Resilience Engineering and Quantification for Sustainable Systems Development and Assessment: Socio-technical Systems and Critical Infrastructure[i]

Ivo Häring[1], Benjamin Scharte[1], Alexander Stolz[1], Tobias Leismann[1], Stefan Hiermaier[1]

[1]Fraunhofer EMI, Freiburg, Germany

Contact: Ivo.Haering@emi.fraunhofer.de

Keywords: Resilience Engineering, Sustainability, Resilience, Quantification, Resilience management cycle, Technical resilience properties, Resilience dimensions, Analytical resilience quantification, Resilience trajectory expansion, Resilience Engineering quantification

Challenge of sustainable, efficient and resilient and systems: definition of technical Resilience Engineering

Modern system development, improvement, innovation and assessment has to take into account an ever increasing variety as well as increasingly competing goals. Such goals include: sustainability, effectiveness, efficiency, user attractiveness but also safety and security (Assembly, 2000). For example, for past automotive vehicles safety was a luxury, since decades at least a basic level is standard. In a similar way, sustainability and cyber security of vehicles are currently novel topics and will evolve to established requirements. Similar arguments are argued to hold true when requiring that (socio) technical systems are capable of coping with adverse events.

This text aims at showing that a thorough Resilience Engineering can substantially contribute to improving safety and security as well as the adaptive capabilities of complex socio-technical systems when they face adverse and potentially disruptive events. Those capabilities, which can be summarized as resilience, are a key characteristic of sustainability. In our modern world that depends on (ultra-)complex, interdependent, coupled networks of infrastructure, sustainable development is only achievable, if we learn to design and optimize our systems in a resilient way (Thoma, 2014). Systems covered range from infrastructure lifelines to small devices.

Resilience Engineering means preserving critical functionality, ensuring graceful degradation and enabling fast recovery of complex systems with the help of engineered generic capabilities as well as customized technological solutions when the systems witness problems, unexpected disruptions or unexampled events (Thoma, Scharte, Hiller, & Leismann, 2016). Hence, Resilience Engineering is a new and innovative approach to improving the resilience of systems with the help of the technical and engineering sciences. Those sciences are able to understand, analyse and improve a vast set of different kinds of systems, ranging from microsystems to global infrastructure networks. In

[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*

particular, RE tries to find ways to enhance the resilience of critical infrastructure, e.g. electric, energy and telecommunication grids.

The resilience of such systems can be defined as their capability to successfully

(1) prepare for
(2) prevent
(3) protect from
(4) respond to, and
(5) recover from

minor up to larger, creeping up to sudden, known up to completely unexampled disruptions, taking into account the societal and technical contexts (Häring, Ebenhöch, & Stolz, 2016; Thoma, Scharte, Hiller, & Leismann, 2016). A system is resilient if it is successful in combining all resilience management phases to minimize the negative effects of any kind of adverse events.

The overview on Resilience Engineering is structured as follows. Section 1 gave an overview and a definition on Resilience Engineering. Section 2 lists main Resilience Engineering objectives, Section 3 discusses frameworks for generating resilience, and Section 4 shows how to develop and measure resilience.

Technical objectives of Resilience Engineering

This section elaborates on the objectives of the technical science-driven Resilience Engineering approach. We categorize 12 resilience engineering objectives (from (i) to (xii)) into 5 main objectives ((A) to (D)).

(A) Technical-engineering Resilience Engineering approach. Resilience engineering aims at making the sufficient generation of resilience of (socio) technical systems a well-defined, scalable and flexible scientific-engineering process that is supported by appropriate methods. Accordingly, objectives of Resilience Engineering are

(i) to provide engineering, technical and natural science founded approaches and processes to achieve resilience of (socio) technical systems. For instance as indicated in section 3.
(ii) to develop tailorable validated methods to conceptualize, design, develop and assess resilient systems. For instance, to refine what it means to achieve overall success in all resilience management phases (1) to (5).

In the same way as risk analysis and control emerged as a new engineering branch in the 1970s and 1980s, it is expected that resilient engineering for handling a large variety of (potential) disruptions will emerge as a new technical science domain. Thus, Resilience Engineering allows fulfilling many of the aims for modern sustainable system developments as listed in the introduction.

