Eur J Secur Res (2016) 1:3–19
DOI 10.1007/s41125-016-0002-4

ORIGINAL ARTICLE

Resilience Engineering as Part of Security Research: Definitions, Concepts and Science Approaches

Klaus Thoma[1] · Benjamin Scharte[1] · Daniel Hiller[1] · Tobias Leismann[1]

Received: 21 December 2015 / Accepted: 22 December 2015

Abstract This article focuses on the rather new concept of Resilience Engineering (RE). Resilience has emerged as a special concept within the vast area of civil security research. Resilience Engineering can provide society and its critical infrastructure with means, methods and technologies to overcome unexampled events with as less harm as possible and to come out even stronger and better prepared afterwards. Civil security research has tended to focus on specific threats. The concept of resilience, by contrast, is inherently holistic. After all, it is about securing the well-being of people. We try to establish RE as a way of thinking that enables us to handle all kinds of adverse events properly. To answer the question about the understanding what RE really is, this article gives an overview of some of the most important developments and definitions concerning resilience. In contrast to the most common focus on human factors in areas like aviation safety, air traffic management (ATM), maritime safety and patient safety we rather suggest to deliberately limit the scope of Resilience Engineering. This limitation—which is necessarily vague due to the nature of resilience as a concept—allows us to distinguish between several ways to enhance the resilience of complex systems. For RE, there needs to be a clear focus on engineering. 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. Finally, the important aspect of a quantitative description of resilience via mathematical modelling of complex systems is introduced. The aim is to produce multimodal simulations that use an

✉ Klaus Thoma
Klaus.Thoma@emi.fraunhofer.de

[1] Fraunhofer-Institut für Kurzzeitdynamik, Ernst-Mach-Institut, EMI, Eckerstraße 4, 79104 Freiburg, Germany

integrated approach to model technological and social systems and the complex interactions between them.

Keywords Security research · Resilience engineering · Resilience engineering review · Critical infrastructure · Modelling of critical systems

1 Introduction

The tsunami, that followed the Tōhoku earthquake on March 11th 2011, hit the Japanese coast at the Fukushima Daiichi nuclear power plant with a height of up to 15 m. Its seawall was only designed to withstand a wave of 5.7 m (Hollnagel and Fujita 2013: 14ff). Could they have known better before? Was there a chance to prevent the Fukushima Daiichi nuclear disaster? Very much like the September 11 attacks, the Tōhoku earthquake and the subsequent tsunami are described as unexampled events, events that "are virtually impossible to imagine" (Hollnagel and Fujita 2013: 16). They were so entirely unexpected that nobody really prepared for them. Of course, the U.S. knew about the general risk of being attacked by Islamic terrorists before and the Japanese evidently are among the most experienced nations when it comes to earthquakes and their consequences. But the sheer dimension of both incidents struck the respective nations unprepared. They exceeded the collective experience of both nations by far (Hollnagel and Fujita 2013: 16).

This article makes a point that although it is "impossible to prepare a response to something that has not been considered in advance" (Hollnagel and Fujita 2013: 16) the newly emerging field of Resilience Engineering (RE) can provide society and its critical infrastructure with means, methods and technologies to overcome even such unexampled events with as less harm as possible and to come out even stronger and better prepared afterwards. The article will thereby concentrate on the resilience of critical infrastructure which can be seen as an example for various different systems but which are also especially important for the functioning of society. Finding ways to minimize the damage a society suffers from so called adverse events is the raison d'être of civil security research. In doing so, civil security research has tended to focus on specific threats (e.g. Linkov et al. 2014: 407). The concept of resilience, by contrast, is inherently holistic. After all, it is about securing the well-being of people (Bruno 2015: 29).

The question then is: What is Resilience Engineering? And to what extend does the "engineering claim" go beyond the conceptual framework, which has already been broadly defined and disputed among various scientific communities? To answer these questions the following article elaborates both on resilience as a conceptual framework as well as on RE with a clear focus on the latter. We have been working on resilience and especially RE for a couple of years now. Our ideas and understanding of the two concepts have been published i.a. in Thoma (2014) and Thoma and Scharte (2015). This article builds on our previous publications. And it goes further when it comes to defining and understanding RE as a useful concept and research topic for civil security research. It integrates findings from the

RE community, namely from researchers like David Woods, Erik Hollnagel, Sidney Dekker and Azad Madni. Those findings are interpreted in the light of a more technologically oriented approach towards RE and merged with our own ideas about it.

We start with the underlying premise that the idea of an accident/incident-free world is not realistic. This "vision zero" will not become a reality because our systems—societal, technical and socio-technical—are too complex to be understood or controlled completely (Dekker 2014: 33). Even in so called high reliability organizations (HROs, on HROs cf. Dekker and Woods 2010), which manage to fulfill a complex task on a daily basis very well, adverse events do happen. No matter, whether triggered from outside or inside the system, by chance or by purpose, disruptions are something, systems have to be able to cope with. This fact could only be changed by dismantling the system as such, which is not a realistic option because we depend on the services provided by complex systems (Dekker 2014: 33). In the following sections we analyze ways how complex systems can deal with problems, unexpected disruptions and unexampled events by using and implementing the concept of Resilience Engineering.

2 Resilience as a Concept Within Civil Security Research

The well-being of people depends on a lot of different variables—ranging from things like personal health, having a family and being employed to overall societal factors like the reliable functioning of critical infrastructure. Security and thus resilience research cannot contribute to all of these variables. But they i.a. are able to help ensuring the sustained functioning of our critical infrastructure in the face of adverse events. In this article we do not concentrate on a specific kind of adverse events. We rather try to establish RE as a way of thinking that enables us to handle all kinds of adverse events properly. In this context, an incident is not necessarily a one-off event and may equally involve long-term changes and their potentially radical consequences. Its causes may be either man-made or natural (all hazards approach) (The National Academies 2012a: 14).

