© 2018 Taylor & Francis Group, London, ISBN 978-0-8153-8682-7

A quantitative approach for applied resilience assessment audits

R. Mock

Institute of Sustainable Development INE, Zurich University of Applied Sciences, Winterthur, Switzerland

ABSTRACT: Today's infrastructural systems are expected to be safe and resilient. In this context, assessment of such systems faces two principal challenges: common approaches in risk assessment have reached their limits in methodology and feasibility in assessing complex and interconnected systems. On the other hand, resilience assessment is in its beginnings and lacks, e.g., a commonly accepted resilience metric. The paper starts to specify a practical definition of resilience and assigned metric: Resilience is characterised by influencing recovery properties of a socio-technical system. Actors and actions are carriers of these properties. This corresponds to the views of system representation by Use Case Diagrams (UCD). In order to quantify an UCD, actions are validated by assessing their compliance level L. Actors are associated with their abilities to respond, monitor, learning, and to anticipate developments. The result is given by the Resilience Priority Value REPV = $L \cdot I$ of actors and overall system. The resilience assessment process is exemplified by a case study of a car park guidance system.

1 INTRODUCTION

Current infrastructural systems show a high level of complexity and technical development will further strengthen this trend. As consequence, such systems will become increasingly difficult to handle for system operating organisations (private and non-private) and managers involved. It already looks as that methodological or practicable limits of, e.g., established risk assessment approaches have been reached. New terms reflecting newly desired system properties (e.g., resilience, smartness) are emerging too. However, the methodology of resilience assessment is in an early stage of development and not (yet) in the focus of most organisations. This is also due to the lack of a practicable, quantitative metric of resilience. In this context, the paper presents an approach to facilitate applied resilience assessment audits. Following the concept of system representation and resilience quantification, the remaining paper is structured as follows: Chapter 2 defines resilience and terms in use. The results of a literature survey on resilience definitions in specified engineering domains are given in Chapter 3. In Chapter 4, resilience assessment is utilised by using quantified Use Case Diagrams (UCD). The case study presented in Chapter 5 serves to proof the concept. The paper closes with discussion of pro and cons of approach and context.

2 TERMS

The view in applied research and development in resilience analysis covers the requirements of users in organisations and enterprises (mainly small to mid-sized enterprises SME). Hence, any resilience assessment approach needs to cover additional demands (cf. (ISO-31010 2009)), which might be unimportant to basic research. A major concern of organisation is method efficiency. Thus, the resilience assessment approach as introduced in this paper aims to finally reach practicability as known in basic risk assessment audits, fire and explosion inspections, annual tests of vehicle safety (Ministry of Transport (MOT) test), among others. According to the author's experience, such a system analysis must be typically performed from one person in about one day.

There are already exhaustive literature surveys on terminology of resilience, where the most common understanding of resilience is exemplified by Scholz et al. (2012): Resilience is the ability of the system to adjust its functioning […] following changes and disturbances, so that it can sustain required operations.

Hosseini et al. (2016) also consider system recovery abilities as crucial part of resilience, where recovery is the capability of a system to absorb and adapt to disruptive events.

Lay et al. (2015) labour characteristics and abilities of resilient systems in more detail, which is finally the definition as used in this paper:

DEFINITION 1 (RESILIENCE) *characterises the abilities of a system to respond to disturbances, to monitor, to learn and to anticipate developments.*

With this, resilience belongs to a set of related engineering terms characterising system capabilities by attributes or system performance function $P(t)$, e.g., availability $A(t)$:

Definition 2 (Availability) *is the probability of finding an unit in an operational condition at time t.*

This definition of availability follows, e.g., DINEN61703 (2002). Note that $A(t)$ encompasses maintenance, which is a system ability to respond to disturbances (failures, incidents, over-fulfilment, etc.), to monitor them (failure identification) and to learn (optimising maintenance processes) and anticipate trends (expected failures). The latter is covered by reliability management processes and preventive maintenance. So far, resilience looks like the generalisation of availability towards the analysis of extended socio-technological systems. Furthermore, management and associated processes are considered as an integral part of such a system in resilience assessment (cf. (Leksin et al. 2018)). By contrast, management tends to play the role of an external controller in risk assessment. Business continuity (BC) also follows the concept of system recovery but concentrating on business impacts:

Definition 3 (Business Continuity) *is a corporate capability. This capability exists whenever organisations can continue to deliver their products and services at accep*table *predefined levels after disruptive incidents have occurred (cf. ISO 22301: 2012).*

Resilience is in line with established approaches to manage deviations, e.g., risk management according to ISO-31000 (2009). Note, that any system assessment approaches cover the subprocesses of event identification, analysis and evaluation. The view of resilience, availability and business continuity is to describe system capabilities with associated performance functions where risk relates to (undesired) events.

3 STATE OF THE ART

The following results of a survey on resilience definitions concentrates around engineering domains which are then used to reason the way of utilisation of resilience assessment as proposed in Chapter 4. Hosseini et al. (2016) give an extended review of definitions. They state that the engineering domain "includes technical systems designed by engineers that interact with humans and technology, such as electric power networks". There, engineering resilience is defined in various points of views:

- Sum of the passive survival rate (reliability) and proactive survival rate (restoration) of a system.
- "Intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions" (Hollnagel et al. 2010).
- "Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event" (NIAC 2009).
- Factors, e.g., minimisation of failure, limitation of effects, administrative controls/procedures, flexibility, controllability, early detection.

Furthermore, Hosseini et al. (2016) state that:

- Many definition focus on the capability of system to *absorb* and to *adapt* to disruptive events, and *recovery* is considered as the critical part of resilience.
- For engineered systems, reliability is considered to be an important feature (e.g. nuclear power systems).
- Returning to steady state performance is needed for resilience; some definitions do not impose that the system returns to the pre-disaster state (e.g. infrastructure).
- Multidimensionality and threat-dependency of resilience definitions.

These lists and the findings of Chapter 2 substantiate: Resilient systems show abilities to preparedness and recovery in general. Then, preparedness is typically covered by a descriptive (i.e. qualitative) and case specific set of attributes $\max_{\bar{x}\in(0,\infty)} f(\bar{x})-g(\bar{x})-h(\bar{x})$. System performance $P(t)$ uses various modelling and simulation approaches to model system dynamics and performance $P(t)$ according to the resilience triangle concept. Definition of preparedness attributes follows methods to design and evaluate questionnaires, check lists, etc., and graphs represent relationships of system abilities. This notation is useful to characterise the common approaches of resilience system analysis:

- *Attributive*: Starting point is the compilation of system specific attributes $\mathbb{A}=\{a_1,a_2, \quad ,a_n\}$, which characterises the presence of or impact on resilience properties, e.g., awareness, flexibility, risk management, competence, and redundancy. Then, analysis follows methods to evaluate questionnaires, check lists, etc. or uses any graphs to represent relationships.
- *Performance*: System performance modelling needs the specification of time dependent and system specific performance measurements, e.g., availability (i.e. function showing the alternation of operation and maintenance), returns (money), among others. Note that $P(t)$ already comprises the recovery properties. Modelling parameters of might base on $\mathbb{A}$. Hence, $P(t)$ can be modelled by graph theory, (e.g. Markovian

models, system dynamics, state diagrams), classical mechanics considering damped harmonic oscillation, (i.e., spring model) as well as control theory using proportional–integral–derivative controller (PID controller).

The definition of resilience performance $P(t)$ results in generic system statements:

- $max\left\{\left|\Delta P(t)\right|\right\} \leqq b$: There is a specified band width b (i.e. defined upper and lower performance levels) which defines system operability (Mock and Zipper 2017).
- $P(t) = 0$: Total system failure (worst case) which ends reparability. Recovery is not possible and system re-construction is equivalent to a different and thus new system. Reconstruction is only possible by supporting measures of the superior system (cf. definition of disaster). Hence, $P(t) = 0$ is associated with fully operable (new) system which is a common boundary condition in reliability analysis.
- $P(t) = k$ and $\dot{P}(t) = 0$: Nominal operation on constant performance level k.
- $\dot{P}(t) \neq 0$: System is in resilience mode.
- $\ddot{P}(t) \neq 0$: Acceleration of performance alteration is an indicator of resilience request.

