Eur J Secur Res (2016) 1:21–58
DOI 10.1007/s41125-015-0001-x

ORIGINAL ARTICLE

Quantifying Resilience for Resilience Engineering of Socio Technical Systems

Ivo Häring[1] · **Stefan Ebenhöch**[1] · **Alexander Stolz**[1]

Received: 16 December 2015 / Accepted: 17 December 2015

Abstract Resilience engineering can be defined to comprise originally technical, engineering and natural science approaches to improve the resilience and sustainability of socio technical cyber-physical systems of various complexities with respect to disruptive events. It is argued how this emerging interdisciplinary technical and societal science approach may contribute to civil and societal security research. In this context, the article lists expected benefits of quantifying resilience. Along the resilience engineering definition objectives, it formulates resilience optimization or minimization problems, which can be further detailed, e.g. in terms of resilience chance optimization. The main focus is on four types of approaches to achieve resilience quantification: (1) qualitative/quantitative/analytical resilience assessment processes and frameworks, (2) probabilistic/statistical static expansion approaches, (3) resilience trajectory/propagation/dynamic approaches, and (4) complex system resilience modeling, simulation and analysis. The article comprises for each quantification option its motivation, a top level derivation as well as formal, tabular, schematic or plot-wise representations, as appropriate. For each approach, a list of application examples of methods are given that could implement the resilience quantification. In particular, the article introduces the concepts and notions of resilience expansion order analysis, resilience transition matrix elements, generation of time-dependent resilience response curves, indicators and distributions, resilience barrier, and resilience tunneling or equivalently resilience gap and resilience bridging, as well as resilience quantity probability density.

Keywords Resilience engineering · Resilience quantification · Socio technical systems · Resilience optimization

✉ Ivo Häring
ivo.haering@emi.fraunhofer.de

[1] Fraunhofer Ernst-Mach-Institut, EMI, Am Klingelberg 1, 79588 Efringen-Kirchen, Germany

1 Introduction: Need for Resilience Quantification of Complex Systems in Civil Security and Safety Research

Today's citizens and societies are challenged with a comprehensive and ever increasing list of potential threats to sustainable development. Only in the last decades the list of threats comprising mainly natural and man-made accidental events had to be amended with man-induced (anthropogenic, natech) and man-made malicious (terroristic) hazard events. Even if such events are in most countries still rare events, their frequency and consequences are increasing in absolute numbers or at least within individual and societal perception. In particular, these events have to be faced in densely populated urban areas due to increasing urbanization, industrial, transport and logistic agglomerations.

At the same time, the potential threats of citizens, society, environment, branches of economy and all governmental and non-governmental organizations and representatives have risen due to an ever increasing reliance and dependency on cyber-physical technical systems at all scales and at all levels of complexity. Individual and collective expectations on technical solutions and services are skyrocketing. At increasing performance levels, they are expected to deliver better environmental footprints, reliability, safety, security, privacy, smartness, adaptability, wearability, visualization, and interfacing. Examples for such socio technical systems include live-line grids and nodes, transport and health care systems and services, accident and catastrophe management systems, smart home systems and components, access control systems, mobile electronic devices, mobility solutions as well as social media and sharing platforms.

The list of potential threats or failures of modern cyber-physical socio-technical systems has significantly increased. The term socio technical systems emphasizes the need to take account of the interaction between humans and technology as well as human behavior and goes beyond examining purely technical systems (Mansfield 2010). It can also be understood to take up strands of key requirements from normal accident theory (Perrow 2011) as well as High Reliability Organization theory (Porte and Todd 1996).

Whereas classical technical systems had to cope with failures of components or subsystems due to various types of physical defects or command failures generated within the system, today's increasingly connected systems have to consider in addition failures that are caused or even steered from without the systems, again by accident or deliberately. Therefore, classical system definitions are fading even if system boundaries are much extended. Due to these causes, the number of possible failure modes of each subsystem, interface or even component is shooting up. This ever increasing number of system states and modes as well as transitions and functions is boosted by further integration and miniaturization of today's multi-technological and multi-disciplinary technical systems. In addition, from a technical functional security and safety perspective, the system performance functions must be amended by a multiplicity of safety and security functionalities.

Summarizing so far, there is an increasing number of potentially known, emerging or even yet unknown threats which is in parts caused but also has to be or

de facto is handled with the help of increasingly complex (emergent) technical interlinked systems. These systems are confronted with an ever increasing and competing list of requirements, most of which explicitly only cover performance requirements for standard operations, scenarios and events. However, in case of threats, at the same time, the same systems have to respond to hazard or disruptive events that are slightly or significantly out of the standard operation requirements. Only if the response of the systems to standard operation events as well as disruptive events, which may in addition be often hardly distinguishable, are both acceptable in the given context, the system is sustainably designed, implemented and operable. The questions arise how such potentially competing aims are assessed and whether they are technically achievable, taking, respectively the contexts into account.

From a technical perspective, the optimization of the response of technical systems to disruptive events is related to the response of the system to minor events, like failures, accidental or statistical events. In both cases the system has to be understood, modeled, simulated, and analyzed. However, in the case of disruptive events, it must be taken into account that the system may and has to rearrange, adapt or learn much more when compared to standard damage events, which typically only affect a very small percentage of a system or its system functions and only one at a time. For instance, in the first case maintenance and replacement of components takes place, in the second reuse of subsystems in new technical and functional contexts.

Whereas for classical system properties, including for instance reliability and availability, a variety of established quantities is already available that measure the respective property within well-defined contexts and boundary conditions, the quantification of the quality of performance of systems with respect to disruptive events is inherently challenging. Challenges range from the pre-identification or at least handling of up to unknown threats and hence potential disruptive events, to system boundary definitions, as well as response phases and time spans to be covered and assessed after disruptive events at different time scales. In all phases, the system has to be understood, modeled, simulated, and analyzed with respect to the quality of its response to the disruptive event. See e.g. Sterbenz et al. (2011) in case of the quality of the dependability response. A review of modeling approaches suitable for the simulation of socio technical systems can be found in Landegren et al. (2014).

Civil security and safety related events are often potentially disruptive events. They are handled by specifically designed and maintained systems or by systems which have in addition to cover such events. In both cases the systems have to perform in accordance with citizen's rights, legal, ethical and psychological requirements.

Summarizing and extending the second part of the introduction, for understanding, designing and optimizing technical systems relevant for civil security and safety research, like for all modern socio technical systems that are challenged by potential disruptive events, it is key to quantify the quality of the response of the systems to disruptive events. This task is methodically challenging even if first approaches exist and can be understood as a significant extension of existing technical system performance assessments.

Based on the introductory remarks, it is further discussed how civil security research is linked to technical resilience engineering. A first answer reads by definition, if resilience engineering is defined to aim at reducing vulnerabilities (in a general sense) or enhancing resilience (non-vulnerability in a general sense) of socio technical systems and processes by using social science informed or driven technical-engineering processes, approaches and methods.

A second option is to define resilience engineering from the perspective of which (socio) technical challenges are resolved with the help of technical, engineering and natural and societal science approaches. In this case, the challenges can be defined to be disruptive events like extreme environmental stress or loadings, unexpected events the system has originally not been designed for, etc. This includes events that may occur on a regular basis as well as events that are the consequences of a very slow deterioration. This definition implies that dealing with disruptive events is not restricted to bouncing back but may also comprise or even require better performance of system and system functions after disruptive events.

With the first formal resilience engineering definition, it becomes immediately obvious that resilience engineering is a key approach to civil and societal security research. In the second case, when requiring a disruptive event to be covered within resilience engineering, the question arises if civil security research always deals with variations of scenarios related to disruptive events. Obviously, there is a high coverage of typical topics of interest within civil security research, including but not limited to na, natech and tech hazards, cyber security, loss of privacy, identity theft, functional safety of internet connected devices, catastrophe management systems, social media response, sharing and caring platforms as well as preparation with respect to known unknowns and unknown unknown (black swan events). Hence the first definition of resilience engineering is adapted, the second is considered a mayor application case.

In the following, the response of systems to disruptive events is understood as their resilience response. The aim is to improve the resilience response of socio technical systems with respect to disruptive events to an acceptable level. For an example of a framework to achieve resilient systems see Jackson (2010). However, it has not yet been defined how to quantify resilience in a systematic way for a broad set of (socio) technical systems. In this sense, resilience quantification is a contribution to resilience engineering of systems when defining it to comprise approaches and methods to quantify how (socio) technical systems prepare for, prevent, protect themselves with respect to, respond to or recover from (creeping) disruptive events in an acceptable way, in particular due to their functional resilience capabilities of sensing, modeling, inference, action, learning, and adaption.

The main aim of the article is to propose and discuss a range of technical quantification options for the resilience of (socio) technical systems. This allows to methodically attack resilience optimization problems as well as other key resilience engineering objectives like the introduced concepts of resilience tunneling and resilience bridging. It is expected that the single resilience quantification methods, their combinations, extensions and variations will contribute to advance sustainable resilient system designs and optimizations.

Section 2 introduces the concept of resilience dimensions, which is used for quantification of resilience in various ways in subsequent Sects. 3–9. Section 3

defines resilience engineering objectives in terms of top level extreme value problems for optimizing resilience. Sections 4–9 present four resilience quantification options.

1. Section 4 covers process-based approaches to quantify resilience, for instance chance/risk management of resilience objectives, of resilience capabilities or of resilience management capabilities, as well as their mutual combinations.
2. In a fundamental and introductory way, Sect. 5 considers the formal assessment of resilience with respect to single resilience dimensions. It shows which strong assumptions are necessary to assess resilience for instance with respect to disjoint resilience management phases, capabilities or generic management dimensions, rather than to take account of possible combinations of resilience dimensional attributes, which is considered to be the more relevant approach. Section 6 applies the expansion approach to expansions with respect to threat events causing disruptive events. Section 7 extends to the assessment of an arbitrary number of resilience dimensions including the threat dimension. In all cases it is explained how uncertainties of the quantification are determined when considering multiple combinations of resilience assessment attributes.
3. When compared with Sects. 5–7, Sect. 8 presents a dynamic resilience assessment approach because it assumes a temporal, causal, physical or analytical ordering for formulating its trajectory-based expansions. Trajectories propagate the (multiple) disruptive events through the resilience assessment layers, including, e.g., verbose, distributional, engineering and physical. Application examples for inductive and deductive resilience quantification using single and multiple initial and final elements are given.
4. Section 9 verbosely and to a limited extend when compared to 1. to 3. also formally describes the modeling, simulation and resilience analysis of socio technical systems. It discusses in detail the resilience assessment quantities that can be generated from such modeling approaches, in particular when using (sub) system (function) non-performance and performance measures. It indicates how to take account of known and unknown uncertainties. Also it introduces the concepts of resilience tunneling and bridging and resilience density distributions.

Section 10 summarizes, concludes and gives a broad outlook emphasizing why the proposed quantitative resilience assessment types and approaches singly and in their combination are believed to be useful for future resilience quantification of (socio) technical systems, in particular also in the context of sustainable system design, improvement and retrofitting, as well as system and service business models.

2 Resilience Dimensions: Resilience Phases, Properties, Criteria and Management Dimensions

Section 2 lays the basis for the formalization effort and resilience quantification approaches, in particular the quantification of resilience engineering objectives of Sect. 3. As Sect. 4 reveals, the compact and flexible notation of Sect. 3 focuses on

semi-quantitative approaches but is easily extended to qualitative as well as quantitative approaches. In particular, the quantitative approaches presented in Sects. 5–9 can be understood and defined to feed in the named overarching objectives of Sect. 3 and processes of Sect. 4.

The term resilience dimension denotes the increasing set of static and dynamic characteristics, categories, assessment steps, response steps, management dimensions, structural and behavioral (functional) properties used to investigate the resilience of social, technical and socio technical systems. Often such dimensions are used in combination or ordered sequence. Table 1 lists sample resilience

Table 1 Resilience dimensions: examples for risk and resilience management, resilience capabilities, general management capabilities relevant for resilient response, resilience assessment criteria, resilience management domains and resilience abilities

No.	Resilience dimension	Resilience attribute description	References
1	Risk management process steps	1. Establish context, 2. Identify risks, 3. Analyze risks, 4. Evaluate risks, 5. Treat risks	AS/NZS ISO 31000:2009 (2009), Baumann et al. (2014), Schoppe et al. (2014)
2	Resilience cycle steps	1. Prepare, 2. Prevent, 3. Protect, 4. Respond, 5. Recover	Thoma (2011), Edwards (2009), Thoma (2014), Baird (2010), Thoma (2011)
3	OODA loop steps	1. Observe, 2. Orient, 3. Decide, 4. Act	Boyd (1995), Osinga (2007)
4	(Technical) Resilience capabilities	1. Observation, situation awareness, 2. Modeling, simulation, 3. Inference, decision making, 4. Implementation, action, 5. Learning and adaption	–
5	General management domains	1. Physical, 2. Information, 3. Cognitive, 4. Social	Alberts and Hayes (2003), Fox-Lent et al. (2015), Linkov et al. (2014)
6	Resilience criteria	1. Robustness, 2. Redundancy, 3. Resourcefulness, 4. Rapidity	MCEER (2006), Baird (2010), Rose (2009), Bruneau et al. (2003), Tierney and Bruneau (2007), Størseth et al. (2010), Dorbritz (2011), Chang and Shinozuka (2004), O'Rourke (2007), Renschler et al. (2011), Cimellaro et al. (2010), Tamvakis and Xenidis (2013)
7	Resilience domains of MCEER	1. Technical, 2. Organizational, 3. Social, 4. Economic	Rose (2009), Tierney and Bruneau (2007), Bruneau et al. (2003), Rose (2004), Chang and Shinozuka (2004), O'Rourke (2007), Renschler et al. (2011), Cimellaro et al. (2010), Tamvakis and Xenidis (2013)
8	Resilience abilities	1. Respond, knowing what to do, 2. Monitor, knowing what to look for, 3. Anticipate, knowing what to expect, 4. Learn, knowing what has happened	van der Vorm et al. (2011), Dekker et al. (2008), Hollnagel et al. (2015)

In each case sample attributes are given along with references, if available

dimensions and attributes that can be used for resilience quantification. Next, the resilience dimensions are used to compactly describe possible approaches to resilience analysis, quantification, evaluation, and optimization as well as resilience response.