Within the last decade, our societies had to witness such events. Terrorist attacks, natural disasters—the occurrence of which may increase because of the effects of climate change—or severe accidents are rare but can have devastating effects. Especially when they cause cascading effects within our closely linked and intertwined systems (Coaffee et al. 2009: 122–132). Growing complexity, dependency and interconnectedness make critical infrastructure susceptible towards disruptive incidents. Current risk analysis often concentrates on specific components of systems as well as known and expected threats (Linkov et al. 2014: 407). This is not enough anymore. In a world which is facing ever more threats and which is intrinsically more vulnerable because of growing complexity we need RE to enable our systems to dynamically adapt to changing conditions.

The occurrence of such disruptive or unexampled events is the reason, why besides classical risk management also reliability of a system is not enough. Reliability in a traditional sense—namely "that safety can be maintained by keeping

system component performance inside acceptable and prespecified bandwidths"—is not the same as security or resilience (Dekker and Woods 2010: 139). High reliability within narrow system boundaries could impede resilient behavior when the system faces unprecedented stress. Reliability is a characteristic of components of complex engineered systems. Such a component understood as just a single part of a system can be reliable but it cannot be resilient (Dekker and Woods 2010: 126). The relationship between reliability and resilience in complex engineered systems needs to be clarified.

But what is resilience? A detailed analysis describing the history of resilience as a concept can be found in Scharte et al. (2014a). For the purpose of this article we will give a brief overview of some of the most important developments and definitions concerning resilience. The concept has come a long way in the past 60 years. It started as an attribute of individuals, who were better able to withstand diseases than others. In physics and materials science resilience is a material's ability to deform elastically when acted upon by energy. As such it can be measured as the maximum energy that the material is capable of absorbing per unit volume without creating a permanent deformation (i.e. without deforming plastically or brittle). Thus, the resilience of materials deals with its elasticity, flexibility and the ability to withstand high loads (Kaufmann and Blum 2012: 237; Plodinec 2009: 1f). This formalistic definition of resilience is just a starting point for a holistic understanding of the concept. Within security research resilience is acknowledged as a property of dynamically adapting complex systems, today (CSS-Analysen 2009: 1; Flynn 2011; Kaufmann and Blum 2012: 237ff; Plodinec 2009: 1).

It was the Canadian ecologist Holling whose work could be called a paradigm shift within resilience research. In 1973, he published an article entitled "Resilience and Stability of Ecological Systems". He was the first to analyze resilience as a characteristic of entire ecosystems instead of individual people. What Holling was interested in was the system's ability to survive abrupt, radical and irreversible disruptions triggered by unusual, unanticipated and surprising events. Without Holling's work, the transfer of the concept of resilience to what is referred to as security research could not have happened (Holling 1973: 14ff, 21; Kaufmann and Blum 2012: 239f; Walker and Cooper 2011: 145ff).

As mentioned above, following Holling resilience was discussed in many scientific disciplines. After our analysis of the history of this concept we concluded that the definition given by the National Academies' Committee on Increasing National Resilience to Hazards and Disasters is a good basis (Scharte et al. 2014a: 15f; Thoma and Scharte 2015: 31). They define it as "the ability to prepare and plan for, absorb, recover from or more successfully adapt to actual or potential adverse events" (The National Academies 2012a: 14). Taken together with Charlie Edwards thoughts on resilience (Edwards 2009: 20ff) we developed our own working definition for the concept:

> "Resilience is the ability to repel, prepare for, take into account, absorb, recover from and adapt ever more successfully to actual or potential adverse events. Those events are either catastrophes or processes of change with

catastrophic outcome which can have human, technical or natural causes" (Scharte et al. 2014a: 17).

To better illustrate this theoretical definition we extended Edwards resilience cycle for our own purposes (Fig. 1). The extended resilience cycle consists of five phases called prepare, prevent, protect, respond and recover. In reality there is no simple chronological order. Real-life systems cannot execute respective actions for all of the phases one after the other. But for the sake of illustration this resilience cycle is a suitable instrument. The five phases—although they cannot be separated completely from each other—embody specific characteristics of resilient systems. For example in the prepare-phase systems have to make thorough preparations for disasters. More or less at the same time they will try to reduce underlying risk factors to prevent severe disruptions from occurring in the first place. This is not possible for all kinds of adverse events, but certainly for some. If an incident or accident still cannot be prevented, resilient systems have physical and virtual protection systems in place that minimize negative effects. In responding to the disruption, such systems are also able to maintain their basic functionality as far as possible and at the same time provide fast, well-organized and effective disaster relief. When it comes to recovering from what happened, resilient systems are able to learn the relevant lessons and adapt their functioning to be better prepared for future hazards.

The resilience cycle illustrates that there cannot be an end in efforts to make a system more resilient. Resilience is a property of dynamic, adaptable systems and not a static condition which can be reached permanently. A resilient system differs from others mainly in its ability to respond dynamically to constant changes in its environment and to adapt to unforeseen events. It is not important what measures the system or its operators take to ensure and enhance resilience. In this sense, resilience is a holistic way of thinking about security. As stated above, this article hereafter concentrates on the engineering part of resilience building, because it is

Fig. 1 The resilience-cycle (Scharte et al. 2014a:17)

the "quality of engineering" that is decisive for a systems ability to survive disruptive and even unexampled events (Rahimi and Madni 2014: 811f). It also concentrates on technological and socio-technical systems, where technology can have a positive impact on resilience.