(B) Extension and where appropriate replacement of (classical) risk approaches. Further main objectives include:

(iii) To extend and where appropriate to replace classical notions of risk analysis and management with resilience concepts, approaches and methods. For instance, to allow

for a more flexible chance enhancement and/or risk control for systems focusing on post event options for response and recovery.

(iv) To allow for extended and novel perspectives on risk events, risk propagation, risk assessment and risk control. For instance, to conduct chance/risk management of long-term system availability objectives.

(v) To be better able to prepare for less expected, seldom, unexpected, unknown or even unexampled – so-called "black swan" – events. For instance by focusing on the chance/risk assessment of technical resilience capabilities.

(C) Seamless extensions of notions of reliability and maintainability. Important aims of resilience engineering are

(vi) To seamlessly link to and to extend classical notions of reliability. For instance, by understanding and investigating the level of resilient performance of technical systems in case of major disruptions as an extension of the classical reliability of systems designed to handle minor statistical and systematic failures.

(vii) To extend maintenance concepts to response and recovery approaches post major disruptive events. For instance, by defining systems (e.g. part of European high-voltage grid >380 kV) to be sufficiently large to be able to consider major disruptions (e.g. local electricity grid failure) as smaller failures.

(viii) To use and improve on resilience indicators that are also relevant for the daily successes of systems and vice versa. For instance, to define current reliability level of electricity supply in case of a set of possible minor up to larger disruptions.

(D) Integration of physical security, technical safety and IT security approaches. Resilience objectives cover all types of potentially disruptive events. Therefore main aims of resilience engineering include:

(ix) To integrate physical security, safety, IT-security approaches. For instance to determine and evaluate the chances and risks on resilience using approaches from all corresponding disciplines and aggregating their analyses semi-quantitatively.

(x) To provide at least conceptual technical and engineering processes and methods that are independent of the type of adverse or disruptive event considered. For instance, by developing analytical resilience assessment approaches.

(E) High societal and organizational commitment. The notions of resilience engineering invite for individual and collective participation as well as organizational involvement. For instance, by focusing on technical capabilities of systems that can be defined in positive terms. More generally speaking resilience engineering objectives include:

(xi) To achieve a high level of individual, organizational and societal commitment of all actors: third party, decision-makers, developers, system designers, system assessment personnel. For instance, by including highly unlikely events and their long-term consequences within risk control.

(xii) To ask for the input and feedback of end-users and third parties. For instance, by focusing on empowerment of actors when using technical resilient systems, by asking for the level of local controllability of scenarios and the time duration of scenarios as well as for taking account of perceived risks.

Generating resilience for (technical) systems and processes: Resilience development framework options

This section indicates how within the Resilience Engineering approach resilience of systems is generated. Feasible strategies to achieve the resilience engineering objectives listed in section 2 include:

(a) To generate metrics and measures for the success of the resilience management phases (1) to (5). For instance, to use qualitative, semi-quantitative up to quantitative approaches.
(b) To identify, specify and develop (technical) resilience capabilities (resilience functionalities, services, or capacities) sufficient for all potential disruptive events. For instance, to require that specific key functions of a technical system are also available in case of loss of the main energy supply.
(c) To identify, operationalize and specify for systems (generic) resilience properties, attributes or specifications which by themselves or in combination suffice for sufficient resilience. For instance, redundancy or physical robustness.
(d) To extend classical risk management and assessment approaches with notions of resilience analysis, management and enhancement (Häring, 2015; Linkov et al., 2014). For instance, to conduct risk analysis and management taking account of response and recovery options.

It can be argued that developing technical resilience capabilities is the most viable approach when focusing on technical systems. Technical resilience capabilities can be defined as any technical capability, function or functionality. Therefore, reliability functions (standard, comfort functions) of a technical system can be supplemented with resilience functions and capabilities. This is very similar to adding functional safety functions for controlling risks in safety relevant or critical systems to reliability functions of systems (Siebold, Larisch, & Häring, 2010).

Furthermore, technical resilience functions can be defined very flexibly in terms of their qualitative and quantitative requirements. In addition, they can be realized independently, mixed with existing functions or completely being part of existing functions.

