Environment Systems and Decisions (2021) 41:286–329
https://doi.org/10.1007/s10669-021-09811-5

A performance-based tabular approach for joint systematic improvement of risk control and resilience applied to telecommunication grid, gas network, and ultrasound localization system

Ivo Häring[1] · Mirjam Fehling-Kaschek[1] · Natalie Miller[1] · Katja Faist[1] · Sebastian Ganter[1] · Kushal Srivastava[1] · Aishvarya Kumar Jain[1] · Georg Fischer[1] · Kai Fischer[1] · Jörg Finger[1] · Alexander Stolz[1] · Tobias Leismann[1] · Stefan Hiermaier[1] · Marco Carli[2] · Federica Battisti[2] · Rodoula Makri[3] · Giuseppe Celozzi[4] · Maria Belesioti[5] · Evangelos Sfakianakis[5] · Evita Agrafioti[6] · Anastasia Chalkidou[6] · George Papadakis[6] · Clemente Fuggini[7] · Fabio Bolletta[7] · Alberto Neri[8] · Guiseppe Giunta[9] · Hermann Scheithauer[10] · Fabian Höflinger[11] · Dominik J. Schott[11] · Christian Schindelhauer[12] · Sven Köhler[12] · Igor Linkov[13]

Accepted: 11 March 2021 / Published online: 10 April 2021

Abstract

Organizational and technical approaches have proven successful in increasing the performance and preventing risks at socio-technical systems at all scales. Nevertheless, damaging events are often unavoidable due to a wide and dynamic threat landscape and enabled by the increasing complexity of modern systems. For overall performance and risk control at the system level, resilience can be a versatile option, in particular for reducing resources needed for system development, maintenance, reuse, or disposal. This paper presents a framework for a resilience assessment and management process that builds on existing risk management practice before, during, and after potential and real events. It leverages tabular and matrix correlation methods similar as standardized in the field of risk analysis to fulfill the step-wise resilience assessment and management for critical functions of complex systems. We present data needs for the method implementation and output generation, in particular regarding the assessment of threats and the effects of counter measures. Also included is a discussion of how the results contribute to the advancement of functional risk control and resilience enhancement at system level as well as related practical implications for its efficient implementation. The approach is applied in the domains telecommunication, gas networks, and indoor localization systems. Results and implications are further discussed.

Keywords Joint risk and resilience analysis and management process · ISO 31000 · System performance function · Tabular and matrix approach · Socio-technical system · Resilience dimensions · Engineering of resilience

1 Introduction

In the past decades, the major progress in the control of risks of socio-technical and technical systems can be attributed to systematic analysis processes and principles (see, e.g., Olechowski et al. 2016), in particular the risk management process of ISO 31000 (see, e.g., Purdy 2010) and related methods collections in ISO 31010. These processes and principles comprise framings, process requirements, and methods that are recommended to fulfill the overall requirements, and process-specific requirements (see also Fig. 1 for a similar structure). As the result of years of application and domain-specific standards and application recommendations, such as for critical infrastructure (Giannopoulos et al. 2012; Giannopoulos and Theocharidou 2015), by now auditable and insurable risk assessment approaches have been generated. For risk assessment even domain-specific standards have been provided such as for compliance management (ISO 19600; ISO 14001), business continuity (ISO 22301), application

Extended author information available on the last page of the article

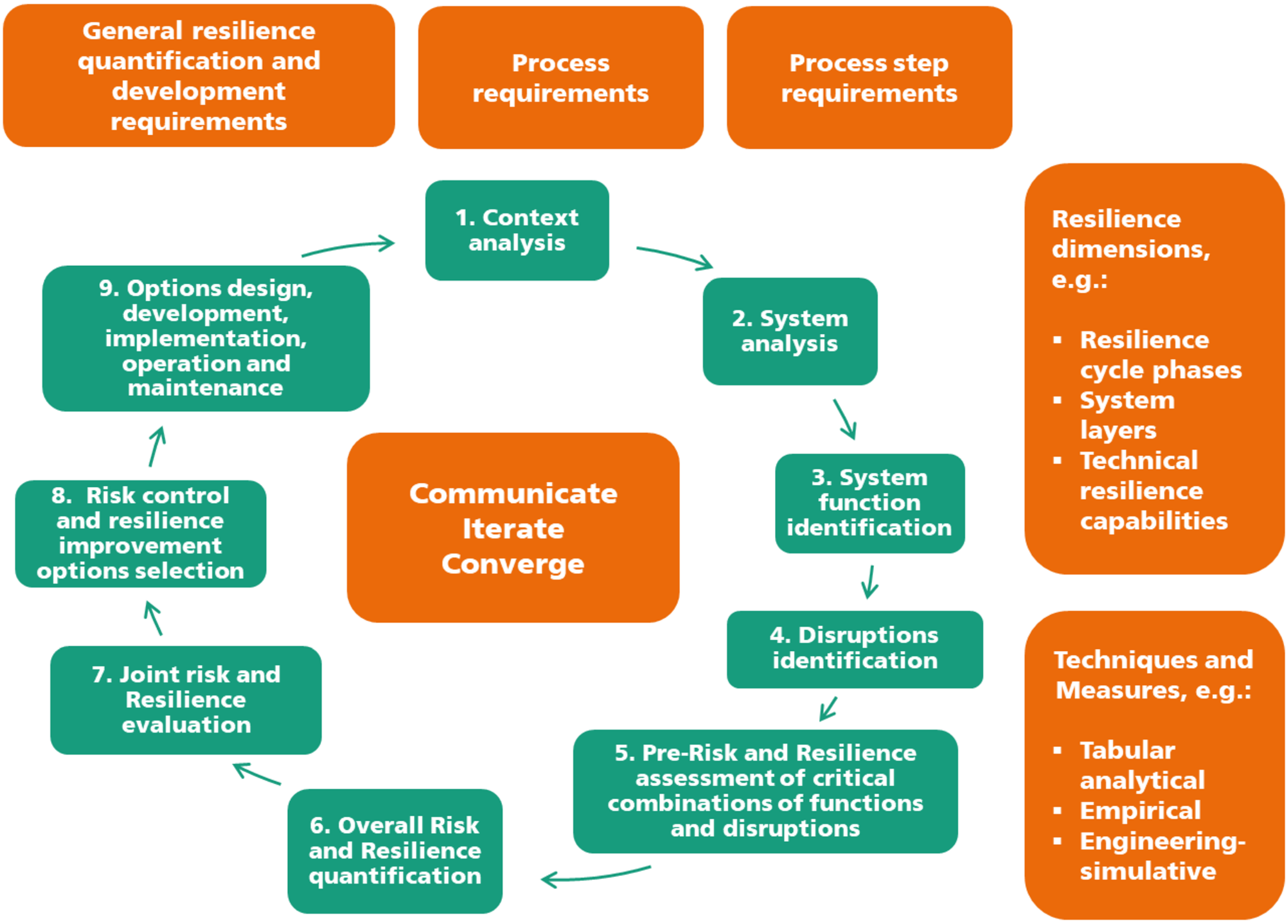

General resilience quantification and development requirements
Process requirements
Process step requirements
1. Context analysis
2. System analysis
3. System function identification
4. Disruptions identification
5. Pre-Risk and Resilience assessment of critical combinations of functions and disruptions
6. Overall Risk and Resilience quantification
7. Joint risk and Resilience evaluation
8. Risk control and resilience improvement options selection
9. Options design, development, implementation, operation and maintenance
Communicate Iterate Converge
Resilience dimensions, e.g.:
▪ Resilience cycle phases
▪ System layers
▪ Technical resilience capabilities
Techniques and Measures, e.g.:
▪ Tabular analytical
▪ Empirical
▪ Engineering-simulative

Fig. 1 Joint resilience and risk analysis and management process

to the environmental domain (ISO 14001), security management, in particular of supply chains (ISO 28000), and emergency and incident management (ISO 22320) and urban resilience (ISO/AWI 22371).

An important observation is that for practical implementation of such classical risk control approaches, tabular or matrix-like methods play a major role. Reasons for the wide-spread use of such methods include their applicability in early assessment stages, the systematic presentation options, the option of informed reuse, and often the possibility of inductive bookkeeper-like conduction. The main reasons for practical success of tabular approaches can be seen in their low (actually employed) implementation costs, their application potential in all phases of product development and deployment (idea, design phase, production and operation), the option to use tiered and nested approaches risk assessments (from qualitative to quantitative), and their high level of acceptance in practice. For example, the combination of the abstract five-step risk management process (context analysis, risk identification, risk computation, risk acceptance evaluation, countermeasure selection) along with appropriate mainly tabular (even look-up table like) and inductive approaches proved to be a successful model of classical risk assessment and control.

The field of resilience assessment and management and its connection with risk assessment and management is less developed and is still a subject of controversy. Many methods, tools, and alternative conceptualizations are proposed (see, e.g., Linkov and Trump 2019 for a recent review). For example, the US National Academy of Sciences considers risk as part of the resilience cycle (namely the response/absorb phase, see NAS 2012, Linkov et al. 2014). In contrast, guidance for resilience assessment for Power Industry places resilience under reliability, which is managed through risk assessment tools (CIGRE C4.47 2019). One of the approaches to connect risk and resilience assessments under a tiered framework that is in place for risk assessment is attempted in Linkov et al. (2018), but it was done in general terms and the application of tabular approaches to resilience management in a more systematic way was not discussed there.

The first attempt to suggest mainly classical tabular system analysis methods for supporting resilience assessment was done by Häring and Gelhausen (2018). Examples of such methods include modified and extended hazard list (HL), preliminary hazard analysis (PHA), hazard analysis (HA) on system level including maintenance and operation and support (O&SHA), variants of failure mode and effects analyses (FMEA), and—in particular at the system function level and subsystem level and for risk evaluation—the risk matrix.

The risk assessment process asks at the very beginning decision makers to formulate of objectives, for evaluation criteria for reaching objectives, and for a broad stakeholder engagement in different stages of the process. The risk management process is focused on controlling risks to objectives identified in the risk assessment step. However, this very subjective identification of objectives and of the risks of not reaching those objectives challenges the traditional application of risk management, in particular when applied to determine resilience. It can therefore be expected that asking for a more explicit deductive process would be helpful that already considers resilience concepts, in particular when combined with tabular methods, and that it would also be efficient for resilience management. Thus, the question arises of whether a system performance (service) function-based process can be defined that supports both more efficient risk assessment and control as well as resilience assessment and management for efficient overall control of risks.

The text is structured as follows: Building on the constructive observations of the introduction, Sect. 2 presents motivations for use of ISO 31000 as foundation for a joint risk and resilience management process along with tabular methods for its implementation. It also shows that the process takes up requirements of known resilience definitions, assessment and management frameworks. In particular that the process asks for and can incorporate quantitative resilience assessments beyond the tabular implementations which are in the focus of the paper. Section 3 motivates the input data selection for the tabular approaches within the defined resilience assessment and improvement process. Section 4 presents the data input for the sample cases telecommunication, gas networks, and indoor localization and provides a tabular overview of analysis options for each process step. Section 5 shows in detail which risk and resilience assessments are feasible for the sample cases in which the process was applied. Section 6 reflects on how to successfully implement such a tabular risk and resilience assessment and improvement process and how to further support it with other methods, in particular for implementing countermeasures that are applicable in case of events. Section 7 provides an overall summary of the joint risk and resilience management process on an abstract level implemented with tabular methods, and provides standardization options.

2 Rationale of overall approach and comparison to existing approaches

Summarizing, and taking up the constructive line of argumentation of the introduction, the following drawbacks of classical risk management, analysis, and control need to be considered (see also more recent and rather fundamental critical reviews of classical risk management as summarized in Leitch (2010), Lalonde and Boiral (2012), (Hollnagel 2017), Selvaseelan (2018), Aven (2019), and Häring et al. (2020):

- Damage events with major effects are often unavoidable due to a wide and dynamic threat landscape and enabled by the increasing complexity of modern systems;
- Focus of classical risk analysis and management on prevention (reduction of frequency of events) as well as protection and robustness (low damage effects in case of events) (see, e.g., Häring 2015) as opposed to considering all resilience dimensions;
- In governance, risk focuses on management, forecast, and reduction of known threats, and does not have a temporal aspect (Larkin et al. 2015);
- There is no systematic and explicit leverage of improved absorption, response and recovery, learning and adoption options during and post events, i.e., not all resilience cycle phases (preparation, prevention, protection, response, recovery) are considered (Thoma et al. 2016);
- The deductive potential based on system performance expectations should be employed by modern approaches versus the rather vague risk on objective approach of classical risk management;
- No simple extension options regarding resilience management and generation of classical risk management process (formally) conformal to and extending ISO 31000 are available;
- Classical risk analysis and management does not make explicit cost-versus-efficiency considerations regarding all risk event control and resilience generation options for achieving efficiently overall system performance objectives;
- Classical risk analysis and management makes no explicit attempt to cover unknown or even unknown events, e.g., in terms of potential effects;
- Socio-technical resilience capabilities and abilities are challenging to grasp in (technically driven) assessment frameworks, see, e.g., contributions in Nemeth and Hollnagel (2014), even when formulated as technical resilience capabilities (Häring et al. 2016b).
- Classical risk analysis and management focuses on probabilities and loss reduction and not on improving

the system's ability to absorb, adjust, or recuperate from an event (Baum 2015);

- In the context of behavior of complex systems affected by threats (Galaitsi et al. 2020), resilience and risk are the subject of active discussions (Linkov and Trump 2019). In particular, resilience and risk are discussed as complimentary concepts that can be connected through a tiered evaluation process (Linkov et al. 2018).
- There is a lack of (deep) uncertainty coverage and appropriate handling in classical risk management.

Baum (2015) carried out further comparison of risk and resilience, finding that risk analysis is not as good as resilience when it comes to four different conditions. The first condition is if (1) the scenario being investigated includes unknown threats. Risk analyses also have poor performance when (2) the probabilities are not available or measurable, (3) when threats can have cascading effects to entire systems, or (4) interconnected networks, or (5) when the threats are on a large scale and cataclysmic (Baum 2015).

In this context, and taking up major challenges and gaps just listed above, Fig. 1 shows the step-wise performance-based joint resilience and risk management process first proposed and exampled in Häring et al. (2017a) for the electrical energy transmission domain, the urban transport domain, and for coupled infrastructures of a regional area in Canada. The approach has also been motivated in Häring et al. (2016c) and was applied to local electrical distribution grids in Tomforde et al. (2019) (OCTIKT 2018–2021) at concept level. In the present paper, applications are discussed in more detail for telecommunication grids, gas transmission systems, and indoor ultrasonic localization systems.

The resilience dimensions used are defined and referenced in Häring et al. (2016a), see also Table 1 for an overview. Resilience dimensions to be considered include resilience cycle phases, e.g., preparation, physical protection, detection, prevention, absorption, response (stabilization), recovery, adaption and learning (introduced and discussed in NAS 2012). Examples of resilience capabilities implemented at system level include sensing (e.g., detection), data analysis (e.g., data fusion), situation representation (e.g., spatial and dynamic situation representation), decision making (e.g., rule based), and action (e.g., activation of protection mechanism). Examples of system layers are physical, engineering (technical), cyber, operational, organizational (decision making), and policy layer (modified after Linkov et al. 2013).

In the following, the present approach is further related to existing definitions, analyses, and improvement management processes for socio-technical system resilience. Regarding the definition of system resilience and resilience aims, it aligns well with ongoing conceptual discussions as, e.g., based on Haimes (2009), Linkov et al. (2014), Zio (2016), Kröger (2019), and Cottam et al. (2019).

Within a general framework of five steps (threat analysis, resilience capability design, resilience cost evaluation, resilience quantification, resilience improvement) and in the context of supply chain resilience, in Hosseini et al. (2016) a Bayesian network approach is applied to quantify resilience using different types of qualitative (discrete) up to quantitative inputs under uncertainty. It is shown that the approach covers the scope of the framework. A similar quantification approach is also applied to the resilience assessment of waterways (Hosseini and Barker 2016) showing that absorptive, adaptive, and restorative capacities can be modeled using the Bayesian network approach. The Bayesian network-based quantification has also been applied to an interdependent electrical infrastructure system (Hossain et al. 2019). In comparison with the present joint resilience and risk management process, the discussed framework is more focusing on a single well-suited resilience quantification approach.

Henry and Ramirez-Marquez (2012) show how to use system performance functions or system figures of merit (FOMs) to generate dimensionless time-dependent resilience functions that show the increase of system performance post disruptions (recovery over initial loss). The present approach also uses system performance functions, in addition also non-performance functions. However, for reasons of end user acceptance and to avoid too high values, the latter are not transformed into performance functions by using one over figure of merit expressions as proposed for consideration in Henry and Ramirez-Marquez (2012).

Measures of criticality of single components of critical infrastructure networks based on vulnerability and recovery behavior of overall networks are proposed and computed in Barker et al. (2013). With similar approaches also, repair prioritization and effects of repair delay on system resilience can be assessed (Fang et al. 2016). Within the present joint risk control and resilience analysis approach, such component importance measures for system resilience could be used within Step 6 using stets of system performance functions and disruption types that cannot be excluded by using only tabular and matrix approaches.

Also simulative assessment results of multilayer analyses of single infrastructures, see, e.g., Nan and Sansavini (2017) for electrical grids, resilience simulations of interlinked infrastructures using functional dependency modeling, see, e.g., Petrenj and Trucco (2014), or generic graph-based approaches, see, e.g., Kong and Simonovic (2018), can be used within the current process framework along with the tabular approaches. In particular, the tables can be

Table 1 Overview of tabular methods for the joint resilience and risk management process

Resilience and risk management step	Sample (Look-up) list and matrix	Preliminary list	Dependency (correlation) matrix	Assessment table or matrix
1 Context analysis	Potential stakeholder list; Potential overall objectives list;	**System-specific stakeholder list; Overall system objectives list**	Correlation (main relevancies) of stakeholders vs. objectives	Prioritized stakeholder list; prioritized objectives list
2 System analysis	Potential system elements list; Potential system functions list	**System elements list** (e.g., subsystems, components); System functions list		Prioritized system elements list
3 System performance function identification	Performance functions list	**System function list and system non-function list**	**Correlation of objectives vs. System (non) performance function; Relation of system (non) performance functions vs. system elements**	Prioritized system (non) performance functions list
4 Threat and disruptions identification	Threat example list per resilience cycle phase; per resilience (technical) capability and resilience ability; and further resilience dimensions	**System threat lists, specified per resilience dimension**	Correlation of threats vs. threats; Correlation matrix of threats vs. system elements; Correlation of threats vs. system functions	Prioritized threat list covering system-relevant resilience dimensions
5 Pre-assessment of critical combinations of threats and functions	Sample single performance function vs. performance function assessment matrix		**Assessment matrix of system (non) performance functions vs. threats considering resilience dimensions;**	
6 Overall risk and resilience assessment: qualitative, quantitative	Sample overall threat vs. performance function assessment matrix		**Tabular overall/collective assessments per threat type; per resilience phase (e.g., overall frequency, absorption, response, recovery)**	
7 Joint risk and resilience acceptance evaluation	Sample risk and resilience evaluation matrix			**System risk and resilience evaluation matrix for single/overall combinations of threats vs. system (non) performance functions resolve per resilience dimension**
8 Risk control and resilience improvement options selection	Improvement measures per resilience cycle phase; per resilience capabilities or abilities	**System-specific improvement measure list**	**Assessment matrix of risk control and resilience issues (critical combinations of system performance functions and threats) vs. improvement measures**	Evaluation matrix of risk control and resilience improvement measures
9 Improvement options design, development implementation operation and maintenance	List of domain-specific system development, implementation, maintenance, and control standards; List of ad hoc assessment options before implementation (e.g., resources and time needed, acceptance, acceptability)	System-specific list of approaches	Assessment matrix of improvement measures and procedures vs. pre-implementation assessment criteria; as well as vs. results of second and third iterations of overall process	**Pre-evaluation table of improvement options; Iteration of overall process to assess secondary and higher order effects**

A minimum and sufficient set of tables and matrices sufficient to implement the joint resilience and risk analysis and management process is given in bold used to collect input for quantitative and simulative assessments.

The present approach takes account of the identified absorptive, restorative, and adaptive resilience capacities metric as identified within a framework for resilience analysis of engineered and infrastructures systems (Francis and Bekera 2014) in terms of requiring to consider the resilience dimensions resilience cycle phases and technical resilience capabilities in particular in Steps 3 to 7 within the system performance function-based process of Fig. 1. Also the framework elements (system identification, resilience objective setting, vulnerability analysis, and stakeholder engagement) proposed by Francis and Bekera (2014) are well covered while being compliant to the classical overall 5-step risk management process of ISO 31000. The present approach also aligns with cornerstone of the framework proposed in Vugrin et al. (2010): the need for context- and system-specific definitions of system performance functions and resilience quantification approaches, a qualitative and quantitative approach to system resilience assessment and improvement.

For representative tabular sample methods, Table 1 presents the tabular structure and table or matrix headlines as well as the relation of tabular methods that support the joint risk control and resilience improvement and assessment process. Multiple sample method classes and methods beyond tabular approaches are listed in Häring et al. (2017a), including the expected suitability of these methods for the nine resilience analysis and management steps.

Table 1 at first proposes to generate lists of information items, for instance, system elements; potential system performance functions in terms of service functions, safety and security functions; potential threat events; or potential (overall) risk control and resilience, simulation and improvement measures. In the following, combinations of these items are considered in matrix-like assessments or correlation assessments, leading to final evaluations. The tabular approaches can be combined and should be filled out iteratively and mutually informed as indicated in the overview scheme of Fig. 1.

