950s is a stream of thinking, which still represents the state-of-the-art (Keller & Modarres, 2005). Further relaxation of what is known is engendered in the concept of ambiguity (Renn & Klinke, 2004), which assumes that there are observations on some phenomena, which proffer several legitimate interpretations of meaning. In air traffic control, ambiguity is termed as "weak signals", and most often, there is no finite interpretation of meaning. There is yet another level of system knowledge, which is characterised by "unexpected" or "unknown". The "dragon king" concept (Sornette, 2009) assumes – and successfully demonstrates – that there are options to anticipate or predict "unknown events" if we have real-time information about the system behaviour with an adequate time granularity (Sornette & Ouillon, 2012).

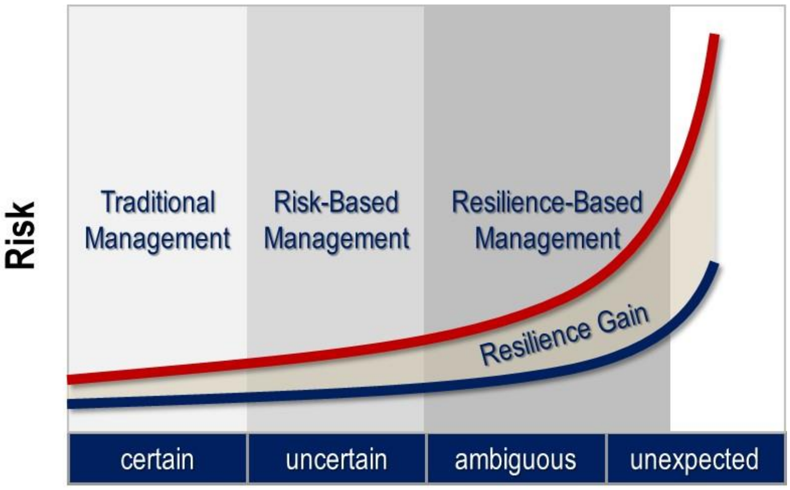

Figure 1: The influence of knowledge domains and a new design and management paradigm on risk. Adapted from (MURRAY et al., 2013).

The y-axis of figure 1 presents the expected adverse consequences for the different categories of knowledge and different management strategies for a system. Up to the 1950s, approaches to design and manage infrastructure systems were based on certainty assumptions. With the emergence of probabilistic risk analysis in the 1950s (Keller & Modarres, 2005), risk management approaches – aiming to eliminate or prevent unacceptable risks – improved the overall safety and security of our systems tremendously. Today's constructed infrastructure systems are more complex and highly connected; these changes have pushed a significant fraction of urban infrastructure systems into the "ambiguous" and "unexpected" knowledge domains, and in turn increased the risk of adverse and ill-defined consequences (upper line, figure 1). Ambiguous and lacking knowledge about a system means that communities, engineers, and governments have to cope with invalid assumptions (Day et al, 2015), either due to unexpected changes in the environment or due to emerging and unforeseen behaviours in critical infrastructure systems (Haimes et al., 2008). Communities must acquire the capacity to ensure infrastructure systems continue to provide critical services and support essential function whenever and wherever invalid assumptions reside (Day et al, 2015). The capacity of a system to cope with invalid assumptions is the hallmark of a resilient system, which unfortunately does not appear in most resilience definitions.

Ambiguous or unexpected phenomena that are emerging have their roots in complexity. Complexity comprises phenomena, which emerge from a collection of interaction objects, and the purpose of complexity science is to understand, predict and control such emergent phenomena (Johnson, 2011). It is remarkable that such emerging phenomena arise without the presence of any central controller or coordinator. There are key properties of the system that are required for emergent behaviour (Johnson, 2011): (1) many interacting objects or "agents", (2) memory or "feedback" is affecting the objects' behaviour, (3) objects can adapt their strategies, and (4) the system is "open", which means its interaction with the environment matters. This perspective raises the question in which systems there are properties of complexity. Human factors, in general, are the first source of complexity. Considering that large-scale infrastructure systems are a compound of engineered, organisational and user subsystems yields that all large-scale infrastructure systems are complex and prone to ambiguous and unexpected behaviour, which calls for resilience management. Cyber components are a second source of complexity. The "smart" trend augments many of our infrastructure systems with semi-automatic or automatic control systems, consisting of sensors, controllers and actuators, which together provide feedback, are adaptive and interacting with the environment. The ongoing digitisation is amplifying human adaptability and the spread of cyber-physical-systems (Lee, 2015), which together will increase ambiguous and unexpected system behaviour.