3 Resilience Engineering Review

Being successful in creating resilient systems depends on a lot of different things. One of these is the nature and the quality of the engineering effort put into building and maintaining the system. We started this article by assuming that Resilience Engineering can provide systems like critical infrastructure with appropriate tools and instruments to withstand disruptions. But what exactly is RE? The discipline of Resilience Engineering is "still in its earliest stage", or even in "its infancy" (Bruno 2015: 9, 33). During the last years there has been a growing interest in RE. Nonetheless the concept still lacks formal definitions and frameworks (Farid 2015: 1). Michael Bruno recently published a review on RE. From his point of view the concept needs a "solid foundation" which "would address interconnectedness; the modelling of the two layers—social and technology, and autonomy; examining failure-cascades, and identifying the various attributes of recovery. Such an effort will need to draw on network theory, game theory, and simulation, including agent-based simulation" (Bruno 2015: 28).

Before going into more detail about the origin and the current state of debate concerning RE, we want to elaborate on the relationship between RE and reliability. Our systems are getting more and more complex. Notwithstanding problems caused by the growing complexity of technical and socio-technical systems, this article does not follow the arguments of Charles Perrow. In his seminal work "Normal Accidents. Living With High Risk Technologies" Perrow argues that the complexity of technological systems such as nuclear power stations makes them inherently vulnerable (Perrow 1999a). Tight couplings—i.e. close linkages between the individual parts of a system, resulting in a high risk of "contagion" in the event of a disturbance—mean that total system failure is inevitable at some point. Since the system failure is both unforeseen and unforeseeable in terms of its specific nature, the responsible actors are unable to respond adequately to it, thereby further hastening the system's collapse. Perrow refers to accidents caused by tight couplings and complexity as "normal accidents"—in his original work, he argued that this type of accident is impossible to prevent (Rijpma 1997: 16).[1] This is not in line with our understanding of complexity and its effects. Complexity may cause cascading effects but it does not inevitably lead to collapse and "normal" accidents. Increasing the system's reliability can be a suitable tool to prevent such accidents from happening (Rijpma 1997: 17). What is reliability? "Reliability in the engineering domain deals with the ability of the system and its components to perform required functions under stated conditions for a specified period of time" (Madni and Jackson 2009: 183). This article states that reliability is a precondition

[1] Later on Perrow himself also advanced his thinking (Perrow 1999b: 150ff).

for resilience but it is not sufficient. Yet, depending on how we build reliability, it could even be a hindrance for resilience (Rahimi and Madni 2014: 813). This resembles Hollings idea of seemingly stable ecosystems which suddenly collapse at a previously unknown tipping point (Holling 1973: 16ff). The same may hold true for complex engineered systems with a high reliability. Their high reliability, which is "executed" via compliance towards formalized rules and procedures, proves to be a valuable asset over a long period of time and a large set of scenarios. But all the sudden something unexpected happens that falls outside the previously specified system boundaries. The formalized rules and procedures then prevent the system from (re)acting and adapting dynamically and flexibly—or resilient (Huber et al. 2009: 91). Although we reject Perrow's idea of a "normal" accident this comes quite close to his thinking. Previously suitable rules and procedures, which became ever more elaborated, complicated and specified over time, may prove to be responsible for a system breakdown when challenged by a minor but unforeseen disruption. Thus, Resilience Engineering needs to balance the benefits and downsides of high reliability for the resilience of systems. On the one hand, without reliability systems cannot be resilient. On the other hand, reliability could be a hindrance towards flexibility and adaptability. A thorough RE needs to accomplish the task to meet both these requirements.

Holling was one of the first to combine the two concepts of resilience and engineering (Holling 1996). He used the term "engineering resilience" rather than Resilience Engineering and he used the term to describe what he called the "two faces of resilience". In this way, engineering resilience is the opposite of "ecological resilience" and is about preserving stability and an ex ante defined equilibrium. Hollings definition of engineering resilience is an interesting starting point for our own understanding of RE. For him, engineering resilience is about preserving the efficiency of function whereas ecological resilience tries to maintain the pure existence of a function. These "contrasting aspects of stability […] are so fundamental that they can become alternative paradigms" (Holling 1996: 33). This is very close to the way we discussed reliability above: RE needs to be able to accomplish tasks associated with engineering as well as ecological resilience.

The discussion on RE as such started in 2004 with the first Resilience Engineering Symposium in Söderköping, Sweden (Nemeth 2008: 3). Since then a community has evolved around researchers like Chris Nemeth, Sidney Dekker and especially David Woods and Erik Hollnagel. Via the building of the Resilience Engineering Association, several subsequent RE symposia and joint publications they have established a first tradition of Resilience Engineering thinking. That is why their ideas have to be the basis for a discussion on RE. To be able to understand the way in which this community discusses resilience and RE, we have to recognize their scientific origins. Most of them come from the safety domain and/or research on human factors. The rationale of their work is summarized by the following statement: "[…] people do not come to work to do a bad job. Behavior is rational within situational contexts" (Dekker 2004: 90). Thus, a lot of the literature on RE deals with human factors in areas like aviation safety, air traffic management (ATM), maritime safety and patient safety. In summary, within the RE community there is no real focus on the engineering part of RE (Huber et al. 2009: 91).