Such technical resilience capabilities should include (Finger, Häring, Siebold, & Hasenstein, 2016) (Häring, Ebenhöch et al., 2016):

1. Sensing and observation, for generating situation awareness,
2. Modelling and simulation for situation representation,
3. Inference and decision-making for selection of response options (if any),
4. Action and response for implementation of response options and
5. Adaptation and change, for improving overall capabilities according to (1) to (4).

Metrics, criteria, indicators for quantifying successful Resilience Engineering

This section shows that by now a variety of approaches and methods have been developed or proposed to quantify resilience. Four main strands can be identified (Häring, Ebenhöch et al., 2016) (Häring, Scheidereiter, et al. 2016):

(A) Analytical resilience quantification, which is based on the nested combination of (semi-) quantitative resilience dimensional assessments, e.g. using as outer cycle the resilience management cycle or risk management cycle. A possible starting point is to focus on chances for

resilience objectives for each resilience management phase (1) to (5) by asking for a systems technical resilience capabilities according to 1. To 5. (Finger et al., 2016) (Baumann, Häring, Siebold, & Finger, 2014) (Schoppe, Häring, & Siebold, 2014) (Schoppe et al., 2015) (Siebold, Hasenstein, Finger, & Häring, 2015);

(B) Resilience expansions with respect to resilience dimensions, e.g. number of events, resilience phases affected, etc. For instance, the assessment may focus on the immediate response in case of double physical cyber events.

(C) Resilience trajectory propagation, mainly for using or combining probabilistic-statistical and standardized engineering-simulative approaches. This approach focuses on the consideration of multiple possible events and their forward and backward propagation. Propagation is understood as mapping event descriptions.
For instance, in case of forward propagation earthquake threat is mapped on/propagated to well-defined seismic events, to regional loadings, to local loadings, to building loading, to physical building damage, to physical person loading, to personnel damage quantification, to building damage evaluation, to personnel damage evaluation, and finally to overall damage evaluation. Examples are: (Fischer, Siebold, Vogelbacher, Häring, & Riedel, 2014) (Fischer, Häring, Riedel, Vogelbacher, & Hiermaier, 2016) (Riedel et al., 2014) (Voss, Häring, Fischer, Riedel, & Siebold, 2012) (Esmiller et al., 2013) (Salhab, Häring, & Radtke, 2011a) (Salhab, Häring, & Radtke, 2011b) (Häring, Schönherr, & Richter, 2009);

(D) Based on socio-technical cyber-physical system simulations (Renger, Siebold, Kaufmann, & Häring, 2015). For instance, recovery times of airport checkpoints after security-induced disruptions can be determined from simulations.

Such Resilience Engineering quantities can be used for formulating overall resilience optimization objectives, for instance (Häring, Ebenhöch et al., 2016)

I. to optimize the probability of an acceptable overall total resilience of a system,
II. to minimize the probability of non-acceptable overall total resilience of a system,
III. to optimize the total chance for fulfilling resilience objectives,
IV. to minimize the total risks on resilience objectives.

Summary and outlook

In summary, Resilience Engineering strongly supports to meet a prerequisite for sustainable and efficient systems: to sufficiently benignly respond to adverse events, i.e. to be resilient (section 1). By that, Resilience Engineering meets several of the most challenging technical objectives of modern system development and overall risk control (section 2). By now, a variety of approaches and frameworks exist how to design resilience in development and improvement of systems (section 3). It is argued that the identification, design and development of technical resilience capabilities is most viable. Resilience can be quantified using fast analytical (table-top) approaches up to complex socio-technical system simulations for generating time-dependent resilience indicators (section 4).

Annotated Bibliography

Assembly, U. G. (2000). United Nations millennium declaration. *Resolution adopted*, *18*.