As shown in Table 1, combinations of item aspects can be used to improve system understanding. Examples include the allocation of users or stakeholders to resilience objectives and system functions, of system elements to system performance functions, the correlation between threats, the correlation between system elements, and the correlation between system functions. The last two examples allow for the assessment of interdependencies and interfaces between system functions and system elements.

The main use of combinations of items, termed a dependency or correlation matrix, is for analyses. This can include the determination of critical system performance functions by relating main system objectives with system functions, the determination of relevant system elements by relating system performance functions to system elements, the determination and evaluation of critical threats for critical system performance functions by assessing the expected effect of threats on system performance functions using all relevant resilience dimensions, the determination of overall risk control and resilience measures by considering the expected relevancy of improvement measures for identified critical combinations of system performance functions and threats, and the consideration of the effects of improvement measures by reiteration of the process until convergence and for regular monitoring purposes.

Within the present process design of Fig. 1 and Table 1, existing human, organizational, and technical resources, redundancies, and response options are considered within Steps 1 to 3. Hence, they are considered within the risk control and resilience assessment Steps 4 to 6, in particular with respect to their efficiency, as well as within the overall risk evaluation Step 7, which needs to take account of risk control and resilience for each potential event and overall. Only if this as-is risk control and resilience is not acceptable do further human and technical intervention options need to be added, as well as possibly system advancements in terms of, for example, less exposure, more robustness, fail operational designs, redundancies, rapidity, more resources for recovery actions, etc. This highlights that, e.g., robustness and redundancy per se are not assets, but of course they are nevertheless in many contexts, see, e.g., Cimellaro et al. (2010).

When inspecting the master Table 1 of tables and matrices proposed to fulfill the joint performance-based risk control and resilience analysis process of Fig. 1, it is emphasized that it assumes an iterative generation and improvement, i.e., going back to the second line if the last line has been reached to assess secondary and higher order effects.

3 Data sources and selection criteria for application cases

The approach is applied to civil infrastructure systems (see, e.g., Gay and Sinha 2013 for further sample systems) and a localization system. Due to its generic nature, it is expected that it could also be applied to community resilience (see, e.g., Berkes and Ross 2013) or even ecological or societal resilience challenges.

For the first sample case, the data sources are expert inputs collected from single persons and small informal expert rounds of persons involved in the EU project RESISTO (2018–2021) on cyber-physical risk control and resilience enhancement of telecommunication infrastructure. More advanced expert opinion gathering could, for example, use Bayesian updating to determine more reliable estimates of system parameters (see, e.g., the overview in Mosleh 2018).

In general, the standard input gathering is the coordinated collection of information on and opinions from single experts in a single tabular document (spreadsheet) and its iterative approval in joint expert sessions documented by joint signature processes. Expert sessions can be in-person or virtual. The rationale of using expert data is to avoid resource-intensive field data gathering while being able to start risk and resilience assessment and improvement in the early phases of project developments.

The input includes the telecommunication infrastructure, performance functions, threats, and improvement measures in both the general sense and specifically for the different use cases tested in the EU project "Resilience enhancement and risk control platform for communication infrastructure operators" (RESISTO 2018–2021) (RESISTO D3.9 2020). This use case allows for a more detailed and specific analysis to be completed.

In the example case of the gas grid based on the EU project SecureGas on "Securing the European Gas network" (SecureGas 2019–2021), data are gathered from project phases focusing on the determination of main end user needs to control risks and enhance resilience, in particular to counter critical threats of the main gas grid functions within the given operational and legal requirements. A further focus is the tabular formulation of the functional and technical requirements definition for improved functions of security and safety systems of gas grid systems which resorts to the resilience concepts introduced within the joint risk control and resilience enhancement process. When compared to Vugrin et al. (2011), the sample case does not focus on a specific threat type and selected spatial areas.

For the example case gas grid, in addition to expert input collection using bilateral, round table and questionnaire-based data collection, the story board methodology is used to link the system non-performance and performance functions to potential threats as well as to improvement measures in terms of technical and functional requirements of extended capabilities of the safety system, even as preparation of concepts of operation (CONOPS) of these functionalities. The storyboard methodology has been formulated in various flavors and is by now supported by tools (Mohd Yusoff and Salim 2014). In particular, (electronic) templates for its implementation have been proposed for a more seamless communication, see, e.g., Roytek (2010). The storyboard methodology can also be put in a broader context regarding human-centered technology design (Harte et al. 2017) and served to generate input for of functional-operational requirements generation and short CONOPS descriptions (Thronesbery et al. 2007).

The sample case gas grid used representative historic cyber events, threats, and attacks, e.g., the database of the European Gas Pipeline Incident Data Group (EGIG 2020), the United Kingdom Onshore Pipeline Operators Association (UKOPA 2020), the European Joint Research Center (JRC) natural hazard list (Poljanšek et al. 2019) tailored to the gas grid domain, the International Disaster Database (EM-DAT 2021), the US Pipeline and Hazardous Materials Safety Administration (PHMSA 2021), as well as the hazard list developed within a Greek project on targeted actions for enhancing the protection of national characterized European critical infrastructure (NCECI 2017–2020).

Regarding the methodology of identification and assessing of potential risk, the present approach takes up approaches by the JRC methodology of relevancy and impact screening of natural hazards (Poljanšek et al. 2019) and the security risk assessment methodology recommended by Gas Infrastructure Europe (GIE) (KPMG 2021). Furthermore guidance provided by the hazard identification (HAZID) (CCPS 2010), the preliminary hazard analysis (PHA) (Ericson 2016), and the Hazard and Operability Study (HAZOP) approach according to (IEC 61882) applied for petro-chemical facilities (Crawley and Tyler 2015), whereby the implementation was supported by the ALOHA (areal locations of hazardous atmospheres) software package covering toxic dispersion, fire and explosive scenarios (ALOHA 2021), and the use of generic events trees as proposed in Vílchez et al. (2011). Main additional points included to consider also risks post event occurrence.

The search for potential threats and their assessment was further supported by focused publications regarding potential threats and disruptions, including statistical analysis of events for long-distance pipelines (Dai et al. 2017), effects of large scale disasters, effects of single and compound hazards on gas infrastructure due to extreme weather (Moftakhari and AghaKouchak 2019), and effects of major disasters (ICF 2019), seismic effects (Urlainis et al. 2015), disruptions caused by conflicts, crises and disruptions and civil unrest (Carvalho et al. 2014) (Lochner and Dieckhöner 2012), threats to the energy infrastructure by cyber-attacks, conventional warfare, unconventional warfare, and criminal activity (Staff 2014), and terroristic cyber and physical attacks (Dancy and Dancy 2017) (Pirani et al. 2009), as well as different types of cyber-attacks (ENISA 2020).

The third example case is an indoor ultrasound localization system (Bordoy et al. 2020) (Ens et al. 2015) (Hoeflinger et al. 2015), which offers high localization accuracy when compared to alternative technologies, e.g., Wi-Fi-based fingerprinting approaches (Tiku et al. 2020), Bluetooth, ZigBee, Ultra Wide Band (UWB), vision and acoustic-based (Zafari et al. 2019). It localizes ultrasound transmitters on objects (e.g., goods, transport systems, robots) using receivers on the ceiling by application of time difference of arrival algorithms (TDOA) for the case of known receiver positions. The time differences of ultrasound signals are determined using autocorrelation analysis for chirp signals. Data are exchanged between the receivers, senders, and a gateway using the ISM (industry, science, and medicine) radio 6.78 MHz band. After cloud-based transmission, the data are analyzed and visualized, e.g., with a standard PC. Input data collection was conducted within a project on quantitative resilience indicators for technical systems (Resilience Measures 2016–2018) and on multimodal resilient indoor localization systems as relevant for industry applications (MERLIN 2019–2021).

Main data used are the determination of system service and technical functions of the localization system when used in industrial (e.g., logistics, production) and consumer applications (e.g., restaurants), potential threats and disruptions, recommended measurements, as well as measurement results regarding the resilience behavior in critical scenarios. System knowledge to determine main system performance functions and potential threats was collected in expert rounds as input for the estimation of the criticality of combinations of system functions and threats. Some of the threats have also been investigated using a simulative approach (Jain 2018), e.g., noise and barriers. Experimental results of the assessment of critical combinations along with a dimensionless resilience measure are documented in Scheithauer (2018).

The danger of not contextualizing the inputs of experts sufficiently, e.g., different assessments of seemingly similar scenarios, is avoided in the proposed approach by asking experts to refer explicitly to the background information of already existing tables, see, e.g., Table 2 columns two and three.

4 Sample data sources used

4.1 Telecommunication grid

In the example case of a telecommunication critical infrastructure, Table 2 lists the type of data collected for the proposed minimal set of tables and matrices as printed in Table 1 in bold fonts. For each entry type examples are given. Even within this slim approach, it is evident that many tables and matrices can be understood as extensions of simpler versions that have been generated in earlier assessment phases, where less information is available. Similar observations can be made when applying tabular approaches to achieve functional system safety in the context of IEC 61508. Also, in the domain of IT security, for example when using the system performance function and risk-based cyber security HEAVENS approach as developed for the automotive domain within a Swedish research project on healing vulnerabilities to enhance software security and safety within the automotive embedded systems domain (Lautenbach and Islam 2016).

Table 2 can be grouped by tables that collect socio-technical system information (columns 1 to 3), tables that collect information on potential failures, threats, and disruptions considering all resilience dimensions (columns 4 and 5), the system-specific assessment of the threats (columns 6 and 7) in terms of effects on system performance functions, and the selection and pre-assessment of improvement measures. The tables can also be grouped into information that is available in rather early steps of the analysis (columns 1, 3, 4, and 8) and tables that need detailed system knowledge (columns 2, 5, 6, 7, 9).

All tables are related to each other. Most tables additionally contain dependencies within themselves. These dependencies describe the relation of system, subsystems and components in the component and system table (-column 2), the relation of system functions, subsystems and components (column 3), and the relation of threats to components, subsystems, and other threats (column 5). Most prominent are the assessment of the combinations of system performance functions with threats (column 6) and the consideration of several such combinations (column 7), as well as the selection and assessment of resilience improvement measures (column 9).

Because the nine tables or matrices (column labeled with 1 to 9 in Table 2) summarize tables and matrices as proposed in Table 1, they can clearly be shown as covering the 9 resilience assessment and management steps as presented in Fig. 1:

Step 1 on context analysis is supported by the stakeholder and objectives table (column 1 of Table 2 entitled 1. Stakeholder and Objectives), which also determines criteria for the degree of the fulfillment of objectives and assessment criteria throughout the process.

Step 2 on system analysis is supported by the tables on subsystems and components (column 2) and the table on system (non) performance functions (column 3), which determines the system boundaries, its interface, and system functions.

Step 3 on system performance function identification determines the most important system performance functions as well as expectations regarding their performance using, respectively, relevant resilience dimensions (column 3 and column 4).

Step 4 on disruptions identification aims at collecting known potential threats, empirically observed threats in other contexts (exampled events), as well as at least potential effects of unknown threats (e.g., recovery

Table 2 Telecommunication grid sample data entries and tabular and matrix assessment examples

Data entry Description	Examples	1. Stakeholder and objectives	2. Components and subsystems	3. System (non) performance functions	4. Resilience Dimensions and Attributes	5. Threats, disruptions	6. System (non) performance functions vs. Threats	7. Overall risk and resilience evaluation matrix	8. Improvement measures selection	9. Improvement measures for critical combinations
1. Stakeholder ID	S1, S2, etc.	X		X	X				X	X
2. Stakeholder description	Operator, technician, prosumer	X								
3. Objective ID	O1, O2, etc.	X		X	X				X	X
4. Objective description	E.g., Low risk; high availability and resilience; low CO_2 footprint; low time and financial resources; high acceptance and acceptability;	X								
5. Objectives fulfillment criteria	E.g., ALARP rationale; (local and non-local) individual and collective risk criteria; short mean down times and recovery times; low medians and percentiles of unmet supply contract requirements; semi-quantitative scales;	X								
6. Level of fulfillment	Qualitative, semi-quantitative (e.g., low, high), quantitative						X	X	X	X
7. Component ID	C1, C2, etc.		X	X					X	X
8. Component description	Fiber optics cables; servers; (embedded) software for operation; firewalls, radio infrastructure; servers		X							
9. Subsystem ID	SS1, SS2, etc.		X	X				X	X	X
10. Subsystem description	core network; internal network; optical network; data center; radio network;		X							
11. Type	Hardware, software, interconnection		X							
12. Quantities	Number of realizations within network		X							
13. Interconnections	Physical/Cyber interconnections		X							
14. System Function ID	SF1, SF2, etc.			X			X	X	X	X
15. SF description	E.g., voice communication			X						
16. Performance quantities	E.g., real time capability			X						

Table 2 (continued)

Data entry Description	Examples	1. Stakeholder and objectives	2. Components and subsystems	3. System (non) performance functions	4. Resilience Dimensions and Attributes	5. Threats, disruptions	6. System (non) performance functions vs. Threats	7. Overall risk and resilience evaluation matrix	8. Improvement measures selection	9. Improvement measures for critical combinations
17. Dependence on other SF	IDs of System functions			X						
18. Resilience Dimension ID	RD1, RD2, etc.			X	X	X	X		X	X
19. RD description	E.g., Resilience cycle phases; (technical) resilience capabilities; system layers; threat is expected to be relevant for (selected) resilience cycle phases, etc.				X					
20. Resilience Attribute ID	RA1, RA2, etc.			X	X	X	X		X	X
21. RA description	E.g., detection and prevention as resilience cycle phases; sensing, modeling, and decision making as technical resilience capabilities; threat is, e.g., expected to reduce physical and cyber sensing and prevention capabilities, etc.				X					
22. Threat ID	T1, T2, etc.					X	X	X	X	X
23. Threat name	E.g., Extreme weather, data extraction, unauthorized access					X				
24. Threat description	E.g., Physical damage by storms; hackers capture data					X				
25. Relation to other threats	Listing of other threat IDs					X				
26. Improvement Measure ID	IM1, IM2, etc.								X	X
27. Name	E.g., generators, physical barriers, training, security review, alerting, redundancy								X	
28. Description	E.g., emergency power supply, protective walls, honey pot sensors								X	

capability loss of unknown origin), and is covered by the table on resilience dimensions and attributes (column 4) and threats (column 5).

Step 5 on the pre-assessment of risk control and resilience is conducted by the matrix that considers all combinations of system performance functions and threats (column 6), in particular in all resilience cycle phases, considering all technical resilience capabilities and all system layers.

Step 6 on **overall resilience quantification** is in parts covered by the table on overall risk and resilience assessment (column 7), which considers not only single combinations of system performance functions and threats but also, for instance, for a single system performance function all threats, or the effect of a single threat on all system performance functions, as well as the combination of threat effects in terms of effects on persons (see details in Sect. 5.1.1 on analysis options).

Steps 7 and Step 8 on resilience evaluation and resilience improvement option selection are supported by tables on improvement measures (column 8) and improvement measure selection (column 9). In the latter case, the evaluation criteria as provided in Step 1 are used.

Step 9 on resilience measure development and implementation is not supported by a table. The table on improvement measures (column 8) and on their specific selection (column 9) is expected to take into account the implementability, monitorability, and incremental improvement potential. As improvement measures are very context- and system-specific, it is expected that domain-specific approaches can be used.

4.2 Gas grid

In the case of the gas transmission grid example, Table 3 lists data entries used in tabular and matrix assessments within the steps of the joint risk and resilience management process according to Fig. 1. They suffice to generate user requirements, mainly system non-performance functions, threats and potential disruptions, the identification of critical combinations of system non-performance functions and threats, functional and technical requirements for improving the security system, respectively, guided by improvement of system performance in all resilience cycle phases before, during and after events and taking several further resilience dimensions into account.

The data are based on the report (SecureGas D1.1 2019) on regulative, organizational, and operational requirements of gas grid security systems when designed as service-oriented architecture (SOA, platform as a service, PaaS) (ISO 22301) (Indu et al. 2018) (Bean 2010). It reports expert feedbacks collected in a questionnaire regarding the three identified types of requirements and requirements of nine similar EU projects as well as an additional expert workshop conducted on the basis of the consolidated feedback with focus on operational requirements (SecureGas D1.2 2019). In addition, technical requirements are considered as provided in the report (SecureGas D1.2 2019). Together with a threat, risk, and vulnerability assessment (SecureGas D1.3 2019), key functional requirements of the gas grid security system formulated as key performance indicators (KPIs) are extracted from SecureGas D2.3 (2019). System mainly non-performance but also performance functions are based on SecureGas D2.3 (2019).

In the application case gas grid, 6 tables and matrices (columns labeled 1 to 6 of Table 3) cover the scope of Fig. 1 using tabular approaches as proposed by Table 1. In overview, the tables and matrices cover the 9 resilience assessment and management steps in the following way:

Step 1 on context analysis is supported by the User/Stakeholder requirements ranking table, see column with label 1 of Table 3. Inspection of the entries requested shows that besides ID, title and short description of the requirements, application showcasing business domain (context of application), the involved users/stakeholders, the main requirement type (legal/regulatory, organizational, operational), respective types (2 + 2 + 7 = 11) and even sub-types (15 + 16 + 48 = 79) are used for each main user requirement type. The requirements are ranked using a semi-quantitative scale.

Step 2 on system analysis as well as Step 3 on system performance function identification is supported by the table covering System (non) performance functions and related (sub) components, see column with label 2 of Table 3. In this sample case, mainly non-performance functions are used. For each system function, an ID, title, and short description are requested. The functions are related to four asset management phases, five gas infrastructure main components and sub-components (4 + 5 + 5 + 9 = 23). This allows to see which system components in which asset management phase are relevant for delivering the system functionality. In addition, the functions are related to user requirements, i.e., which system functions are relevant to fulfill given requirements allowing to trace the coverage of requirements by system functions. Note that the business value chain elements affected are included, which are strongly related to the system elements considered given the asset management phase.

Step 4 on disruptions identification is covered by a table named Threats and disruptions ranking using resilience dimensions, see column with label 3 of Table 3. Each threat with ID, title, and description is classified using a rich resolution with 12 threat categories an in total 98 event categories (threat sub-categories). In addition, 5

Table 3 Gas network sample data entries and tabular and matrix assessment examples

Data entry Description	Examples	1. User/ Stakeholder requirements ranking	2. System (non) performance functions, (sub) components	3. Threats and disruptions ranking using resilience dimensions	4. Critical combinations of (non-)performance functions and threats	5. Technical req. improvement measures and requirements coverage	6. Functional KPIs of improvement measures and req. coverage
1. Stakeholder/End user ID	S1, S2, etc.	X	X			X	
2. Stakeholder/End user description	Management, operator, technician/worker, sources, storages, regional consumers, third party	X					
3. Application/Business cases (BC) affected (3 cases)	Security asset management through life cycle of gas grids (BC1); impact and cascading effects of joint attacks (BC2); Cyber-physical resilience of selected installations (BC3)	X				X	X
4. End user requirement ID	E.g., RE-EULEG-08, O-OR-SYST-09, O-OP-DSD-18	X	X			X	X
5. User and stakeholder main requirement types (3 categories)	Regulatory (RE), organizational (OR), operational (OP)	X					
6. Regulatory (RE) requirement types (2 types, 15 sub-types)	EU legislation (EUREG, e.g., EU charter, directives, regulations), national legislation (NREG, e.g., Greek, Lithuanian)	X					
7. Organizational (OR) requirement types (2 types, 16 sub-types)	International standards (STAN, e.g., ISO, IEC) and management systems (SYST, e.g., asset, integrity, safety and security)	X					
8. Characteristics of security systems (8 categories)	Flexibility, scalability, interoperability, authentication, authorization, trust management, user-friendly interface					X	
9. Operational (OP) requirement types (7 types)	Confidentiality, data protection and safety (CONF); Conditions (CON), e.g., extendibility, all threats; interoperability (INTER); detection, situational awareness and decision support (DSD); usability (USA); information management (INFOR); cost (COST)	X					
10. Operational requirement sub-types (48 sub-types in total)	E.g., sub-types of DSD is leakage detection and a sub-type of USA is short recovery time	X					
11. Stakeholder and end user requirement title and descriptions;	See examples above; Further Examples: fast prediction of effects of disruptions sufficient for counter measure selection	X					
12. Priority level of user requirements	Low, medium, high	X					
13. System non-performance and performance function ID	E.g., D&A-TRANS-01-001, O&M-ACCS-01-001; O&M-TREAT-04-001		X		X	X	X
14. Title and description	E.g., number of non-detected leakages		X		X		
15. Asset management phases (4 phases)	Design and analyze (D&A); construct/deconstruct (CONS); operate, maintain and repair (O&M); evaluate and plan (operational) (E&P)		X				
16. Sys. component ID	E.g., EXTR-02, TREAT-05, TRANS-05, ACSS-09		X				

Table 3 (continued)