3 Optimization and Minimization Problems of Resilience Engineering: Quantification of Overall Resilience Engineering Objectives

Section 3 derives general expressions of resilience probabilities and risk/chance quantities of interest when quantifying, assessing and optimizing resilience. As argued in the Sect. 1, resilience analysis, assessment, and optimization cover key activities of technical-engineering approaches to societal security and safety research questions. Societal science informed technical resilience engineering is one way of achieving this objective. Section 3 discusses top level quantitative approaches for this question.

The overall aim of resilience management and analysis can be defined as a maximization

$$0 \leq \Pr(\text{total resilience of system acceptable}) \stackrel{!}{=} \max \approx 1 - \epsilon \leq 1 \tag{1}$$

or as a minimization problem

$$0 \leq \Pr(\text{total resilience of system not acceptable}) \stackrel{!}{=} \min \approx \epsilon \leq 1 \tag{2}$$

of probability quantities measuring, respectively the context dependent and complex event or degree of belief statements "total resilience of system acceptable" or "total resilience of system not acceptable". The quantity ϵ typically is a small number and may differ in (1) and (2). Hence $1 - \epsilon$ in (1) means that the probability of acceptable resilience should be reasonably close to 100 %, and non-acceptable total resilience in (2) close to 0 %.

Another top level approach is to define the overall aim of resilience management and analysis in terms of maximizing total chances of successful risk management and analysis

$$\text{Ch}_{\text{total}}(\text{intended events relevant for resilience management}) \stackrel{!}{=} \max \geq \text{Ch}_{\text{total}}^{\text{crit}} \tag{3}$$

or minimizing total risks to successful resilience management and analysis

$$R_{\text{total}}(\text{unintended events relevant for resilience management}) \stackrel{!}{=} \min \leq R_{\text{total}}^{\text{crit}}. \tag{4}$$

In (3) and (4) the comparison operation with critical total chances $\geq \text{Ch}_{\text{total}}^{\text{crit}}$ and risks $\leq R_{\text{total}}^{\text{crit}}$ is shorthand for a range of context-dependent assessment options, e.g. taking account of individual risks using critical local risks and individual exposure profile dependent risks as well as collective (group) F-N criteria.

Chances and risks may be defined to depend on probability of events

$$\Pr((\text{un})\text{intended event}_i) \tag{5}$$

and measures of their consequences

$$\mathrm{C}((\text{un})\text{intended event}_i). \tag{6}$$

The subscript index i in (5) and (6) numbers the chance or risk events considered.

Using (5) and (6) in (3) and (4) results in a straightforward quantification, assessment and optimization option of resilience of the considered system taking account of the whole resilience management cycle and life cycle, or other resilience dimensions as exemplarily listed in Table 1, with the following interpretations: The total chances for successful resilience management covering the whole resilience life cycle are acceptably high

$$\begin{aligned} &\sum_{i=1}^{N_{\text{events}}} \Pr(\text{intended event}_i \text{ during resiliene management and life cycle}) \\ &C(\text{intended event}_i) \geq \mathrm{Ch}_{\text{total}}^{\text{crit}} \end{aligned} \tag{7}$$

or the total risks on resilience management covering the whole resilience management and life cycle are acceptably low

$$\begin{aligned} &\sum_{i=1}^{N_{\text{events}}} \Pr(\text{unintended event}_i \text{ during resiliene manag. and life cycle}) \\ &C(\text{unintened event}_i) \leq R_{\text{total}}^{\text{crit}}. \end{aligned} \tag{8}$$

Again, the assessment criteria in (7) and (8) are shorthand and may not only consist of comparison of numbers.

Since the expressions (1) and (2) use the language of probability theory operating on general statements, they are very flexible. For instance, all types of events are considered, in particular combinations of events, non-linear propagation effects due to events, as well as yet unknown or very uncertain events.

The chance/risk management and assessment approach of (3) and (4) is more intuitive and allows to refer to a broad set of existing approaches and methods suitable for a wide range of applications, from natural science, technical, engineering, cyber to individual, social, societal, and political systems and combinations thereof. However, in the present context of resilience, security and safety quantification, assessment and optimization, it is important to state that the most often used (only) interpretation of risks or chances is not sufficient when using (5) and (6) as well as (7) and (8). Namely risks determined by the probabilities of hazard events and their consequences or chances determined by the successful avoidance of hazards and the corresponding positive consequences. However, for resilience quantification also the risks and chances during and after the disruptive events have to be considered.

The following combinations of the probability and chance/risk approach are illustrative. It applies the general probability expressions of (1) and (2) and to the

general statements formulated in the language of chance and risk management (3) and (4). The following resilience quantification, assessment and optimization approaches are feasible:

1. Optimization of the probability of acceptably high total chances for successful resilience management (OPHC)

$$\Pr\left(\mathrm{Ch}_{\mathrm{total}}(\text{intended events relevant for resilience management}) \geq \mathrm{Ch}_{\mathrm{total}}^{\mathrm{crit}}\right) \geq 1-\epsilon, \tag{9}$$

2. Optimization of the probability of acceptably low total risks on successful resilience management (OPLR)

$$\Pr\left(R_{\mathrm{total}}(\text{unintended events relevant for resilience management}) \leq R_{\mathrm{total}}^{\mathrm{crit}}\right) \geq 1-\epsilon, \tag{10}$$

3. Minimization of the probability of unacceptably low total chances for successful resilience management (MPLC)

$$\Pr\left(\mathrm{Ch}_{\mathrm{total}}(\text{intended events relevant for resilience management}) \leq \mathrm{Ch}_{\mathrm{total}}^{\mathrm{crit}}\right) \leq \epsilon, \tag{11}$$

4. Minimization of the probability of unacceptably high total risks on successful resilience management (MPHR)

$$\Pr\left(R_{\mathrm{total}}(\text{unintended events relevant for resilience management}) \geq R_{\mathrm{total}}^{\mathrm{crit}}\right) \leq \epsilon. \tag{12}$$

In analogy to system reliability and safety assessment, it can be conjectured that the expression that uses the optimization of the probability of high chances (OPHC) resilience analysis of (9) is most motivating but also most cumbersome for implementation, in particular when compared to the optimization of the probability of low risks (OPLR) and the minimization of the probability of high risks (MPHR) resilience analysis of (9) and (10), respectively. This conjecture assumes that for socio technical systems there are most often more roots to success than to failure. This is expected to hold true also in the case of chance or risk assessment of technical resilience capabilities. Further, that it is more challenging to define the success of a socio technical system performance mode when compared to its failure.

However, it is questionable whether the conjectures of the last text paragraph hold true for emerging novel systems, for systems which are too complex to model all failure modes, for non-linear system behavior, in case of organizational resilience assessments, and in particular in all cases where humans are dominating the response and recovery of systems. In the latter case, for instance, an OPHC resilience analysis and assessment might prove much more favorable for individual and organizational commitment.

Next the four resilience quantification approaches 1. to 4. are detailed (see the overview at the end of Sect. 1).

4 Process-Oriented Quantification of Resilience Based on Resilience Dimensions

As first example, a resilience quantification process based on chance or equivalently risk management and the sample resilience management dimensions 1–7 of Table 1 is described. This is a rather basic algebraic endeavor when compared to the quantification approaches (2) to (4).

Let $N_{\mathrm{RD}} \geq 1$ be the number of the resilience dimensions (RD) considered, $N_1^{\mathrm{RA}} \geq 2, \ldots, N_{N_{\mathrm{RD}}}^{\mathrm{RA}} \geq 2$ the numbers of resilience attributes (RA) considered within each resilience dimension and $1 \leq i_1 \leq N_1^{\mathrm{RA}}, \quad 1 \leq i_2 \leq N_2^{\mathrm{RA}}, \ldots, 1 \leq i_{N_{\mathrm{RD}}} \leq N_{N_{\mathrm{RD}}}^{\mathrm{RA}}$ the respective indices used for each dimension. When using Table 1, e.g. $N_{\mathrm{RD}} = 7, N_1^{\mathrm{RA}} = 5, N_2^{\mathrm{RA}} = 5, \ldots, N_7^{\mathrm{RA}} = 4$.

Within a minimum risk (chance) assessment of resiliency, for instance the following steps of Sects. 4.1–4.5 are conducted (see second line of Table 1).

4.1 Resilience Context

First, $N_{\mathrm{RO}} \geq 1$ resilience objectives (RO) are identified. They belong to resilience dimension 1 risk management and its first resilience attribute establish context: $i_1 = 1$ (see Table 1). The resilience objectives are identified and categorized using at least one of the resilience dimensions 4 (technical) resilience capabilities and 6 resilience criteria. Formalized, each verbose resilience objective can be represented by

$$O_{i_1=1,i_4,i_6;j}, \quad 1 \leq j \leq N_{\mathrm{RO}}. \tag{13}$$

Equation (13) is a powerful notation because it allows to use the same and unique resilience objective in different (combinations of) resilience dimensions and respective attributes. On the other hand, this information can also be absorbed in the last subscript if the objective is defined more specifically. In the latter case, the resilience attribute indices formalize the verbose information. Furthermore, the order of the subscripts implies an order of assessment: the indices to the right are defined to loop first.

At least one resilience stakeholder (RS) for each resilience objective is set to be required and can be found by using for instance in addition optionally the resilience dimensions 5 general management domains and 7 resilience domains for stakeholder identification and characterization,

$$S_{i_1=1,i_4,i_5,i_6,i_7;j;k}, \quad 1 \leq k \leq N_{\mathrm{RS}} \geq N_{\mathrm{RO}}. \tag{14}$$

4.2 Resilience Chance and Risk Identification

Second, knowing resilience objectives and stakeholders, at least one resilience chance (RCh) for each resilience objective or alternatively resilience risk (RR) on each resilience objective is identified and verbosely described. For this step, the resilience dimensions 2 resilience cycle steps and 3 OODA loop steps are included for a complete assessment,

$$\{\mathrm{Ch}, R\}_{i_1=2,i_2,i_3,\cdots,i_7;j;k;l}, 1 \leq l \leq N_{\{\mathrm{RCh,RR}\}} \geq N_{\mathrm{RO}}. \tag{15}$$

In (15), the indices indicate to which combination of resilience dimensions and attributes the resilience risk or chance is believed to belong most to. Hence, (15) is a shorthand for the verbose description of the resilience chance or risk deemed relevant for resilience quantification. The curved bracket notation allows to combine the very similar expressions for the resilience chances and risks in a single formal expression.

4.3 Probabilities and Consequences of Resilience Chances and Risks

Third, for each resilience chance or risk identified, its qualitative, semi-quantitative or quantitative probability (P) and consequence (C) are determined quantitatively or semi-quantitatively, respectively,

$$\{P, C\}^{\{\mathrm{Ch},R\}}_{i_1=3,i_2,i_3,\ldots,i_7;j;k;l} = \prod_{\substack{1 \leq \imath_2 \leq N_2^{\mathrm{RA}} \\ \ldots \\ 1 \leq \imath_7 \leq N_7^{\mathrm{RA}} \\ 1 \leq m \leq N_{\{p\mathrm{Ch},pR,c\mathrm{Ch},cR\}} \geq N_{\mathrm{RO}}}} \{p, c\}^{\{\mathrm{Ch},R\}}_{1;j;i_1=3,\imath_2,\imath_3,\ldots,\imath_7;j;k;l;m}. \tag{16}$$

Expression (16) takes account of the challenging fact that probabilities and consequences of each resilience risk and chance may depend on much more resilience dimensions and attributes than identified at first hand in (15) of Sect. 4.2. Of course, also only some of the probability factors p and consequence factors c might contribute, i.e. are different from unity. For instance, the resilience chance of a fast recovery with respect to rebuilding private houses can be first attributed to the recovery phase only and then be found to depend on preparation (e.g. fast planning processes), protection (e.g. strong building base) and response (e.g. controlled shut down of potentially damaging building functions) as well.