In summary, there is no common understanding of resilience and how to model resilience. Many authors define key abilities of resilience by their own. The lowest common denominator is the ability of a resilient system to respond to disturbances and, hence, functional preserving capabilities (i.e. recovery). In order to verify these findings, Table 1 uses Def. 1 of resilience to allocate the specified attributes of resilience for infrastructure systems as named in references.

Table 1 also shows that "respond" to disturbance is the main property of a resilient system. The remaining properties are less frequently listed. From the author's point of view, this table exemplifies the uncertainty of how to deal with resilience key capabilities other than "respond", and that it is still necessary to utilise the resilience concept for concrete applications.

Table 1. Key abilities of resilience for infrastructure systems.

System	Respond	Monitor	Learn	Anticipate	Reference
System homeland security	robustness, consequence mitigation	threat and hazard assessments	adaptability, harmonisation od purposes, comprehensive of scope	risk-informed planning and investment	(Hosseini et al. 2016)
Telecommunication network	maintainability	reliability, safety, confidentiality, availability, integrity performance	–	–	(Hosseini et al. 2016)
Communication network	defend, remediate, recover	detect, diagnose	refine	–	(Hosseini et al. 2016)
Infrastructure system	absorb, recover	–	adabt	anticipate	(Lay et al. 2015)
Critical infrastructure	responsiveness, timely recovery, minimum level of service while undergoing changes, flexibility	–	–	coordinated planning	(Lay et al. 2015)
Infrastructure network	ability to regain a previous state	–	adopt the stress–strain model	–	(Bergström et al. 2015)
Infrastructure	recovery (bouncing back)	–	–	–	(Lundberg and Johansson 2015)
Critical infrastructures	robustness, (availability of redundancy, resourcefulness and efficiency of supporting measures)	–	–	–	(BABS 2013)

4 UTILISATION

Chapter 4 identifies the interrelationships among system elements by UCD and how to quantify system resilience by attributes as given in Def. 1.

4.1 *Use Case Diagram UCD*

The Unified Modeling Language (UML) is a quasi-standard of system representing diagrams offering conformance in syntax and semantics. UML 2.5 defines thirteen types of diagrams, divided into three major categories: Structure Diagrams, Behaviour Diagrams, and Interaction Diagrams (cf. www.uml.org) UML diagrams are standardised by (ISO-19501 2005), where UCD is the most simple structure diagram in UML. This Chapter gives a short introduction into the concept of UCD by referencing to the mentioned standard unless otherwise stated.

Definition 4 (Use case) *is a kind of classifier representing a coherent unit of functionality provided by a system, a subsystem, or a class as manifested by sequences of messages exchanged among the system (subsystem, class) and one or more outside interactors (called actors) together with actions performed by the system (subsystem, class).*

A use case is shown as an ellipse containing the name of the use case which characterises activities of actors.

Definition 5. *"An [actor] defines a coherent set of roles that users of an entity can play when interacting with the entity. An actor may be considered to play a separate role with regard to each use case with which it communicates".*

The standard stereotype icon for an actor is a "stick man" figure with the name of the actor.

There are three types of relationships among use cases (actions) and association

- *Association*: The participation of an actor in a use case. In Figure 1, associations are shown by solid lines.
- *Extend*: An extend relationship from use case A to use case B indicates that an instance of use case B may be augmented (subject to specific conditions specified in the extension) by the behaviour specified by A.
- *Include*: An include relationship from use case E to use case F indicates that an instance of the use case E will also contain the behaviour as specified by F.
- *Generalisation*: A generalisation from use case C to use case D indicates that C is a specialisation of D.

The author considers UCDs as especially useful for resilience assessment purposes in order to depict actors and associated actions on technical and organisational level (i.e., modelling socio-technical systems).