Data entry Description	Examples	1. User/ Stakeholder requirements ranking	2. System (non) performance functions, (sub) components	3. Threats and disruptions ranking using resilience dimensions	4. Critical combinations of (non-)performance functions and threats	5. Technical req. improvement measures and requirements coverage	6. Functional KPIs of improvement measures and req. coverage
17. Title and description	E.g., Pipelines or pumping stations of transmission system		X				
18. Gas infrastructure main components (5 components)	Extraction (EXTR); treatment (TREAT); transport and distribution (TRANS); automation, control and safety systems (ACSS)		X				
19. Gas infrastructure sub-components (4 + 5 + 5 + 9 = 23)	EXTR: blow-out-preventer, Christmas tree, corrosion inhibitors injection, gas lift system; TREAT: Separator, sweetening, liquification, storage, regasification; TRANS: pipelines, pumping station, metering station, pressure reduction, odorizing box; ACSS: supervisory control and data acquisition; pipeline management, control and safety; process control systems safety systems; integrated control and safety systems (ICSS); telecom and security/surveillance systems; data transmission systems; asset optimization and maintenance support; information management systems;		X				
20. Technical req. ID	E.g., CRS-FUN-01, CRS-FUN-07, RAW-IMP-03					X	X
21. Technical requirement domains (13 domains)	CRS: Cross-sectional; DSS: decision support system requirements; UAV: unmanned aerial vehicle; IPM: information processing and management (including data analytics and machine learning for cyber security); OTS: operational technology network security; BCH: blockchain for data transmission and integrity; DET: detection, identification and early warning including intrusion and defects detection (IDD); RMG: risk and resilience modeling and management; GNS: gas network simulation; IMPS: implementation of standard component requirements; INT: integration requirements; GEO: geohazard assessment for decision support; RAW: risk aware information of the population					X	X
22. Technical requirement subdomains for each category (19 + 20 + 9 + 10 + 6 + 6 + 7 + 14 + 9 + 9 + 15 + 3 + 20 = 147)	E.g., within category cross-sectional multiple event correlation (cyber and physical); within category decision and support system a common alerting protocol (CAP) and simulative capability					X	
23. Technical requirement types or dimensions (6 types)	Functional (FUN); input/output interface (I/O); security requirement (SEC); operating requirement (OPR); design requirement (DES); implementation requirement (IMP);					X	X

Table 3 (continued)

Data entry Description	Examples	1. User/ Stakeholder requirements ranking	2. System (non) performance functions, (sub) components	3. Threats and disruptions ranking using resilience dimensions	4. Critical combinations of (non-)performance functions and threats	5. Technical req. improvement measures and requirements coverage	6. Functional KPIs of improvement measures and req. coverage
24. Technical requirement title and description	E.g., Critical node identification; Graph-model or simulative-engineering-based identification of critical nodes				X	X	
25. Threat or disruption event ID	E.g., PGS-08, CYBER-12, NH-16, PHW-03			X	X	X	X
26. Threat categories (12 categories)	political, geopolitical, societal (PGS); explosion (EX); chemical, biological, radiological, nuclear (CBRN); ground works (GW); critical utilities failure (CUF); cyber-attacks (CYBER); operational, management (OM); natural hazards (NH); criminal (CRIM); technical, man-made intentional, terroristic (TMMIT); indirect/command threats (INDT); physical hardware vulnerability (PHW);			X			
27. Threat event categories/sub-categories (8 + 5 + 4 + 5 + 4 + 12 + 6 + 16 + 2 + 16 + 3 + 9 + 5 + 3 = 98)	Examples for each category: blockade, invasion; improvised explosive device (IED); local C-event; third party interference (TPI) through drainage work; failure of power supply system; identity theft; improper maintenance; near urban fire; high power microwave (HPM); blackmailing of operators; mechanical impact; domino effects caused by other infrastructure; corrosion			X			
28. Resilience dimensions considered for threat event (5 dimensions)	(i) Cyber-physical category; (ii) system layer; (iii) persons affected; (iv) classical risk analysis phases affected; (v) risk control and resilience cycle phases affected; (iv) technical resilience capabilities needed for mitigation			X			
29. Attributes considered within each resilience dimension (3 + 7 + 5 + 7 + 4 = 26)	(i) Cyber, physical, cyber-physical; (ii) mechanical/physical, electrical/ hardware, cyber (software, protocols), operational (workers, operators, maintenance, support), management, societal/ geopolitical, environment; (iii) context analysis, risk identification, risk analysis (frequency and consequence determination), risk evaluation, risk mitigation; (iv) preparation, detection, prevention, protection, response, recovery, learning and adoption; (v) sensing/ surveillance, situation representation/ awareness, sense and decision making, action, modification and adoption			X			
30. Relevancy ranking of threat dimensional attributes; of criticality of combination of (non)	E.g., semi-quantitative scale from 1 to 6: (1) not affected/ negligible, (2) very low (3) low, (4) medium, (5) high and (6) very high influence			X	X	X	

Table 3 (continued)

Data entry Description	Examples	1. User/ Stakeholder requirements ranking	2. System (non) performance functions, (sub) components	3. Threats and disruptions ranking using resilience dimensions	4. Critical combinations of (non-)performance functions and threats	5. Technical req. improvement measures and requirements coverage	6. Functional KPIs of improvement measures and req. coverage
performance functions and threats; or of technical requirement							
31. Title and short description of threat	E.g., Cyber-induced physical damage, criminal attack, cyber-physical timed coordinated attack			X			
32. Code Key Performance Indicator (KPI) of improvement measures	E.g., CRS-FUN-07, DSS-OPR-03, DSS-IMP-01, UAV-FUN-01, RAW-FUN-05						X
33. KPI field (overview) for technical components resolved with respect to technical type/dimension (5 + 4 + 1 + 4 + 3 + 4 + 5 + 6 + 3 + 4 + 4 + 6 = 49)	*CRS:* FUN: reliability: false alarm, cross correlation, latency, time to notify, autonomy: threat coverage, automatic threat detection and decision support, I/O: interoperability with legacy systems, OPR: usability through multilingualism, resilience: self-testing, controlled degradation; *DSS:* OPR: decision support, retention, physical-cyber threats, IMP: heterogeneous system implementation; *UAV:* FUN: Pipeline inspection; *IPM:* FUN: Scope, OPR: reliability in terms of precision, recall and time to detect; *OTS:* FUN: SCADA system protection, alert sending via API interfaces, DES: SCADA protocols support; *BCH:* FUN: data integrity in terms of reliability of keyless signature infrastructure (KSI) and of verification of data properties, SEC: privacy, I/O: availability; *DET/IDD:* FUN: leak alert, intrusion alert, physical threats, I/O: interoperability, OPR: service reliability (locally), regulation, effectiveness, DES: monitoring domain, user friendly; *RMG:* FUN: effectiveness (coverage of threats and consequence reductions, localization), I/O: interoperability from various terminals, OPR: (local) reliability, regulation, effective risk and resilience management, DES: usability; *GNS:* FUN: transient predictions and steady-state predictions (respectively area size, resolution, computing time) I/O: needed inputs/generated outputs; *INT:* FUN: alerting, I/O: connectivity, covering standards, OPR: service continuity; *GEO:* FUN: alert, I/O: rain measurement and forecast, digital terrain model (DTM), geotechnical/physical inputs, OPR: rain data; *RAW*: FUN: reactivity, content suggestion efficiency and precision, forensics, interface, OPR: stakeholders						X
34. KPI indicator and description (11 + 4 + 6 + 4 + 3 + 4 + 11 + 10 + 11 + 4 + 4 + 6 = 78)	E.g., for technical component cyber security for IT and OT weakness (OTS) in the field SCADA protection the indicator New host detection						X

Table 3 (continued)

Data entry Description	Examples	1. User/ Stakeholder requirements ranking	2. System (non) performance functions, (sub) components	3. Threats and disruptions ranking using resilience dimensions	4. Critical combinations of (non-)performance functions and threats	5. Technical req. improvement measures and requirements coverage	6. Functional KPIs of improvement measures and req. coverage
35. KPI metric and target value	For the indicator above the metric is binary (0 or 1) and the target value is new host is detected (1)						X

resilience dimensions with in total 26 attributes are used to classify the threats, e.g., whether threats mainly challenge the technical detection capability, which system layer they affect, and in which resilience cycle phase. For each case, the relevancy of the attributes and hence threats is ranked.

Step 5 on the pre-assessment of risk control and resilience is conducted by the matrix entitled Critical combinations of (non-)performance functions and threats, see column with label 4 of Table 3. It covers the IDs and titles of the (non) performance functions and threats, respectively, and for each combination a semi-quantitative assessment of its criticality. The assessment considers the information provided in the last three tables.

Step 6 on overall resilience quantification is again only in parts covered by the table on Critical combinations of (non-)performance functions and threats. For instance, for each performance function the relevancy of all threats or potential disruptions is considered and hence can be jointly evaluated as described along with Eq. (1) below. Using this equation, also the effect of given threats on all performance functions can be assessed. However, the equation assumes that the threat events are occurring independent of each other. Nevertheless, if a performance function is affected by more than one threat event type, it is a strong candidate for further quantitative assessment, which by definition of the presented approach is not covered within the pre-assessment Step 5 but subject of Step 6 as exemplarily shown in Sect. 5.1.4.

Steps 7 on resilience evaluation and Step 8 on resilience improvement option selection are supported by tables on Technical requirements for security and safety improvement measures including their coverage of user requirements and main relevancy for performance functions and threats addressed as well as a table on Key performance indicators (KPIs) for the technical requirements, see columns with label 5 and 6 of Table 3, respectively. In detail, the technical requirements table structures each requirement using 13 requirement domains related to technical security solutions (e.g., capabilities of UAV-based detections, fiber-sensor and simulation-based technical solutions) with in total 147 subdomains with high technical specificity. Resorting to the already introduced tables, each technical requirement can be related to users, application use case contexts, main end user requirements, system performance functions supported, and threats countered. In addition, a sorting with respect to 6 standard technical requirement types is feasible (e.g., functional, interfacing). This is further supported by providing quantitative metrics for the requirements in terms of KPIs covering 12 technical requirement domains. No KPIs are provided for the implementation of standard component requirements (IMPS). For each of the 49 KPI fields, at least 1 up to 7 indicators are provided resulting in 78 indicators. The indictors are described and a metric and a numeric threshold are provided.

Step 9 on resilience measure development and implementation is not supported by a table. Similar as in the application case telecommunication infrastructure, it is assumed that based on the detailed technical specification requirements table and quantitative KPIs table as just described sufficient input is provided for a technical development supported by domain-specific standards.

4.3 Indoor localization system

Using very first example entries given in Häring et al. (2017b), Table 4 gives an overview of tables and matrices used in the case of the indoor localization sample system introduced in Sect. 3.

For the indoor ultrasonic localization system, 6 tables and matrices (columns labeled 1 to 6 in Table 4) support the joint risk control and resilience improvement process of Fig. 1 using table and matrices as proposed in Table 1 covering all 9 steps of the process:

Step 1 on **context analysis,** Step 2 on **system analysis**, and Step 3 on **system performance function identification** of Fig. 1 are supported by two tables. The table on System functions ranking and related users (see column with label 1 in Table 4) covers 8 functions of the localization system on operational system level as relevant for applications in the industrial, service, and health sector and 11 technical system functions as well as related stakeholder users. It is strongly linked with the table on System functions and related system elements (see column with label 2 in Table 4) necessary for the realization of the system functions, e.g., transmitter tags to be localized. Independent of the technical functionalities, the system service functions are ranked on a semi-quantitative scale from 1 to 10. The system is, as described in Sect. 3, divided in 5 subsystems and 8 main component types that are used in the various subsystems.

Step 4 on **disruptions identification** is covered by the table on Failures, disturbances, and disruptions ranking (see column with label 3 in Table 4). Events have been categorized in system failure including systematic design failures, degradation, or error; external disturbance or disruption; and intentional disturbances. In total, 42 sub-types are provided. The ranking is conducted at the level of subtypes and assessing all system functions.

Step 5 covering the **pre-assessment of risk control and resilience** is covered by the matrix on Critical combinations of system functions and disturbance causes (see column with label 4 in Table 4). It resolves the relevancy of disruptions and disturbances for the service functions, mainly the non-performance function absolute localization error. Note that for each combination the probability of the disturbance as well as the expected consequences on system service level are estimated.

In this application case of a smaller technical distributed system, the Step 6 on **overall resilience quantification** is conducted by the sequential experimental assessment of disruption events of different kinds that are ranked to be most relevant across all application domains regarding probability and potential effects, see the table on Disruption effects quantification experiment ranking (column with label 5 in Table 4). Besides the threat description, experimental set-up characteristics are added including room geometry, ultrasound reflection properties, and the time evolution of the threats.

Finally, Step 7 on **resilience evaluation** and Step 8 on **resilience improvement option selection** are supported by a ranked table of improvement measures (column with label 6 in Table 4) taking into account all ranked and experimentally assessed potential disruptions as well as system functions and related components subject to potential modification. Considered are minor architecture and interface changes, software and algorithm changes, and improvement of hardware components. As improvement measures are linked in addition to users, system service functions their feasibly can be assessed.

5 Data analyses performed

The section shows for the telecommunication grid, security system of gas transmission grid and an indoor localization system how to employ the data provided in Tables 2, 3, and 4 by using some of the tabular and matrix approaches proposed in Table 1 to fulfill the joint risk and resilience management process of Fig. 1.

5.1 Telecommunication grid

5.1.1 Assessments and quantities accessible for the telecommunication domain

Several (simple) analysis options and related examples are given. They mainly refer to the telecommunication domain, the sample input data of which are provided in Table 2.

Regarding qualitative and discrete analysis, the following (basic) numbers are accessible:

- The number of stakeholders, objectives, assessment criteria, components, subsystems, system functions, system performance functions, threats, resilience dimensions and respective number of attributes, number of combinations of system performance functions and threats that need improvement measures, and number of iterations of the overall resilience assessment and

Table 4 Indoor localization sample data entries and tabular and matrix assessment examples

Data entry Description	Examples	1. System functions ranking and related users	2. System functions and related system elements	3. Failures, disturbances, and disruptions ranking	4. Critical combinations of system functions and disturbance causes	5. Disruption effects quantification experiment ranking	6. Improvement measures ranking
User ID; User title and short description	E.g., Management (U1); operator (U2); technician (U3); service; service production or logistics employee (U4)	**X**					
System function ID; title and short description	E.g., local absolute localization error (OPR-01), updating time of localizations (OPR-03)	**X**	**X**		**X**	**X**	**X**
System performance function types and metrics (8 + 11 = 19)	Operational/ functional (OPR): Localization local error (absolute deviation) in meter; measure for local uncertainty of localization in meter; localization time resolution in seconds (updating time); allowed speed of movement of tag in meter per second; number of tags per area that can be distinguished (dimensionless); acquisition time for new tag (time needed from switch on till localization) in seconds; interfacing options with production and logistic systems; scalability of approach (e.g., maximum number of tag IDs); adaptability of approach to different room geometries (e.g., types of room geometries allowed); mean service time intervals of tags and receivers in days Technical (TECH): number of receivers per area needed for coverage depending on room geometries (dimensionless); energy consumption per tag or receiver in joule; maximum operational life of tag or receiver in hours; range of single ultrasound transmitter (sender) in meter; aperture angle of ultrasonic transmitter and receiver (in degree); necessary spatial accuracy of calibration of receiver positions in meter; system resources used for ISM communication, for gateway, for cloud-based interfacing and for storage and PC-based analysis and for visualization (e.g., as percentage of standard hardware and software services)	**X**					

Table 4 (continued)

Data entry Description	Examples	1. System functions ranking and related users	2. System functions and related system elements	3. Failures, disturbances, and disruptions ranking	4. Critical combinations of system functions and disturbance causes	5. Disruption effects quantification experiment ranking	6. Improvement measures ranking
System element ID; System element title and short description	E.g., tag (TX) uses ultrasonic transmitter (TX-01), ISM band (TX-02), D/A and A/D converters (TX-03, TX-04, TX-05), microcontroller (TX-06), peripheral electronic (TX-07) and energy supply (TX-08)		**X**				
Subsystems (5)	Ultrasound tag (sender, transmitter) (TX) and receiver, respectively, with ISM band (center frequency 6.78 MHz, bandwidth 30 kHz) (RX); gateway server for ISM band (GATE); internet/cloud interfacing and storage (CLOUD); portal for analysis and visualization using PC resources (ANA)		**X**				
System component types (12)	Ultrasonic transmitter and receiver; ISM band transmitter and receiver (antenna); A/D and D/A transformer; microcontroller including clocks; embedded software; energy supply; peripheral electronic of embedded system; cloud services; PC hardware including displays; PC software		**X**				
ID of degradation, failure, disturbance or disruption; title and short description	E.g., Position of ultrasonic receiver imprecise is a systematic system failure (SYS-17); Barrier between several lines of sight of senders and receivers (EXT-07) is a transient or systematic disturbance			**X**	**X**	**X**	**X**
Type of failure, disruption (3 types)	System failure, degradation or error (SYS); external disturbance, disruption (EXT); intentional disturbance (INTENT)			**X**			

Table 4 (continued)

Data entry Description	Examples	1. System functions ranking and related users	2. System functions and related system elements	3. Failures, disturbances, and disruptions ranking	4. Critical combinations of system functions and disturbance causes	5. Disruption effects quantification experiment ranking	6. Improvement measures ranking
Sub-types of disturbance, failure, disruption (23 + 15 + 6 = 42)	SYS: loss/degradation of ultrasonic transmitter or receiver; of ISM band; of DA or AD transformer; of further peripheral embedded electronics; of energy supply; error of embedded software, of gateway or of PC software; failure of local nets, of internet, of cloud interfacing or of cloud service; PC hardware failure; unfavorable room geometry (e.g., very high or low ceilings); receiver positions not well selected or imprecise; tag moving too fast; too many tags; tag out of range of receivers; anisotropic ultrasonic radiation behavior; resonant vibrations at ultrasonic sender site; byzantine fault EXT: high-temperature gradient; wind; noise; physical coverage of transmitter or receiver; barriers within direct line of sight; wet, salty, or dusty environment; specific sounds of, e.g., machinery or jingling of bunch of keys; reflections on moving transport machinery; fast changing geometry; electromagnetic compatibility (EMC) disturbances; moving single and several persons INTENT: jamming of ultrasound frequencies or of IMS band; IT-attack; change of position of receivers; removal of receivers or senders;			X			
Classification of failure (3 classes)	Statistic, transient (soft), systematic			X			
Resilience dimensions considered	System layers; resilience cycle phases		X	X			X
Relevancy scale of system functions; of threats; of combinations of system functions and threats in terms of frequency and consequences; of adequacy of counter measures	Semi-quantitative scale from 1 (negligible) to 10 (very relevant)	X		X	X	X	X

Table 4 (continued)

Data entry Description	Examples	1. System functions ranking and related users	2. System functions and related system elements	3. Failures, disturbances, and disruptions ranking	4. Critical combinations of system functions and disturbance causes	5. Disruption effects quantification experiment ranking	6. Improvement measures ranking
ID, title, and short description of experimental disruption scenario	E.g., switching off and on of tag (transmitter)/ Loss of past localization history (EXP-01); persons orbiting around tag (EXP-02); barrier disrupting line of sight between sender and receivers (EXP-03); time-limited switching off of several receivers (EXP-05)					**X**	
(Operational) Application domains covered (8)	Industrial production (lines), indoor logistic, health care (hospitals), smart home applications, industrial maintenance and repair, construction, shopping centers, specific consumer electronics involving user positioning and orientation (e.g., motion games)					**X**	
Geometry and ultrasonic characteristics (5 types)	Overall room type and geometry, e.g., hall, corridor, geometry shape and dimensions; surfaces' geometries and ultrasonic reflection and absorption properties; local coverage characteristics of transmitters or receivers including material properties; of (moving) barriers within room, e.g., columns, machinery robots, automated guided vehicles (AGV), panels; of minor structures and furniture within room, e.g., pallet racks, material within racks, seating; and of (groups) of persons					**X**	
Time dependence characterization of disturbance (4 categories)	Duration, e.g., long-term, short term; increasing and decreasing behavior of disruption in phases; periodic behavior; time-dependent strength of disturbance						
ID, title, and short description of improvement measure	E.g., increase of initial frequency of position updates, more receivers per area,						**X**

Table 4 (continued)

Data entry Description	Examples	1. System functions ranking and related users	2. System functions and related system elements	3. Failures, disturbances, and disruptions ranking	4. Critical combinations of system functions and disturbance causes	5. Disruption effects quantification experiment ranking	6. Improvement measures ranking
Types of improvements (3 types) and examples	System design (DES): additional receivers to allow for sufficient line-of-sight ultrasound propagation time measurement (redundancy); consideration of reflections (e.g., distinction of line of sight time of propagation measures and direct measures); use of ultrasound frequencies less prone to noise and disturbances; replacement of ISM band communication with ultrasound data transmission Software/Algorithm (SW): Modification of localization algorithm (e.g., considering less past positions, using less outlier-sensitive distance measures); more position updates; modification of tag initial acquisition and relocation after disturbance (e.g., higher frequency of initial localizations); increase of robustness against noise by using more robust ultrasound signals that can be better distinguished from noise by autocorrelation analysis (e.g., using distinct chirp pulses); advancement of battery management system Hardware/component (HW): Use of more isotropic ultrasound senders; use of low-energy components; motion wake-up sensor; temperature sensor;						**X**

improvement cycle. All these numbers should be greater than one to ensure minimum formal coverage.

- Objectives per stakeholder, system performance functions per objective, number of subsystems and components per system performance function, and threats per system performance function, all of which should be greater or equal than one to ensure consistency and coverage.
- Critical threats per system performance function; number of threats affecting a resilience attribute for each performance function for each resilience dimension, e.g., to answer which resilience cycle phases, resilience capabilities, or system layers are most often affected by threats (this has been, e.g., also used within the EU project SecureGas (2019–2021) on securing the European gas network for the vulnerability, risk, and resilience analysis for potential threats and disruptions); number of improvement measures per critical combination of threats and system performance functions; number of improvement measures per resilience attribute for each resilience dimension (for each critical combination or overall).