In addition, (16) can be interpreted in terms of a probability and consequence base rate, which carry the units, times mitigation and enhancement factors. This is somewhat similar to the refinement of (15) by the product of the resilience probabilities and consequences of (17) below. Most importantly, Eq. (16) allows for input from the whole range of the humanities, the natural and technical sciences.

4.4 Evaluation of Resilience Chances and Risks

Forth, each resilience chance or risk is qualitatively or (semi) quantitatively computed and assessed

$$\{\mathrm{Ch}, R\}_{i_1=4,i_2,i_3,\ldots,i_7;j;k;l} = P^{\{\mathrm{Ch},R\}}_{i_1=3,i_2,i_3,\ldots,i_7;j;k;l} C^{\{\mathrm{Ch},R\}}_{i_1=3,i_2,i_3,\ldots,i_7;j;k;l} \{\geq, \leq\} \{\mathrm{Ch}_{\mathrm{crit}}, R_{\mathrm{crit}}\}(P^{\{\mathrm{Ch},R\}}_{\ldots}, C^{\{\mathrm{Ch},R\}}_{\ldots}). \tag{17}$$

In the simplest case, the assessment criterion at the right hand side of (17) just uses the product of probability and consequence and hence only a single critical chance or risk value for each assessment. The expression at the right hand side of (17) also allows to take account of societal or individual risk aversion. For instance, in the case of the same risk value, low probability and very high consequence risks on resiliency objectives may be assessed less favorable than very high probability and low consequence risks. In a similar way, it is interesting to investigate how to assess resilience chances with low probability and very high consequence versus very high probability and low consequences in given contexts.

A simple collective or group assessment criterion reads

$$\sum_{i_2,i_3,\ldots,i_7;j;k;l} \{\mathrm{Ch}, R\}_{i_1=4,i_2,i_3,\ldots,i_7;j;k;l} \{\geq, \leq\} \{\mathrm{Ch}_{\mathrm{critcoll}}, R_{\mathrm{critcoll}}\}, \tag{18}$$

where the left hand side sums over all chances or risks and is the overall (total) chance of resilience or risk on resilience. It is expected that typically individual as well collective criteria are simultaneously necessary for resilience assessment, for which basic examples are given in (17) and (18).

4.5 Measures, Functions and Services to Improve Resilience

Fifth, it may be defined that for each resilience chance (set) that is evaluated to be non-acceptably low at least one resilience improvement measure (IM) or for each resilience risk (set) that is evaluated non-acceptably high, at least one counter measure (CM) mitigating the risk on resilience must be selected,

$$\{\mathrm{IM}, \mathrm{CM}\}_{i_2=5,i_4,i_5,i_6,i_7;j;k;l;m}, 1 \leq m \leq N_{\{\mathrm{IM},\mathrm{CM}\}}. \tag{19}$$

Improvement measures and counter measures include the specification and implementation of functionalities, functions or services that increase the chances on resilience objectives or decrease the risks on resilience objectives.

The sample resilience analysis, quantification and assessment steps of Sects. 4.1–4.5 are iterated until (17) and (18) are both acceptable and converged.

4.6 Further Examples

Next it is shown how to represent other sample processes where other dimensions are dominating the resilience management, analysis, quantification and/or improvement process. The selection or new definition of the most applicable resilience dimensions depends inter alia on the application domain, the organizational resources and the available technical-scientific methods. Furthermore, the selection or new definition of the resilience attributes is paramount for successful resilience analysis, quantification and optimization. Hence it is challenging to define such a top level resilience assessment and improvement framework for each system under investigation.

For instance, to obtain an overview of the level of resilience just the combination of two key resilience dimensions could be analyzed and assessed, e.g. the chances or risks on performance of combinations of the OODA resilience dimension 3 and the general management resilience dimension 5 (see Table 1)

$$\{\mathrm{Ch}, R\}_{i_3,i_5;j}, 1 \leq j \leq N_{\{R\mathrm{Ch},RR\}}, \tag{20}$$

which could even be only directly assessed and compared as in (18) with critical values.

In case it is appropriate to assess resilience within each resilience management step separately, the formalization reads as (13)–(19), however, before each subscript i_1, the subscript i_2 is added. In a similar way, other approaches can be represented and implemented, typically resulting in nested multi-tabular assessment schemes. The final results can be visualized in resilience chance or risk matrices, similar to classical risk matrices. For instance, as the references of Table 1 disclose, the combination of resilience dimension 6 and 7 has already been applied.

5 Resilience Dimensional Assessment with and without Resilience Dimension Partitioning

Resilience of systems becomes evident during the response to potentially disruptive events. Disruptive events may be defined to cover a wide range, from physical to cyber, from statistical to systematic, from accidental to malevolent or even terroristic, from internal to external, from disruptive to creeping, from minor to massive, from man-made to natural, etc. In this sense, resilience assessment is in particular a generalization of classical system safety, security, reliability, and maintenance assessment.

First it is assumed that the resilience management response takes part in defined phases, or can be assessed using another single resilience dimension that can be distinguished using resilience attributes as introduced in Sect. 2. For intuitive sample notation, the attributes are called phase_i. By assumption, the resilience

attributes form a partition of the overall resilience assessment space, see the rectangles in Fig. 1, which do not overlap but cover all possible systems.

Now using the total law of probability for (1) (and (2)) one obtains

$$\begin{aligned}&\Pr(\text{total reslience of system (not) acceptable})\\&=\sum_{i=1}^{N_{phase}}\Pr(\text{total reslience (not) acceptable}\cap\text{phase}_i\text{ occures})\\&=\sum_{i=1}^{N_{phase}}\Pr(\text{total reslience (not) acceptable}\,|\text{phase}_i\text{ occures})\Pr(\text{phase}_i\text{ occures}).\end{aligned}\tag{21}$$

For instance, one might distinguish in (21), using the following 5 phases: preparation (before any knowledge of a pending event); prevention (reduction of probability of occurrence of event); protection (reduction of consequences of event); (immediate) response (to event); and recovery (long term response), see Table 1 resilience dimension number 2. Similar interpretations can be found for the other resilience dimensions.

The expansion (21) shows it is important to consider all phases of a well-defined resilience management process and analysis. Also, given the partition property, it is sufficient to consider the (non) acceptability of the resilience management and analysis efforts in each phase. The quantification and assessment task is thus strongly structured. However, for each addend, the conditional probability (see first factor in the last line of (21)) and also the base rate (see last factor of (21)) has to be determined.

Since the statements total reslience (not) acceptable given phase$_i$ occures are already rather specific, it is easier to decide which variant of (21) (with or without not) is easier to compute (see also the discussion after (12)). Also the last and second last line of (21) are alternatives of assessment, the latter comprising event base rates.

However, the partitioning of the resilience dimensions as assumed in (21) is a strong and often unrealistic proposition for resilience analysis. Can this assumption be canceled? To this end one computes

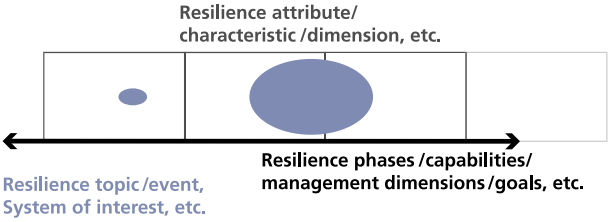

Fig. 1 Schematic of one-dimensional static resilience quantification. Includes examples for the resilience dimensional labeling (see labeling of x-axis), resilience dimension attributes (see labeling of *black boxes*) and systems under investigation (see *grey ellipses*). For instance, the system represented at the *right* hand side contributes to two resilience management phases only, e.g. response and recovery

$$
\begin{aligned}
&\Pr(\text{total reslience of system (not) acceptable}) \\
&\quad = \Pr(\text{total reslience (not) acceptable (even) due to combinded activities in all phases}) \\
&\quad = \Pr\Big(\text{total resilience (not) acceptable} \cap (\text{activity in phase}_1 \cup \cdots \cup \text{act. in phase}_{N_{\text{phase}}})\Big) \\
&\quad \equiv \Pr\Big((\text{no) resilience} \cap (\text{phase}_1 \cup \cdots \cup \text{phase}_{N_{\text{phase}}})\Big) \\
&\quad = \Pr\Big((\text{no) resilience} \cap \text{phase}_1 \cup \cdots \cup \text{resilience} \cap \text{phase}_{N_{\text{phase}}}\Big) \\
&\quad = \sum_{j=1}^{N_{phase}} \Pr\big((\text{no) resilience} \cap \text{phase}_j\big) - \sum_{1 \le j_1 < j_2 \le N_{phase}} \Pr\big((\text{no) res.} \cap \text{phase}_{j_1} \cap \text{phase}_{j_2}\big) \\
&\qquad + \sum_{1 \le j_1 < j_2 < j_3 \le N_{phase}} \Pr\big((\text{no) resilience} \cap \text{phase}_{j_1} \cap \text{phase}_{j_2} \cap \text{phase}_{j_2}\big) - \cdots \\
&\quad = \sum_{i=1}^{N_{phase}} (-1)^{i+1} \sum_{1 \le j_1 < j_2 < \cdots < j_i \le N_{phase}} \Pr\big((\text{no) resilience} \cap \text{phase}_{j_1} \cap \text{phase}_{j_2} \cap \cdots \cap \text{phase}_{j_i}\big),
\end{aligned}
\tag{22}
$$

where in (22) the distributive law and the inclusion–exclusion principle were used.

The last but one expression and the compact final line show that in general it must be understood and computed how the combination of activities in two, three, etc. different resilience dimensional attributes combine to achieve acceptable resilience. Therefore, (22) should be used as the starting point. Then it can be shown whether (21) is a sufficient approximation: only if the first addend of the second last expression of (22) is dominating all the other addends, (21) is a valid approximation.

In a similar way, if it is believed that second-order effects suffice for analysis, it should be shown that order two terms in the last expression of (22) suffice and all other terms are sufficiently small, which is much different from omitting higher order terms from the very beginning. Analogously, for third-order effects, etc. Equation (22) does not assume d that the activities in the different phases are mutually statistically independent. If this proposition holds, further simplifications of the expressions of the last line of (22) are straightforward.

From (22), the following special cases of Bool's inequalities can be derived, which allow to estimate resilience, in case the full expression (22) is too demanding:

$$
\begin{aligned}
&\sum_{j=1}^{N_{\text{phase}}} \Pr\big((\text{no) resilience} \cap \text{phase}_j\big) \\
&\quad - \sum_{1 \le j_1 < j_2 \le N_{\text{phase}}} \Pr\big((\text{no) resilience} \cap \text{phase}_{j_1} \cap \text{phase}_{j_2}\big) \\
&\quad \le \Pr(\text{total resilience (not) acceptable}) \le \sum_{j=1}^{N_{\text{phase}}} \Pr\big((\text{no) resilience} \cap \text{phase}_j\big); \cdots.
\end{aligned}
\tag{23}
$$

For instance, the next inequality of (23) indicated by $\cdots$ uses the last but one expression of (22) as upper bound (third-order expression) and the same expression with one more negative term (fourth-order expression) as lower bound, etc. The inequalities of (23) hold independent of the number of resilience dimension attributes or the single resilience dimension considered.

The intervals defined by (23) and similar expressions can also be used to assess the degree of uncertainty of an assessment. Since the bounds of (23) always end with a plus term, new boundary assessments are only available, if two more orders of the expansion are computed.

6 Threat or Disruptive Expansions for Resilience Assessment

Section 5 provided resilience quantification with respect to generalized resilience management phases, assessment dimensions or properties, which proofed to be suitable for structuring the quantification of resilience. Section 6 introduces along the same lines an expansion of resilience not with respect to single resilience dimensions but with respect to the number of (sets of) threats. In a similar way all characteristics that determine the threat or disruptive events can be used for expansion. The top level distinction between the two types of expansions is between resilience responses as in Sect. 5 and resilience question or challenge as in the present Sect. 6, each of which can be characterized exclusively or non-exclusively. In this sense, this could also be termed a posteriori and a priori resilience quantification, respectively.

The discussion of the last text paragraph and suggested terminology implies that independent of any resilience concepts, it should be possible to determine which (potential) types or combinations of threats must be considered for resilience assessment. This statement is computationally appealing and seems plausible for classical and man-made and natural threats. For instance, it is known which sequences of bad weather are to be expected or to which combined standard loadings and stresses systems are exposed to. For instance, simultaneous heat and heavy rain, wind or hail loading, only at first sight seem not plausible for Middle European weather conditions. However, even within a short sequence of time, they are almost conditional for summer thunderstorms. A since Fukushima well known double threat event is earthquake and tsunami.

