A Systematic Tabular Approach for Risk and Resilience Assessment and Improvement in the Telecommunication Industry

Mirjam Fehling-Kaschek, Katja Faist, Natalie Miller, Jörg Finger, Ivo Häring

Safety Technology and Protective Structures, Fraunhofer Institute for High-Speed Dynamics, Germany. E-mail: Mirjam.Fehling-Kaschek@emi.fraunhofer.de, Katja.Faist@emi.fraunhofer.de, Ivo.Haering@emi.fraunhofer.de

Marco Carli, Federica Battisti

Department of Engineering, Roma Tre University, Italy. E-mail: marco.carli@uniroma3.it, federica.battisti@uniroma3.it

Rodoula Makri

Microwaves and Fiber Optics Lab, Institute of Communication and Computer Systems (ICCS) of the National Technical University of Athens, Greece. E-mail: rodia@esd.ece.ntua.gr

Giuseppe Celozzi, Giuseppe Amato

Ericsson Telecomunicazioni S.p.A., Via Madonna di Fatima 2, 84016 Pagani (SA), Italy. E-mail: giuseppe.celozzi@ericsson.com, giuseppe.amato@ericsson.com

Maria Belesioti, Evangelos Sfakianakis

Hellenic Telecommunications Organization (OTE) S.A., Kifissias Ave 99, Kifissias Avenue, GR 15124, Maroussi, Athens, Greece. E-mail: mbelesioti@oteresearch.gr, esfak@oteresearch.gr

The economic and social well-being of citizens depends on the reliable functioning of critical infrastructures, and in particular, the provision of a reliable telecommunication system. Integrated risk and resilience analysis and improvement processes have been proposed and adopted to critical infrastructure systems. However, fast, tabular, and in operational contexts realizable implementations are still lacking. The paper proposes a set of interlinked tables for a fast, semi-quantitative implementation of such a process. The sequence and structure of the tables is chosen to capture the relevant input for the risk and resilience analysis and management process. Pulling from previous literature, four main constituents are identified and implemented as separate tables: system components, system functions, threats and mitigation options. The linkage between the tables and their contents, including minimum consistency requirements are expected to be sufficient for a successful implementation of the resilience analysis and management process. The linkage allows for direct computation of the correlations between the four constituents, e.g. system components with system functions, system functions with potential disruptions to identify critical combinations and threats with potential counter measures. Furthermore, quantification options and potential counter measures for the critical combinations can be inferred. Sample entries are given for the telecommunication infrastructure and the advantages of the approach are discussed.

Keywords: Risk, resilience, system function, threat, assessment, tabular, telecommunication.

1. Introduction

The aim of the proposed fast and flexible risk and resilience management process is to assess and improve the risk control, the resilience, and the efficiency of systems. The outcome of this process allows to identify system vulnerabilities and efficiently manage and mitigate the events.

Aim of this paper is to introduce a fast and flexible resilience analysis through a template-based approach (FRAT). The method is currently deployed in the EU-H2020 project RESISTO[1], aiming at improving the resilience of communication infrastructures in the light of cyber, physical and combined cyber-physical attacks. The framework of this project serves as an example case study throughout this paper.

The paper is organized as follows: first, an extension of the ISO-31000 risk management process towards an integrated risk and resilience management process is introduced in Section 2. A detailed description of FRAT is given in Section 3, including an introduction to necessary components (Section 3.1), specific contents and examples (Section 3.2) and finally examples of a first analysis with semi-quantitative results (Section 3.3). Finally, the conclusions are drawn in Section 4.

[1] http://www.resistoproject.eu/

Proceedings of the 29th European Safety and Reliability Conference.
Edited by Michael Beer and Enrico Zio

Proceedings of the 29th European Safety and Reliability Conference.
Edited by Michael Beer and Enrico Zio

Published by Research Publishing, Singapore.
ISBN: 978-981-11-2724-3; doi:10.3850/978-981-11-2724-3_0242-cd

2. ISO-31000 conform Resilience Management Extension

A combined risk and resilience assessment process, described in Häring (2017), is an extension of the ISO 31000 standard. Originally completed for the 2009 version of the standard, the extension still holds true for the updated 2018 version.

The ISO 31000 (2018) process has five steps:

- System context definition
- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment

Within the first step of system context definition, the scope and risk criteria are defined. The risk assessment process, within the larger, overall risk management process, includes risk identification, analysis and evaluation, which are followed by the risk treatment. For the resilience management extension of the standard, the ISO steps are divided into further stages to allow a resilience assessment to be completed, as shown in Fig. 1 (right).

The resilience management extension includes nine steps:

- Context analysis
- System analysis
- Identification of system performance function
- Identification of disruptions
- Functions and disruptions pre-assessment
- Quantification of overall resilience
- Evaluation of resilience/cost
- Selection of resilience modification options
- Implementation of resilience modification options

Within the first step (context analysis) the economic, legal, societal and ethical contexts are generally described. Other aspects of the context are defined, including stakeholder identification, resilience objectives, and the criteria that will be used in the evaluation of the system.