Nevertheless, the principles developed by them are useful to create our own theory and understanding of Resilience Engineering. Following Hollnagel, Woods and their colleagues complex systems often are designed to withstand well-known threats but are unable to cope with the unexpected. Accident analysis necessarily has to be done ex post and tends to fall victim to the so-called "hindsight bias".[2] In hindsight the reasons for accidents seem to be completely clear. The established causal relationship goes: If person A did not act that way, there would have been no accident. According to the RE approach this is an invalid simplification and reduction of complexity and the dynamic interactions of real-world systems. Another effect of ex post accident analysis is "distancing through differencing" which means that people tend to see the differences to their own field of responsibility rather than underlying systematic similarities (Madni and Jackson 2009: 183; Woods 2003: 2, 5). And as the principle "engineering systems are designed to operate within, but not outside, certain conditions" applies here, putting the emphasis on already known threat scenarios may lead to a fatal neglect of unexpected novel damaging events (Nemeth 2008: 5).

Hindsight bias often leads to blaming people as (solely) responsible for accidents. This is where the RE community disagrees. The starting point for developing the theory of Resilience Engineering is the notion that in complex systems blaming people for accidents is of no help to sustain and improve the system and prepare it for future disruptions. Hollnagel and Woods consider RE to be a consistent and systematic continuation and extension of classical safety analysis (Hollnagel and Woods 2011: 356). Resilience Engineering is about possibilities and not probabilities. Resilient systems are able to handle unexpected disruptions or even unexampled events by means of RE. For that, they need to have adequate safety margins. Such systems will keep up their distinct functionality even when a highly unexpected adverse event occurs (Hollnagel and Woods 2011: 348; Madni and Jackson 2009: 182ff; Nemeth 2008: 6). The next step then is central to the thinking of the RE community. They shift their focus from analyzing accidents to analyzing things that go right or the normal case. Even very complex systems normally function fluently in everyday life. Hollnagel, Woods and their colleagues thus argue that concentrating on maximizing the number of things that go right is more useful for increasing resilience than minimizing failure (Hollnagel 2011: xxxiv–xxvi). The RE community understands Resilience Engineering as all means to increase the number of things that go right in complex systems. Summarized in one sentence they say that "Resilience Engineering, however, defines safety as the ability to succeed under varying conditions" (Hollnagel 2011: xxix). Especially in HROs it is easier to increase the number of successes than to reduce failure. And furthermore, optimizing successful and well-functioning processes is not only useful under extreme conditions but for everyday operations, too (Hollnagel 2011: xxix). This understanding of RE is not very specific when it comes to concrete engineering. It is rather broad, as Hollnagel states when he says that "the goal of Resilience

[2] A very interesting essay on the hindsight bias and why the term may be misleading can be found in Dekker (2004).

Engineering becomes how to bring about resilience in a system" (Hollnagel 2011: xxxvii).

A lot of useful ideas can be found in the discussions on Resilience Engineering within the RE community. Nevertheless, we find that their understanding of the concept is insufficient in two ways, compared to what it could provide to the security research community. First of all, it is too generic. For Hollnagel, Woods and their colleagues, RE is about bringing resilience into a system by all means possible. A resilient system is able to anticipate threats, withstand disasters, learn from disruptions and adapt to changing conditions. "Resilience engineering, therefore, must address the principles and methods by which these capabilities can be created" (Madni and Jackson 2009: 187). From our point of view this is not selective enough. If we used RE as a proxy for all ways to improve the resilience of a system, there would be no difference to "building resilience" and we would not need to use the term "engineering". We rather suggest to deliberately limit the scope of Resilience Engineering. This limitation—which is necessarily vague due to the nature of resilience as a concept—allows us to distinguish between several ways to enhance the resilience of complex systems. For RE, there needs to be a clear focus on engineering.

This leads us to the second insufficiency: The RE community focuses on human factors. Resilience Engineering "considers humans as an integral part of resilience and does not focus only on technical components or redundancy as the main elements for enhancing safety in systems" (Huber et al. 2009: 91). We do not doubt that it is important to include humans as decisive factors when it comes to creating and maintaining resilient systems. But there is no need to call the concept Resilience Engineering, when means, methods and technologies from the engineering world do not play the essential part in it. On the other hand, classical engineering thinking, which views "resilience as a property of materials and infrastructure" and which is "typically associated with physical intervention, or structural measures, for disaster risk reduction" is also not enough (MacAskill and Guthrie 2014: 667). Thus, we need to further specify what RE really is. Following Hollnagel "the concepts and principles of Resilience Engineering have been tested and refined by applications in such fields as air traffic management, offshore production, health care, and commercial fishing" (Hollnagel and Fujita 2013: 13). This may hold true for their understanding of RE. As elaborated above, our own definition has to be different from that. We need to take a step back and consider that we are not yet able to apply concepts and principles of RE, but need to clarify them in the first place.

4 Resilience Engineering as an Engineering Discipline

We start with the ideas of the RE community and refine them with respect to the engineering sciences. Dekker and Woods think of safety (or rather resilience) as the availability of specific abilities to manage hazardous situations—and not as the "absence of negatives". Systems (or their operators) need to check constantly whether their ideas about the risk they are facing, are still in line with reality. Only then, the specific abilities will still be useful (Dekker and Woods 2010: 125, 138f).

But what if something completely unexpected happens, an unexampled event like the Tōhoku earthquake and the subsequent tsunami? If the system had only case-specific abilities, it would very likely fail.