As in the case of the resilience response expansion, a resilience threat or disruptive event expansion should be outcome of the resilience assessment, rather than input or even axiomatic basis. For instance, if not double but triple threat events are critical, this will not be revealed when restricting the expansion to double threat events. A final conclusion is to give the order of multiplicity of threats or disruptive events considered along with the resilience assessment results. A notation that shows that threat events up to oder N_{threat} are considered reads

$$\Pr(\text{total resilience (not) acceptable}) = p_{r\text{eslience (not) acceptable}} + O(N_{\text{threat}} + 1), \quad (24)$$

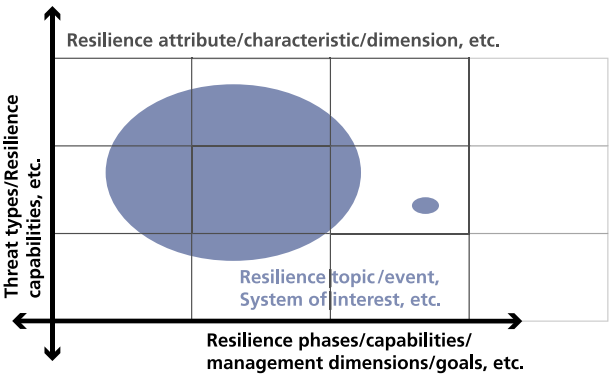

Fig. 2 Schematic for two-dimensional static resilience quantification

A similar derivation as for (22) results in the resilience probability expansion with respect to generalized threat types, threat characteristics or disruptive events, which also summarizes the section,

$$\begin{aligned}&\Pr(\text{total resilience (not) acceptable})\\&\quad=\cdots=\Pr((\text{no) resilience}\cap(\text{threat}_1\cup\cdots\cup\text{threat}_{N\_\text{threat}}))\\&\quad=\sum_{i=1}^{N_\text{threat}}(-1)^{i+1}\sum_{1\le j_1<j_2<\cdots<j_i\le N_\text{threat}}\Pr\big((\text{no) resilience}\cap\text{threat}_{j_1}\cap\text{threat}_{j_2}\cap\cdots\cap\text{threat}_{j_i}\big).\end{aligned}\tag{25}$$

As in (23), for (25) upper and lower bounds are accessible by replacing in (23) phase with threat.

7 Multi-Dimensional Resilience Assessment Expansions with Respect to Resilience Dimensions and Threats or Disruptive Events

This section assumes that resilience quantification depends on multiple resilience dimensions as well as multiple threats (disruptive events). For illustration, the computation starts with two resilience dimensions, see Fig. 2.

The further steps are less straightforward when compared to (22) to (25). The computation results read

$$
\begin{aligned}
&\Pr(\text{totalreslience(not)acceptable}) \\
&= \Pr(\text{totalreslience(not)acceptableconsideringallphasesandthreats}) \\
&= \Pr\big((\text{no})\text{resilience} \cap (\text{phase}_1 \cup \cdots \cup \text{phase}_{N_{\text{phase}}}) \cap (\text{threat}_1 \cup \cdots \cup \text{threat}_{N_{\text{threat}}})\big) \\
&= \Pr\left(\bigcup_{\substack{1 \le i \le N_{\text{phase}} \\ 1 \le j \le N_{\text{threat}}}} (\text{no})\text{resilience} \cap \text{phase}_i \cap \text{threat}_j\right) \\
&= \Pr\left(\bigcup_{1 \le k \le N_{\text{phase}} N_{\text{threat}}} (\text{no})\text{resilience} \cap \text{phase}_{k/N_{\text{threat}}+1} \cap \text{threat}_{k \bmod N_{\text{threat}}}\right) \\
&= \sum_{1 \le k \le N_{\text{phase}} N_{\text{threat}}} \Pr\big((\text{no})\text{resilience} \cap \text{phase}_{k/N_{\text{threat}}+1} \cap \text{threat}_{k \bmod N_{\text{threat}}}\big) \\
&\quad - \sum_{1 \le k_1 < k_2 \le N_{\text{phase}} N_{\text{threat}}} \Pr\left(\begin{array}{c}(\text{no})\text{resilience} \cap \text{phase}_{k_1/N_{\text{threat}}+1} \cap \text{threat}_{k_1 \bmod N_{\text{threat}}} \\ \cap \text{phase}_{k_2/N_{\text{threat}}+1} \cap \text{threat}_{k_2 \bmod N_{\text{threat}}}\end{array}\right) \\
&\quad + \sum_{1 \le k_1 < k_2 < k_3 \le N_{\text{phase}} N_{\text{threat}}} \Pr\left(\begin{array}{c}(\text{no})\text{resilience} \cap \text{phase}_{k_1/N_{\text{threat}}+1} \cap \text{threat}_{k_1 \bmod N_{\text{threat}}} \\ \cap \text{phase}_{k_2/N_{\text{threat}}+1} \cap \text{threat}_{k_2 \bmod N_{\text{threat}}} \\ \cap \text{phase}_{k_3/N_{\text{threat}}+1} \cap \text{threat}_{k_3 \bmod N_{\text{threat}}}\end{array}\right) \\
&\quad - \cdots \\
&= \sum_{l=1}^{N_{\text{phase}} N_{\text{threat}}} (-1)^{l+1} \sum_{\substack{1 \le k_1 < k_2 < \cdots \\ < k_l \le N_{\text{phase}} N_{\text{threat}}}} Pr\left(\begin{array}{c}(\text{no})\text{resilience} \\ \cap \text{phase}_{k_1/N_{\text{threat}}+1} \cap \text{threat}_{k_1 \bmod N_{\text{threat}}} \\ \cap \cdots \\ \cap \text{phase}_{k_l/N_{\text{threat}}+1} \cap \text{threat}_{k_l \bmod N_{\text{threat}}}\end{array}\right)
\end{aligned}
\tag{26}
$$

employing the bijection

$$
\begin{aligned}
(i,j) &\to k = (i-1)N_{\text{threat}} + j \\
(i,j) &= (k/N_{\text{threat}} + 1, k \bmod N_{\text{threat}}) \leftarrow k
\end{aligned}
\quad , \tag{27}
$$

which uses the floor and modulo functions, the distributive law and Bool's expansion.

To expand terms of (26) explicitly, equivalences of the type

$$
k_1 < k_2 \overset{\text{iff}}{\Leftrightarrow} i_1 = i_2 \wedge j_1 < j_2 \wedge i_1 < i_2 \wedge j_1 = j_2 \wedge i_1 < i_2 \wedge j_1 < j_2 \tag{28}
$$

are used results in

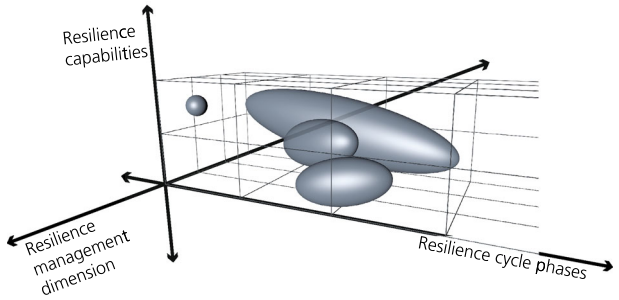

Fig. 3 Schematic of three-dimensional static resilience quantification (see three axes and three-dimensional *boxes*) of systems (*grey*). Sample resilience dimensions label the three axes

$$
\begin{aligned}
&\Pr(\text{total reslience (not) acceptable}) \\
&= \sum_{\substack{1 \le i \le N_{\text{phase}} \\ 1 \le j \le N_{\text{threat}}}} \Pr\big((\text{no}) \text{ resilience} \cap \text{phase}_i \cap \text{threat}_j\big) \\
&\quad - \sum_{\substack{1 \le i_1, i_2 \le N_{phase} \\ 1 \le j_1, j_2 \le N_{threat} \\ i_1 = i_2 \wedge j_1 < j_2}} Pr\big((no) resilience \cap phase_{i_1} \cap threat_{j_1} \cap threat_{j_2}\big) \\
&\quad - \sum_{\substack{1 \le i_1, i_2 \le N_{phase} \\ 1 \le j_1, j_2 \le N_{threat} \\ i_1 < i_2 \wedge j_1 = j_2}} Pr\big((no) resilience \cap phase_{i_1} \cap phase_{i_2} \cap threat_{j_1}\big) \\
&\quad - \sum_{\substack{1 \le i_1, i_2 \le N_{phase} \\ 1 \le j_1, j_2 \le N_{threat} \\ i_1 < i_2 \wedge j_1 < j_2}} Pr\big((no) resilience \cap phase_{i_1} \cap threat_{j_1} \cap phase_{i_2} \cap threat_{j_2}\big) \\
&\quad + \cdots .
\end{aligned}
\tag{29}
$$

For the third order of expansion in (29) two equivalences as in (28) have to be used, etc.

In a similar way, three and more resilience dimensions, in general $N_{\text{resilience}} \geq 1$ resilience dimensions, now in addition including (sets of) threats or disruptive

events can be used for expansion, see Fig. 3 for an example of three dimensional resilience assessment. The starting point for the resilience assessment expansion reads

$$\begin{aligned}&\Pr(\text{total reslience (not) acceptable})\\&= Pr\left(\begin{array}{ll}\displaystyle\bigcup_{\substack{1\le n_1\le N_1\\ \cdots\\ 1\le n_{N_{\text{reslience}}}\le N_{N_{\text{resience}}}}} & \text{(no) resilience} \cap \text{reslience dimension}_{n_1}\\ & \cap \text{reslience dimension}_{n_2}\\ & \cap\cdots\\ & \cap \text{reslience dimension}_{n_{N_{\text{reslience}}}}\end{array}\right)\end{aligned} \tag{30}$$

and the same methods as for the derivation of (29) have to be employed. In particular, (28) and (29) can be generalized to more than 2 dimensions.

It is illustrative to compare the expansion (22), which applies one resilience dimension, as well as (25), which applies threats (or disruptive events), both using one assessment dimension with expansion (29), which applies threats and one resilience dimension, hence uses two assessment dimensions. In case of the 1-dimensional resilience assessment expansion in the sense of (22) and (25), the first inequality (upper bound) for the probability of (not) acceptable resilience in the sense of (23) requires the assessment of multiple intersections of 2 generalized events (e.g. (no) resilience $\cap$ phase$_i$), the second inequality (lower bound) of 3 (e.g. (no) resilience $\cap$ threat$_{j_1}$ $\cap$ threat$_{j_2}$), the third (upper bound) of 4, etc.

However, in case of the 2-dimensional resilience assessment expansion as in (29), the first inequality (upper bound) for the probability of (not) acceptable resilience in the sense of (23) requires the assessment of multiple intersections of 3 generalized events (e.g. (no) resilience $\cap$ phase$_i$ $\cap$ threat$_j$), the second (lower bound) of 4 (e.g. (no) resilience $\cap$ phase$_{i_1}$ $\cap$ threat$_{j_1}$ $\cap$ threat$_{j_2}$ or (no) resilience $\cap$ phase$_{i_1}$ $\cap$ phase$_{i_2}$ $\cap$ threat$_{j_1}$) or 5 (e.g. (no) resilience $\cap$ phase$_{i_1}$ $\cap$ threat$_{j_1}$ $\cap$ phase$_{i_2}$ $\cap$ threat$_{j_2}$), the 3rd (upper bound) of 6 and 7, etc.

In the general case of N_{resience}-dimensional resilience assessment expansion, the 1st inequality (upper bound) for the probability of (not) acceptable resilience in the sense of (23) requires the assessment of multiple intersections of $1 + N_{\text{resilience}}$ generalized events, the second (lower bound) of $1 + N_{\text{resilience}} + 1, 1 + N_{\text{resilience}} + 2, \ldots, 1 + 2N_{\text{resilience}}$, the third (upper bound) of $1 + 2N_{\text{resilience}} + 1, \ldots, 1 + 3N_{\text{resilience}}$, etc.

Hence Bool's expansions show that the use of more dimensions for resilience assessment results in significantly more effort when assessing resilience. The number of possible generalized event combinations increases significantly. In addition, these events are increasingly more specified. In typical applications it is expected to be challenging to determine or compute such completely specified events. On the other hand, a minimum characterization of threat/disruptive events and activities related to maintain or achieve acceptable resilience seems necessary.

Summarizing the discussed resilience computation options and constraints, the conjecture is that a crucial part of resilience analysis, quantification and assessment is the identification of suitable assessment dimensions as well as resilience resolutions within each dimension (resilience attributes). Resilience resolution can be understood as the number of attributes, for instance phases, attack types, disruptive event types, resilience capabilities, resilience management capabilities, or resilience criteria considered within each resilience dimension, respectively.

Depending on the type or resilience quantification in terms of optimization of acceptable total resilience (1) or of minimization of non-acceptable resilience (2), lower or upper bounds are more advisable to be used as the last order that is still computed according to any of the sample static resilience expansion (22), (25) or (29). This also holds true when optimizing in the sense of (9) and (10) or minimizing in the sense of (11) and (12), using total chances and risks as well as risk and chance criteria, respectively.