Baumann, D., Häring, I., Siebold, U., & Finger, J. (2014). A web application for urban security enhancement. In K. Thoma, I. Häring, & T. Leismann (Eds.), *9th future security. Berlin, September 16 - 18, 2014; proceedings* (pp. 17–25). Stuttgart: Fraunhofer-Verlag.
Example of an engineering application expert tool for enhancing resilience

Esmiller, B., Curatella, F., Kalousi, G., Kelly, D., Amato, F., Häring, I., . . . Katzmarekt, K. U. (2013). FP7 Integration Project D-Box: Comprehensive Toolbox for Humanitarian Clearing of Large Civil Areas from Anti-Personal Landmines and Cluster Munitions. In *International Symposium Humanitarian Demining* (pp. 21–22).
Example of an application toolbox for enhancing resilience

Finger, J., Häring, I., Siebold, U., & Hasenstein, S. (2016). Analytical resilience quantification for critical infrastructure and technical systems. In *European Safety and Reliability Conference (ESREL).*
Example for analytical semi-quantitative resilience quantification.

Fischer, K., Häring, I., Riedel, W., Vogelbacher, G., & Hiermaier, S. (2016). Susceptibility, vulnerability, and averaged risk analysis for resilience enhancement of urban areas. *International Journal of Protective Structures*, *7*(1), 45–76. doi:10.1177/2041419615622727
Example for statistical-empirical and fast engineering-simulative resilience quantification with focus on the assessment of the level of prevention, protection and what-if vulnerability.

Fischer, K., Siebold, U., Vogelbacher, G., Häring, I., & Riedel, W. (2014). Empirische Analyse sicherheitskritischer Ereignisse in urbanisierten Gebieten. *Bautechnik*, *91*(4), 262–273. doi:10.1002/bate.201300041
Example for statistical-empirical-historical resilience quantification with focus on preparation in terms of the identification of possible events and statistical-empirical frequency and damage assessments.

Häring, I. (2015). *Risk analysis and management: Engineering resilience*. Singapore: Springer.
Textbook on engineering risk analysis and management for the civil security and safety research domain and how its approaches contribute to Resilience Engineering with focus on preparedness, prevention, protection, what-if vulnerability, and post-event counter measures.

Häring, I., Ebenhöch, S., & Stolz, A. (2016). Quantifying Resilience for Resilience Engineering of Socio-Technical Systems. *European Journal for Security Research*, *1*(1), 21–58. doi:10.1007/s41125-015-0001-x
Literature for detailing section 4 on options for resilience quantification.

Häring, I., Schönherr, M., & Richter, C. (2009). Quantitative hazard and risk analysis for fragments of high-explosive shells in air.*Reliability Engineering & System Safety*, *94*(9), 1461–1470. doi:10.1016/j.ress.2009.02.003
Example for statistical-engineering-simulative quantification of risks of moving explosive sources for increasing preparedness, prevention and protection.

Häring, I., J. Scheidereiter, Ebenhöch, S, von Ramin, M., Riedel, W., & Stolz, A. (2016). Combining engineering and simulation approaches for effective risk and resilience management and analysis of critical infrastructure. In *Conference protect 2016 Leipzig, Germany.*
Literature for detailing section 4 on options for resilience quantification.

Linkov, I., Kröger, W., Renn, O., Scharte, B. et al. (2014). *Risking Resilience: Changing the Resilience Paradigm*, Commentary to Nature Climate Change, 4(6), 407-409.
Literature on the Resilience paradigm.

Renger, P., Siebold, U., Kaufmann, R., & Häring, I. (2015). Semi-formal static and dynamic modeling and categorization of airport checkpoints. *Nowakowski, T.: Safety and reliability: Methodology and applications: Proceedings of the European Safety and Reliability Conference, ESREL 2014, Wrocław, Poland, 14 - 18 September 2014. Boca Raton, Fla.: CRC Press, 2015, pp. 1721-1731.* doi:10.1201/b17399-234
Example for modelling a complex socio technical system in the security domain sufficient for security risk quantification with respect to disruptive events. In this case illicit goods or dangerous goods passing airport checkpoints.

Riedel, W., Niwenhuijs, A., Fischer, K., Crabbe, S., Heynes, W., Müllers, I., . . . Häring, I. (2014). Quantifying urban risk and vulnerability – a tool suite of new methods for planners. In K. Thoma, I. Häring, & T. Leismann (Eds.), *9th future security. Berlin, September 16 - 18, 2014; proceedings* (pp. 8–16). Stuttgart: Fraunhofer-Verlag.
Engineering application tool for increasing the resilience of urban quarters with respect to the terroristic threat.