This is, why Bergström et al. introduced the concept of generic competencies into the debate about Resilience Engineering (Bergström et al. 2009: 89). Those generic competencies allow for successfully handling unexpected or even unexampled situations. Bergström et al. examined an experiment which centered around the influence of rules and procedures on the success of trained and untrained crews in complicated maritime operations. They found out that teaching people generic competencies is of great use for their success rate—namely saving the life of passengers as well as the ship itself in maritime operation simulations (cf. Bergström et al. 2009). At this point we transfer their ideas into the engineering world: Resilience Engineering is the ability to create generic capabilities—as technical systems do not have competencies but capabilities—that enable complex systems to withstand, survive and adapt to disruptions with the help of solutions from the engineering sciences. In the military domain there is a similar concept called "broad utility". Despite experiencing unexpected adverse events, military systems need to function within a huge set of different scenarios (Goerger et al. 2014: 867). As it is impossible to specifically prepare for unknown threats, complex engineered systems like our critical infrastructure need to have heuristics in place which can be applied to a broad set of disruptions and accept the possibility of black swan events (Hollnagel and Fujita 2013: 19; Madni and Jackson 2009: 189).

Resilience Engineering is about creating generic capabilities to be able to handle disruptions. But it has to be more than that to be of any use for engineers who have to design and operate resilient technical systems. To be able to do that it is worthwhile to have a look at two examples from the US where ideas of RE are already implemented. The two examples are the study "Disaster Resilience. A national imperative" and the Presidential Policy Directive 21 "Critical Infrastructure Security and Resilience", published by the White House in February 2013. The study "Disaster Resilience. A national imperative" conducted by the National Research Council of the US National Academies looked for ways to increase the resilience of the United States against natural disasters. The overall result of the National Academies' study were six recommendations (The National Academies 2012a: 1ff, 9ff). As risk cannot be eliminated completely, the second recommendation is about tools, which need to be developed to minimize the damage a system suffers when disruptions occur. For this, structural as well as non-structural measures have to be applied. Structural measures could be the use of cutting-edge technologies which include resilience thinking in the design phase, already. From this, resilient construction methods can emerge (The National Academies 2012a: 13, 2012b: 4). For Resilience Engineering this recommendation offers two interesting aspects: First of all, resilience should be taken into account during the design phase of complex systems, already. And second of all, state of the art as well as cutting-edge technologies has to be used to design critical infrastructure in a resilient way. The Presidential Policy Directive 21 also contains some important ideas on how Resilience Engineering can be understood. It is about establishing a cooperative national effort to ensure security, functionality and resilience of critical

infrastructure in the US. Within PPD 21 the president of the United States appoints several tasks on the Department of Homeland Security (DHS) (The White House 2013: 1–12). One of these tasks i.a. asks the DHS to strengthen its support for research in resilient design and resilient construction ideas, tools and methods for critical infrastructure. The task also includes the request to enhance and optimize existing methods for modelling and simulation of complex systems, especially with regard to cascading effects (The White House 2013: 8). All of these different aspects—including resilience-by-design, using and improving cutting edge technologies to build and sustain critical infrastructure, increasing research in resilient construction ideas and tools as well as in methods to model and simulate complex systems—are important parts of Resilience Engineering.

The approaches and methods involved, examined and improved by RE, can be applied both, in situations where known threats appear as well as in case of any unexpected disruptions. A thorough RE, which focuses on the creation of technologically advanced generic capabilities, is even able to prepare complex systems for unexampled events. Thus, Resilience Engineering has to involve the consistent incorporation from an early stage of technological solutions to all kinds of security problems into every aspect of the planning and implementation of major social projects—from the individual to the overall system level. Its goal is to maintain the critical subfunctions of systems in a controlled manner, even when severe damage forces them to operate outside normal parameters, in other words allowing catastrophic and abrupt total system failure to be averted (graceful degradation). "What matters is preserving critical functionality, not the pre-existing system" (Bruno 2015: 11, emphasis by the present writers). This insight is decisive. RE may not be able to preserve the characteristics of systems in the face of a disruption, especially when it comes to unexampled events. But RE allows us to maintain the most critical subfunctions of a system, which are literally vital to our societies, with generic capabilities created via research and development into latest technologies and their appropriate incorporation into complex engineered systems. Besides that, it also requires customized technologies for increasing the resilience of individual, specific infrastructure. The effectiveness of such specific solutions and their impact on the system as a whole must be optimized, and they should be complemented by smart solutions from other fields like economics, ecology and the social sciences.

We now use the findings from the examples, the theoretical basis of Holling, Woods and their colleagues and the idea of generic capabilities and match them with the two decisive aspects of preserving critical functionality and ensuring graceful degradation. Taken together we acknowledge that Resilience Engineering as a concept offers the potential to deal with the constantly rising complexity of modern systems, in particular regarding a multitude of different threats (Woods and Hollnagel 2006: 6). There are some characteristics, or heuristics as Madni and Jackson describe them, which a system needs to have to be able to act and react in a resilient way when disaster occurs. Those include redundancy, backups, predictability, complexity avoidance and more (Madni and Jackson 2009: 189). Resilience Engineering seeks for means, methods and technologies to build these

characteristics into complex systems. Summing up all these thoughts and ideas, our own definition of Resilience Engineering goes as follows:

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.

This definition can be illustrated with the help of a diagram that shows the performance P of a system over time t (Fig. 2). The diagram is a rather simple visualization for the complex concept of resilience, of course. Nevertheless, it is useful to better understand our ideas about RE. The system witnesses a disruption at a certain point in time which leads to a performance loss L (defined as $L(t) = P(a) * (c - a) - \int_a^c P(t)\mathrm{d}t$). We can apply the five resilience phases to this situation and ask, how a resilient system would behave in such a case. First of all, it will try to prevent adverse events from happening. Then the performance P at any given time t would stay the same, namely $P(t) = \text{const}$. If this is not successful, the resilient system will be well prepared and have appropriate protection measures in place. In our diagram this means that a resilient system will minimize the degree to which performance level decreases [min $(P(a) - P(b))$] and maximize the time span of this decrease (max $(b - a)$) Thus, it will preserve its critical functionality ($P(b) > P_{\text{critical}}$) and ensure a graceful degradation. As soon as possible (min $(c - b)$) the system will start to respond to the disruption with the objective of re-establishing the performance level $P(a)$ again. And it will try to recover from the negative effects of the disruption as fast as possible (min $(d - b)$) and even learn from it by increasing the overall system performance (max P(d)). The objective of RE is to minimize the performance loss L by all engineering means possible. To further concretize it we need to have a look at real world systems and their performance functions.