4.2 *Semi-quantified resilience assessment by UCD*

Establishing the resilience assessment audits at organisations needs an approach which is resource saving and follows established ways of system representation, e.g., by UML. In a first step, it is suggested to use the interrelationships among system elements by UCD and to assess system resilience by means of the resilience attributes as given in Def. 1. As mentioned above, the UCD differentiates between actors and actions. In engineering terms, actions can be evaluated by assessing their level of compliance with standards, best practices, etc. It is assumed that a high compliance level has a positive effect on the system resilience. Actors are the carriers of system resilience where their impact on recovery abilities is evaluated. For this, the Resilience Priority Value *REPV* of an actor is introduced, which uses the definition of resilience as given in Def. 1:

$$REPV = L \cdot I(d,m,l,a), \tag{1}$$

where

- *REPV*: Resilience Priority Value of an actor
- *L*: compliance fulfilment level of an use case (action)
- *I*: impact of recovery ability of an actor
- *d*, *m*, *l*, *a*: actor's abilities to respond disturbances, to monitor, to learn and to anticipate.

All assessments use ordinal scales of range [1, 2, …, 10], where 1 indicates best and 10 worst cases. The concept follows the familiar idea of estimating risk priority figures, even if resilience is understood as a positive system property.

So far, the assessment of *L* is the result of audits and expert judgement about the proven record of reached compliance levels of actions or associated technology, e.g., the operation of IT security management. In the best case, the rating of *L* bases on already available reports of compliance certifications, e.g., according to ISO/IEC-27002 (2005).

Actors are considered as the intrinsic carriers of resilience. As mentioned above and following Def. 1, the impact of recovery ability *I* depends on four attributes, which are rated by ordinal scales of range [1, 2, …, 10]. *I*(*d*, *m*, *l*, *a*) of an actor is assessed by the mean value of these abilities. The abilities of learning *l* and anticipation *a* are currently covered by humans. However, trends in smart manufacturing and artificial intelligence blur this classification.

The analysis of system resilience needs rules to make use of UCD. For a very first proof of concept, the following procedural steps are defined:

1. An estimated compliance fulfilment level $L_{i,e}$ of $i = 1,2, \quad ,k$ is assigned to each use case U_i.
2. Considering relationships for assessing L_i of U_i
   - Apply the mean value of all *incoming* extend associations
   - Apply the mean value of all values assigned to *outgoing* include associations
   - Compute the mean of both values
3. Rounded off to the next integer
4. Repeat the process until all use cases (actions) are assessed.

In summary, every use case (action) U_c is characterised by a number of extend and include relationships R (i.e., edges): $U_c\left(R_{c;ext};R_{c;inc}\right)$. For further resilience computation, only subsets of relationships are needed. For this, every U_c is assessed by the mean values $\bar{x}$ of compliance levels L of associated incoming extend relationships and outgoing include relationships, i.e. $U_{c;L}\left(\bar{x}_{c;L_{in-ex}};\bar{x}_{c;L_{out-incl}}\right)$. The mean of both values finally gives the looked for compliance level L_{U_c} of an action.

Next, every actor $A_j, j = 1,2, \quad ,k$ is evaluated by the following rules:

1. Assign values of $I_j\left(d_j,m_j,l_j,a_j\right)$
2. Compute the mean of assigned values in I_j which is the looked for impact value of recovery ability of an actor $I_{j,a}$.

Then every actor shows an impact value $I_{j,\,a}$ and is assigned with a use case value L_i (if there are more than two associations use the mean value of L_i's). With that, all values are given to compute $REPV_J$ as defined in Eq. 1. System resilience is estimated by the mean value of all actors' $REPV$ and again rounded of to next integer.

4.3 *Proposed audit process*

The utilisation process of resilience assessment is finalised by auditing a system. The following steps roughly structure such an audit:

- Step 1 – Drafting use cases and actors of sociotechnical system to be audited
- Step 2 – Transfer of use cases and actors into the UCD
- Step 3 – Quantification of UCD
- Step 4 – Evaluation of results and $REPV$.

Steps 1 and 2 follow the basic steps of creating any UCDs. In terms of risk and resilience assessment Step 1 covers the identification process and Step 3 the analysis process. The resulting REPVs might be evaluated by a matrix or threshold approaches as known in risk assessment. However, this step is not elaborated in this paper.