It is expected that most assessment quantities only converge after iteration of the process. For instance, the number of critical threats will decrease with iterations. The ambition is that with consideration of improvement measures, all critical threats per system performance functions can be reduced, e.g., to acceptable threats.

Regarding system analyses based on the table contents, (topological) graphs are available illustrating the level of dependence of, for example, components, subsystems, and system functions, as well as system functions on subsystems and components and objectives on system functions. The links can be used to express the level of relation, allowing for more accurate assessment of the expected effects of threats. Examples are given in Fehling-Kaschek et al. (2019).

Further assessment options are presented in Table 1, which lists several relation matrices that are not made explicit in Table 2, e.g., the relation between threats and improvement measures.

Regarding semi-quantification and quantification, the use of overall resilience quantities is recommended. Resilience quantities should cover sufficient resilience dimensions for all system performance functions and threats. Examples for system dimensions are system layers, resilience cycle phases, and (technical) resilience capabilities, see, e.g., Häring et al. (2016a) for further resilience dimensions. In this way, the total overall risk considering system performance functions, threats, and resilience dimensions reads

$$R_{res} = \sum_{i=1}^{N_{threat}} P_{i,PF(i),T(i),RD(i),RA(i)} C_{i,PF(i),T(i),RD(i),RA(i)}, \tag{1}$$

where N_{threat} labels the different threats considered for which probabilities (frequencies, likelihoods) and consequences (effects, impacts) are determined. In Eq. (1), $PF(i)$ is the set of performance functions affected by the threat, $T(i)$ the set of threat types the identified threat belongs to, $RD(i)$ is the set of resilience dimensions relevant for the categorization of the threat, and $RA(i)$ are sets of attributes (one set for each resilience dimension) relevant for each resilience dimension. For each risk event, all sets are required to be not empty: $|PF(i)| \geq 1$, $|T(i)| \geq 1$, $|RD(i)| \geq 1$, and $|RA(i)| \geq 1$. Thus, each risk event affects at least one system (non) performance function, can be attributed to at least one threat category, categorized with at least one resilience dimension (e.g., system layers), and can be sorted into at least one resilience dimensional attribute (e.g., physical layer). The total risk on risk control and resilience objectives in (1) is an extreme quantity in the sense that the consideration of further potential risk events and threat types as well as resilience dimensions will not significantly increase the risk, i.e., add additional significant risk contributions.

Let N_{PF} be the number of all performance functions considered. Then for $1 \leq j \leq N_{PF}$

$$R_{res}(j) = \sum_{i=1}^{N_{threat}} (PF(i) = j)_{lb} P_{i,PF(i),T(i),RD(i),RA(i)} C_{i,PF(i),T(i),RD(i),RA(i)}, \tag{2}$$

is the total risk for each system performance function, where the logic bracket has been used which evaluates as one if the statement is true and zero otherwise. As risk events can be attributed to several performance functions, one has only $\sum_{j=1}^{N_{PF}} R_{res}(j) \geq R_{res}$. However, Eq. (2) provides a risk ranking for each performance function.

In a similar way as in (2), threat types can be ranked using the number of threat types N_T, the relevancy of resilience dimensions using the number of resilience dimensions N_{RD}, and resilience attributes using the number of resilience attributes within each resilience dimension $N_{RA}(k), 1 \leq k \leq N_{RD}$. Examples for system performance functions, threats to be considered, resilience dimensions and attributes used are given for each application case in Sects. 4.1, 4.2, and 4.3 as well as respective sample tables in Sects. 5.1.2, 5.2.2, and 5.3.2.

Equations (1) and (2) employ risk addition (superposition) of single risks to achieve coverage of all risk aspects on system level. They are not normalized and can be used for relative comparison of system modifications, system versions, and system improvement options when anticipating their effects and when assessing their effects in a second iteration of the overall resilience management process.

For further illustration, Eqs. (1) and (2) can also be applied solely to the phases up to absorption of a disruption events (e.g., prevention, building protection, detection, immediate consequences) to cover risk control as well as only to the specific resilience cycle phases during and post events (e.g., response (stabilization), recovery, adoption, and learning) to cover resilience improvement. Similarly, it can for instance be distinguished between threats affecting engineering-technical system layers (e.g., physical, engineering, and cyber) and all non-technical layers (e.g., operational, decision making, and policy). Furthermore, socio-technical resilience capabilities could be assessed separately, considering the options to detect (sensing, situation awareness), to represent, to model and decide (representing, sense making, and decision making), and to act and improve (activation, reconfiguration, adoption, action). Using these perspectives, a strong (even somewhat redundant) focus can be placed on post-event assessment and post-event capabilities, thus thoroughly covering the resilience aspect in addition to classical risk control.

Using Eq. (1) and related sub-sums, classical risk matrix plots are accessible, e.g., all risks identified post event for a selected performance function, or all risks for a selected post-event phase, etc. By providing acceptance criteria (e.g., green: acceptable, yellow: improve if feasible and reasonable, and red: should be reduced), single risks can be evaluated, e.g., in terms of expected monetary loss, see examples given in Sects. 5.1.3 and 5.1.4.

Data visualization can assist users in digesting risks. Bubble charts are accessible and can be used, for instance, to visualize risks with bubble size depending on risk within a system performance versus threat matrix for all combinations or sets of combinations of threats, e.g., to compare natural, anthropogenic, accidental, intentional (sabotage, criminal), and terroristic threats, see Fig. 6 for an example.

For overall or group risk assessment besides the risk matrix determination and evaluation, the use of modified FN diagrams and related criteria is proposed (see, e.g., Proske 2008 for an introduction). For separate consequence categories (e.g., injured, fatalities, monetary loss, environmental damage) the following tuples are convenient:

$$\left(C_{cat}, P\left(\text{events with} C_{i,PF(i),T(i),RD(i),RA(i)} \geq C_{cat}\right)\right), C_{cat} > 0, \tag{3}$$

where C_{cat} is typically increased by a factor (e.g., 2 or 10) to allow a double logarithmic plotting of the group risk tuples. In (3) for each system performance function and threat combination, all probabilities are combined. This is acceptable given that the effects are measured using the same consequence category.

Overall comparisons are accessible if there are joint scales for probabilities and consequence categories, respectively. For instance, regarding fatalities (and related financial quantifications) classical FN criteria can be used, e.g., the Dutch FN criterium with F(1)=1.0 × 10^{-3} per year and aversion factor 2, hence, e.g., F(10)=1.0 × 10^{-5} per year, see, e.g., Trbojevic (2005). For further criteria, see, e.g., Spouge et al. (2014) for risk level and acceptance criteria for passenger ships as an example for a domain-specific FN criterium selection.

5.1.2 Sample tables for the telecommunication domain

The sample tables used in this Section come from one of the use cases of the RESISTO project, see RESISTO D3.9 (2020). Further examples for performance-based resilience analysis can be found in Häring et al. (2020). For each use case in RESISTO, a full analysis has been completed, including the tables mentioned in this paper. In this general example, a telecommunication network experiences a multitude of common threats faced by telecommunication network operators including cyber-attacks such as distributed denial-of-service attack (DDoS) attacks and physical threats like cable cuts or break ins. As mentioned in Sect. 3, the input for these tables comes from experts as well as the use case description.

The main objectives and related stakeholders within the sample application are summarized in Table 5. The stakeholders and objectives were determined with a survey sent to telecommunication network operators within the RESISTO project. Questions in the survey that helped with the context analysis included defining the industry the company operates in, if there were separate or joint physical and cyber security teams within the company, and the amount of the IT budget that was earmarked specially for IT security. The main objective is a refinement of use cases with the goal of identifying critical threats, in particular those which can be addressed within the instruments provided by project partners. The joint risk and resilience management approach was applied to determine the as-is risk control regarding system objectives and resilience ranking considering already implemented measures of 4G telecommunication standards. The ranking did not consider the feasibility of countermeasures and improvement measures as planned during the project or similarly in real-world applications. However, it was used as input for such decision making to determine the most efficient countermeasures and improvement measures.

The process of obtaining this information from the operators began with the creation of the spreadsheet tables.

The tables were created with the operators' time constraints in mind. The drop-down menus were predefined, and comments with explanations were added to each column. The operators were given a set deadline by which to return the filled out tables. Once the tables were returned, the use case descriptions were added. In this way, a full picture of the scenarios and the operators' specific networks was created. The tables were then sent back to the operators for an evaluation. In many cases, one-on-one meetings occurred with each operator to discuss the specifics.

Figure 2 is an excerpt from the table for the system components. For each of the components, additional information is acquired, as discussed in Table 2, including the subsystem, the type, the quantity, and the interconnections. Some of these columns are formatted as drop-down menus to limit the responses to a few categories. This is done for the subsystems, in which case responses were limited to different networks common to telecommunication. The component type also has a drop-down menu and is limited to common components like software or hardware. This use case had other system components besides the ones seen in the figure, including workstations and servers, network security equipment, and equipment shelters and sensors (Miller et al. 2020).This corresponds to the input for row 3 of Table 1 on system analysis, namely the provision of system elements such as subsystems and components and their relation.

When filling out this first table, operators had to decide how in-depth to make their list of components. In a few cases, to save time, operators might put broadband network or simply fiber optic (FO) infrastructure. Many times, operators did not break down the different components or input the smallest components. However, they might put the list of components in the description. For example, if TV headend were the main component, the description might include "coders, multiplexors, and others." This presents a challenge for future steps of the resilience management cycle, as the components listed in the spreadsheet tables may not be too general for the network flow diagrams provided, and thus may not be the ones that are simulated.

Figure 3 provides the system functions for the use case. Many of the use cases shared similar system functions, such as voice services, mobile and fixed data services, and connectivity. This is because all operators and telecommunication networks are providing a service for customers and need to be able to measure the availability of the service. This corresponds to row 4 of Table 1 on system function analysis.

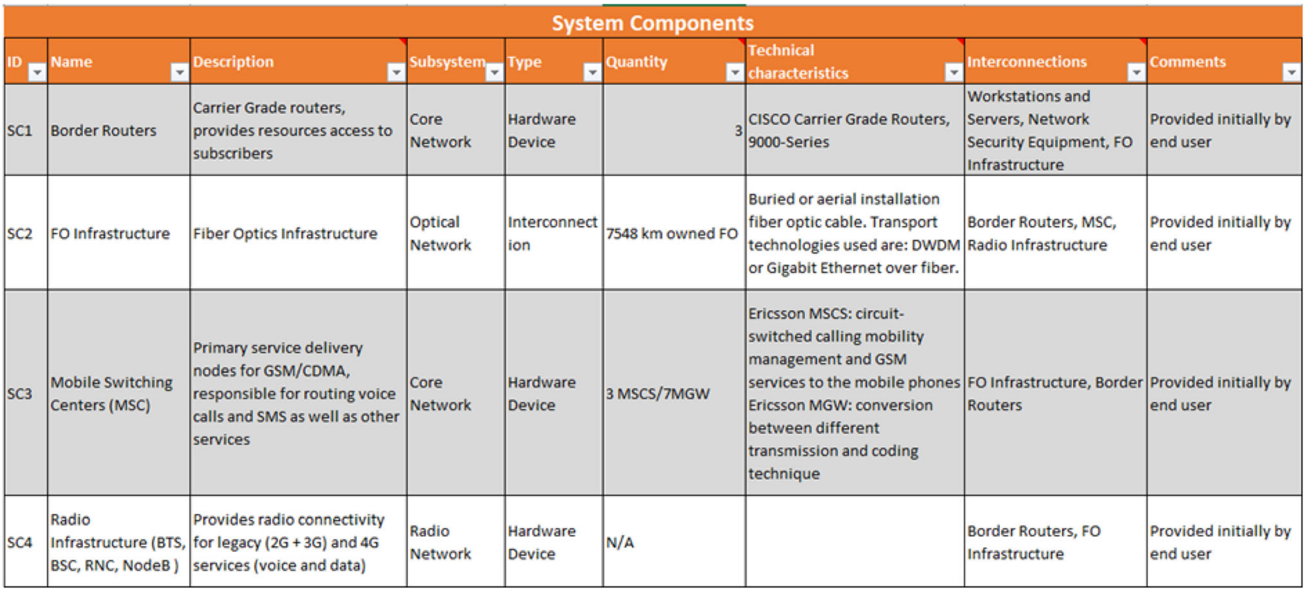
An important column when defining the system functions is that of the linked system components. Defining how the system functions link to the system components defined in the earlier table is the basis of the correlation matrix that is determined later. As seen in Fig. 3, multiple components can be linked to a single system function and components can be linked to multiple functions.

When discussing the system functions, operators mentioned Service Level Agreements (SLA) and Service Level Objectives (SLO). SLAs are the agreements the operators have with their customers that define the requirements for performance. SLOs define the penalties if the objective or agreement is not met. The SLOs can be used when defining the system functions. Examples of SLOs include monthly availability, downtime incidents, packet loss, and jitter. Utilizing the SLOs when completing the tables allows for the operators to have more context when selecting the impact that a threat may have on the network as many of the penalties are economical.

Threats are defined in Fig. 4. These were defined by the operators as well as based on the use case scenarios. The threats have many characteristics, as mentioned in Table 2. Figure 4 covers input to Table 1 on threat and disruptions and the pre-assessment of such events up to overall assessment (if no cumulative risk and resilience analysis is conducted), i.e., the joint risk and resilience assessment Steps 4 to 6. The frequency and impact (either economic or social) are used to create a hazard matrix, as seen in the next section. For the correlations, the linked components and system functions are recorded. To get a full idea of the threats experienced by telecommunication networks, cyber, physical, and cyber-physical threats are listed. The cause of each hazard is also defined to be natural, man-made (attack), man-made (accidental), or a technical/system failure.

Table 5 Examples of the main stakeholders and their objectives

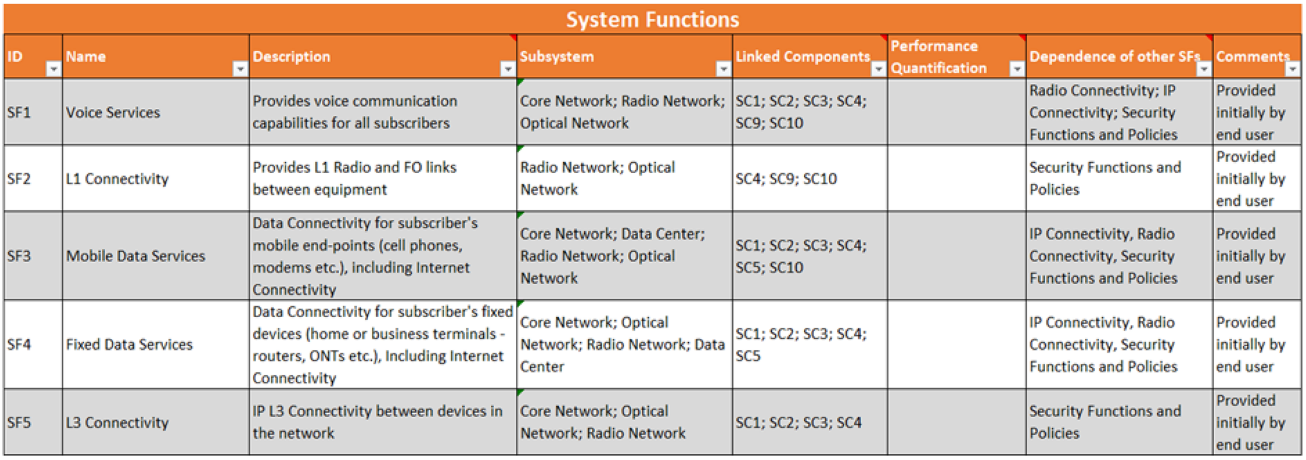
Stakeholders	Objectives
1. Telecommunication network operators	Profits; reliable equipment; resilient system (includes classical risk control and post-event resilience); efficient compliance with legal and standard requirements
2. Telecommunication network operator technical staff	More efficient risk event identification, control, and handling; transparent but not cumbersome processes and assessments sufficient
3. Investors	Profits; good public image
4. General public/Consumers	Receive reliable services; reasonable pricing; data security; useful customer service



System Components

ID	Name	Description	Subsystem	Type	Quantity	Technical characteristics	Interconnections	Comments
SC1	Border Routers	Carrier Grade routers, provides resources access to subscribers	Core Network	Hardware Device	3	CISCO Carrier Grade Routers, 9000-Series	Workstations and Servers, Network Security Equipment, FO Infrastructure	Provided initially by end user
SC2	FO Infrastructure	Fiber Optics Infrastructure	Optical Network	Interconnection	7548 km owned FO	Buried or aerial installation fiber optic cable. Transport technologies used are: DWDM or Gigabit Ethernet over fiber.	Border Routers, MSC, Radio Infrastructure	Provided initially by end user
SC3	Mobile Switching Centers (MSC)	Primary service delivery nodes for GSM/CDMA, responsible for routing voice calls and SMS as well as other services	Core Network	Hardware Device	3 MSCS/7MGW	Ericsson MSCS: circuit-switched calling mobility management and GSM services to the mobile phones Ericsson MGW: conversion between different transmission and coding technique	FO Infrastructure, Border Routers	Provided initially by end user
SC4	Radio Infrastructure (BTS, BSC, RNC, NodeB)	Provides radio connectivity for legacy (2G + 3G) and 4G services (voice and data)	Radio Network	Hardware Device	N/A		Border Routers, FO Infrastructure	Provided initially by end user

Fig. 2 A few of the system components provided for the sample use case



System Functions

ID	Name	Description	Subsystem	Linked Components	Performance Quantification	Dependence of other SFs	Comments
SF1	Voice Services	Provides voice communication capabilities for all subscribers	Core Network; Radio Network; Optical Network	SC1; SC2; SC3; SC4; SC9; SC10		Radio Connectivity; IP Connectivity; Security Functions and Policies	Provided initially by end user
SF2	L1 Connectivity	Provides L1 Radio and FO links between equipment	Radio Network; Optical Network	SC4; SC9; SC10		Security Functions and Policies	Provided initially by end user
SF3	Mobile Data Services	Data Connectivity for subscriber's mobile end-points (cell phones, modems etc.), including Internet Connectivity	Core Network; Data Center; Radio Network; Optical Network	SC1; SC2; SC3; SC4; SC5; SC10		IP Connectivity, Radio Connectivity, Security Functions and Policies	Provided initially by end user
SF4	Fixed Data Services	Data Connectivity for subscriber's fixed devices (home or business terminals - routers, ONTs etc.), Including Internet Connectivity	Core Network; Optical Network; Radio Network; Data Center	SC1; SC2; SC3; SC4; SC5		IP Connectivity, Radio Connectivity, Security Functions and Policies	Provided initially by end user
SF5	L3 Connectivity	IP L3 Connectivity between devices in the network	Core Network; Optical Network; Radio Network	SC1; SC2; SC3; SC4		Security Functions and Policies	Provided initially by end user

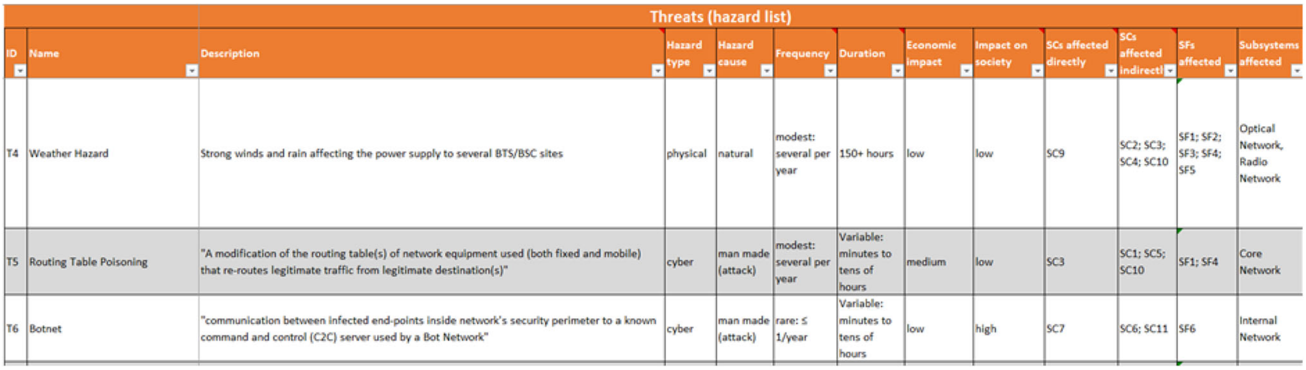
Fig. 3 Some of the system functions defined for the sample use case

It is interesting to note that when operators were compiling threats, a few mentioned difficulties in selecting the impact economically. For example, if there is a data exfiltration, the economic impact can vary depending on which data are leaked. If the leak is of confidential data about the customers, this could lead to fines within the EU. If it is not, there would be no fine. These fines can cost the operators significant money, so the difference between the two is quite large and would have very different economic impacts. In this case, two different threats were created, one data exfiltration that led to a fine and one that did not.

Improvement measures are defined in Fig. 5. Each threat has components and threats linked to it. Therefore, all of the tables are now linked together and the relationships between all four tables can be visualized. These improvement measures may already be implemented in the networks today. Some operators had a degree of difficulty listing improvement measures. This was especially the case regarding 5G networks. 5G networks have many improvements over 4G, such as having the ability to create new virtual components on demand and generally having more virtualization. The question was raised as to whether these characteristics of 5G networks could be used as specific improvement measures.