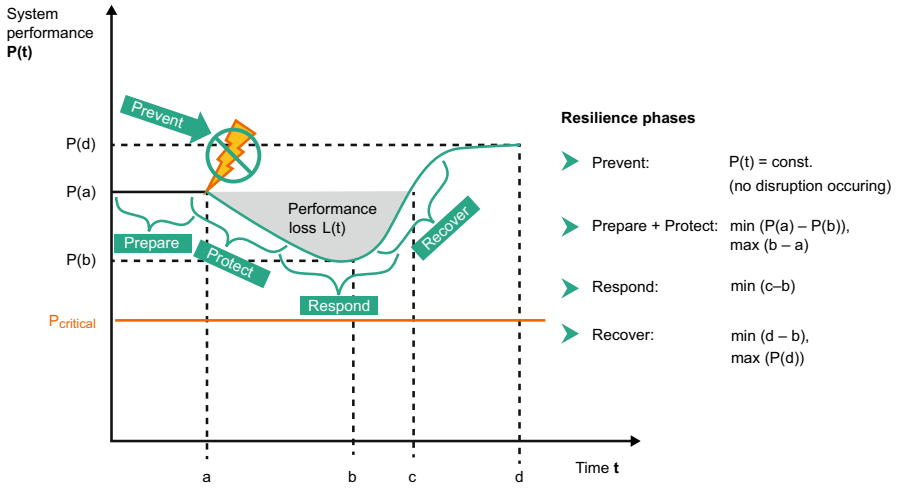

Fig. 2 Applying the principles of RE to a generic system

Examples for RE might include technologies such as self-healing, adaptive materials or smart, adaptable buildings that use energy self-sufficient automated sensor networks. Resilience Engineering also prevents the development of incompatible isolated solutions. This is where the holistic aspect of resilience comes in, since future technologies will need to be compatible both with each other and with any other potential external solutions. In the upcoming years and decades our critical infrastructure will face a huge set of challenges, ranging from climate change to terrorism and most probably some that we do not even think about, yet (Bruno 2015: 18–21). To sustain our systems and prepare them for the future, we need to start working on Resilience Engineering and the implementation of RE thinking into security research now.

5 Measuring and Modeling Resilience as Part of RE

One of the most important preconditions as well as parts of RE is the ability to quantify and measure resilience. To date, there is no well-established way to measure resilience that a majority of researchers within the field of critical infrastructure protection (CIP) could agree upon (Bruno 2015: 8). It is a tough challenge to develop suitable measurements for resilience. There are conceptual difficulties and potential methodological pitfalls. As resilience is a complex concept, it is not clear which variables are important, how to operationalize them, how to compare the resilience of different systems, which dimensions have to be integrated or whether to use qualitative or quantitative, absolute or relative measures, for example (Bara and Brönnimann 2011: 32f). However, only if we find ways to measure resilience properly, systems can be compared with regard to their resilience and thus be optimized. A suitable measurement for resilience has to integrate the all-hazards-approach and should be applicable to different kinds of systems (The National Academies 2012b: 10). If we could differentiate between several degrees of resilience in specific systems, we would be able to learn from especially resilient subsystems by detailed analyses of their experiences. We also could identify the least resilient parts and provide them with help. The development of valid indicators and rigorous metrics, thus, is a key aspect of RE (Bruno 2015: 8; Farid 2015: 1; Madni and Jackson 2009: 188).

Another essential part of RE is the modelling and simulation of complex systems. Designing systems in a resilient way requires exact and detailed knowledge about the behavior of the relevant systems in case of disruptions. Even during normal operations complex systems do not follow a simple causal logic. Their functions are intertwined and interdependent. The systems do not tend to work transparently. This makes it hard to explain why A leads to B and not to C. This opacity, the interdependencies and the complex causal interrelations get worse when the system witnesses stress which lies outside of the previously specified system parameters. The challenge for RE now is to develop suitable methods for modelling and simulation of complex systems that can handle these difficulties. As a part of risk analysis and risk management, such modelling and simulation tools have been used for decades in the field of CIP (cf. e.g. Renn 2008a, b). But classical risk analysis

focuses on forecasting the vulnerability of subsystems and system components against defined and excepted threats. When it comes to our complex, interconnected networks of critical infrastructure this is not enough anymore. The behavior of complex systems cannot be predicted by simulating only individual components and their function within prescribed and prespecified scenarios. Complexity and also the occurrence of unexpected disruptions or even unexampled events force us to improve our capacities and competencies to model and simulate the behavior of systems in the field of CIP (Al-Khudhairy et al. 2012: 574ff; Linkov et al. 2014).