Policymakers and practitioners are facing the issue of whether risk management is still a useful approach or whether resilience management should augment it. Risk management is always an appropriate methodology in domains in which adaptive system components are of minor significance, which is right for "mechanistic" processes, such as some natural hazards. Fields in which human factors have been dominating, such as geopolitical, social and financial hazards are calling for a resilience-based management approach. As mentioned above, digitalisation has been amplifying effect on the adaptive behaviour of humans, which will make this request even more critical. Domains in which cyber-physical systems or cyber-physical-human systems are dominating are requesting a resilience-based management approach, too.

Strategies to build resilience

In the introduction, we defined resilience in terms of generic system functions, consisting of four biophysical functions: (1) resist within acceptable limits of degradation, (2) restabilize the crucial functions, (3) rebuild functionality up to a sufficient level, and (4) reconfigure flows of services and the enabling physical structures. These biological and physical capabilities are coupled with five cognitive functions: (5) perceive the state of the system and its environment, (6) understand its significance and meaning, (7) retrieve purposeful courses of actions, (8) release the most meaningful action, and (9) learn and adapt. Each of those nine functions contributes to resilience, which represents a multi-objective optimisation problem with an efficiency frontier (Pareto frontier), at which no single function can be improved without decreasing the performance of at least one of the other eight functions. Unfortunately, we do not understand the trade-space yet. We hypothesise that three functions have a considerable leverage effect: resist within acceptable limits of degradation (robustness), reconfigurability, and understanding the significance of the system state and its environment (sense-making).

Robustness is a pre-event strategy to identify system designs that perform well when facing variations in conditions of use, with time and use, and in production and manufacturing, whereas variations mean deviations from design assumptions (Saleh et al., 2003). Robust optimisation proved to be useful to identify optimal courses of action for the protection and the extension of large infrastructure systems (Caunhye & Cardin, 2017; Costa et al., 2018; Rahmat et al., 2017). However, it has not been widely used by policymakers and practitioners.

Reconfigurability is a post-event strategy to repeatedly change and rearrange the components of a system cost-effectively, thus attaining different states with new or modified capabilities, over time (Setchi & Lagos, 2004). The concept has its origin in reconfigurable computing of the 1960s, appearing in reconfigurable robotics in the 1980s, and spreading to reconfigurable manufacturing systems in the 1990s. To our knowledge, there is no significant research on reconfigurability of infrastructure systems, which calls for a new research thrust to be developed. Of course, some of the fundamental concepts, such as modularity, integrability, or convertibility seem to have significant potential. Many resilience papers have been highlighting the role of adaptability, which – in its narrow sense – means to move limit state thresholds without fundamental structural change. Thus, this strategy is less effective than reconfigurability.

Mindfulness sense-making is a during-event organisational process, aiming to stay attentive to what is going on in the present (mindfulness refers to staying in the present) and to create a meaningful group-mental model that is useful to identify and to release useful courses of action (Weick et al., 2008). For a long time, research in organisational behaviour has been focusing on decision-making, thus neglecting what has to happen before, problem framing (Simon et al., 1986). It is problematic and even misleading to map ambiguous and uncertain events to predefined mindsets and assumptions, which bears high risk to result in wrong assessments of the situation and ineffective actions. Weick (1993) started his research on mindfulness with so-called "Mann Gulch Forest Fire", in which 13 firefighters lost their lives due to a wrong sense-making. Research is still at an early stage, but it seems that organizational processes matter (Sutcliffe, 2018), in particular (1) staying engaged with changing physical realities of the internal and external environments, (2) communicating and coordinating, (3) meaning management, dealing with the meaning of people's experiences, and (4) connection management to collectively bear the burden of adversity.

Previous considerations implicate that building resilience has a positive effect. The question is how resilience affects the risks of a system of interest. Building robustness significantly reduces the vulnerability of the system, and consequently, adverse events will result in lower consequences. Modifying a system for reconfigurability reduces the rehabilitation efforts, which equals a reduction in the cost of consequences. Overall, building resilience will result in a risk reduction (see resilience gain in figure 1), which emphasises that resilience-based is augmenting risk-based management strategies. Another question is if a transition of a system from a pre-event to a post-event state can be actively managed. Managing disasters stems from organisational capacity and processes, which means that there is some guiding idea how the rehabilitated system should look like that is driving the disaster management activities. Experience yields that organisational capacities, processes and culture have a significant effect how a society or societal group is managing a disruption cycle, starting with a shock, going on to restabilization of critical functions, and ideally resulting in the reconfiguration of the flow of essential services and their enabling physical structures.

Annotated bibliography

Caunhye, A. M. & Cardin, M.-A. (2017). An approach based on robust optimization and decision rules for analyzing real options in engineering systems design. *IISE Transactions, 49*(8), 753-767. Model case how to identify system designs that are robust and flexible.