Finally, it is interesting to discuss whether the sketched methods of computation can be extended, for instance, to unknown threats and disruptive events, or not completely specified resilience assessment or management dimensions. Formally, for instance in the case of threat events, the set of events of unknown events can be added,

$$\Omega \backslash (\text{threat}_1 \cup \cdots \cup \text{threat}_{N_{\text{threat}}}) \tag{31}$$

and the set of events can be extended with this set. Hence the presented expansions work even for unknown unknowns. Obviously, the challenge is only shifted and it remains to define the total set of all possible threat events Ω. However, by starting with a threat type characterization (taxonomy), the threat types are typically inventoried deductively, whereas Ω in (31) can be determined inductively by collecting all types of thinkable threat events and combinations. In this sense, (31) offers an alternative option to identify further threat events.

Similar and better arguments hold true for other resilience assessment dimensions. Covering unexpected events can be approached by the extension of existing resilience dimensional attributes. In particular, using the technical resilience capability dimension 4 of Table 1 is considered to be a promising approach.

8 Trajectory, Causal, Temporal or Layer Expansion for Dynamic Resilience Assessment: Deductive and Inductive

Section 8 derives three generic expressions to compute resilience quantities based on the assumption of causal, logical, physical and/or temporal ordering or layering of possible events. It can also be interpreted in terms of resilience trajectories. In this sense this approach is dynamic, in particular when a time-ordering is used for defining the layers of expansion, analysis and modeling.

Let E_{00} be a single final resilience event (E) of interest, for instance total resilience (not) acceptable, recovery after man-made event acceptable (e.g. fast

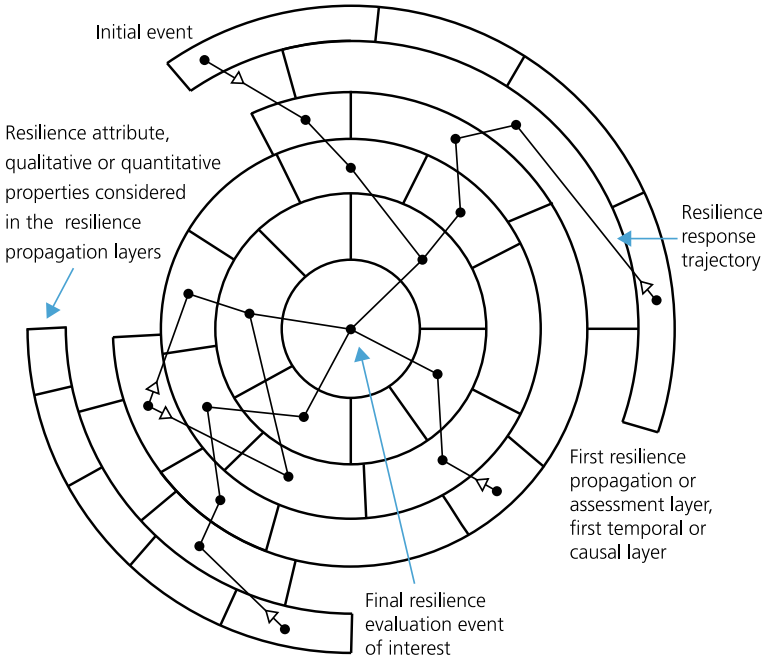

Fig. 4 Deductive, backward, top down or inverse resilience analysis. The root causes (see *black dots* at the beginning of the resilience propagation trajectories) for a single final disruptive event (see *black bullet* in the center) are evaluated. Multiple event trajectories contribute originating from different propagation, assessment, temporal or causal layers. The layers are partitioned for instance with respect to attributes of assessment, qualitative or quantitative intervals

enough, efficient enough), etc. The repeated application of the law of total probability results in the expansion

$$\begin{aligned}
\Pr(E_{00}) &= \sum_{i_1=1}^{N_1} \Pr(E_{00} \cap E_{1i_1}) \\
&= \sum_{i_1=1}^{N_1} \Pr(E_{00}|E_{1i_1}) \Pr(E_{1i_1}) \\
&= \sum_{i_1=1}^{N_1} \sum_{i_2=1}^{N_2} \Pr(E_{00}|E_{1i_1}) \Pr(E_{1i_1}|E_{2i_2}) \Pr(E_{2i_2}) \\
&\cdots \\
&= \sum_{i_1=1}^{N_1} \sum_{i_2=1}^{N_2} \cdots \sum_{i_{N_res}=1}^{N_{N\text{res}}} \Pr(E_{00}|E_{1i_1}) \Pr(E_{1i_1}|E_{2i_2}) \cdots \Pr\left(E_{N_{\text{res}}-1,i_{N_{\text{res}}-1}}|E_{N_{\text{res}},i_{N_{\text{res}}}}\right) \Pr\left(E_{n,i_{N_{\text{res}}}}\right),
\end{aligned} \tag{32}$$

where $N_{\text{res}} \geq 2$ is the order of the deductive resilience assessment expansion, $E_{1,1}, E_{1,2}, \ldots, E_{1,N_1}$ is the first resilience partition event set layer (closest to the final resilience event E_{00} of interest), $E_{2,1}, E_{2,2}, \ldots, E_{2,N_1}$ is the second resilience partition

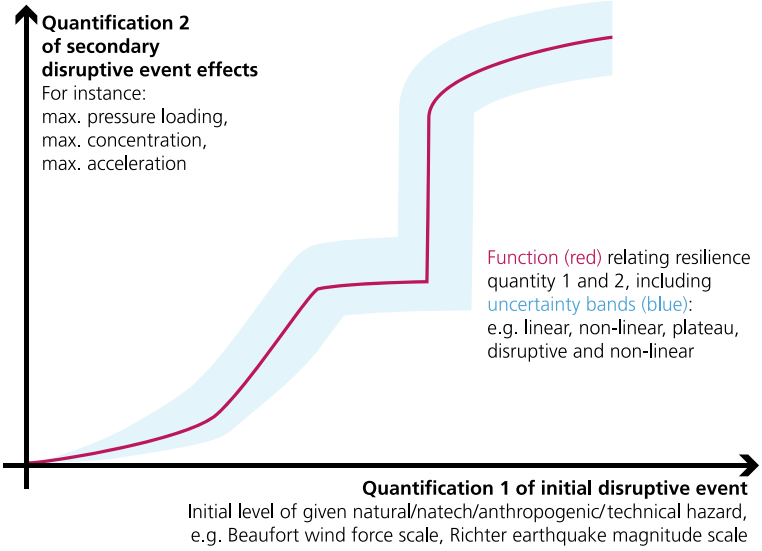

Fig. 5 Example for the propagation of quantities assessing the effects of disruptive events: propagation of an initial resilience propagation expansion quantity 1 to a secondary expansion quantity 2 for the computation of transitions between physical, engineering, causal or temporal layers of resilience assessment. The *red curve* links the two expansion quantities. The uncertainty band is indicated in *blue*. Intuitive examples for quantities that can be propagated are given. The curve and its uncertainty bands determine the transition matrix elements including uncertainties

event set layer, etc., and $E_{N_{\text{res}},2},\ldots,E_{N_{\text{res}},N_{N_{\text{res}}}}$ the N_{res}-th and initial resilience assessment layer (resilience root cause layer), and $N_1 \geq 1, N_2 \geq 1,\ldots,N_{N_{\text{res}}} \geq 1$ are the cardinal numbers of the expansion sets.

A generalization of (32) is illustrated in Fig. 4. Beyond (32), the expression visualized in Fig. 4 allows for the splitting of resilience trajectories as well as their start in resilience assessment event layers after the most initial (outer) layer.

In (32), in particular the second line implies a directional deductive use of the conditional probability. The question is what are the (root) cause events of E_{00}? For instance, what are the causes for successful response of smart production systems, mobile systems or structures? Such causes or steps before the event of interest could be, e.g., access control events during the response phase after the threat event, implemented structural and topological design choices in the preparation and protection layers of assessment, consideration of all possible threat events or all resilience capabilities, etc.

Key elements of (32) are factors of the type $\Pr(E_{1i_1}|E_{2i_2})$. Very similar expressions are also used in (33) and (34) below. To give a simple example, such resilience trajectory transition elements can be visualized as in Figs. 5 and 6, which show two such transitions linking an abstract threat to a hazard quantity and the hazard quantity to a damage quantity, respectively. In this case $N_{\text{res}} = 3$ expansion sets are used.

A further overall example for the propagation method is given in Fig. 7, which illustrates which transition matrix elements are suitable for wind threat resilience

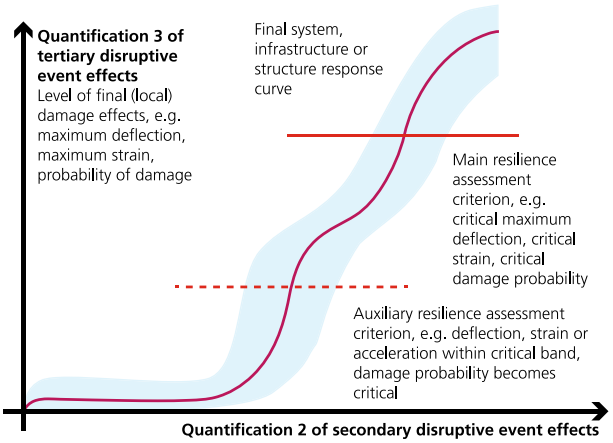

Fig. 6 Example for the propagation of a secondary resilience expansion quantity 2 to a tertiary quantity 3 for the computation of the effects of disruptive events. For the latter intuitive examples are given. In the sample, the final effect of the disruptive event is assessed using two resilience assessment criteria

assessment. In this case $N_{\text{res}} = 4$ expansion sets are used. In particular, the loading depends on the local geography.

Figure 8 depicts an example that is especially interesting for deductive or inverse trajectory-based resilience assessment. It illustrates a rather remote trajectory leading to cyber access to security and safety critical cyber infrastructure. In this case, it is indicated that the transition elements can also be computed using continuum-mechanical numerical simulation. As in Fig. 7, the abstract threats have to be specified and the results of the detailed physical-engineering assessment must be interpreted in terms of relevancy for the red teaming and penetration test question: What are possible access roots to the cyber infrastructure as well as cyber functionalities of the server building?

By applying the alternative conditional probability definition, i.e. by switching the order of the two sets in the right hand side of the first line of (32), neither a deductive nor an inductive ordering can be obtained. However, one may set $N_{\text{res}} = 1$ in (32). This results in the inductive resilience assessment expression

$$\Pr(E_{00}) = \sum_{i_1=1}^{N_1} \sum_{i_2=1}^{N_2} \cdots \sum_{i_{N_{\text{res}}-2}=1}^{N_{N_{\text{res}}-2}} \sum_{i_{N_{\text{res}}-1}=1}^{N_{N_{\text{res}}-1}} \Pr(E_{00}|E_{1i_1}) \Pr(E_{1i_1}|E_{2i_2}) \cdots \cdot \Pr\left(E_{N_{\text{res}}-2,i_{N_{\text{res}}-2}}|E_{N_{\text{res}}-1,i_{N_{\text{res}}-1}}\right) \Pr\left(E_{N_{\text{res}}-1,i_{N_{\text{res}}-1}}|E_{N_{\text{res}},1}\right) \Pr\left(E_{N_{\text{res}},1}\right), \tag{33}$$

for the single initial or seed resilience event $E_{N_{\text{res}},1}$. Now the final resilience event E_{00} as well as the initial resilience event $E_{N_{\text{res}},1}$ may be defined, each of which can be very broad or restricted (specific). If $E_{N_{\text{res}},1}$ is specific (e.g. a certain type of anthropogenic emerging threat or IT security challenge) and E_{00} very broad (e.g. overall resilience not acceptable), then (33) is an inductive resilience assessment

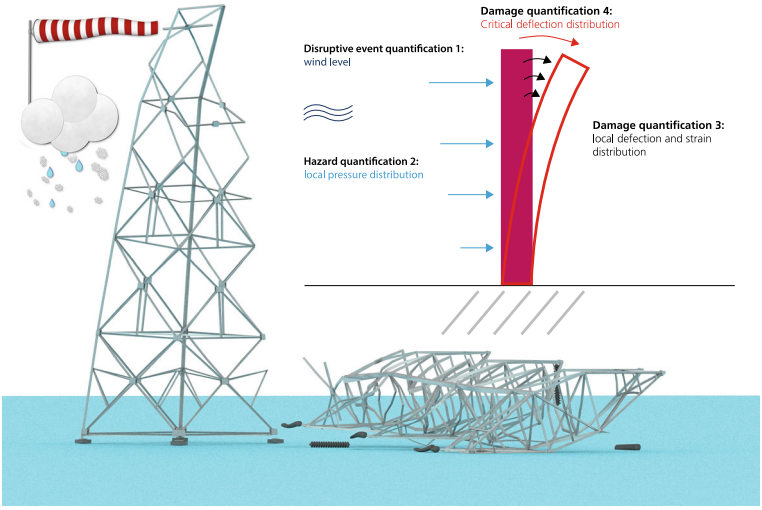

Fig. 7 Example for resilience trajectory/layer propagation quantities used for resilience assessment in case of natural or natech (anthropogenic) disruptive events: resilience trajectory propagation in case of extreme weather events using 4 complete expansion sets. In this case, the critical final event of interest could be critical loss of infrastructure supply capability

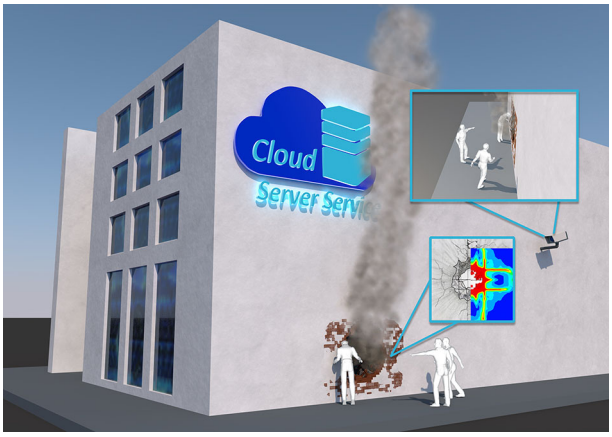

Fig. 8 Access trajectory to cyber infrastructure. Example for deductive trajectory-based resilience assessment. The propagation of the effects of the disruptive event indicated in this case takes account of the effects of surveillance (*top right*). It uses in addition a detailed coupled mechanical-fluid dynamics numerical computation (*bottom right*) for assessing the physical access in case of the displayed disruptive explosive event

expression. The drawback of this derivation and interpretation is the need to argue that $E_{N_{\mathrm{res}},1}$ is a resilience partition.