There is a need for improvements in basic research, for example in mathematics and computer sciences, as well as in enhancing the development of concrete methods and software tools applicable to complex systems and especially critical infrastructure. We need even more comprehensive, ultra-advanced methods, which have to be capable of capturing the local interactions between a wide range of interconnected components and subsystems. Only then, they can realistically predict global system behavior. Such new modelling techniques will enable operators of critical infrastructure to identify weak spots of their systems, plan counter-measures to harden or avoid them and correct possible faults so that the system is as thoroughly prepared as possible in case of a disruption appearing. Another central capability of system modelling as part of RE has to be the ability to reliably identify system-critical nodes and interfaces, where failure has a high potential to lead directly to cascading effects. Failure at these spots has to be averted because it tends to cause the breakdown of the whole system. To identify such nodes and interfaces is a precondition for preserving critical functionality in the face of disaster. Taken together, future modelling techniques need to fulfill a huge set of requirements. This will only be possible, if we invest a lot of effort into research for techniques that are able to stochastically simulate components and subsystems to describe the behavior of the entire system without resorting to predefined scenarios or system states (Scharte et al. 2014b: 88). “The aim is to produce multimodal simulations that use an integrated approach to model technological and social systems and the complex interactions between them” (Scharte et al. 2014c: 120). A sound and valid model, which could forecast the probable behavior of complex systems for a wide range of possible disruptions and would be able to evaluate the effects of different resilience-enhancing measures, would be an extremely useful tool for infrastructure operators and managers, urban planners, emergency forces and other officials.

6 Conclusion

All our efforts within security research center around assuring and securing the life and well-being of people and our societies. The newly emerging field of Resilience Engineering offers a promising path to help us succeed in this task. RE can provide societies and especially their critical infrastructure with means, methods and technologies to withstand everyday problems, unexpected disruptions and even unexampled events like the Tōhoku earthquake and the subsequent tsunami with as less harm as possible. As a discipline RE is still very young and the concept is not

sufficiently clear let alone established, yet. It lacks formal definitions and frameworks.

Within this article we found out that the discourse among the RE expert communities is insufficient in two ways, so far. It is too generic and it focuses on human factors. There is a serious gap when it comes to the concrete engineering part of RE. How could this gap be filled? The thoughts of the RE community were useful as a starting point. By transferring the idea of generic competencies into the engineering world it becomes evident that we need solutions from the engineering sciences to enable complex systems to withstand, survive and adapt to disruptions. Besides that, a thorough Resilience Engineering has to make use of and improve cutting edge technologies, for example to build and sustain critical infrastructure. RE has to include resilience-by-design thinking and thus foster research in resilient construction ideas and tools. Taken together, these findings form a consistent image of RE: Resilience Engineering then 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. Two of the most important aspects of such an understanding of RE are the abilities to measure and quantify resilience as well as model and simulate the behavior of complex systems previous to, during and following a disruption. Measuring resilience allows for a differentiation between varying degrees of resilience in real-world systems. And modelling and simulating complex systems enables us to identify weak spots and system-critical nodes and interfaces. Both of these challenges, measuring and modelling resilience, are hard to meet. But it is worthwhile to foster research on these topics. In light of an ageing infrastructure with a high need for maintenance and repair and at the same time shrinking public budgets we need to be able to find out, which infrastructure is the most vulnerable, how measures will affect the overall system and where the "adjusting screws" are to avoid system breakdown and preserve critical functionality in the face of an adverse event. Only then, we will be able to prioritize action and take the right steps (Bruno 2015: 25).

Currently, Resilience Engineering is a highly debated topic in both the world of academia and research as well as in industry. Just like resilience as such, the concept has become a hot topic. Researchers from the engineering sciences like Amro Farid have begun to develop applicable and tangible frameworks for Resilience Engineering. They try to translate the complex social science concept of resilience into practice, into numbers and equations (cf. Farid 2015). In the face of global challenges like climate change, resource scarcity, terrorism and failing states, these developments are both necessary and encouraging. We must work on RE as a concept substantiated by means, methods and ideas from the engineering sciences. This article is a first step towards an understanding of Resilience Engineering that is useful and applicable for engineers within security research. We firmly believe Resilience Engineering to be an absolute necessity if we want to sustain our societies and their most important systems, like critical infrastructure and prepare them for an uncertain future. And for that, we need to start working on the implementation of RE thinking into CIP and security research right now.

References

Al-Khudhairy D, Axhausen K, Bishop S, Herrmann H, Hu B, Kröger W, Lewis T, MacIntosh J, Nowak A, Pickl S, Stauffacher D, Tan E (2012) Towards integrative risk management and more resilient societies. Eur Phys J Spec Topics 214(1):571–595

Bara C, Brönnimann G (2011) CRN Report. Risk analysis. Resilience—trends in policy and research (Focal Report 6, Crisis and Risk Network). Center for Security Studies (CSS), ETH Zürich, Zürich

Bergström J, Dahlström N, van Winsen R, Lützhöft M, Dekker S, Nyce J (2009) Rule- and role retreat: an empirical study of procedures and resilience. J Marit Stud 6(1):75–90

Bruno M (2015) A foresight review of resilience engineering. designing for the expected and unexpected. A consultation document, July 2015, https://www.stevens.edu/ses/sites/ses/files/Foresight_Review_Resilience_Engineering_final_draft_July8_1.pdf. Accessed 20 Aug 2015

Coaffee J, Wood D, Rogers P (2009) The everyday resilience of the city. How Cities Respond to Terrorism and Disaster. New Security Challenges. Palgrave Macmillan, Basingstoke

CSS-Analysen (2009) Resilienz: Konzept zur Krisen- und Katastrophenbewältigung. CSS Analysen zur Sicherheitspolitik 60. Center for Security Studies (CSS), ETH Zürich, Zürich

Dekker S (2004) The hindsight bias is not a bias and not about history. Human Fact Aerosp Saf 4(2):87–99

Dekker S (2014) The problems of vision zero in work safety. Malays Lab Rev 1(8):25–36

Dekker S, Woods D (2010) The high reliability organization perspective. In: Salas E, Maurino D (eds) Human factors in aviation, 2nd edn. Wiley, New York, pp 123–146