The system analysis performed in step two includes the definition of boundary conditions, the interfaces and evaluating the system environment. A model of the systems static and dynamic behavior is developed. Any restrictions of resilience are also defined in these steps.

In step three, the system performance function identification, quantitative and qualitative descriptions of the system performance functions and services are defined. The combination of performance functions covers all system behaviors that are expected.

Disruption identification as step four indicates, includes classical risk events, like threats and hazards that can influence the system behavior. For each threat, hazard or disruption identified, the system functions, technical resilience capabilities and system layers that can potentially be affected are determined as well.

During the pre-assessment step, an analysis of combinations from system functions (step three) and identified disruptions (step four) is completed. Critical combinations are identified and evaluated further in a semi-quantitative approach.

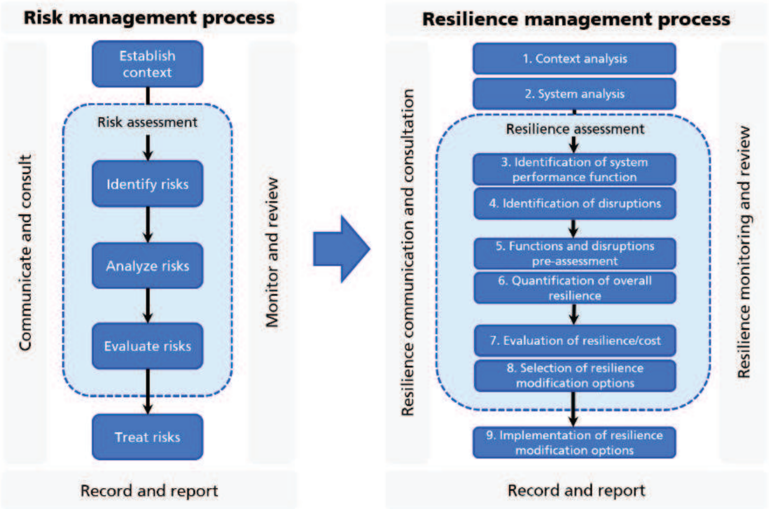

Risk management process
Establish context
Risk assessment
Identify risks
Analyze risks
Evaluate risks
Treat risks
Communicate and consult
Monitor and review
Record and report
Resilience management process
1. Context analysis
2. System analysis
Resilience assessment
3. Identification of system performance function
4. Identification of disruptions
5. Functions and disruptions pre-assessment
6. Quantification of overall resilience
7. Evaluation of resilience/cost
8. Selection of resilience modification options
9. Implementation of resilience modification options
Resilience communication and consultation
Resilience monitoring and review
Record and report

Fig. 1. The ISO 31000 (2018) risk management process (left) models the process as defined by the standard. The extension towards a resilience management process (right) allows for application to resilience

In step six, the overall resilience analysis is quantified. This quantification includes the system performance functions, identified threats and builds on the pre-assessment completed in step five. Resilience assessment quantities are determined as well.

For step seven, the evaluation of resilience, different approaches are considered: performance loss analysis, evaluation of threat acceptance levels and performance comparisons, for example, with historical values. The outcome of steps five and six are evaluated in this phase.

For modification and mitigation options in step eight, an inventory of all resilience improvement options is created and selection is based on decision-making methods. An iterative process of the resilience management steps is conducted to determine the overall resilience gain.

Finally, during the last step, the modification options determined in step eight are implemented. Domain-specific standards and efficient methods are considered during the implementation and development. The subsystems resilience levels are also considered.

The resilience management process is an iterative process, which allows for retesting and refinement of the system if necessary. For example, after the implementation of a mitigation measure that changes the system, this process should be redone.

3. Tabular Implementation

Dedicated input from experts of the system, in our case telecommunication infrastructure providers, is needed for conducting the extended risk and resilience management process. To allow for a fast and flexible assessment of the information, a tabular implementation was chosen for FRAT.

3.1 *Input requirements for the risk and resilience management steps*

The necessary inputs needed in order to perform the risk and resilience management process are identified in the following. A focus is set on the tables contributing to FRAT.

Step 1 – Context analysis: To establish the context, a general overview over the system and its objectives is needed. Within the RESISTO project, interviews with the telecommunication experts were conducted to gain a broad knowledge on their requirements, security status and technical aspects of their systems.

Step 2 – System analysis: The system analysis step in the resilience management process is covered by the table of system components (SC) and graphical presentations of the telecommunication network. Users are able to add the different SCs to the table, keeping in mind the level of complexity and the need for a realistic system model. For each SC, additional information like technical specifications or the connection to other SCs is collected in the tabular format.

Step 3 – System performance function identification: A second table identifies system performance functions (SF) needed to quantify the resilience of the system. The SF table contains their specifications and a linkage to SCs needed for the SFs to work properly.