5.2 Sample matrix assessments and quantities for the telecommunication domain

Once the tables have been filled in by operators, an analysis of correlations and relationships can be completed, using many of the tools mentioned in Sect. 5.1.1. The results below include a correlation matrix, or a bubble chart, as



Threats (hazard list)

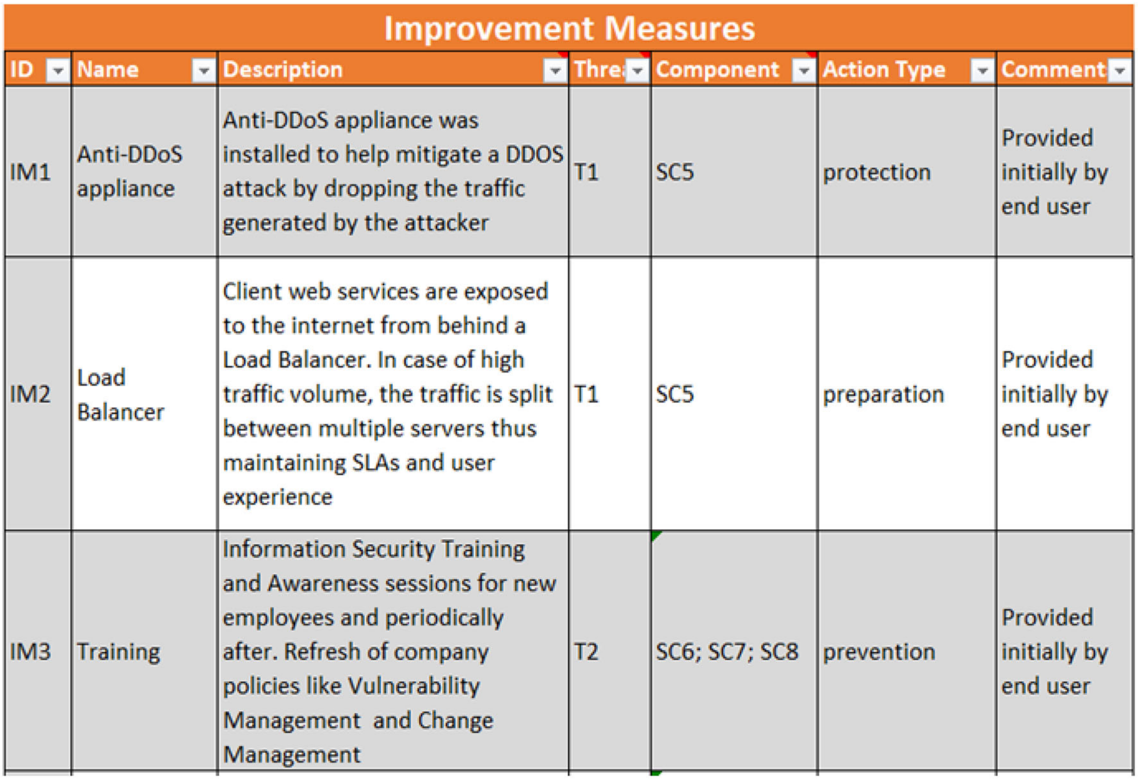
ID	Name	Description	Hazard type	Hazard cause	Frequency	Duration	Economic impact	Impact on society	SCs affected directly	SCs affected indirectl	SFs affected	Subsystems affected
T4	Weather Hazard	Strong winds and rain affecting the power supply to several BTS/BSC sites	physical	natural	modest: several per year	150+ hours	low	low	SC9	SC2; SC3; SC4; SC10	SF1; SF2; SF3; SF4; SF5	Optical Network, Radio Network
T5	Routing Table Poisoning	"A modification of the routing table(s) of network equipment used (both fixed and mobile) that re-routes legitimate traffic from legitimate destination(s)"	cyber	man made (attack)	modest: several per year	Variable: minutes to tens of hours	medium	low	SC3	SC1; SC5; SC10	SF1; SF4	Core Network
T6	Botnet	"communication between infected end-points inside network's security perimeter to a known command and control (C2C) server used by a Bot Network"	cyber	man made (attack)	rare: ≤ 1/year	Variable: minutes to tens of hours	low	high	SC7	SC6; SC11	SF6	Internal Network

Fig. 4 An example of the threats provided for the sample use case and their assessments

described in Sect. 5.1, and a risk matrix plot, also described in the previous section. These results were then shared with the operators.

The correlation matrix, Fig. 6, depicts the relationships between the threats and the performance functions. The circles of dark blue are the more critical combinations, meaning these combinations should be further investigated in the resilience cycle. For example, the relationship between power outages and voice services has a very dark circle indicating a critical combination. The rest of the steps in the resilience management cycle, such as the simulations and resilience quantification, would focus on this relationship. The simulations would have voice services as a performance function and a power outage as the simulated threat.

To get a better idea of the most relevant threats, the threats are ranked with the following equation, where EI is the economic impact, SI is the social impact, and FQ is the frequency of the threats. All of these attributes are defined by the experts in the threats table (Fig. 4). Each of these attributes is originally defined on a scale (low, medium, high) which is then transformed to numerical values. Depending on which aspects of the threat are most relevant for the particular inquiry, the equation to calculate the risk and resilience score may be adjusted:



Improvement Measures

ID	Name	Description	Threa	Component	Action Type	Comment
IM1	Anti-DDoS appliance	Anti-DDoS appliance was installed to help mitigate a DDOS attack by dropping the traffic generated by the attacker	T1	SC5	protection	Provided initially by end user
IM2	Load Balancer	Client web services are exposed to the internet from behind a Load Balancer. In case of high traffic volume, the traffic is split between multiple servers thus maintaining SLAs and user experience	T1	SC5	preparation	Provided initially by end user
IM3	Training	Information Security Training and Awareness sessions for new employees and periodically after. Refresh of company policies like Vulnerability Management and Change Management	T2	SC6; SC7; SC8	prevention	Provided initially by end user

Fig. 5 Excerpt from the improvement measures defined by operators for the sample use case

$$Score = (EI + SI)FQ. \tag{4}$$

When inspecting Eq. (1) introduced above, it can be inferred that Eq. (4) is a special case that incorporates within the economic and societal impact the costs of response and recovery and any improvement measures. The users decided not to separate risk control and resilience generation cost assessments. However, it was ensured that they considered the costs until full recovery of threats and disruptions, in particular of more frequent ones.

In Fig. 7, the score can be seen in green. Each of the threat attributes that corresponds to the specific threat score can also be seen: frequency (FQ) in light blue, social impact (SI) in dark blue, and economic impact (EI) in black. The threats are ranked from the highest score to the lowest. The highest-ranking threat is a DDoS attack; this is logical as it has the largest frequency. Threats considered include fiber optic (FO) infrastructure cuts, power outage in mobile switching center (MSC) sites, and many more, see the y-axis labeling of Fig. 7.

Finally, the threats can be organized in a risk matrix plot. For an introduction to risk matrix plots, see Sect. 5.1. Within this matrix, the threats are positioned corresponding to their economic impact and frequency considering all resilience cycle phases. A high economic impact and a high frequency results in the red zone. Most of the threats for this particular use case fall in the green zone, indicating they are low risk hazards. DDoS attacks, however, fall into the orange zone, indicating that this threat should be mitigated. As the economic impact is already low, this can be done by reducing the frequency. The hazard matrix is another way to organize the threats to determine which ones need to be further addressed.

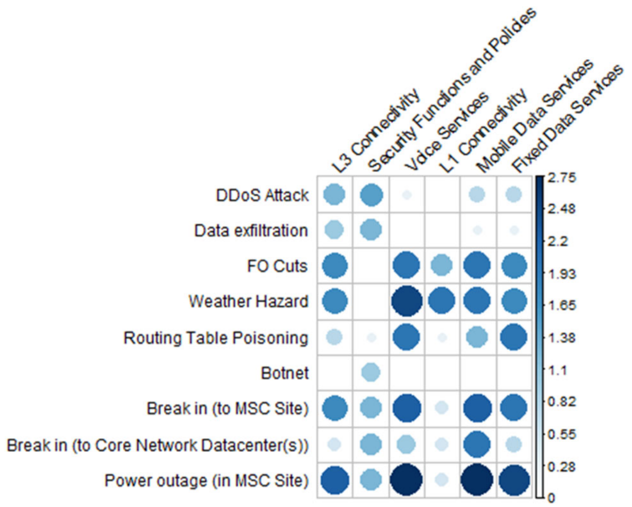


Fig. 6 The correlation matrix for the threats and the system functions. The bubble size and color give the measure of criticality. The bubbles that are dark blue and larger indicate a more critical combination

Once the results were shared with the operators, the discussion centered around the accuracy of the results. For example, in Fig. 8, the highest-ranking threat is a DDoS attack. However, this is a common attack that the operators expect to occur. Therefore, the operators have mitigation measures in place to prevent or reduce the damages of an attack of this type. These mitigation measures are not considered within the threat ranking or hazard matrix. In this sense, the threat analyses do not give very clear answers on which threats need to be further investigated, as the ones that rank highly may already be very well covered by mitigation measures.

5.2.1 Simulation supporting tabular and matrix assessments for the telecom domain

To determine the impact of the implementation of improvement measures, the analysis is run again. To do this, the values in the spreadsheet tables are updated. For a DDoS attack, an improvement measure would be an anti-DDoS appliance. When this improvement measure is incorporated into the analysis, the frequency of DDoS attacks decreases. This change in frequency can be seen in Figs. 9 and 10. While a DDoS attack is still ranked the highest, it is no longer in the orange region in the hazard matrix. For a data exfiltration, the improvement measures of more training, governance, and alerts can reduce the economic impact of the attack. When improvement measures are incorporated, the attack has a smaller impact, and data exfiltration also changes position in the hazard matrix. This change is also evident in Figs. 9 and 10.

To see the effects of the improvement measures more clearly, a simulation was completed, the results of which can be seen in Fig. 11. This simulation highlights how improvement measures taken against a DDoS attack can have an effect on the repair time and/or the probability of an attack. The best results occur when improvement measures affect both the repair time and the probability of attack (see the green line in Fig. 11). For more details about the simulation, see Fehling-Kaschek et al. (2020).

As seen from the analysis output, much analysis is completed based on the tables. Already only halfway through the resilience management process and clear information has been uncovered regarding the relations of components, system functions, threats, and improvement measures. The most critical combinations are determined, with the results setting the stage for the latter half of the resilience management process, during which implementation and the analysis of counter and improvement measures take place. It was shown that even before detailed risk and resilience simulation and quantification takes place, the main issues and expected improvements, at least

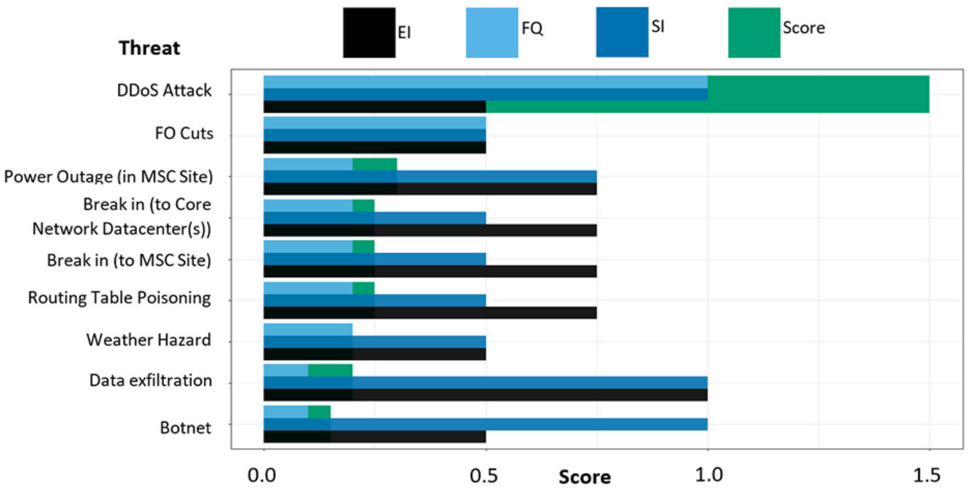


Fig. 7 The threat ranking for the use case. A score is calculated for each threat that incorporates the economic impact, the frequency, and the social impact. All scores are measured on the same scale

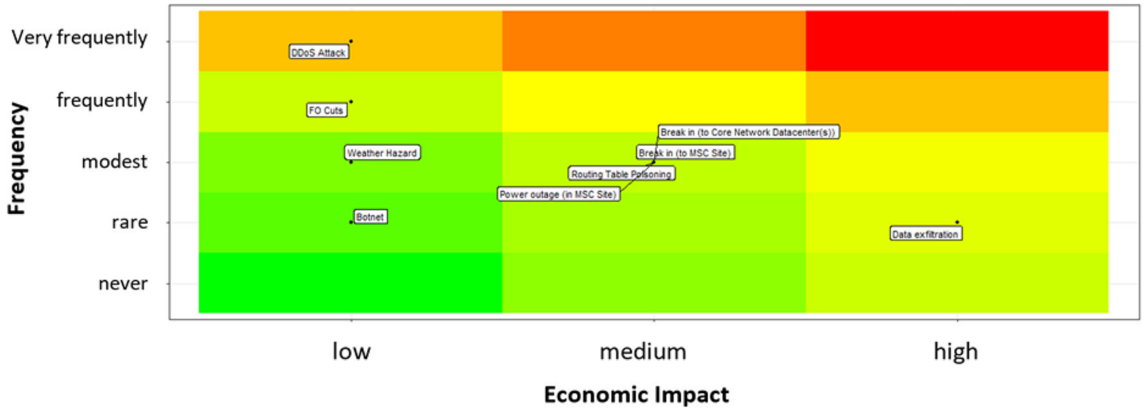


Fig. 8 The hazard matrix for the different threats. This hazard matrix is based on frequency and economic impact; however, the matrix can also be created with the social impact or with a combination of these impacts

within this telecommunication sample case can be identified.

In addition, the application case showed how more detailed tabular as well as numerical assessments allow for a more accurate determination of the level of risk control of and resilience to identified threats and disruptions. Such analysis was also shown to be useful for the selection of countermeasures and improvement measures. In particular,

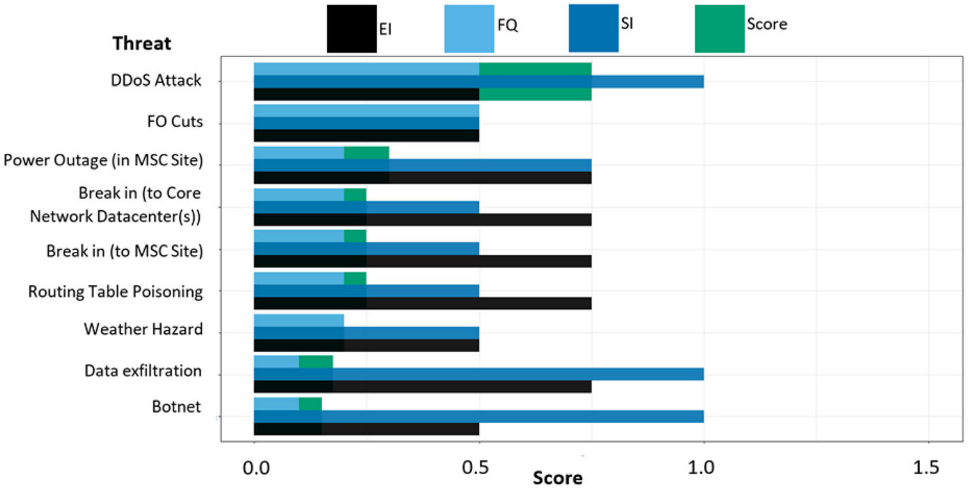


Fig. 9 The new threat ranking with improvement measures incorporated for a DDoS attack and a data exfiltration attack. A score is calculated for each threat that incorporates the economic impact, the frequency, and the social impact. All scores are measured on the same scale

in the example given, the detailed analysis of the DDoS attacks confirmed the tabular analytical assessment of the effects of countermeasures (see Figs. 9 and 10).

This example shows how to conduct tabular overall risk and resilience assessment (Step 6) and resilience acceptance evaluation (Step 7) of the risk and resilience management process, as well as demonstrating the selection of improvement methods (Step 8), see Table 1, respectively. This example also illustrates how to design overall risk and resilience assessment and improvement measure selection matrix tables (as according to Table 2).

5.3 Gas grid

5.3.1 Assessments and quantities accessible for gas grid

In the case of the gas network, based on the input data of Sect. 4.2 as detailed in Table 3, using only tables and matrices, at least the following assessments are accessible:

- Prioritization and categorization of regulatory, organizational and operational requirements for gas grids with focus on security and safety systems;
- Identification of stakeholders for given business cases and requirements;
- System function prioritization in terms of fulfillment of requirements;
- Identification of system components necessary for system functions;
- Threats prioritization taking account of several resilience dimensions (considering all system functions);
- Identification of critical combinations of system functions and threats;
- Security system functional and technical requirements prioritization;
- Identification of system components necessary for fulfillment of security system functions;
- Coverage of user requirements by security system functions;
- Threats countered by security functions;
- Key performance indicators (KPIs) to quantify requirements for security system functions.

In Sect. 5.2.2 for some of the assessment sample, tables and matrices are provided.

5.3.2 Sample tables and matrices for gas grid

Table 6 shows the legal and regulatory, organizational and operational requirements for security- and safety-related systems of transmission gas grid networks, prioritized from an end user and stakeholder perspective. It gives examples for selected representative highly prioritized requirements. Regarding regulatory and legal requirements, further examples include EU Directive 2004/67/EC, Council Directive 2008/114/EC, EU Regulation 2009/715, EU Regulation 2010/994, EU Regulation 2016/67, EU NIS (network and information security) Directive 2016/1148 as well as the Charter of fundamental Rights of the European Union 2010/C 83/02 (SecureGas D1.1 2019). Example for national regulations is the Italian Law No. 481/1995 covering competition rule compliance of utilities services.

For organizational requirements, one examples is given in Table 6. The security management systems is also asked to operationally align with the standards ISO 9001 ISO 14001 ISO 22301 ISO 22396 ISO 27000 ISO 31000 and ISO 55000 and covering in particular asset management, risk control, and business continuity best practices. Also, organizational requirements are formulated regarding management systems for pipeline integrity, IT security, emergency/disaster, life cycle, operations integrity, and asset integrity, including operation within the context of the operation and maintenance manual and the crisis manual.

Operational requirements cover a wide range, see Table 3 for an overview, see row 9. Categories identified comprise beyond the six examples within Table 6:

- Confidentiality, data protection, and safety (CONF), e.g., software and hardware secure, safe and resilient, authentication and authorization, encryption;
- Conditions (COND), e.g., “plug and operate” for example when relocating and adding new sensors, various/all threats, flexible with respect to legacy and new system elements, different extensions of facilities from 1 km to 1000s of kilometers, resource scalability;
- Interoperability (INTER), e.g., with existing systems, generating output for existing systems, interoperability with mobile device, operational interoperability;
- Detection, situational awareness, and decision support (DSD), e.g., cyber threats/attacks, landslide hazards, intrusion and motion detection, third-party interference detection, leak detection, drone detection, fire/heat/explosion detection, asset manipulation, alerting, alert confirmation, accuracy of detection localization, risk level of event generation, decision support and action recommendation, sharing information with the public, simulation capability, compliant storage of supervision data, manual alert, detection of non-available subsystems/sensors;
- Usability (USA), e.g., user friendly, multilingual interface, maintainability of security system, modularity, accurate information, replaceability/back-up, short recovery time/ less than a couple of hours, high availability, training;
- Information management (INFOR), e.g., information filtering based entity involved, filtering based on

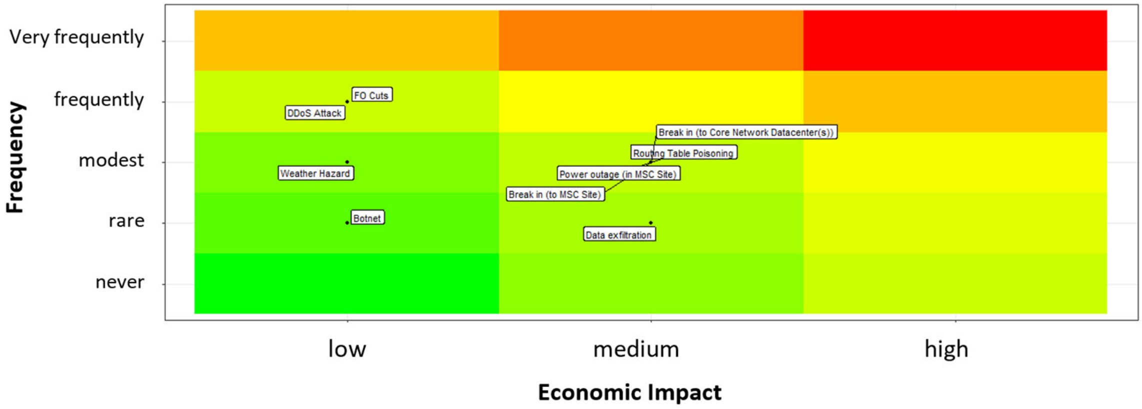


Fig. 10 The new hazard matrix for the different threats with improvement measures incorporated for a DDoS attack and a data exfiltration attack. This hazard matrix is based on the frequency and economic impact; however, the matrix can also be created with the social impact or the combination of the economic and social impacts