The visualization of Fig. 9 generalizes (33), because it represents multiple final evaluation events in various resilience analysis layers.

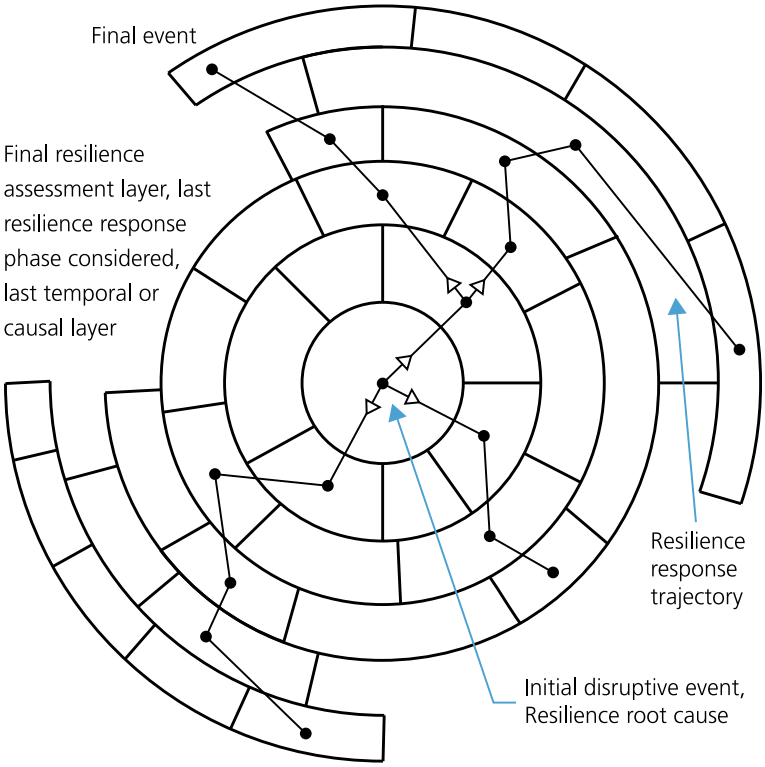

Fig. 9 Inductive, forward or bottom up resilience assessment. A single disruptive event generates multiple causal or temporal trajectories resulting in final events that are evaluated with respect to their effect on resilience

To overcome the challenge indicated in the last text paragraph, it is rewarding to consider the following conditional resilience assessment expansion for a final resilience assessment event E_{final}, e.g. critical system function not available, given the initial resilience event E_{initial}, e.g. technical subsystem degradation,

$$\begin{aligned}
\Pr(E_{\text{final}}|E_{\text{initial}}) &= \sum_{i_1=1}^{N_1} \Pr(E_{\text{final}}|E_{\text{initial}} \cap E_{1i_1}) \Pr(E_{1i_1}|E_{\text{initial}}) \\
&= \sum_{i_1=1}^{N_1} \sum_{i_2=1}^{N_2} \Pr(E_{\text{final}}|E_{\text{initial}} \cap E_{1i_1}) \Pr(E_{1i_1}|E_{\text{initial}} \cap E_{2i_2}) \Pr(E_{2i_2}|E_{\text{initial}}) \\
&\quad \cdots \\
&= \sum_{i_1=1}^{N_1} \sum_{i_2=1}^{N_2} \cdots \sum_{i_{N_{\text{res}}=1}}^{N_{N_{\text{res}}}} \Pr(E_{\text{final}}|E_{\text{initial}} \cap E_{1i_1}) \Pr(E_{1i_1}|E_{\text{initial}} \cap E_{2i_2}) \cdots \\
&\qquad \cdot \Pr\left(E_{N_{\text{res}}-1,i_{N_{\text{res}}-1}}|E_{\text{initial}} \cap E_{N_{\text{res}}i_{N_{\text{res}}}}\right) \Pr\left(E_{N_{\text{res}}i_{N_{\text{res}}}}|E_{\text{initial}}\right).
\end{aligned} \tag{34}$$

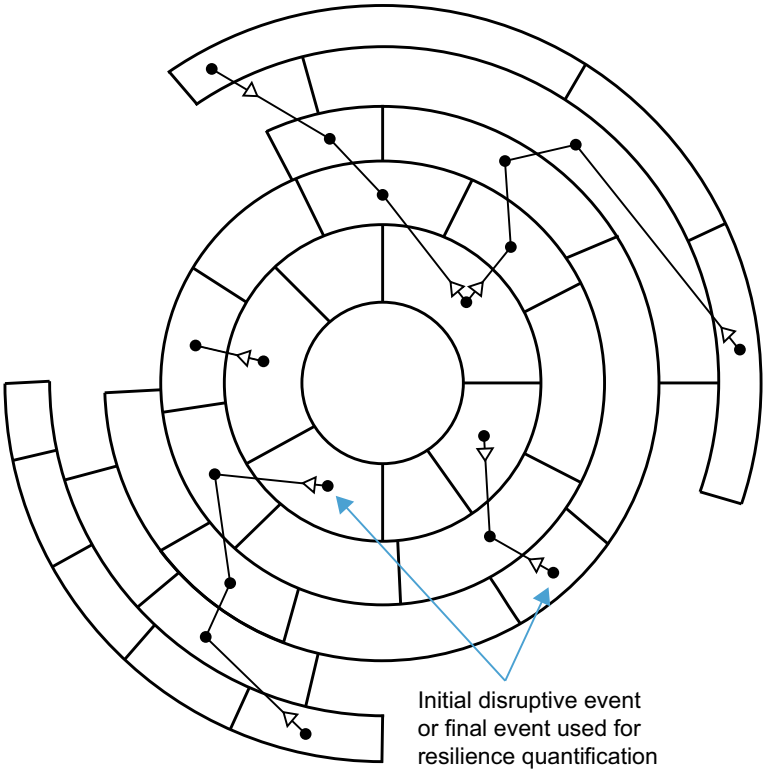

Fig. 10 Inductive and deductive trajectory-based/causal/temporal dynamic resilience assessment allowing for multiple initial and final events for overall resilience assessment

The trajectory approach (34) needs a careful interpretation, which differs from the interpretation of (33). It can be understood as an inductive approach asking for the consequences of the initial disruptive event in terms of the final resilience assessment event. Equation (33) is illustrated by a single trajectory of Fig. 9 that may fork but must join in a single final event. When comparing (34) with (33) it becomes obvious that there is no event base rate probability (see the last factor in the last line of (33)), also all expansion base events are conditional the initial event.

Figure 10 is a generalization of (32) to (34), because it allows in addition for multiple initial as well as final events for inductive and deductive trajectory-based dynamic resilience quantification.

9 Resilience Quantification Based on Modeling, Simulation and Analysis of Socio Technical Cyber Physical Systems Using Time-Dependent System Function (Non) Performance and Resilience Densities

Today a multiple system modeling languages exist for almost all technical and process domains. Besides this, modeling languages were developed that claim to bridge the gap between different technical domains and disciplines, for instance the Systems Modelling Language (SysML), which is based on the object oriented Unified Modelling Language (UML).

Besides these technical efforts, in multiple approaches this originally technical and systems engineering modelling languages have been extended to the modeling of organizations, information flows, logistics and distribution networks as well as decision making processes. Furthermore, there are ongoing efforts to merge and interconnect different system modeling domains, or at least to seamlessly interface between them, for instance in the realm of numerical finite element and multi physical simulation or in the realm of engineering simulations, in particular in discrete and analog electronics, datalinks, mechatronics, pneumatics, hydraulics, etc. Also geo-data based modeling and simulation is based on a strong unifying data management approach developed by the geo information technology community.

The interconnection of modeling domains can also be conducted by using software interfaces, operator or user models, or behavioral models for other model elements, for instance societal groups. This is conduced within certain modeling boundaries and also termed agent-based or agent supported modeling and simulation.

Modeling is the first step to simulate systems. If models are very abstract, simulations are rather basic and sometimes just animations, e.g. in the case of SysML models. In technical and engineering approaches, the models contain all the input information and often also already the parameter data sufficient to start physical-technical simulations. For standard environments and standard stresses and loadings during operations, such simulation approaches allow by now in informed applications predictive assessments of selected behaviors and responses of (socio) technical systems.

The question arises whether such coupled modeling and simulation approaches are also capable to model and simulate disruptive events, in particular major stress and loading events beyond standard events. This includes also cumulating events or creeping deteriorations that reach a tipping point.

The interesting observation is that some typical engineering modeling and simulation tools even do not allow to enter system designs that do not function properly, for instance circuit simulation tools, or semiformal models used for software generation and development. Also, if failure models are taken account of, they are typically restricted to certain standard failures, e.g. in case of electronics to interruption, shortcut and drift.

Of course, much advanced failure models and loading response models and simulations can be added to the standards system models and simulations. This can

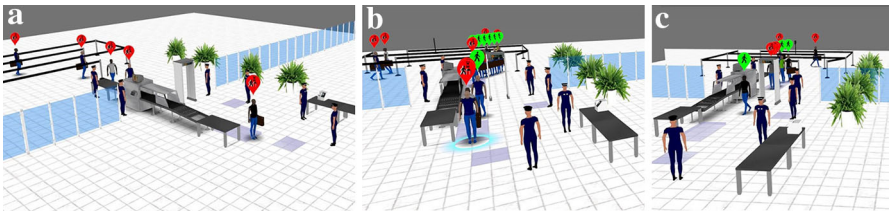

Fig. 11 Example for a socio technical cyber physical system modeling, simulation and analysis: airport checkpoint. The sequence of pictures shows the response of the system to the standard disruptive event passenger rush. *Left* almost empty checkpoint; *middle*: crowded checkpoint, *right* again smooth operation. Another disruptive event of interest is a passenger carrying dangerous or illicit goods

be obtained by transferring modeling and simulations approaches from neighboring domains. For instance, dynamical response modeling is standard for crash simulations but not for structural static mechanical response modeling. In a similar way, high voltage and current loadings are standard for air bag ignition elements, high voltage trains in electro vehicle applications, but not expected in standard automotive electronics. Such transfer is challenging as well as the necessary adaption to the new application domains.

In the following, several resilience quantities are identified that can be extracted from modeling and simulation. The extraction of the resilience quantities of interest may be termed model and simulation based resilience analysis.

Based on the modeling and simulation of systems and depending on the resolution and coverage of the used approaches, quantities of interest for resilience assessment can be generated and analyzed. An example for the modeling of a socio technical cyber physical system is given in Fig. 11.

In the following, it is first assumed that the system quantities analyzed depend on time. Also time-independent quantities are discussed below. Nevertheless, such quantities often can be derived from time-dependent system behavior. For instance, the maximum top-level quantifiable damage of a system can be output of a time-dependent simulation as shown in Fig. 11.

In Fig. 11, performance quantities of interest include individual and collective throughput, security gain or individual and collective risk reduction. The checkpoint modeled uses an extended semi-formal SysML model that contains all information of the respective subsystem models used (Renger et al. 2015). The model allows direct access to a variety of (time-dependent) system quantities that can be used for the quantification of the resilience of the socio technical system. Disruptive events might include: alarm resolutions of various kinds, breakdown of subsystems (detectors, scanners), increase of overall alert level, (massive) common cause events, selected operator behavior or passenger rush.