Edwards C (2009) Resilient Nation. Demos, London

Farid A (2015) Static resilience of large flexible engineering systems: axiomatic design model and measures. IEEE Syst J to be published 1–12

Flynn S (2011) A national security perspective on resilience. Resilience: Interdisciplinary Perspectives on Science and Humanitarianism 2:i–ii

Goerger S, Madni A, Eslinger O (2014) Engineered resilient systems: a DoD perspective. Proc Comp Sci 28:865–872

Holling C (1973) Resilience and stability of ecological systems. Annu Rev Ecol Syst 4:1–23

Holling C (1996) Engineering resilience vs. ecological resilience. In: Schulze P (eds) Engineering within ecological constraints. National Academy Press 1996, Washington, D.C., pp 31–44

Hollnagel E (2011) Prologue: the scope of resilience engineering. In: Hollnagel E, Pariès J, Woods D, Wreathall J (eds) Resilience engineering in practice. A guidebook. Ashgate, Farnham, Surrey, pp xxix–xxxix

Hollnagel E, Fujita Y (2013) The Fukushima disaster—systemic failure as the lack of resilience. Nucl Eng Technol 45(1):13–20

Hollnagel E, Woods D (2011) Epilogue: resilience engineering precepts. In: Hollnagel E, Pariès J, Woods D, Wreathall J (eds) Resilience engineering in practice. A guidebook. Ashgate, Farnham, pp 347–358

Huber S, van Wijgerden I, de Witt A, Dekker S (2009) Learning from organizational incidents: resilience engineering for high-risk process environments. Process Saf Progess 28(1):90–95

Kaufmann S, Blum S (2012) Governing (In)security: the rise of resilience. In: Gander H-H, Perron W, Poscher R, Riescher G, Würtenberger T (eds) Resilienz in der offenen Gesellschaft. Symposium des Centre for Security and Society, Nomos, Baden-Baden, pp 235–257

Linkov I, Kröger W, Renn O, Scharte B et al (2014) Risking resilience: changing the resilience paradigm. Commen Nat Clim Change 4(6):407–409

MacAskill K, Guthrie P (2014) Multiple interpretations of resilience in disaster risk management. Proc Econ Fin 18:667–674

Madni A, Jackson S (2009) Towards a conceptual framework for resilience engineering. IEEE Syst J 3(2):181–191

Nemeth C (2008) Resilience engineering: the birth of a notion. In: Hollnagel E, Nemeth C, Dekker S (eds) Resilience engineering perspectives, vol 1., Remaining sensitive to the possibility of failureAshgate, Farnham, pp 3–9

Perrow C (1999a) Normal accidents. Living with high risk technologies (Revised edition). Princeton University Press, Princeton

Perrow C (1999b) Organizing to reduce the vulnerabilities of complexity. J Conting Crisis Manag 7(3):150–155

Plodinec M (2009) Definitions of resilience: an analysis. Community and Regional Resilience Institute
Rahimi M, Madni A (2014) Toward a resilience framework for sustainable engineered systems. Proc Comput Sci 28:809–817
Renn O (2008a) Concepts of risk: an interdisciplinary review. Part 1: disciplinary risk concepts. GAiA 17/1:50–66
Renn O (2008b) Concepts of risk: an interdisciplinary review. Part 2: integrative approaches. GAiA 17/2:196–204
Rijpma J (1997) Complexity, tight-coupling and reliability: connecting normal accidents theory and high reliability theory. J Conting Crisis Manag 5(1):15–23
Scharte B, Hiller D, Leismann T, Thoma K (2014a) Introduction. In: Thoma K (ed) Resilien Tech. Resilience by design: a strategy for the technology issues of the future (acatech STUDY). Herbert Utz Verlag, München, pp 9–17
Scharte B, Hiller D, Leismann T, Thoma K (2014b) Resilience: International Perspectives. In: Thoma K (ed) Resilien Tech. Resilience by Design: a strategy for the technology issues of the future (acatech STUDY). Herbert Utz Verlag, München, pp 51–91
Scharte B, Hiller D, Leismann T, Thoma K (2014c) Summary. In: Thoma K (ed) Resilien Tech. Resilience by Design: a strategy for the technology issues of the future (acatech STUDY). Herbert Utz Verlag, München, pp 117–125
The National Academies (2012a) Disaster Resilience. A National Imperative. Washington, D.C.
The National Academies (2012b) Disaster Resilience. A National Imperative. Summary. Washington, D.C.
The White House (2013) Presidential Policy Directive/PPD-21, subject: critical infrastructure security and resilience. https://www.fas.org/irp/offdocs/ppd/ppd-21.pdf. Accessed 03 Sep 2015
Thoma K (2014) (ed) Resilien Tech. Resilience by design: a strategy for the technology issues of the future (acatech STUDY). Herbert Utz Verlag, München
Thoma K, Scharte B (2015) Building a resilient society. per Concordiam. J Eur Secur Def Issues 6(1):30–35
Walker J, Cooper M (2011) Genealogies of resilience. from systems ecology to the political economy of crisis adaptation. SECUR DIALOGUE 42(2):143–160
Woods D (2003) Creating foresight: how resilience engineering can transform NASA's approach to risky decision making. Testimony on the future of NASA for committee on commerce science and transportation. http://history.nasa.gov/columbia/Troxell/Columbia%20Web%20Site/Documents/Congress/Senate/OCTOBE~1/Dr.%20Woods.pdf. Accessed 09 Feb 2016
Woods D, Hollnagel E (2006) Prologue: resilience engineering concepts. In: Hollnagel E, Woods D, Leveson N (eds) Resilience Engineering. Ashgate Publishing Limited, Hampshire, pp 1–6