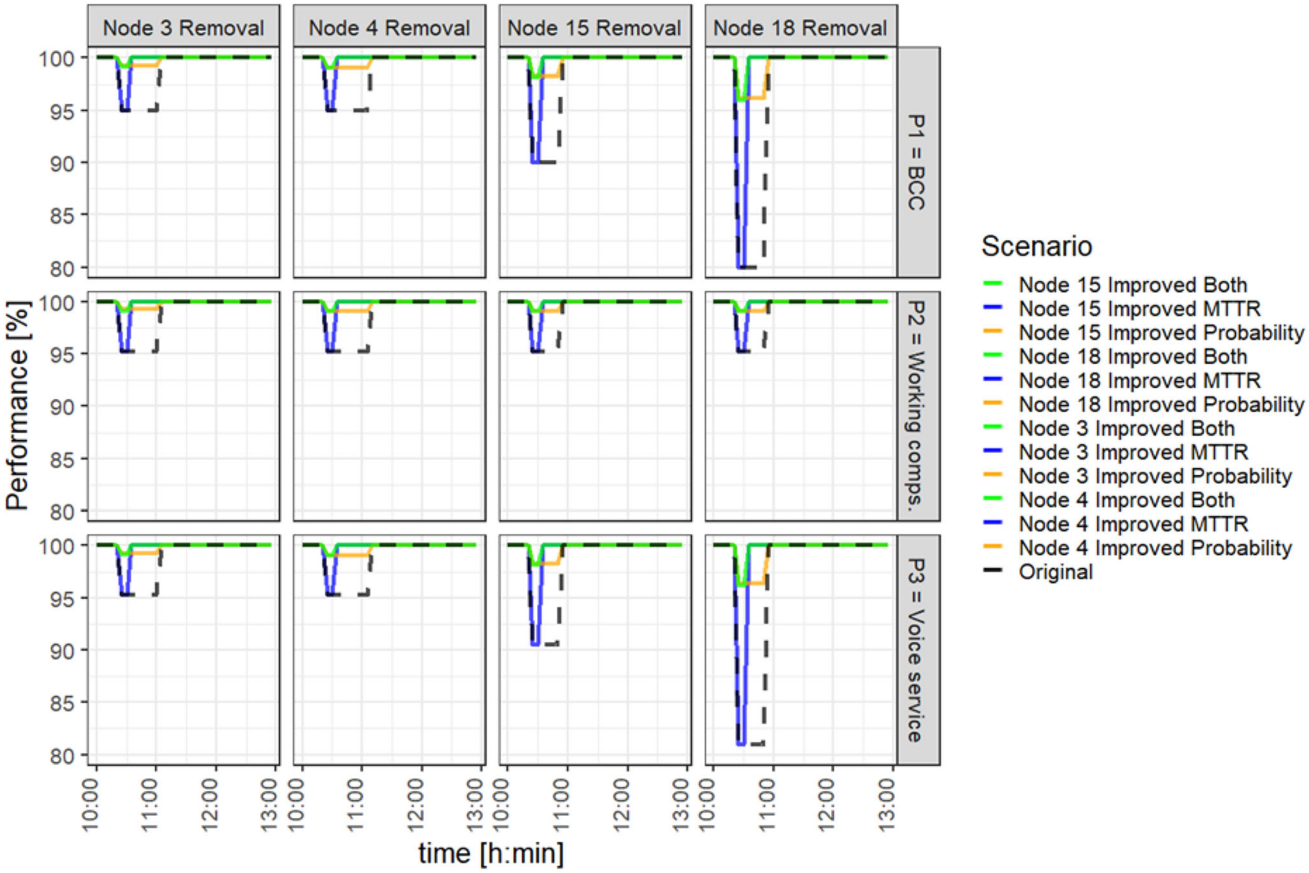


Fig. 11 Simulation of a DDoS attack with improvement measures included. Improvement measures can either improve the mean time to repair or the probability of occurrence or both; see the blue lines, orange lines, and green lines, respectively. The original curve is a dashed black line. The analysis considers the removal of 4 different representative nodes of a telecommunication grid consisting of about 20 nodes. The effect of the removal is shown for three cases: the effect on the most important connected component; on all working components; and on the voice services of the overall system

Table 6 Examples of legal/regulatory, organizational and operational requirements

Type of requirement	Category	Code	Title	Description	Priority Level
Regulatory	EU Legislation	RE-EULEG-02	EU Regulation 2017/1938	The security system should comply with the principles of the EU Regulation 2017/1938 concerning "measures to safeguard the security of the gas supply and repealing Regulation (EU) No 994/2010"	High
Organizational	International Standards	OR-STAN-06	ISO 22301	The security system should operate within the context of the ISO 22301 on Business Continuity Management Systems and should not affect its implementation	High
Operational	Detection, situation awareness, and decision support	OP-DSD-12	Risk level of events	The security system should provide information on the risk level of the various physical and cyber threats targeting end users' network	High
Operational	Usability	OP-USA-07	Recovery time	The system recovery should be fast (i.e., within a couple of hours)	High

importance/criticality, based on response level, information classification and categorization, combination of security management data with other data such as maps, CBRNE risks, exposition, weather forecast, event register, incident reporting; and

- Cost (COST), e.g., cost efficiency and low after-sales service costs.

Examples for management systems include Pipeline Integrity Management System, Safety Management System, Security Management System, Emergency/Disaster Management System, Life Cycle Management System, Operations Integrity Management System, Asset Integrity Management system, Operation and Maintenance Manual for Natural Gas Distribution Networks, and Crisis Manual for Natural Gas Distribution Networks.

In total 79 requirements, consisting of 15 legal and regulatory, 16 organizational, and 48 organizational requirements, are prioritized using the three categories high (absolutely needed), medium (important), and low (interesting) (SecureGas D1.1 2019). They are used together with technical requirements and threat criticality assessment to prioritize system (resilience) functions.

Table 7 shows sample entries of gas security and safety non-performance functions. Other examples of mainly non-performance system functions include (SecureGas D2.3 2019) the number of unauthorized interferences with pipeline; number of leaks; number of damage events due to operator failure; number of validated or non-validated security threats or alarms; number of attacks to various IT devices; pipeline temperature; average time to complete tasks; mean times to detection, to appearing in control system, to response and to repair; downtime and availability of pipeline sections, nodes and consumer supply at main nodes; number of unplanned stops; times allocated to training, administration and management; delayed works of repair or renovation; amount or ratio of valves' remote control; cost benefit ratio for prevention and for mitigation; cost per incident; and operational cost.

According to the legal, regulatory, organizational, and operational requirement to cover all threats, a further prioritization option of technical requirements is the assessment of the level of risk control and resilience achieved regarding known threats and potential disruptions. To this end threats are categorized into 12 categories and 98 subcategories or threat event types, see in Table 3 the corresponding lines. Using 5 resilience dimensions with in total 26 attributes and a semi-quantitative scale, the level of coverage of threats by current best-practice transmission grids can be assessed. Table 8 shows for sample threats high-ranking resilience dimensional attributes.

Table 9 shows examples assessing several combinations of gas system non-performance functions and threats or disruptions based on inputs of Tables 6, 7, and 8. In addition, requirements for technical improvement measures and related functional key performance indicators (KPIs) are added, which are further detailed in Tables 10 and 11. In Table 9, for brevity only the titles of each entry are given without further resolution regarding ID-coding of the entities and further classifications as detailed in Table 3 (see column with label 4).

Technical requirements cover mainly within operational requirements contexts qualitative and quantitative descriptions of additional system functions and resilience functions that are expected to support the risk control and resilience enhancement of gas distribution systems. According to Table 3, a ranked listing and coverage assessment of user requirements as given in Table 10 is feasible. In addition, as listed in Table 3, the complete coverage of all user requirements can be assessed by listing for each user requirement the technical requirements that contribute to its coverage.

Table 7 Sample gas security system non-performance functions and related gas infrastructure components

System non-performance function title	Asset management phase; and sub-phase	Gas infrastructure main components	Gas infrastructure sub-components	Code	User requirements covered
Number of pipeline damage incidents; Number of pipeline near-miss incidents; Number of pipeline incidents that have not yet been detected	Operation and maintenance (O&M); Evaluate and Plan (E&P);	Transport and distribution (TRANS)	Pipelines	O&M-TRANS-01-001, -002, -003	E.g., RE-EULEG-02, OP-DSD-12
Number of IT devices infected by viruses or harmful software within gas transmission system	Operation and maintenance (O&M);	automation control and safety systems (ACSS)	All components in ACCS with software	O&M-ACCS-01-001, O&M-ACCS-02-001	E.g., OP-USA-07

Table 8 Sample threats/disruptions and how they are assessed using resilience dimensions and attributes

Threat category	Threat event type/sub-category	Code	Description	Example 1 Resilience dimension, resilience attribute, semi-quantitative assessment	Example 2	Example 3
Cyber (CYBER)	Botnets	CYBER-07	Botnet attack to comprise network components and connections	Dimension: Cyber-physical distinction; Attribute: cyber; Semi-quantitative Rating: very high (most affected category)	Dimension: Persons affected; Attribute: operator in control room; Semi-quantitative rating: Very high (no access to components)	Dimension: technical resilience capabilities; Attribute: sensing/surveillance; semi-quantitative rating: very high (loss of capability)
Ground Works (GW)	Third-Party Interference (TPI)	GW-01	Mechanical damage of pipeline during ground works	Dimension: System layers; Attribute: physical–mechanical; Semi-quantitative Rating: very high (most affected layer)	Dimension: 5-step risk management process; Attribute: Risk analysis; Semi-quantitative rating: Very high for frequency and consequences (very high risk)	Dimension: Resilience cycle; Attribute: Response; semi-quantitative rating: very high (response is crucial)
Operation and Management (OM)	Incorrect operation	OM-04	Incorrect operation/process hazards (accidental or intentional)	Dimension: System layers; Attribute: organizational; Semi-quantitative Rating: very high (most affected layer)	Dimension: Resilience cycle; Attributes: Preparation; semi-quantitative rating: very high	Dimension: Technical resilience capabilities; Attribute: detection/surveillance; rating: very high

In total, 7 technical requirement types with in total 148 sub-types were considered, to cover all user requirements, see Table 3 for an overview.

Combining technical requirements with key performance indicators (KPIs) allows a quantification of the improvement measures as input for security system specifications and developments. To this end for each technical requirement domain, e.g., requirements related to UAVs functionalities or to blockchain, see Table 10, for each requirement type relevant, e.g., functional or interface, indicators are described along with a metric and a target value. Again, respectively Table 3 gives an overview on the different entry types. In this way, 78 indicators are defined which belong to 49 fields of indicators that are related to 12 technical domains of security systems, see Table 11 for example entries.

5.3.3 Sample assessments and quantities for gas grid

The main goal in the application of the tabular approach for the gas grid application are a ranking of technical requirements for several technical domains that were refined during the application of the approach for advancing gas security and safety systems countering cyber-physical threats. To this end, user requirements are ranked (see as example Table 6) as well as system non-performance functions (Table 7) and threats (Table 8). In addition, critical combinations of system performance functions and potential threats and disruptions are assessed (Table 9). This allows a ranking of security system technical functions (Table 10), including the provision of quantitative KPIs (Table 11).

The overview and discussion of assessment options along with Table 3 and in Sect. 5.2.1 show that already 6 tables and matrices are sufficient to achieve the main goal for the application case gas grid.

5.4 Indoor localization system

5.4.1 Assessments and quantities accessible for indoor localization system

Based on data collected according to Table 4, the following assessments are accessible:

- User and stakeholder listing and ranking;
- System analysis in terms of subsystems and components;
- Identification of system functions and technical functions subsystems and components involved;
- Ranking of system functions and related technical functionalities;
- Overall disruption, failure, and disturbance categorization and ranking;
- Criticality ranking of combinations of system functions and disruptions;
- Ranked list of tentative experiments to assess critical combinations (critical scenarios);
- Experimental assessments of critical combinations;
- Overall risk control and resilience assessment of critical combinations;
- Ranked list of improvement options based on experimental results;
- Relevancy of improvement options for system functions, technical functionalities, subsystems and components.

For each critical scenario, experiments can be repeated to generate representative resilience answers of the system. As an example, for the main non-performance measure time-dependent absolute localization error a quantitative assessment can be obtained in the following way. First, for each distinct disruption scenario the types of resilience answers are identified. Second, for each resilience answer type, phases of the answer type are identified. Third, for each resilience response answer phase quantities are extracted from the non-performance function to characterize the phase quantitatively. For instance, in the absorption phase high resilience in the present case can be defined to be related to a small increase of the localization error. It should occur in a short time when compared to the time scale the user needs for applications to avoid too long latency of response of the localization system to disturbances.

Let $i = 1, 2, \cdots, N_{\text{event}}$ be the number of different event types, N_{ij} be the number of phases considered for each event type and

$$q_{ijk} = \begin{cases} \Delta t_{ijk}/\Delta t_{ijk}^{scale} \\ \Delta q_{ijk}/q_{ijk}^{scale} \\ m_{ijk}/m_{ijk}^{scale} \\ A_{ijk}/A_{ijk}^{scale} \\ \cdots \end{cases} \tag{5}$$

for $k = 1, 2, \cdots, N_{\text{ijk}}$ be the number of dimensionless quantities considered for each phase of each event type to assess the risk control and resilience achieved for each event type. The sample quantities given in (5) use measures for time duration, for difference of the (non) performance function, for slopes and for areas of performance loss, respectively, measured in scales relevant for the event type and phase considered, e.g., the time scale Δt_{ijk}^{scale}, etc. For each quantity, it can be decided if it should be minimized or maximized for overall risk control and resilience. A total measure of resilience then reads

$$R_{\text{tot}} = \sum_{i=1}^{N_{event}} P_i C_i = \sum_{i=1}^{N_{event}} P_i \prod_{j=1}^{N_{ij}} \prod_{k=1}^{N_{ijk}} {q_{ijk}}^{a_{ijk}}, \tag{6}$$

where P_i is the probability (frequency, likelihood) of an event type, C_i is a measure for its consequence, $a_{ijk} = 1$, if the quantity should be minimized (using direct proportionality) and $a_{ijk} = -1$, if the quantity should be maximized (using indirect proportionality).

In Eq. (6), instead of the multiplicative measure for each event type also an additive measure or a logarithmic measure could be used. In the former case, the last two multiplication operators are replaced by sums in Eq. (6). In the latter case, in addition a logarithm is applied to the addends. In the example application for the use case localization system, Eq. (6) sums over threat events already identified as critical for all system performance functions and could be further resolved according to Eqs. (1) and (2).

Table 9 Examples for critical combinations of system non-performance functions and threats

System non-performance functions	Threat event type	Criticality ranking	User requirement	Technical requirement	Functional KPI
Number of non-detected (minor) leaks; number of minor leaks (known); number of major leaks;	Corrosion; third-party interference (accidental); geohazard issues;	6 (very high)	Leakage detection	leak detection with sensors onboard UAV; simulation-based leakage detection; landslide hazard detection with Video and IR onboard UAV; laser-fiber-based pipeline damage detection; alerting system	Leak alert function sensitivity; leak location accuracy; leak detection reliability; coverage of different threat types
Number of cyber-attacks directed to company's IT systems; damage made due to human factor by IT system administrators; valves' non-availability for remote control during one-year period; amount of valves ' remote control failures during one-year period	Cyber-attack; physical access to SCADA system; IT failure caused by personnel	6 (very high)	Detection of non-authorized access or remote cyber-enabled steering of valves	Detection of potential cyber threats, such as attacks on SCADA and other control systems; Provision of decision support and recommendation service to operator in order to mitigate the effect of a cyber-attacks; Adoption of communication protocols/ whitelisting mechanisms that perform the authentication of the authorized devices inside the system in order to avoid spoofing attacks; Blockchain for data transmission and integrity verification mechanism	Reliability of issuing blockchain keyless signature Infrastructure (KSI) (short delay); Reliable verification of data protection to assure data integrity; Privacy of input data when using KSI blockchain; high service availability when using KSI blockchain; coverage of different types of cyber events; high precision and recall of cyber events detected; short time to detection; new host detection within SCADA system; SCADA protocol identification;

5.4.2 Sample tables and matrices for indoor localization system

Users and stakeholders main groups identified include actual users often without any technical background, persons responsible in teams for the use of localization systems that are interested in simple instructions and seamless operation, technical staff interested in efficient maintenance, and management persons interested in data-driven digital production or service process optimization, see the categories given in Table 4.

Regarding system service functions, the main functions turned out to be cost-efficient coverage of areas or volumes and low localization error sufficient for the application context, typical in the order of decimeters. For instance, the concept of localization error visualization was assessed to be rather complicated for many applications. Similar arguments were given against prioritizing other system performance measures very high as listed in Table 4.

Based on the table of ranked system performance functions, ranked potential disruptions, and mainly the matrix of critical combinations of system functions and disruptions, Table 12 of experiments was generated to experimentally assess the criticality of scenarios.

5.4.3 Sample experimental resilience assessment quantities for indoor localization system

For the sample experimental assessment, the probabilities in Eq. (6) can be estimated. All other quantities in (6) are extracted from experimental data on system response regarding critical disruptions as identified in Table 12. Figure 12 shows how barriers at different positions for given tag position affect the localization error. The localization error increases from ca. 10 cm up to significant fractions of a meter and even several meters if several receivers are covered.

Figure 13 shows the assessment of all sample disruption scenarios using the total resilience measure defined in (6). Three different measures are used. The last two clearly identify 5 scenarios as critical. In all cases, the 7-th experimental scenario is assessed as most critical. The three measures according to (6) can be distinguished as follows: (1) uses all options namely scaled time durations, performance ratios to measure performance change before and after disruptions, scaled slopes and scaled total performance loss area; (2) uses scaled time differences, performance ratios and areas; and (3) uses only scaled performance loss area. In summary, the last risk control and resilience measure for event types was for the shown

Table 10 Sample technical requirements and how they cover the legal, organizational, and operational risk control and resilience enhancement requirements

Technical requirement category	Sub-category, Title	Type	Code	Description	Application/ Business case covered	User requirements covered
Decision Support System (DSS)	Simulation capabilities	Functional (FUN)	DSS-FUN-09	Attack simulation, Assessment of countermeasures (in all resilience cycle phases), optimization of countermeasures	All	OP-DSD-15
Gas network simulation (GNS)	Simulative leakage identification and plausibility of sensor data	FUN	GNS-FUN-06	Identification of leakage size and location by comparing sensor data with simulation results	All	OP-DSD-15, OP-DSD-05, OP-USA-07
GNS	Risk control and resilience analysis capability	FUN	GNS-FUN-02, GNS-FUN-04	Overall risk control estimate in terms of frequency of event estimate and damage effects computation of single and multiple events taking into account counter, response and recovery measures	All	OP-DSD-15, OP-USA-07

Table 11 Key performance indicators (KPIs) fur improvement measures (security system)

Technical requirement domain	Requirements dimension/type	KPI field	KPI indicator	KPI description	Metric	Target value
Unmanned Aerial Vehicle (UAV)	Functional (FUN)	Alert	Landslide hazard	Time to provide notification to the user in case of possible slope instabilities	hours	< 12
Blockchain for data transmission and integrity verification mechanisms	FUN	Data integrity	Reliability	Blockchain issues KSI signatures that enable the properties of data to be verified; Verifying data properties to assure data integrity	Time (sec)	< 2.0 < 0.02
As above	Interface (INTER)	Availability	Access to service	When using KSI blockchain the service availability is 99,95%	Time not available per year (min)	< 263

example the most robust one. However, the second was more sample specific. The first introduced terms that diverged without being related to major application specific implications.

The assessment of the criticality of the events can be used to conduct (minor) design changes and in particular localization algorithm changes for given geometries. In the present case, for instance the rate of localization updates was increased, the influence of past positions was decreased, and a software flaw was removed that disturbed the switching on and registration of tags.

As the probability of scenarios strongly depends on application contexts, e.g., localization of material for production versus localization of customers in restaurants, the sample experimental quantifications, as identified to be relevant using the tabular and matrix approach in Sect. 5.3.2, are conducted focusing on different scenarios only. If different design options are compared, it is found to be favorable to use the total measure of risk control and resilience as given in Eq. (6) using all known potential disruption scenarios with estimated probability factors.

6 Recommendations, practical implementation proposals, and managerial insights

The presentation of the approach shown here provides direct implementation guidance by providing well-defined process steps and supporting tables for each step. For implementation, the following tabular framework is deemed sufficient (see also the bold-typed tables and matrices in Table 1), and recommended for practical implementation:

- Generation of the table of process steps, which should include process step names, objectives, and approaches used, and in particular supporting tables and matrices. They can be based on Fig. 1 and Table 1 which contains a superset of tables to be used.
- Generation of a master table as provided for the application examples in Tables 2, 3, and 4, where duplications should be carefully avoided and similar entries should be systematically reused.
- Filling of tables as planned within a spreadsheet application or using a computer algebra and statistics package such as R and the shiny package (Chang et al. 2019) as used in the first application example. See examples in Sects. 5.1.2, 5.2.2 and 5.3.2.
- Evaluation of tables as discussed for the examples in Sects. 5.1.3, 5.1.4, 5.2.3, and 5.3.3.
- Executive verbal summary and evaluation of overall risk reduction in terms of classical risk control and resilience improvement.

Main advantages of the presented approach from a practical management perspective include that it consists of an iterative generation and updating of tables and matrices that do not require demanding methodologies and tools per se. Furthermore, the joint risk control and resilience analysis and management process has been shown to be conformal with ISO 31000 (Häring et al. 2017a). This facilitates from a management perspective to identify responsible persons, as ISO 31000 and related standards are by now well established.

The tables and matrices are capable to summarize and to include existing in-depth analyses as well as to identify the need for further such assessments and quantifications, see Sects. 5.1.4 and 5.3.3 for examples. Thus, a further main advantage is reducing the overall effort by requiring for most cases only concise and well-documented expert assessment instead of resource-intensive risk and resilience quantification. From a management perspective, the summarizing capability is well suited for overall steering and control of resources deployed.