The suggested resilience audit process opens developments towards semi-automated processes to support auditors. The generation of UCDs is a well-known activity in software engineering and there are many tools available to do that (cf. Chapter 5). The computation process of UCDs follows ideas of using complexity metrics as common to characterise computer codes and associated UMLs (cf. (Mock et al. 2015)). Altogether, it is intended to develop the following audit supporting steps: The auditor has to identify actions and actors for UCD generation. Both aspects are plant or system specific. However, there are repetitive elements, e.g., associated with IT security, fire and explosion protection, and occupational safety. These elements are typically standardised and subject of compliance checks. Frequently occurring or, e.g., industry branch specific actions and actors can thus be deposited in a tool library. An auditor then selects the appropriate ones by a drop down menu.

In a next step, the auditor has to identify and create the relationships among actions and actors. This step is tool supported too.

Finally the auditor needs to input the estimated impact values I for every action with only one relationship and to assign $I_j\left(d_j,m_j,l_j,a_j\right)$ for every actor. The remaining computations will be done by the tool.

In the end, the auditor needs more knowledge in system relationships as, e.g., for filling check lists or to perform an FMEA. On the other hand, the usual actions and actors as well as associated $I_{j,\,a}$ and L_i ratings should be known by an experienced auditor as they are close to common checks and results of site-specific compliance checks.

5 CASE STUDY: CAR PARK GUIDANCE

The audited system in this case study is a car park guidance system as implemented in a Swiss city. The system is designed to manage and optimise car traffic flow between a parking lot outside town ("Castle") and a car park building in city centre. ("Town"). All parking spaces are equipped with sensors, networked and controlled by a Supervisory Control and Data Acquisition system (SCADA). Parking space allocation is visible for drivers by displays in "Town".

Step 1 – Drafting actors and use cases

The actors are defined by

- Driver (Family): The family is on a getaway. The Driver (Family) speaks German and strictly follows the parking guiding displays in order to avoid looking for parking space. The Driver (Family) first drives to the display at the car park in the city.

- Driver (Tourist: The foreign Driver (Tourist does not understand German and feels unconfident with display symbols. Hence, this driver ignores the parking guiding displays and makes ad-hoc decisions where to park.
- Car Park Operator (Town): There are no specifications about sensors. Car Park Operator (Town) is assumed to be responsible for car park and system operation. The operator might start parking place managing activities.
- Parking Lots Operator (Castle): There are no specifications. Parking Lots Operator (Castle) is assumed to be responsible for 84 parking lots and system operation. The operator might start parking place managing activities.

Actions (use cases) are defined as

- *Display:* The only car parking display is located at the car park "City" in town and shows the number of free parking spaces at "City" (max. 340) and "Castle" (two parking spaces small and big: 10 + 74 = 84) nearby the Castle. It is assumed that display hardware does not fail at any time within the observation period of 4.5 years of operation. The associated system software is remotely updated and patched via Internet.
- *Gateway*: Kerlink LoRa IoT Station (2 identical stations) "is an industrial solution suitable for people who want to mount the gateway outside and who have sufficient technical skills to connect, mount and maintain the device themselves. … somewhat older software, that is being used, [and] this device will do the job. A trained software engineer will be able to update the device using the [firm] software" (source: thethingsnetwork.org). The Gateways link the 84 *Sensors(Castle)* with the Internet by the Swisscom Mobile network.
- *Sensors (Castle)*: The "Fastpark Flush-Mounted Sensor" (in total 84 sensors) are part of Parking Management System (PMS). "The wireless system uses smart sensors installed in parking spaces and guides drivers to areas with vacancies via electronic panels …" (source: www.worldsensing.com). The *Sensors(Castle)* are linked with associated Gateways and Parking Management System PMS(Castle). Sensors might fail but are not maintained in observation time. The sensors are battery operated and uses the novel Low Power Wide Area (LPWA) technology for gateway communication.
- *PMS Operation*: PMS operation and associated data storage is done by a separated EU computing centre.
- *Sensors (Town):* There are no specifications about sensors of car boxes. It is only assumed that there are sensors which provide display data.
- *PMS (Castle)*: SCADA device in order to process and monitor data from *Sensors(Castle)*. The SCADA serves as Human Machine Interface (HMI). The operator is considered as an integral part of *PMS (Castle)* who then might startparking place managing activities.