Figure 11 shows the visualization of an airport checkpoint modeling and simulation approach that focuses on the interactions of the passengers with different subsystems that aim at enhancing the security of air transport. In this case a variety of subsystems with different technologies are interconnected. There are users (passengers) and operators of the system. For all subsystems, humans and interfaces,

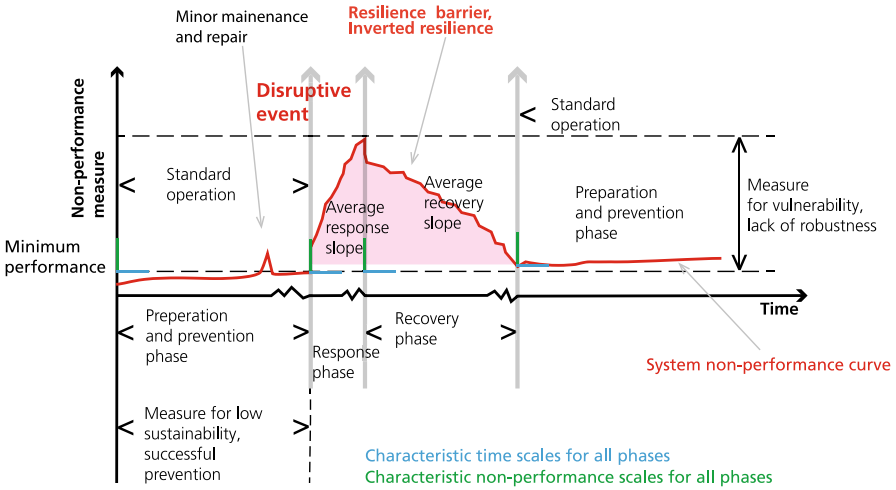

Fig. 12 Resilience assessment quantities based on time-dependent system, system function or system service non-performance curve

different top level and partly interconnected models are used. Each simulation considers one instantiation of the possible use of the airport checkpoint.

Only if modeling and simulation also comprise the response of the system to disruptive events, it suffices for resilience assessment of the system. In case of a disruptive event, non-performance curves of the system or system functions or services increase see Fig. 12, for instance average time per passenger or risk per passenger.

Figure 12 separates different phases of the system response before and after the disruptive event: preparation and prevention, response and recovery. For resilience quantification, in particular the following quantities are of interest: the duration of the phases, the non-performance increase and slopes of performance decrease and increase. The time axis may use different scales, e.g. years for the preparation and protection phase, days for the response and months for the recovery phase. Also the y-axes may vary. For instance, the characteristic scale for assessing non-performance in the preparation and prevention phase (see green unit arrow at the left hand side) might be of the order of 1 % of the overall system performance, whereas the characteristic length scale for the performance during the response phase and recovery phase could be 10 % of the overall performance.

Figure 12 can be understood as the realization of a single possible event or an averaged superposition of multiple possible events, see Fig. 13. In the latter case, the modeling and simulation approach to resilience also delivers uncertainty estimates, as indicated.

A very similar discussion as for Fig. 12 can be based on system or system function performance measures, see Fig. 14.

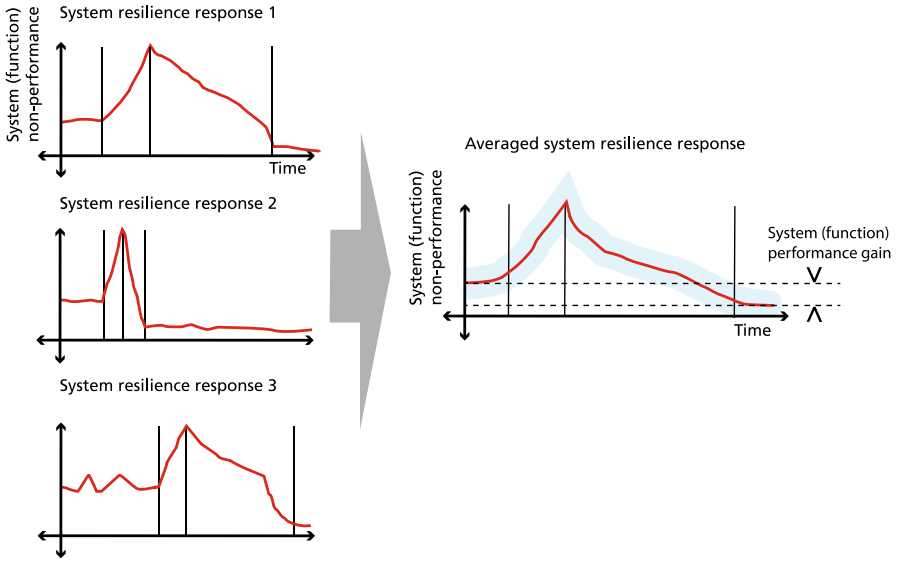

Fig. 13 Averaging of time-dependent system performance curves for the determination of averaged system resilience response with respect to disruptive events. The uncertainties are represented by the *blue* band. In this case after the disruptive event the system (function) exhibits higher performance

As indicated by the characteristic scales, all the quantities of Fig. 12 can be made dimensionless, including the area of the resilience barrier, and the slopes. Thus, they can be combined to overall resilience indicators (RI). For instance, a refinement of (1) and (2) may read, using the notation introduced at the beginning of Sect. 4,

$$\Pr\left(\mathrm{RI} = \sum_{i=1}^{N_2^{\mathrm{RA}}} \frac{\Delta t_i}{\Delta P_i} \int_{t_i^{\mathrm{lower}}}^{t_i^{\mathrm{upper}}} P(t)\mathrm{d}t\{\leq, \geq\}\mathrm{RI}_{\mathrm{crit}}\right) \overset{!}{=} \{\min,\max\}, \tag{35}$$

where Δt_i and ΔP_i are the characteristic time and (non-)performance scales and $\left[t_i^{\mathrm{lower}}, t_i^{\mathrm{upper}}\right]$ the time intervals of the resilience response phases that are distinguished. The fraction $\Delta t_i/\Delta P_i$ in (35) can also be understood and replaced by a single weighing factor w_i, which expresses the relative weight of the resilience management phases. Equation (35) with min and max belongs to Figs. 12 and 14, respectively.

The risk indicator $\mathrm{RI}_{\mathrm{crit}}$ are in general different. Of course, using only a single critical risk indicator $\mathrm{RI}_{\mathrm{crit}}$ and combining all the contributions of all resilience management phases is a rather strong simplification. One could also use risk indicators for each temporal phase.

In a similar way, other possible resilience optimization options include to (see Figs. 12 and 14)

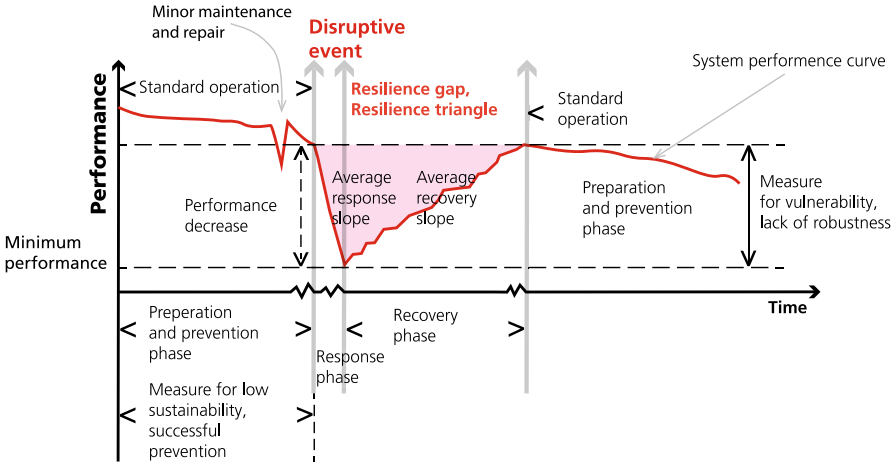

Fig. 14 Resilience quantities derived from time-dependent system or system function performance curve

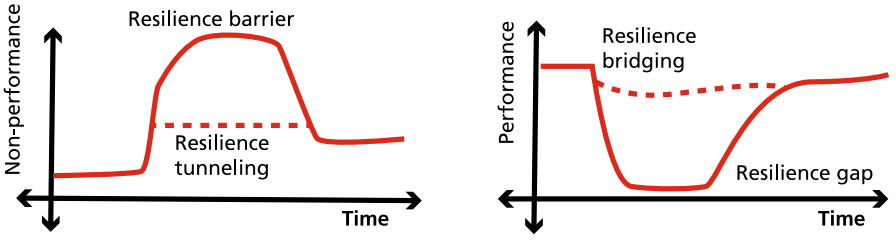

Fig. 15 Resilience tunneling and resilience bridging. *Left* successful resilience engineering results in system or system function non-performance curves that tunnel (*dashed red line* in left figure) when compared to the non-optimized system response (*red line* in left figure). *Right* successful resilience engineering results in resilience bridging (*dashed red line* in right figure) when compared to system performance without resilience engineering (*red line* in right figure)

(a) maximize the time of the preparation and prevention phase,
(b) minimize (e.g. in case also a very fast recovery is aimed at) or maximize the response time or the absolute value of the response slope (e.g. in case of fire events to allow for response),
(c) minimize vulnerability,
(d) minimize recovery time,
(e) maximize the absolute value of the recovery slope and to
(f) minimize vulnerability.

In each case, optimization conditions in the form

$$\Pr\left(\frac{(\text{expectation value of})\,\text{resilience quantity}}{\text{characteristic scale}}\{\leq,\geq\}\text{RI}\right)\overset{!}{=}\{\min,\max\},\quad(36)$$

can be formulated.

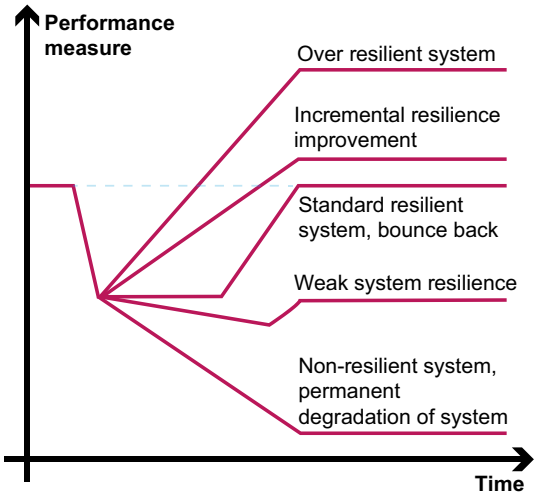

Fig. 16 Exemplary system function response and recovery path options after disruptive events

However, the optimization conditions strongly depend on the context. For instance, in case of aiming at over resilient response of a system as sketched in Fig. 16 below, it might be more efficient to allow for sufficient planning, e.g. in case of rebuilding critical infrastructure after local events. In general, several resilience optimization requests of the form (35) and (36) have to be combined. In this case, in general the relative weights of the optimization or minimization constraints must be determined. This requires again non-technical input and goes beyond the identification of characteristic scales.

Figure 15 shows two options to visualize the improvement of the resilience response of systems during the response and recovery phase. If time-dependent non-performance measures are used the resilience barrier can be tunneled, i.e. the system, a system function or even only a critical sub-function is provided with a sufficiently low non-performance level. In a similar way, when using performance measures, the resilience gap can be bridged by a sufficiently performant system or subsystem (function).

Figure 16 shows a range of resilience response options when using system (function) performance measures. A similar schematic can be derived when using non-performance measures. Ambitious resilience engineering should aim at least at incremental system performance improvement.

Figure 17 shows how one-dimensional resilience quantities are generated from multiple simulations. Each instance of simulation generates a discrete value for the quantity. These quantities are combined and result in one-dimensional distributions for the quantity of interest. A possible estimate for the quantity is the mean value of the density of the resilience quantity. The advantage of distributions is that they also represent the uncertainty of the model and simulation based resilience quantities.

The multiple options for the quantification of resilience based on modeling, simulation and analysis of (socio) technical systems as presented in Sect. 9 highlights the potential of this approach.

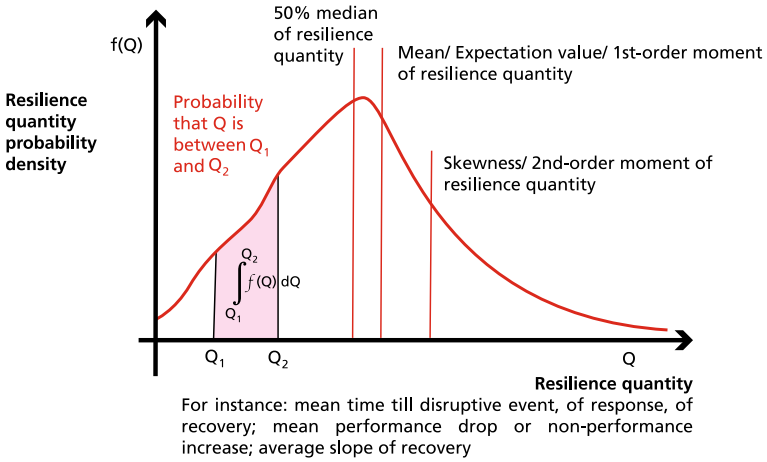

Fig. 17 Probability density of resilience quantity with sample interpretations and sample resilience quantities

10 Summary, Conclusions and Outlook

In the introduction, the article detailed some of the most pressing needs for resilience quantification of modern (socio) technical systems, in particular persisting and novel natural, natech and man-made threats as well as ever increasing system complexity, interdependence, connectivity, intelligence and the resulting man-made potential threats. However, even in the case of security and/or safety critical or relevant systems or in the case of systems on which modern citizens critically rely and depend on, resilience requirements often are neither the only nor the most relevant requirements for overall system assessment. This holds true despite the consensus that acceptable resilience is fundamental for all the other requirements of sustainable systems. For instance, low carbon dioxide footprint is prerequisite for future systems, despite the increasing necessity and societal demands on the resiliency of the systems.