A further advantage is that the tabular and matrix approaches are well established in terms of different types of (preliminary) hazard analyses, HAZOP, and FMEA-type assessments, see, e.g., Ericson (2016) Crawley and Tyler (2015), Tietjen and Decker (2020), and Carlson (2012). Thus, the approach builds on known and lived practices, often only by addition of additional columns, see the examples given in the application cases. Further general arguments for the suitability of the analytical approaches are given in Häring and Gelhausen (2018).

The approach enables management stakeholders to consider business-relevant systems and business cases including already implemented risk control and improvement options. For such systems, they can identify already existing risk control and resilience measures that have not yet been considered so far (including potential implicit approaches) as well as identify the need for further security and safety systems. Both applications can be used to document compliance with standards. In addition, the approach is capable to generate technical specifications of improvement measures and related KPIs, see the use case gas transmission network.

A most concise summary of the criticality of threats is the pre-assessment of the criticality of combinations of system performance functions and (multiple) threats as required in Step 5 of Fig. 1 taking into account all options

Table 12 Sample critical combinations of system function and disruptions

System (non) performance function	ID and title of disruption experiment	Disruption description	Semi-quantitative assessment before experiments	Semi-quantitative assessment after experiments
Absolute localization error	EXP-01, Switch on of tag (receiver)	Switch on of ultrasound transmitter at position 1	2	6
As above	EXP-02, Person movement around static tag	Person orbiting 12 times around position 1	4	5
As above	EXP-03, -04, -05, -06; Barrier in line of sight between tag and receivers	Barrier at $y = -0.7$ m; barrier at $y = +0.7$ m; barrier at $x = +0.7$ m; barrier at $x = -0.7$ m	6, 6, 6, 6	1, 1, 6, 10
As above	EXP-07; Tag movement	Transport from position 1 to position 2	3	5
As above	EXP-08; Person movement around static tag	Person orbiting 12 times around position 2	4	5
As above	EXP-09, -10; Switch off and on of tag	Switch off and on of transmitter	2	6

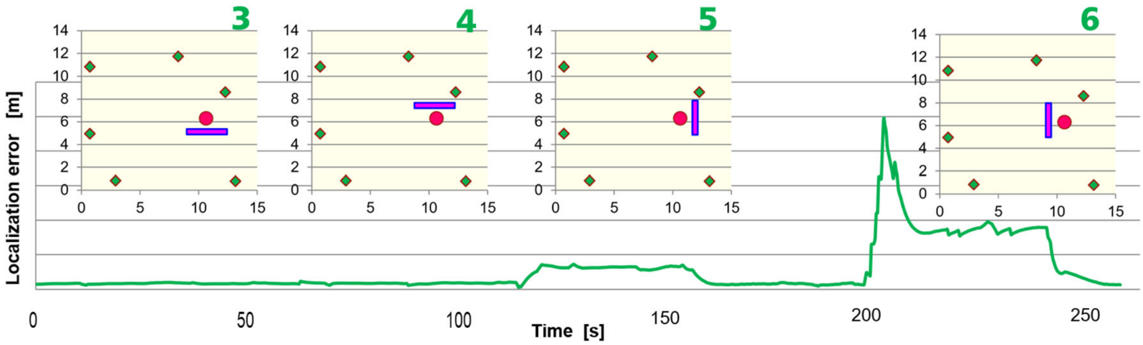


Fig. 12 Example absolute experimental localization errors for disruption scenarios that ware assessed as potentially critical

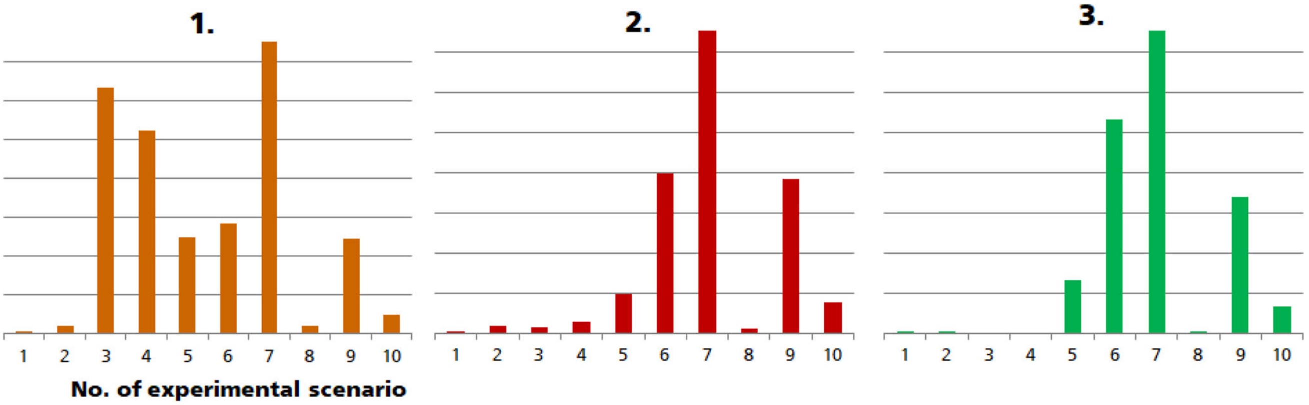


Fig. 13 Three different normalized measures of consequences of lack for risk control and resilience for each experimental scenario of Table 12

of risk control and resilience improvement by different resilience concepts and respective resilience dimensions and attributes, see Sect. 2. Within further iterations, this assessment takes up more quantitative results of Step 6. Thus, it provides a matrix of the level of criticality of events to business services that is well suited for the evaluation at management level in Step 7. In particular, it allows management to identify risks to key system service functions as relevant from business perspective and key threats to such services.

7 Conclusions

This paper confirms that tabular and matrix approaches within the process framework of traditional risk management, such as the hazard list, hazard analyses, and FMEAs, have substantially contributed to the success of risk management. We argue that tabular and matrix approaches can also be leveraged for performance-based resilience management, which both incorporates and substantially extends traditional risk management. This is reasonable because classical risk control may be defined to focus on successful disruption event avoidance, i.e., extending the mean time to failure, and reducing the initial loss, increasing robustness, and reducing vulnerability, whereas supplemental improvement in system resilience can focus on fast response, i.e., stabilization, fast recovery, and even improvement and learning.

This extension from risk control of components to overall systemic risk management driven by resilience concepts opens new innovative ways to achieve the overall objective of highly available, reliable, resource-efficient, safe, and secure systems. This can be accomplished by, for instance, very fast recovery, short-time redundancy only on demand, and/or reconfiguration while using limited resources.

The material presented in this paper provides process steps, process step objectives, and several tables or correlation (dependency) matrices for each process step, including headings of table columns and of rows for each table or matrix. This work documents how this approach has been implemented for the telecommunication domain, for gas networks and an indoor localization system. In addition, further examples are discussed. A minimum set of tables and matrices to be used has been proposed by providing a master table (Table 1) along with the joint risk control and resilience analysis and management scheme (Fig. 1). For each application, case-specific master tables have been derived (Tables 2, 3, and 4).

The advantage of tabular approaches is demonstrated in terms of qualitative, discrete, semi-quantitative, and quantitative evaluations. It is shown that risk and resilience quantities are available for single threats (e.g., threat ranking in terms of performance functions, of resilience cycle phases, or of system layers affected), for performance functions (e.g., extended risk matrix for all resilience cycle phases), and for overall risk (e.g., overall risk for performance functions, overall consequences of threats, extended and modified risk matrices and FN diagrams). Completeness and consistency requirements can be defined and assessed, as well as convergence effects of the iterative assessment and improvement approach. Due to the highly interlinked nature of the approach, it is also expected that implicit knowledge surfaces, often due to the many dependency matrices generated (e.g., relations between components, subsystems, system functions, and threats).

The present approach shows that it is suitable to identify which system model-based quantitative risk and resilience computations and simulations should be conducted. In addition, it can be used to support the collection of information and data necessary for setting up the models. This was detailed through sample tables and matrices as developed within the EU project RESISTO for critical telecommunication infrastructure or the definition of critical scenarios for experimental determination of resilience of a localization system.

In the application case of the transmission gas grid, it was shown within the EU project SecureGas that the approach is useful to identify improvement measures of security systems countering cyber and physical threats of critical distributed infrastructure. Considering the rich application context, a variety of mainly non-performance functions of gas transmission grids were identified that are sensitive to potential threats. This enabled along with a highly structured threat assessment the identification of functional requirements and related quantitative indicators as well as technical requirements of most promising improvement measures.

The application of the approach to an indoor ultrasound localization system allowed the identification and ranking of its key performance functions and relevant threats. The criticality matrix assessment of system performance functions versus disturbing up to disruptive events lead to the ranking of scenarios for experimental assessment. The quantitative evaluation of the experimental scenarios allowed to identify technical improvement needs and options.

The user experience described in the paper shows that the approach can be applied successfully to real-world implementations. The approach was generally accepted by the end users. In particular, it was found very helpful to structure system knowledge in terms of system elements and functions, to identify threats and disruptions in need of more advanced analytical and quantitative analyses. Additionally, end users found the approach useful for supporting the selection of efficient counter and improvement measures and because it leverages similar analytical approaches as already familiar from classical risk control.

In terms of such generic requirements as, e.g., documentability, reusability, scalability, tailorability, extendability, responsibility sharing and documentation, auditability, certifiability, litigability, insurability, and financeability, in all these cases, high levels can be reached due to the tabular nature. In particular, even check-lists can be generated rather easily based on tabular approaches for application in similar application domains, e.g., for the business continuity and consultancy applications.

Standardization of resilience assessments and its integration under structures that are in use in traditional risk management may be important for solidifying this emerging field. Future studies could focus on closing the methodological gap in quantitative assessments of integrated risk and resilience, especially as it relates to integration of social and physical/engineering science methodology and tools. Last but not least, the approach could serve as one input for standardization in the domain of resilience quantification driven by technical science and strengthening of socio-technical systems.

Funding Open Access funding enabled and organized by Projekt DEAL. The current work has in parts received funding from the European Union's Horizon 2020 research and innovation program projects RESISTO (Grant agreement number 786409: Ivo Häring, Mirjam Fehling-Kaschek, Natalie Miller, Katja Faist, Marco Carli, Federica Battisti, Rodoula Makr, Giuseppe Celozzi, Maria Belesioti, and Evangelos Sfakianakis) and SecureGas (Grant agreement number 833017: Ivo Häring, Sebastian Ganter, Kushal Srivastava, Jörg Finger, Alexander Stolz, Evita Agrafioti, Anastasia Chalkidou, George Papadakis, Clemente Fuggini, Fabio Bolletta, Alberto Neri, and Guisepp Giunta) on cyber-physical security of telecommunication and of gas critical infrastructure, respectively. The work was in parts also supported by a grant from the Ministry of Science, Research and the Arts of Baden-Württemberg as well as supported as Fraunhofer High Performance Center Sustainability through projects covering the topics resilience measures for socio-technical systems and multimodal resilient indoor localization systems (Ivo Häring, Aishvarya Kumar Jain, Georg Fischer, Kai Fischer, Hermann Scheithauer, Fabian Höflinger, Dominik Jan Schott, Christian Schindelhauer, and Sven Köhler).

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

ALOHA (2021) Areal Locations of Hazardous Atmospheres, ALOHA, Software. With assistance of United States Environmental Protection Agency, EPA. Available at https://www.epa.gov/cameo/aloha-software. Accessed on 10 Feb 2021

Aven T (2019) Recent advancements in risk analysis and management. In: Beer M, Zio E (eds) Proceedings of the 29th European Safety and Reliability Conference (ESREL 2019). ESREL. Hannover, Germany, 22-26 September 2019. European Safety and Reliability Association (ESRA). Research Publishing Services, Singapore, pp 1–8

Barker K, Ramirez-Marquez JE, Rocco CM (2013) Resilience-based network component importance measures. Reliab Eng Syst Safety 117(2):89–97. https://doi.org/10.1016/j.ress.2013.03.012

Baum SD (2015) Risk and resilience for unknown, unquantifiable, systemic, and unlikely/catastrophic threats. Environ Syst Decis 35(2):229–236. https://doi.org/10.1007/s10669-015-9551-8

Bean J (2010) Core SOA principles, SOA and web services interface design principles, techniques, and standards. Morgan Kaufmann, Burlington, pp 25–41. https://doi.org/10.1016/B978-0-12-374891-1.00002-2

Berkes F, Ross H (2013) Community resilience: toward an integrated approach. Soc Nat Resour 26(1):5–20. https://doi.org/10.1080/08941920.2012.736605

Bordoy J, Schott DJ, Xie J, Bannoura A, Klein P, Striet L et al (2020) Acoustic indoor localization augmentation by self-calibration and machine learning. Sensors (Basel, Switzerland). https://doi.org/10.3390/s20041177

Carlson C (2012) Effective FMEAs. Achieving safe, reliable, and economical products and processes using failure mode and effects analysis (Quality and reliability engineering series, 1). Wiley, Hoboken

Carvalho R, Buzna L, Bono F, Masera M, Arrowsmith DK, Helbing D (2014) Resilience of natural gas networks during conflicts, crises and disruptions. PLoS ONE 9(3):e90265. https://doi.org/10.1371/journal.pone.0090265

CCPS (2010) A practical approach to hazard identification for operations and maintenance workers. Wiley-AIChE, Oxford

Chang W et al (2019) Shiny: web application framework for R. Version 1.4.0. Available online at https://cran.r-project.org/web/packages/shiny/index.html

CIGRE C4.47 (2019) International Survey on adoption of resilience within the Electricity Sector. With assistance of CIGRE C4.47 Working Group on Power System Resilience. 2019 CIGRE Symposium. Aalborg, Denmark, 4.-7.6.2019. International Council on Large Electric Systems. Conseil international des grands réseaux électriques, CIGRE, Paris

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

Cottam BJ, Specking EA, Small CA, Pohl EA, Parnell GS, Buchanan RK (2019) Defining resilience for engineered systems. EMR 8(2):11. https://doi.org/10.5539/emr.v8n2p11

Crawley F, Tyler B (2015) HAZOP: guide to best practice. Guidelines to best practice for the process and chemical industries, 3rd edn. Elsevier, Amsterdam, Boston, Heidelberg

Dai L, Wang D, Wang T, Feng Q, Yang X (2017) Analysis and comparison of long-distance pipeline failures. J Pet Eng 2017:1–7. https://doi.org/10.1155/2017/3174636

Dancy JR, Dancy VA (2017) Terrorism and oil and gas pipeline infrastructure: vulnerability and Potential Liability for Cybersecurity Attacks. One J 2(6):579–619

EGIG (2020) Gas pipeline incidents. 11-th Report of the European Gas Pipeline Incidence Darta Group (EGIG). Edited by EGIG. Available at https://www.egig.eu/reports. Accessed on 9 Feb 2021

EM-DAT (2021) Emergency Events Database (EM-DAT): The International Disaster Database. Centre for Research on the Epidemiology of Disasters—CRED. Available at https://www.emdat.be/database. Accessed on 10 Feb 2021

ENISA (2020) ENSIA Threat Landscape 2020. Edited by European Union Agency for Cybersecurity (ENISA). Available at https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends. Accessed on 10 Feb 2021

Ens A, Hoeflinger F, Wendeberg J, Hoppe J, Zhang R, Bannoura A et al (2015) Acoustic self-calibrating system for indoor smart phone tracking, ASSIST. Int J Navig Obs. https://doi.org/10.1155/2015/694695

Ericson CA (2016) Hazard analysis techniques for system safety, 2nd edn. Wiley, Hoboken

Fang Y-P, Pedroni N, Zio E (2016) Resilience-based component importance measures for critical infrastructure network systems. IEEE Trans Rel 65(2):502–512. https://doi.org/10.1109/TR.2016.2521761

Fehling-Kaschek M, Faist K, Miller N, Finger J, Häring I, Carli M et al (2019) A systematic tabular approach for risk and resilience assessment and Improvement in the telecommunication industry. In: Beer M, Zio E (eds) Proceedings of the 29th European Safety and Reliability Conference (ESREL 2019). ESREL. Hannover, Germany, 22-26 September 2019. European Safety and Reliability Association (ESRA). Research Publishing Services, Singapore, pp 1312–1319

Fehling-Kaschek M, Miller N, Haab G, Faist K, Stolz A, Häring I et al (2020) Risk and resilience assessment and improvement in the telecommunication industry. In: Baraldi P, DiMaio F, Zio E (eds) Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference. ESREL2020 and PSAM15. European Safety and Reliability Aassociation (ESRA), International Association for Probabilistic Safety Assessment and Management (PSAM). Research Publishing Services, Singapore. Available at https://www.rpsonline.com.sg/proceedings/esrel2020/pdf/3995.pdf. Accessed on 25 Sept 2020

Francis R, Bekera B (2014) A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliab Eng Syst Saf 121(4):90–103. https://doi.org/10.1016/j.ress.2013.07.004

Galaitsi SE, Keisler JM, Trump BD, Linkov I (2020) The need to reconcile concepts that characterize systems facing threats. Risk Anal. https://doi.org/10.1111/risa.13577

Gay LF, Sinha SK (2013) Resilience of civil infrastructure systems: literature review for improved asset management. IJCIS 9(4):330. https://doi.org/10.1504/IJCIS.2013.058172

Giannopoulos G, Theocharidou M (2015) Risk assessment methodologies for critical infrastructure protection (EUR. Scientific and technical research series, 27332). Publications Office of the European Union, Luxembourg

Giannopoulos G, Filippini R, Schimmer M (2012) Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. Institute for the Security and Protection of the Citizen (ipsc), Joint Research Center (JRC), European Commission, Ispra

Haimes YY (2009) On the definition of resilience in systems. Risk Anal 29(4):498–501. https://doi.org/10.1111/j.1539-6924.2009.01216.x

Häring I (2015) Risk analysis and management. Engineering resilience. Springer, Singapur

Häring I, Gelhausen P (2018) Technical safety and reliability methods for resilience engineering. In: Haugen S, Barros A, van Gulijk C, Kongsvik T, Vinnene JE (eds) Safety and Reliability—Safe Societies in a Changing World. Safety and Reliability—Safe Societies in a Changing World, Proceedings of the 28-th European Safety and Reliability Conference (ESREL), Trondheim, Norway, 17–21 June 2018. CRC Press, Boca Raton, pp 1253–1260

Häring I, Ebenhöch S, Stolz A (2016a) Quantifying resilience for resilience engineering of socio technical systems. Eur J Secur Res 1(1):21–58. https://doi.org/10.1007/s41125-015-0001-x

Häring I, Scharte B, Hiermaier S (2016b) Towards a novel and applicable approach for Resilience Engineering. In: Stal M, Sigrist D, Wahlen S, Portmann J, Glover J, Bernabe N et al (eds) 6-th International Disaster and Risk Conference: Integrative Risk Management—towards resilient cities//Integrative risk management—towards resilient cities. Global Risk Forum, GRF, Davos, pp 272–276

Häring I, Scharte B, Stolz A, Leismann T, Hiermaier S (2016c) Resilience engineering and quantification for sustainable systems development and assessment: socio-technical systems and critical infrastructures. In: Linkov I, Florin M-V, Trump B (eds) IRGC Resource Guide on Resilience, vol 1. International Risk Governance Center, Lausanne, pp 81–89

Häring I, Sansavini G, Bellini E, Martyn N, Kovalenko T, Kitsak M et al (2017a) Towards a generic resilience management, quantification and development process: general definitions, requirements, methods, techniques and measures, and case studies. In: Linkov I, Palma-Oliveira JM (eds) Resilience and risk. Methods and application in environment, cyber and social domains. NATO Advanced Research Workshop on Resilience-Based Approaches to Critical Infrastructure Safeguarding (NATO science for peace and security series. Series C, Environmental security). Springer, Dordrecht. Available at https://www.springer.com/de/book/9789402411225

Häring I, Scheidereiter J, Ebenhöch S, Schott D, Reindl L, Koehler S et al (2017b) Analytical engineering process to identify, assess and improve technical resilience capabilities. In: Čepin M, Briš R (eds) ESREL 2017 (Portoroz, Slovenia, 18-22 June, 2017). The 2nd International Conference on Engineering Sciences and Technologies. High Tatras Mountains, Tatranské Matliare, Slovak Republic, 29 June–1 July 2016. CRC Press, Boca Raton

Häring I, Schäfer J, Vogelbacher G, Fischer K, Riedel W, Faist K et al (2020) From event to performance function based resilience analysis and improvement processes for more sustainable systems, (Final acceptance for publication, open for subscription). Int J Sustain Mater Struct Syst. Available at https://www.inderscience.com/info/ingeneral/forthcoming.php?jcode=ijsmss. Accessed on 17 Oct 2020

Harte R, Glynn L, Rodríguez-Molinero A, Baker PM, Scharf T, Quinlan LR, ÓLaighin G (2017) A human-centered design methodology to enhance the usability, human factors, and user experience of connected health systems: a three-phase methodology. JMIR Hum Factors 4(1):e8. https://doi.org/10.2196/humanfactors.5443

Henry D, Ramirez-Marquez JE (2012) Generic metrics and quantitative approaches for system resilience as a function of time. Reliab Eng Syst Saf 99(2):114–122. https://doi.org/10.1016/j.ress.2011.09.002

Hoeflinger F, Bordoy J, Simon N, Wendeberg J, Reindl LM, Schindelhauer C (2015) Indoor-localization system for smart phones. In: Sach R (ed) M&N, 2015 IEEE International Workshop on Measurement and Networking: proceedings. October 12-13, Coimbra, Portugal. 2015 IEEE International Workshop on Measurements and Networking (M&N). IEEE, Coimbra, Piscataway, pp 1–6