Step 2 – Creating UCD

Information on actors and actions is used to build up the UCD of Figure 1. The software tool PlantUML (www.plantuml.com) creates UCDs from textual inputs. It is a plug-in, e.g., of Eclipse. The possibility of integrating PlantUML into various software development frameworks is considered as pre-condition for further resilience software tool development.

Step 3 – Quantification of UCD

Table 2 shows the quantification of UC as given in Figure 1.

Computation in Table 2 is exemplified by considering the Action U_8: The auditor estimates and

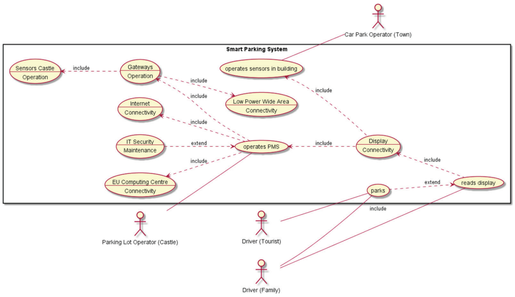

Figure 1. UCD of case study.

Table 2. Estimation of compliance fulfilment level L_i by use case (actions) U_i.

i	Action Ui	Li, e	L_i
1	Sensors Castle	8	$= L_{1,e}$
2	Gateways	–	8
3	Internet	9	$= L_{3,e}$
4	IT Security	8	$= L_{4,e}$
5	EU Comp. Centre	9	$= L_{5,e}$
6	Operates sensors in build.	9	$= L_{6,e}$
7	Low power WA	9	$= L_{7,e}$
8	Operates PMS	–	9
9	Display	–	7
10	reads display	–	9
11	Parks	10	$= L_{10,e}$

$L_{i,e}$: input by auditor; L_i: input by computation

Table 3. Estimation of impact value of recovery ability *Ij* of actors.

j	Actor A_j	d_j	m_j	l_j	a_j	I_j	Mean $\bar{x} = I_j$
1	Car par operator (town)	8	7	6	7	7	7
2	Parking lot operator (castle)	9	10	7	9	8	8
3	Driver (family)	9	7	6	5	6	6
4	Driver (tourist)	7	5	2	1	3	3

Table 4. Resilience priority value REPV of actors.

j	Actor A_j	L_i	I_j	$REPV_j$	Comment
1	Car par operator (town)	9	7	63	
2	Parking lot operator (castle)	9	8	72	
3	Driver (family)	10	6	60	$L_3 = \frac{10+9}{2}$
4	Driver (tourist)	10	3	30	

assigns a compliance fulfilment level of $L_{8,e} = 8$ to the action "operates PMS". This action points to three other actions by include relationships associated with (8+9+9). The mean value including $L_{8,e}$ gives 9. There is an input of an extend relationship $L_{4,e} = 8$ which then gives the final mean value of $L_8 = \frac{9+8}{2} = 9$ (rounded off to the next integer).

Every actor is assigned to an impact value of recovery ability using I_j d_j, mj, l_j, a_j.

Step 4 – Evaluation of results and REPV

As a result from Table 4 the actor Driver(Tourist) shows lowest resilience properties. The overall resilience value of the car park guidance system is the mean of all REPV's, i.e., $REPV_{syst} = 56$ indicating a system with medium resilience.

6 CONCLUSIONS

In view of extended socio-technical system analysis, developing a closed resilience assessment approach is subject of research (cf. (Mock and Zipper 2017). However, this research only makes sense if the understanding of resilience finally results in a different approach as already established by the concepts of, e.g., risk, BCM and availability. From the author's experience, discussion about resiliency often follows synonymous paths as already given by these established concepts (cf. (Leksin et al. 2018)).).