Costa, A., Georgiadis, D., Ng, T. S., & Simm M. (2018). An optimization model for power grid fortification to maximize attack immunity. *International Journal of Electrical Power & Energy Systems, 99*, 594-602. Model case how to identify protection measures against malicious attack.

Day, J. C., Ingham, M. D., Murray, R. M., Reder, L. J., & Williams, B. C. (2015). Engineering resilient space systems. *INCOSE Insight, 18*(1), 23-25. Proposed the levels of knowledge we have about a system linked to management approaches, illustrated in figure 1.

Haimes, Y. Y., Crowther, K., & Horowitz, B. M. (2008). Homeland security preparedness: Balancing protection with resilience in emergent systems. *Systems Engineering, 11*(4), 287-308. An early paper emphasizing the importance of unexpected events, and assessing the trade-offs between protection and resilience.

Heinimann, H. R. & Hatfield, K. (2017). Infrastructure resilience assessment, anagement and governance - State and perspectives. In I. Linkov & J. M. Palma-Oliveira (Eds.), *Resilience and* *risk: Methods and applications in environment, cyber and social domains* (pp. 147-187). Dordrecht, NL: Springer. Comprehensive resilience framework and discussion of the state-of-the-art in related fields of science.

Johnson, N. F. (2011). *Simply complexity. A clear guide to complexity theory.* Oxford OX2 7AR: Oneworld Oxford. Comprehensive introduction into complexity science.

Keller, W., & Modarres, M. (2005). A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: A tribute to the late Professor Norman Carl Rasmussen. *Reliability Engineering & System Safety, 89*(3), 271-285. Review of the development trajectory of risk management.

Lee, E. A. (2015). The past, present and future of cyber-physical systems: A focus on models. *Sensors, 15*(3), 4837-4869. Overview on cyber-physical systems, including a perspective on development trends.

Murray, R. M., Day, J. C., Ingham, M. D., Reder, L. J., & Williams, B. C. (2013). Engineering resilient space systems. Retrieved from http://www.kiss.caltech.edu/study/systems/. Proposed the levels of knowledge we have about a system linked to management approaches, illustrated in figure 1.

Rahmat, M., Caunhye, A. M, & Cardin, M.-A. (2017). *Flexibility and real options analysis in design for long-term generation expansion planning of power grids.* ASME 2017 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Cleveland, Ohio, USA, August 6–9, 2017. Model case how to extend a power grid for robustness.

Renn, O., & Klinke, A. (2004). Systemic risks: A new challenge for risk management. *EMBO Reports, 5(1)*, 41-46. Introduction of the ambiguity and unexpectedness as challenges of systemic risks.

Saleh, J. H., Hastings, D. E., & Newman, D. J. (2003). Flexibility in system design and implications for aerospace systems. *Acta Astronautica, 53*(12), 927-944. Framework for robust and flexible system design.

Setchi, R. M., & Lagos, N. (2004). *Reconfigurability and reconfigurable manufacturing systems: State-of-the-art review*. IEEE international conference on industrial informatics, 529-535. Review of the reconfigurability concept.

Simon, H. A., Dantzig, G. B., Hogarth, R., Plott, C. R., Raiffa, H., Schelling, T. C., Shepsle, K. A., Thaler, R., Tversky, A., & Winter, S. (1986). Report of the Research Briefing Panel on Decision Making and Problem Solving. In *Research Briefings 1986*, E. Committee on Science, and Public Policy, Editor (pp. 17-36). Washington, DC: National Academy Press. Comprehensive review on the state-of-the-art in decision-making and problem solving.

Sornette, D. (2009). *Dragon-kings, black swans and the prediction of crises*. Swiss Finance Institute Research Paper, (09-36). Introduction of a novel behavioural regime for complex systems that is beyond the so-called "self-organised criticality" regime, which is an assumption of extreme-value statistics.

Sornette, D., & Ouillon, G. (2012). Dragon-kings: Mechanisms, statistical methods and empirical evidence. *The European Physical Journal Special Topics, 205*(1), 1-26. Review of the state-of-the-art in Dragon King regimes, including mechanisms that describe regime shifts.

Sutcliffe, K. M. (2018). Organizational resilience in action. International Conference on Infrastructure Resilience, Zurich. Emphasis that organisational processes matter, as opposed to the study of organisational capabilities.

Weick, K. E. (1993). The collapse of sensemaking in organizations: The Mann Gulch disaster. *Administrative Science Quarterly*, 628-652. Seminal paper illustrating that the problem framing phase matters in emergency situations, proposing the mindfulness framework.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: Processes of collective mindfulness. *Crisis Management, 3*, 81-123. Organisational science view, emphasizing that keeping awareness in the present is required to overcome prejudgments and the mapping of phenomena to predefined mental models.