Hollnagel E (2017) Safety-II in practice. Routledge, Abingdon

Hossain NUI, Jaradat R, Hosseini S, Marufuzzaman M, Buchanan RK (2019) A framework for modelingand assessing system resilience using a Bayesian network: a case study of an interdependent electrical infrastructure system. Int J Crit Infrastruct Protect 25:62-83. https://doi.org/10.1016/j.ijcip.2019.02.002

Hosseini S, Barker K (2016) Modeling infrastructure resilience using Bayesian networks: a case study of inland waterway ports. Comput Ind Eng 93(7):252–266. https://doi.org/10.1016/j.cie.2016.01.007

Hosseini S, Al Khaled A, Sarder MD (2016) A general framework for assessing system resilience using Bayesian networks: a case study of sulfuric acid manufacturer. J Manuf Syst 41(18):211–227. https://doi.org/10.1016/j.jmsy.2016.09.006

ICF (2019) Case studies of natural gas sector resilience. Available at https://www.socalgas.com/1443742022576/SoCalGas-Case-Studies.pdf. Accessed on 10 Feb 2021

IEC 61508 (2010) Functional safety of electrical/electronic/programmable electronic safety-related systems, part 1 to 7. Available at https://webstore.iec.ch/publication/5515. Accessed on 18 Feb 2021

IEC 61882, 2016-03: Hazard and operability studies (HAZOP studies)—Application guide. Available at https://webstore.iec.ch/publication/24321. Accessed on 10 Feb 2021

Indu I, RubeshM AP, Bhaskar V (2018) Identity and access management in cloud environment: mechanisms and challenges. Eng Sci Technol Int J 21(4):574–588. https://doi.org/10.1016/j.jestch.2018.05.010

ISO 31000: Risk management—guidelines. Available at https://www.iso.org/standard/65694.html. Accessed on 18 Feb 2021

ISO 28000: Specification for security management systems for the supply chain. Available at https://www.iso.org/standard/44641.html. Accessed on 17 Oct 2020

ISO 19600, Ed. 1: Compliance management systems—guidelines. Available at https://www.iso.org/standard/62342.html. Accessed on 17 Oct 2020

ISO 14001, 2015: Environmental management systems—Requirements with guidance for use. Available at https://www.iso.org/standard/60857.html. Accessed on 17 Oct 2020

ISO 22301 (2019) Security and resilience—Business continuity management systems—Requirements. Available at https://www.iso.org/standard/75106.html. Accessed on 17 Oct 2020

ISO 22320 (2018) Security and resilience—Emergency management—Guidelines for incident management. Available at https://www.iso.org/standard/67851.html. Accessed on 17 Oct 2020

ISO 22396, 2020-02: Security and resilience—Community resilience—Guidelines for information exchange between organizations. Available at https://www.iso.org/standard/50292.html. Accessed on 21 Jan 2021

ISO 27000, 2018-02: Information technology—Security techniques—Information security management systems—overview and vocabulary. Available at https://www.iso.org/standard/73906.html. Accessed on 21 Jan 2021

ISO 31000, 2018-02: Risk management—guidelines. Available at https://www.iso.org/standard/65694.html. Accessed on 21 Jan 2021

ISO 55000, 2014-01: Asset management—overview, principles and terminology. Available at https://www.iso.org/standard/55088.html. Accessed on 21 Jan 2021

ISO 9001, 2015-09: Quality management systems—requirements. Available at https://www.iso.org/standard/62085.html. Accessed on 21 Jan 2021

ISO/AWI 22371 (2020) Security and resilience—Urban resilience—Framework, model and guidelines for strategy and implementation, Under development. Available at https://www.iso.org/standard/50274.html; https://www.iso.org/news/ref2412.html. Accessed on 17 Oct 2020

Jain AK (2018) Simulation of Indoor ultrasound localization system for assessment of disruptive events and resilience improvement options. Master Thesis. Friedrich-Alexander-Universität Nürnberg-Erlangen, Fraunhofer EMI. International Audio Laboratories Erlangen Research Center, AudioLabs, Erlangen

Kong J, Simonovic SP (2018) A model of interdependent infrastructure system resilience. Int J SAFE 8(3):377–389. https://doi.org/10.2495/SAFE-V8-N3-377-389

KPMG (2021) GIE Security Risk Assessment Methodology: Risk Assessment Tool. Prepared by KPMG for GIE. With assistance of KPMG Advisory S.p.A. Gas Infrastructure Europe, GIE. Available at https://gie.eu/index.php/giepublications/position-papers/22643-gie-security-risk-assessment-methodology-risk-assessment-tool. Accessed on 10 Feb 2021

Kröger W (2019) Achieving resilience of large-scale engineered infrastructure systems. In: NoroozinejadFarsangi E, Takewaki I, Yang T, Astaneh-Asl A, Gardoni P (eds) Resilient structures and infrastructure, vol 24. Springer, Singapore, pp 289–313

Lalonde C, Boiral O (2012) Managing risks through ISO 31000: a critical analysis. Risk Manag 14(4):272–300. https://doi.org/10.1057/rm.2012.9

Larkin S, Fox-Lent C, Eisenberg DA, Trump BD, Wallace S, Chadderton C, Linkov I (2015) Benchmarking agency and organizational practices in resilience decision making. Environ Syst Decis 35(2):185–195. https://doi.org/10.1007/s10669-015-9554-5

Lautenbach A, Islam M (2016) Security models, Deliverable 22 of EU project HEAVENS: Healing vulnerabilities to enhance software security and safety. Edited by HEAVENS project consortium, Research program Vinnova/FFI, Sweden. Available at http://autosec.se/wp-content/uploads/2018/03/HEAVENS_D2_v2.0.pdf, Accessed on 17 Oct 2020

Leitch M (2010) ISO 31000:2009—the new international standard on risk management. Risk Anal Off Publ Soc Risk Anal 30(6):887–892. https://doi.org/10.1111/j.1539-6924.2010.01397.x

Linkov I, Trump BD (2019) The science and practice of resilience. Springer International Publishing, Cham

Linkov I, Eisenberg DA, Plourde K, Seager TP, Allen J, Kott A (2013) Resilience metrics for cyber systems. Environ Syst Decis 33(4):471–476. https://doi.org/10.1007/s10669-013-9485-y

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

Linkov I, Fox-Lent C, Read L, Allen CR, Arnott JC, Bellini E et al (2018) Tiered approach to resilience assessment. Risk Anal 38(9):1772–1780. https://doi.org/10.1111/risa.12991

Lochner S, Dieckhöner C (2012) Civil unrest in North Africa—risks for natural gas supply? Energy Policy 45(7):167–175. https://doi.org/10.1016/j.enpol.2012.02.009

MERLIN (2019–2021) Multimodale effiziente und resiliente Lokalisierung für Intralogistik, Produktion und autonome Systeme, Multimodal efficient and resilient localization for intralogistics, production and autonomous systems. Demonstration Project, Funded by: Ministerium für Wirtschaft, Arbeit und Wohnungsbau Baden-Württemberg, Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg, Fraunhofer-Gesellschaft für angewandte Forschung, e.V., Albert-Ludwigs-Universität Freiburg. Edited by Sustainablity Center Freiburg. Available at https://www.leistungszentrum-nachhaltigkeit.de/demoprojekte/merlin/. Accessed on 27 Sept 2020

Miller N, Fehling-Kaschek M, Haab G, Faist K, Stolz A, Häring I (2020) Resilience analysis and quantification for Critical Infrastructures. In: Soldatos J, Philpot J, Giunta G (eds) Cyber-physical threat intelligence for critical infrastructures security: a guide to integrated cyber-physical protection of modern critical infrastructures. [S.l.]. Now Publishers, Delft, pp 365–384

Moftakhari H, AghaKouchak A (2019) Increasing exposure of energy infrastructure to compound hazards: cascading wildfires and extreme rainfall. Environ Res Lett 14(10):104018. https://doi.org/10.1088/1748-9326/ab41a6

MohdYusoff N, Salim SS (2014) A review of storyboard tools, concepts and frameworks. In: Zaphiris P, Ioannou A (eds) Learning and collaboration technologies. Designing and developing novel learning experiences. Springer, Cham, pp 73–82

Mosleh A (2018) Ask the expert. Plenary talk, ESREL 2018, 2018-06-19. European Safety and Reliability Aassociation (ESRA). Trondheim, Norway, 2018. Available at https://www.ntnu.edu/documents/1272224149/0/keynote-lecture-ali-mosleh.pdf/c324fe37-ab05-4f8c-8a77-fd23a1c7d3af

Nan C, Sansavini G (2017) A quantitative method for assessing resilience of interdependent infrastructures. Reliab Eng Syst Saf 157:35–53. https://doi.org/10.1016/j.ress.2016.08.013

NAS (2012) Disaster resilience. A national imperative. National Academies Press, Washington, D.C.

NCECI (2017–2020) Targeted Actions for enhancing the protection of National Characterized European Critical Infrastructure—NCECI. Greek EU-cofunded research project, European internal security fund. Available at http://www.ciprotection.gr/index.php/en/. Accessed on 10 Feb 2021

Nemeth CP, Hollnagel E (eds) (2014) Resilience Engineering in Practice, Volume 2. Becoming Resilient (Ashgate Studies in Resilience Engineering), vol 2. CRC Press, Boca Raton

OCTIKT (2018–2021) Ein Organic-Computing basierter Ansatz zur Sicherstellung und Verbesserung der Resilienz in technischen und IKT-Systemen. German BMBF Project. Available at https://projekt-octikt.fzi.de/. Accessed on 18 Feb 2021

Olechowski A, Oehmen J, Seering W, Ben-Daya M (2016) The professionalization of risk management: what role can the ISO 31000 risk management principles play? Int J Project Manag 34(8):1568–1578. https://doi.org/10.1016/j.ijproman.2016.08.002

PHMSA (2021) Gas Distribution Leaks per 1,000 Miles. Edited by US DOT Pipeline and Hazardous Materials Safety Administration. Available at https://portal.phmsa.dot.gov/analytics/saw.dll?Portalpages&PortalPath=%2Fshared%2FPDM%20Public%20Website%2F_portal%2FGD%20Performance%20Measures&Page=Leaks. Accessed on 10 Feb 2021

Petrenj B, Trucco P (2014) Simulation-based characterisation of critical infrastructure system resilience. IJCIS 10(3/4):347. https://doi.org/10.1504/IJCIS.2014.066366

Pirani S, Stern JP, Yafimava K (2009) The Russo-Ukrainian gas dispute of January 2009. A comprehensive assessment (OIES papers on natural gas, NG 27). Oxford Institute for Energy Studies, Oxford

Poljanšek K, Casajus Valles A, Ferrer M, De Jager A, Dottori F, Galbusera L et al (eds) (2019) Recommendations for National Risk Assessment for Disaster Risk Management in EU. EUR

29557 EN, JRC114650. Publications Office of the European Union. Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften, Luxemburg

Proske D (2008) Catalogue of Risks. Natural, technical, social and health risks. Springer, Berlin, Heidelberg

Purdy G (2010) ISO 31000:2009—setting a new standard for risk management. Risk Anal Off Publ Soc Risk Anal 30(6):881–886. https://doi.org/10.1111/j.1539-6924.2010.01442.x

Resilience Measures (2016–2018): Resilienzmaße zur Optimierung technischer Systeme, Resilience measures for optimizing technical systems, Research Project, Sustainabilty Center Freiburg, 2016–2018. Available at https://www.leistungszentrum-nachhaltigkeit.de/pilotphase-2015-2018/resilienzmasse/. Accessed on 27 Sept 2020

RESISTO (2018–2021): Resilience enhancement and risk control platform for communication infrastructure operators. EC Grant agreement ID: 786409. Available at https://cordis.europa.eu/project/id/786409. Accessed on 18 Feb 2021

RESISTO D3.9 (2020) Analytical security assessment application to use cases and their refinement, SecureGas, Deliverable 3.9. EC Grant agreement ID: 786409. Edited by SecureGas. Available at http://www.resistoproject.eu/. Accessed on 18 Feb 2021

Roytek MA (2010) Enhancing instructional design efficiency: methodologies employed by instructional designers. Br J Edu Technol 41(2):170–180. https://doi.org/10.1111/j.1467-8535.2008.00902.x

Scheithauer H (2018) Enwicklung von Resilienzmaßen, Pilot-Resilienzbestimmung und Optimierung, Development of resilience measures, pilot determination of resilience measures and optimization. Abschlussbericht, Final Report. Hahn-Schickard, Villingen-Schwenningen

SecureGas D1.1 (2019) Organizational, operational and regulatory requirements. Deliverable D1.1, EU Project SecureGas, Securing the European Gas Grid Network. SecureGas D1.1, Genova

SecureGas D1.2 (2019) Technical requirements. Deliverable D1.2, EU Project SecureGas, Securing the European Gas Grid Network. SecureGas D1.2, Genova

SecureGas D1.3 (2019) Risks, threats and vulnerabilities. Deliverable D1.3, Main report, EU Project SecureGas, Securing the European Gas Grid Network. SecureGas D1.3, Genova

SecureGas D2.3 (2019) SecureGas High Level Reference Architecture (HLRA). Intermediate version. SecureGas D2.3, Genova

SecureGas (2019–2021): Securing the European gas network, EU H2020 project, 2019–2021, Grant agreement ID: 833017. Available at https://cordis.europa.eu/project/id/833017/en; https://www.securegas-project.eu/. Accessed on 19 Jan 2021

Selvaseelan J (2018) Development and Introduction of the Risk-Sentience Auxiliary Framework (RSAF) as an Enabler to the ISO 31000 and ISO 31010 for High-Risk Environments. Adm Sci 8(2):22. https://doi.org/10.3390/admsci8020022

Spouge J, Smith E, Olufsen O, Rolf S (2014) Risk acceptance criteria and risk based damage stability. Final Report, part 1: risk acceptance criteria. European Maritime Safety Agency, EMSA (2015-0165, Rev. 1). Available at http://www.emsa.europa.eu/implementation-tasks/ship-safety-standards/item/2419-study-1-emsa-3-risk-acceptance-criteria-and-risk-based-damage-stability-part-1-part-2.html

Staff (2014) Threats to energy resources and infrastructure. In: Edwards M (ed) Critical infrastructure protection (NATO science for peace and security series. E, Human and societal dynamics), vol 116. IOS Press, Amsterdam, pp 45–54

Thoma K, Scharte B, Hiller D, Leismann T (2016) Resilience engineering as part of security research definitions, concepts and science approaches. Eur J Secur Res 1(1):3–19. https://doi.org/10.1007/s41125-016-0002-4

Thronesbery C, Molin A, Schreckenghost DL (2007) A storyboard tool to assist concept of operations development. In: Bryan E, Profet K, Richard M, Chad W (eds) IEEE Aerospace Conference Digest 2007. IEEE, Big Sky, pp 1–8

Tietjen T, Decker A (2020) FMEA-Praxis: Einstieg in die Risikoabschätzung von Produkten, Prozessen und Systemen, 4 überarbeitete Auflage. Carl Hanser Verlag, Munich

Tiku S, Pasricha S, Notaros B, Han Qi (2020) A Hidden Markov Model based smartphone heterogeneity resilient portable indoor localization framework. J Syst Architect 108(4):101806. https://doi.org/10.1016/j.sysarc.2020.101806

Tomforde S, Gelhausen P, Gruhl C, Häring I, Sick B (2019) Explicit consideration of resilience in organic computing design processes. ARCS workshop 2019 and 32nd International conference on architecture of computing systems. Joint conference. VDE Verlag GmbH, Copenhagen, Berlin, pp 51–56

Trbojevic VM (2005) Risk criteria in EU. Risk 10(5):1945–1952

UKOPA, Lyons CJ, Goodfellow GD, Haswell JV (2020) UKOPA - pipeline product loss incidents and faults report (1962–2018). United Kingdom Onshore Pipeline Operators' Assoziation. Available at https://www.ukopa.co.uk/wp-content/uploads/2020/04/UKOPA-Product-Loss-Incidents-Faults-Report-1962-2018-1.0_Feb-2020.pdf, Accessed on 9 Feb 2021

Urlainis A, Shohet IM, Levy R (2015) Probabilistic risk assessment of oil and gas infrastructures for seismic extreme events. Proc Eng 123(18):590–598. https://doi.org/10.1016/j.proeng.2015.10.112

Vílchez JA, Espejo V, Casal J (2011) Generic event trees and probabilities for the release of different types of hazardous materials. J Loss Prev Process Ind 24(3):281–287. https://doi.org/10.1016/j.jlp.2011.01.005

Vugrin ED, Warren DE, Ehlen MA, Camphouse RC (2010) A framework for assessing the resilience of infrastructure and economic systems. In: Gopalakrishnan K, Peeta S (eds) Sustainable and resilient critical infrastructure systems. Simulation, modeling, and intelligent engineering, vol 24. Springer, Berlin, pp 77–116

Vugrin ED, Warren DE, Ehlen MA (2011) A resilience assessment framework for infrastructure and economic systems: quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. Proc Safety Prog 30(3):280–290. https://doi.org/10.1002/prs.10437

Zafari F, Gkelias A, Leung KK (2019) A survey of indoor localization systems and technologies. IEEE Commun Surv Tutorials 21(3):2568–2599. https://doi.org/10.1109/COMST.2019.2911558

Zio E (2016) Critical infrastructures vulnerability and risk analysis. Eur J Secur Res 1(2):97–114. https://doi.org/10.1007/s41125-016-0004-2

Authors and Affiliations

Ivo Häring[1] · Mirjam Fehling-Kaschek[1] · Natalie Miller[1] · Katja Faist[1] · Sebastian Ganter[1] · Kushal Srivastava[1] · Aishvarya Kumar Jain[1] · Georg Fischer[1] · Kai Fischer[1] · Jörg Finger[1] · Alexander Stolz[1] · Tobias Leismann[1] ·

Stefan Hiermaier[1] · Marco Carli[2] · Federica Battisti[2] · Rodoula Makri[3] · Giuseppe Celozzi[4] · Maria Belesioti[5] · Evangelos Sfakianakis[5] · Evita Agrafioti[6] · Anastasia Chalkidou[6] · George Papadakis[6] · Clemente Fuggini[7] · Fabio Bolletta[7] · Alberto Neri[8] · Guiseppe Giunta[9] · Hermann Scheithauer[10] · Fabian Höflinger[11] · Dominik J. Schott[11] · Christian Schindelhauer[12] · Sven Köhler[12] · Igor Linkov[13]

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

Mirjam Fehling-Kaschek
mirjam.fehling-kaschek@emi.fraunhofer.de

Natalie Miller
natalie.miller@emi.fraunhofer.de

Katja Faist
katja.faist@emi.fraunhofer.de

Sebastian Ganter
sebastian.ganter@emi.fraunhofer.de

Kushal Srivastava
kushal.srivastava@emi.fraunhofer.de

Aishvarya Kumar Jain
aishvarya.kumar.jain@emi.fraunhofer.de

Georg Fischer
georg.fischer@emi.fraunhofer.de

Kai Fischer
kai.fischer@emi.fraunhofer.de

Jörg Finger
joerg.finger@emi.fraunhofer.de

Alexander Stolz
alexander.stolz@emi.fraunhofer.de

Tobias Leismann
tobias.leismann@emi.fraunhofer.de

Stefan Hiermaier
stefan.hiermaier@emi.fraunhofer.de

Marco Carli
marco.carli@uniroma3.it

Federica Battisti
federica.battisti@uniroma3.it

Rodoula Makri
rodia@esd.ece.ntua.gr

Giuseppe Celozzi
giuseppe.celozzi@ericsson.com

Maria Belesioti
mbelesioti@oteresearch.gr

Evangelos Sfakianakis
esfak@oteresearch.gr

Evita Agrafioti
agrafioti@gapanalysis.gr

Anastasia Chalkidou
chalkidou@gapanalysis.gr

George Papadakis
papadakis@gapanalysis.gr

Clemente Fuggini
clemente.fuggini@rina.org

Fabio Bolletta
fabio.bolletta@rina.org

Alberto Neri
alberto.neri@leonardocompany.com

Guiseppe Giunta
giuseppe.giunta@eni.com

Hermann Scheithauer
hermann.scheithauer@hahn-schickard.de

Fabian Höflinger
fabian.hoeflinger@imtek.uni-freiburg.de

Dominik J. Schott
dominik.jan.schott@imtek.uni-freiburg.de

Christian Schindelhauer
schindel@informatik.uni-freiburg.de

Sven Köhler
koehlers@informatik.uni-freiburg.de

Igor Linkov
igor.linkov@usace.army.mil

[1] Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, EMI, Freiburg, Germany

[2] Department of Engineering, Roma Tre University, Rome, Italy

[3] Institute of Communication and Computer Systems (ICCS) of the National Technical University of Athens, Athens, Greece

[4] Ericsson Telecomunicazioni S.P.A., Pagani, SA, Italy

[5] Hellenic Telecommunications Organization (OTE) S.A., Maroussi, Athens, Greece

[6] Gap Analysis, Crete, Greece

[7] RINA Consulting, Rozzano, Italy

[8] Leonardo Company, Rome, Italy

[9] ENI, San Donato Milanese, Italy

[10] Hahn-Schickard, Villingen-Schwenningen, Germany

[11] Department of Microsystems Engineering, IMTEK, University of Freiburg, Freiburg, Germany

[12] Computer Networks and Telematics, University of Freiburg, Freiburg, Germany

[13] Engineering Research and Development Center, US Army Corps of Engineers, Concord, MA, USA