On the other hand, resilience assessment methodology is in its beginnings and still beyond entrepreneurial interests and has not fixed as state of technology yet. Thus, the paper is understood as a step toward utilisation of resilience assessments of complex systems. For this, a simple REPV is defined and the assessment process uses standardised system representation by UCD, which properly differentiates between actions and actors. This property covers well the inclusion of socio-technical aspects, where actors are carriers of major properties of resilience (e.g., learning). They are integral parts of the audited system, which is then becomes describable as a socio-technical system. By defining rules to quantify UCDs, the proposed resilience assessment approach opens paths for software tool development in order to support resilience assessment audits of, e.g., infrastructural systems. The case study serves as a proof of concept.

Discussions at ESREL conference in 2017 have given rise to fears that the inclusion and detailed understanding of the technical functioning of (infrastructural) systems could be neglected in resilience assessments. The use of UCD provide a practical way out of this situation, since UCDs are based on comprehensive descriptions of actions, actors and their relationships supporting a systemic analysis approach.

The proposed concept of system assessment supports auditors to check to what extend infrastructural systems are resilient. However, the approach still needs verification of quantification rules, which are presumably too simplistic. The approach also needs an extended review based on a broader application example. Further developments consider the inclusion of complexity measures in order to increase the meaningfulness of UCD quantification.

REFERENCES

BABS (2013, Apr. 29). Risikoausbildung BABS: Glossar der Risikobegriffe., Bundesamt für Bevölkerungsschutz. Bergström, J., R. van Winsen, & E. Henriqson (2015). On the rationale of resilience in the domain of safety: A literature review. *141*, 131–141.

DIN-EN61703 (2002). Mathematische Ausdrücke für Begriffe der Funktionsfähigkeit, Verfügbarkeit, Instand-haltbarkeit und Instandhaltungsbereitschaft. DIN EN 61703:2002–09, DIN Deutsches Institut für Normung.

Hollnagel, E., C.K. Tveiten, & E. Albrechtsen (2010, August). Resilience engineering and integrated operations in the petroleum industry. Technical Report SINTEF A16331.

Hosseini, S., K. Barker, & J. Ramirez-Marquez (2016). A review of definitions and measures of system resilience. In *Reliability Engineering & System Safety*, Volume 145, pp. 47–61.

ISO-19501 (2005). Unified modeling language specification (version 1.4.2). ISO/IEC 19501:2005(E), ISO.

ISO-31000 (2009). Risk management – principles and guidelines. ISO 31000:2009, ISO.

ISO-31010 (2009). Risk management – risk assessment techniques. ISO/IEC 31010:2009, ISO.

ISO/IEC-27002 (2005). Information technology code of practice for information security management. ISO/IEC 27002:2005(E), ISO/IEO.

Lay, E., M. Branlat, & Z. Woods (2015). A practitioner's experiences operationalizing resilience engineering. In *Reliability Engineering & System Safety*, pp. 63–73.

Leksin, A., U. Barth, & R. Mock (2018). The Kursk submarine disaster in view of resilience assessment (in print). In *Proc. of European Safety and Reliability Conference (ESREL 2018*), London. Taylor & Francis Group.

Lundberg, J. & B. J. Johansson (2015). Systemic resilience model. Volume 141, pp. 22–32.

Mock, R., B. Truninger, P. Brunner, G. Pociupa, & T. Hruz (2015). It risk audit tool to enhance IT risk assessments. In *Proc. of European Safety and Reliability Conference (ESREL 2015)*, pp. 4029–4036.

Mock, R. & C. Zipper (2017). Embedding resilience assessment into risk management. In *Proc. of European Safety and Reliability Conference (ESREL 2017)*, pp. 1009–1014.

NIAC (2009, Sept. 8). Critical infrastructure resilience: Final report and recommendations. Technical report, National Infrastructure Advisory Council (NIAC).

Scholz, R.W., Y.B. Blumer, & F.S. Brand (2012). Risk, vulnerability, robustness, and resilience from a decisiontheoretic perspective. In *J. of Risk Research*, Volume 15, pp. 313–330.