Therefore, for sustainable development and design of new systems as well as for optimizing and retrofitting existing systems, the quantification of resilience is of key interest. This was formulated in the article in generic resilience extreme value problems in terms of acceptable overall resilience. For their solution resilience quantification is key input.

The quantification of resilience allows to compare different systems with respect to their resilience performance. More importantly, it allows to balance resilience requirements with other requirements. Resilience quantification enables to optimize systems throughout all their credible life cycles, rather than assuming a single standard life cycle. This forms the basis for sustainable, secure and safe response, recovery and development in the advent of disruptive events.

The presentation of several resilience quantification approaches of increasing methodological complexity showed that resilience quantification is often a

significant extension of existing approaches to understand, model, simulate and analyze (socio) technical systems. Also novel approaches will be required, which are able to deal with the often non-linear, discontinuous, quality changing or highly dynamic quantitative response of systems. In particular, the approaches have to cover changes of behavior or dynamic of systems as well as of the structure and architecture of the systems. These general observations encourage the expectation that the technical system capabilities system (self) monitoring and situation awareness (sensing), system modeling and inference, system action as well as reconfiguration, adaption and learning will be extendable and predictable much beyond standard operation and maintenance along with increasing resilience quantification options. Thus, resilience quantification strongly supports or even leverages the design and operation of significantly improved sustainable systems.

Resilience quantification with respect to all resilience response phases, properties or other resilience dimensions as appropriate allows to motivate and advance new system developments and designs. Such flexible resilience designs exhibit, for instance, strong response and recovery properties rather than being very preventive or protective. They could be smart but need only few material resources. In a similar way, traditional no-risk or low-risk assumptions can be lifted and replaced by quantitative resilience assessments and thus also allow for innovative business models.

The following main objectives can be achieved from resilience quantification of (socio) technical systems for resilience engineering:

(a) understand and formalize resilience concepts,
(b) validate resilience concepts,
(c) design resilient systems,
(d) optimize and retrofit systems regarding resiliency,
(e) extend, carry forward, renew and tailor concepts of reliability and maintenance, dependable systems, safety relevant and critical systems, security, vulnerability, chance and risk.

Within the article, resilience quantification was categorized and exemplarily derived in four different approaches:

1. qualitative/quantitative/analytical resilience assessment processes and frameworks,
2. probabilistic/statistical static resilience order expansion approaches,
3. resilience trajectory/propagation/transition matrix/dynamic approaches,
4. system modeling, simulation and analysis for the generation of (time-dependent) resilience curves, indicators and resilience density distributions.

Typical respective methods and applications for the four approaches include:

1. qualitative and semi-quantitative fast societal, technical and natural science expert estimates, expert assessment and exploration of issues relevant for more detailed resilience assessment in terms of the approaches 2. to 4.

2. statistical historical, empirical and data mining approaches for empirically based resilience assessments,
3. technical-engineering computations and simulations that take advantage of combined domain knowledge along with established human and societal behavior modeling approaches,
4. coupled simulations of multi-technology and multi-domain small and large socio technical systems at various scales, complexity and levels of abstraction, allowing as well for complex human and societal models, e.g. agent-based, using graph modeling or coupled engineering simulations.

For the quantification options 1. to 4. the formal expressions are introduced, explained, discussed and examples are given. This includes the discussion of assumptions and limitations of the expressions. The key ideas for the derivation of the expressions are stated. The expressions derived are suitable as a starting point and are expected to be readily adoptable to practical applications. Since the assumptions of the quantification efforts are made explicit, the most appropriate approaches and combinations can be selected.

As shown in Sect. 3, at a high level of abstraction, the probability and uncertainty concept allows for short notations. However, it requires further concretization and discussion as exemplarily conducted in Sects. 4–9. In its very definition, the concept often asks for non-technical inputs: thresholds for acceptable resilience, acceptable uncertainty thresholds regarding the resilience quantification results and finally relative weighting of competing resilience objectives.

Subsequently, conclusions on the formal rigor of the resilience quantification approaches are given:

1. Even if the qualitative, semi-quantitative and quantitative resilience assessment process examples of Sect. 4 use rather basic expressions, their combinations and iteration processes allow for the design of elaborated resilience assessment frameworks and processes, which can be tailored to take account of available resources.
2. When ordering the approaches with respect to formal rigor, the resilience expansions beginning with Sect. 5 and in particular the higher order expansions of Sects. 6 and 7 are most formal.
3. The resilience event propagation approach of Sect. 8 can be intuitively visualized using resilience trajectories, even if the deductive and inductive multi-layer expressions contain rather cumbersome conditional probabilities. These matrix elements can be nicely linked to a whole range of existing technical and societal science approaches, in particular engineering assessments.
4. Section 9 uses formal expressions only to quantify typical results of socio technical system resilience analysis based on modeling and simulations of the systems. Therefore, the main formal effort is hidden. Even so, it is shown that a variety of different types of resilience quantities is necessary to quantify and compare the resilience of systems in given contexts. In particular, aggregation of quantities might lead to an oversimplification.

In summary, the article motivated four resilience quantification approaches suitable for socio technical systems, gave elementary sample derivations and selected possible application examples. Alongside, it introduced the concepts of resilience dimension, process-based resilience assessment, resilience dimensional expansion, resilience trajectory expansion set, resilience transition matrix element, resilience response time-history curves and resilience quantity density distributions for uncertainty assessments. Most illustrative are the concepts of resilience partition, resilience propagation trajectory as well as resilience barrier and resilience tunneling or equivalently resilience gap and resilience bridging.

When quantifying the resilience of a single (socio) technical system, the approaches 1. to 4. have in general to be combined. It is expected that the introduced concepts, formal expressions and graphical schemes comprise an important subset of resilience quantification approaches that have to be implemented in case of resilience quantification of existing, emerging and future systems.

Acknowledgments The authors thank Uli Siebold for the figures provided in Fig. 11.

References

Alberts DS, Hayes RE (2003) Power to the edge. Command, control in the information age. CCRP Publication Series (Information age transformation series), Washington, DC

AS/NZS ISO 31000:2009 (2009) Risk management – principles and guidelines

Baird (2010) The phases of emergency management

Baumann D, Häring I, Siebold U, Finger J (2014) A web application for urban security enhancement. In: Thoma K, Häring I, Leismann T (eds) 9th future security, pp 17–25. Berlin, September 16–18, 2014; proceedings. Security Research Conference. Fraunhofer-Verlag, Stuttgart

Boyd J (1995) The essence of winning and losing. a five slide set by Boyd, 6/28/1995

Bruneau M, Chang SE, Eguchi RT, Lee GC, O'Rourke TD, Reinhorn AM et al (2003) A framework to quantitatively assess and enhance the seismic resilience of communities. Earthq Spectra 19(4):733–752. doi:10.1193/1.1623497

Chang SE, Shinozuka M (2004) Measuring improvements in the disaster resilience of communities. Earthq Spectra 20(3):739–755. doi:10.1193/1.1775796

Cimellaro GP, Reinhorn AM, Bruneau M (2010) Framework for analytical quantification of disaster resilience. Eng Struct 32(11):3639–3649. doi:10.1016/j.engstruct.2010.08.008

Dekker S, Hollnagel E, Woods D, Cook R (2008) Resilience Engineering: New directions for measuring and maintaining safety in complex systems. Final report. In: Lund University School of Aviation

Dorbritz R (2011) Assessing the resilience of transportation systems in case of large-scale disastrous events. In: Cygas D, Froehner KD, Breznikar A (eds) Environmental engineering, pp 1070–1076. Selected papers, No 1867-M. Vilnius Gediminas Technical University press "Technika" (VGTU Press "Technika" scientific book, No 1867-M), Vilnius

Edwards C (2009) Resilient nation. London

Fox-Lent C, Bates ME, Linkov I (2015) A matrix approach to community resilience assessment. An illustrative case at Rockaway Peninsula. Environ Syst Decis 35(2):209–218. doi:10.1007/s10669-015-9555-4

Hollnagel E, Tveiten CK, Albrechtsen E (2015) Resilience engineering and integrated operations in the petroleum industry. In: IO-center (SINTEF) report no: SINTEF A16331

Jackson S (2010): Architecting resilient systems. Accident avoidance and survival and recovery from disruptions. John Wiley & Sons (Wiley series in systems engineering and management), Hoboken

Landegren F, Johansson J, Samuelsson O (2014) Review of computer based approaches for modeling and simulating critical infrastructures as Socio-Technical Systems. In: Steenbergen RDJM, VanGelder PHAJM, Miraglia S, Vrouwenvelder ACWM (eds) Safety, reliability and risk analysis: beyond the horizon, pp 2047–2054. Netherlands Org Appl Sci Res Delft Univ Technol Dutch Soc Risk

Management and Reliabil Anal European Safety and Reliabil Assoc. CRC PRESS-Taylor & Francis Group, Boca Raton

Linkov I, Bridges T, Creutzig F, Decker J, Fox-Lent C, Kröger W et al (2014) Changing the resilience paradigm. Nat Climate Change 4(6):407–409. doi:10.1038/nclimate2227

Mansfield J (2010) The nature of change or the law of unintended consequences. An introductory text to designing complex systems and managing change. Imperial College Press; Distributed by World Scientific Pub, London, Singapore, Hackensack, NJ

MCEER (2006) MCEER's resilience framework

O'Rourke TD (2007) Critical infrastructure, interdependencies, and resilience. In: The Bridge

Osinga FPB (2007) Science, strategy and war. The strategic theory of John Boyd. Routledge (Strategy and history, 18), London, New York

Perrow C (2011) Normal accidents. Living with high risk technologies. Princeton University Press, Princeton

Porte La, Todd R (1996) High reliability organizations: unlikely, demanding and at risk. J Conting Crisis Manag 4(2):60–71

Renger P, Siebold U, Kaufmann R, Häring I (2015) Semi-formal static and dynamic modeling and categorization of airport checkpoints. In: Nowakowski T (ed) Safety and reliability: methodology and applications, pp 1721–1731. Proceedings of the European Safety and Reliability Conference, ESREL 2014, Wrocław, Poland, 14–18 September 2014. CRC Press, Boca Raton. doi:10.1201/b17399-234

Renschler CS, Frazier AE, Arendt LA, Cimellaro GP, Reinhorn AM, Bruneau M (2011) A framework for defining and measuring resilience at the community scale: the PEOPLES resilience framework. In: MCEER-10-006, University at Buffalo (SUNY), The State University of New York, Buffalo

Rose Adam (2004) Defining and measuring economic resilience to disasters. Disaster Prevent Manag 13(4):307–314. doi:10.1108/09653560410556528

Rose A (2009) Economic resilience to disasters

Schoppe CA, Häring I, Siebold U (2014) Semi-formal modeling of risk management process and application to chance management and monitoring. In: Steenbergen RDJM (ed) Safety, reliability and risk analysis. Beyond the horizon. Taylor & Francis Group, London, pp 1411–1418

Sterbenz JPG, Çetinkaya EK, Hameed MA, Jabbar A, Qian S, Rohrer JP (2011) Evaluation of network resilience, survivability, and disruption tolerance. Analysis, topology generation, simulation, and experimentation. Telecommun Syst. doi:10.1007/s11235-011-9573-6

Størseth F, Tinmannsvik RK, Øien K (2010) Building safety by resilient organization – a case specific approach. In: Briš R (ed) Reliability, risk and safety. Theory and applications; proceedings of the European Safety and Reliability Conference, ESREL 2009, Prague, Czech Republic, 7–10 September 2009. CRC Press/Balkema, Leiden

Tamvakis P, Xenidis Y (2013) Comparative evaluation of resilience quantification methods for infrastructure systems. Procedia Soc Behav Sci 74:339–348. doi:10.1016/j.sbspro.2013.03.030

Thoma K (ed) (2011) European perspectives on security research. Springer (Acatech diskutiert), Berlin

Thoma K (2014) Resilien-Tech: «Resilience by Design»: a strategy for the technology issues of the future. Acatech STUDY. In: Acatech

Tierney K, Bruneau M (2007) Conceptualizing and measuring resilience. A key to disaster loss reduction. TR News 250:14–18

van der Vorm J, van der Beek D, Bos E, Steijger N, Gallis R, Zwetsloot G (2011) Images of resilience: the resilience analysis grid applicable at several organizational levels? In: Hollnagel E, Rigaud E, Besnard D (eds) Proceedings of the fourth Resilience engineering symposium. 8–10 June, 2011, Sophia Antipolis, Transvalor-Presses des Mines (Collection Économie et gestion), France. Paris, pp 263–269