Salhab, R., Häring, I., & Radtke, F. (2011a). Formalization of a quantitative risk analysis methodology for static explosive events. In C. Soares (Ed.), *Advances in Safety, Reliability and Risk Management* (pp. 1311–1320). CRC Press.
Detailed formalization of a statistical-engineering approach to quantify frequency, consequences and individual and collective risks in case of explosions for improving preparation in terms of prevention (reducing frequency) and protection (reducing vulnerability).

Salhab, R., Häring, I., & Radtke, F. (2011b). Fragment launching conditions for risk analysis of explosion and impact scenarios. In C. Soares (Ed.), *Advances in Safety, Reliability and Risk Management* (pp. 1579–1587). CRC Press.
Example for hazard threat source characterization as key input for risk and resilience assessment appraoches.

Schoppe, C., Zehetner, J., Finger, J., Baumann, D., Siebold, U., & Häring, I. (2015). Risk assessment methods for improving urban security. In T. Nowakowski, M. Młyńczak, A. Jodejko-Pietruczuk, & S. Werbińska-Wojciechowska (Eds.), *Safety and reliability. Methodology and applications, proceedings of the European Safety and Reliability Conference, ESREL 2014, Wrocław, Poland, 14-18 September 2014* (pp. 701–708). London: Taylor & Francis Group.
Examples for risk and resilience assessment methods regarding urban security and safety threats.

Schoppe, C. A., Häring, I., & Siebold, U. (2014). Semi-formal modeling of risk management process and application to chance management and monitoring. In Steenbergen, R. D. J. M. (Ed.), *Safety, reliability and risk analysis. Beyond the horizon* (pp. 1411–1418). London: Taylor & Francis Group.
Example for migrating and tailoring risk management towards a chance management process for urban security and safety enhancement taking account of the urban context.

Siebold, U., Hasenstein, S., Finger, J., & Häring, I. (2015). Table-top urban risk and resilience management for football events. In L. Podofillini, B. Sudret, B. Stojadinović, E. Zio, & W. Kröger (Eds.), *Safety and reliability of complex engineered systems. Proceedings of the 25th European Safety and Reliability Conference, ESREL 2015, Zürich, Switzerland, 7-10 September 2015* (pp. 3375–3382). Boca Raton: CRC Press.
Example for migrating and tailoring risk management towards a chance management process for public security and safety enhancement in case of football events.

Siebold, U., Larisch, M., & Häring, I. (2010). Using SysML Diagrams for Safety Analysis with IEC 61508. In *Sensoren und Messsysteme. Vorträge der 15. ITG-GMA-Fachtagung vom 18. bis 19. Mai 2010 in Nürnberg.* Berlin, Offenbach: VDE-Verl. Retrieved from http://www.vde-verlag.de/proceedings-de/453260131.html
Example for identifying and modelling safety functions using semi-formal methods. In a similar way, resilience functions could be identified and modeled for resilient system design.

Thoma, K., Scharte, B., Hiller, D., & Leismann, T. (2016). Resilience Engineering as Part of Security Research: Definitions, Concepts and Science Approaches. *European Journal for Security Research*, *1*(1), 3–19. doi:10.1007/s41125-016-0002-4
Programmatic article for defining Resilience Engineering as a technical science discipline.

Thoma, K. Ed. (2014). Resilien Tech. Resilience by Design: a strategy for the technology issues of the future (acatech STUDY). München: Herbert Utz Verlag.
Programmatic book on the definition of resilience science, technology and engineering.

Voss, M., Häring, I., Fischer, K., Riedel, W., & Siebold, U. (2012). Susceptibility and vulnerability of urban buildings and infrastructure against terroristic threats from qualitative and quantitative risk analyses. In *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012. (PSAM11 ESREL 2012); Helsinki, Finland, 25 - 29 June 2012* (pp. 5757–5767). Red Hook, NY: Curran

Description of the combination of empirical-statistical and engineering-simulative quantitative descriptions of multiple possible adverse (malicious, terroristic) events. The aim is to assess frequency, damage and risks of threats to reduce susceptibility and vulnerability and to improve preparation in terms of increasing prevention and protection. Approach can also be applied to accidental and natural events.