Step 4 – Disruptions identification: For disruption identification, a table of potential threats, hazards and disruptions is created. The users add different kind of threats to their system (physical, cyber and combined ones) and include supplementing information like hazard classification and effects on both SCs and SFs.

Step 5 – Pre-assessment of the criticality of combinations of system functions and disruptions: From the information collected in the tables, correlation estimates can be drawn for SFs and threats, serving as a semi-quantitative pre-assessment of critical combinations of threats and SFs. This correlation is particularly important for identifying and assessing the combined cyber-physical threats in telecommunication infrastructures, especially in cases of non-simultaneous impact.

Step 6 – Overall resilience quantification: Additional tools are needed for an advanced resilience quantification, based on the outcome of the previous step and the system specifications in step 2. Dedicated network simulators are used for this step within the RESISTO project.

Step 7 – Resilience evaluation: Feedback from experts and stakeholders is needed to make decisions based on the outcome of the resilience analysis in steps 5 and 6. This is supported by tabular and graphical presentations of the results.

Step 8 – Selection of options for improving resilience: A final table created is dedicated to potential mitigation or prevention options for the residual critical threats encountered. For each improvement measure, the threat(s) aimed to be mitigated is linked as well as the SCs impacted.

Step 9 – Development and implementation of options for improving resilience: The final development and implementation of mitigation options needs to be carried out by system experts. It is not part of FRAT, but it exploits its outputs and analysis.

In total, four tables are identified as main content of FRAT, summarized in Table 1.

Table 1. List of input tables identified for FRAT with inter-linkages to other tables

Table Name	Abbre-viation	Resilience step	Linkage to other tables			
			SC	SF	T	IM
System Components	SC	2				
System Functions	SF	3	x			
Threats	T	4	x	x		
Improvement Measures	IM	8	x		x	

3.2 *Structures of the tables*

This section provides a detailed description of the structure and contents of FRAT. While the general structure can be directly transferred to any other system, specific information defined in dropdown menus (see 3.2.2) corresponds to our example case study of telecommunication infrastructures.

3.2.1 *Linkage*

A main advantage of FRAT is that information for different steps of the resilience management process is collected in one file. This simplifies further analysis by allowing to directly link items of one table to the items of another table, e.g. identify which system components are affected by a given threat. The linkage is implemented by generating automated dropdown menus from the list of identifiers of each table.

3.2.2 *Classification definitions*

A separate sheet is included in FRAT to define dropdown menus for the main tables. These menus provide a structure for categorization and classification of information, e.g. to classify a threat as either cyber, physical or cyber-physical. It is intended to facilitate the process of inserting new information in FRAT and help preventing from inconsistencies in the further analysis, e.g. due to misspellings. FRAT was extended with a Visual Basic macro to allow selecting multiple options from the dropdown menus.

3.2.3 *System components*

The SC table of FRAT has a general structure that can be applied to any system. However, the listed contents of the corresponding dropdown menus are specific to our telecommunication case study. The following columns are included in the SC table:

- ID: a unique identifier for each component using the prefix SC, i.e. SC1, SC2, etc.
- Name: short name of the component
- Description: general information about the component
- Subsystem: a classifier to identify in which subsystem the component is integrated (Radio Network, Optical Network, Satellite Network, Core Network, Data Center, Applications, Internal Network)
- Type: a classifier specifying the kind of the component (Hardware Device, Software Tool, Interconnection, Mechanical, Built structure)
- Quantity: rough number of how many entities are included in the network, or network segment under consideration.
- Technical characteristics: information on the component relevant for its functioning and/or assessment of disruption impacts e.g. throughput, time delays, physical dimensions, energy consumption
- Interconnections: possible direct linkages to other components of the system
- Comments: any additional information.

An example of the SC table is shown in Table 2.

3.2.4 *System functions*

The SF table of FRAT also has a general structure that can be applied to other systems, while the contents of the dropdown menus are specific to the telecommunications example. The following contents are collected by the SF table:

- ID: a unique identifier for each function using the prefix SF, i.e. SF1, SF2, etc.
- Name: short name of the function
- Description: general information about the function
- Subsystem: a classifier to identify which subsystem(s) function covers (Radio Network, Optical Network, Satellite Network, Core Network, Data Center, Applications, Internal Network)
- Linked Components: a drop-down menu to select all system components, from the SC table, needed for a full function performance
- Performance Quantification: definition of a minimal or critical performance rate

- Dependence of other SFs: a drop-down menu to select possible other SFs on which the specific SF depends
- Comments: any additional information.

An example of the SF table is shown in Table 3.

3.2.5 *Threats*

The table of potential threats, hazards, and disruptions contains the following information:

- ID: a unique identifier per threat starting with the prefix T, i.e. T1, T2, etc.
- Name: a short name related to the hazard cause, e.g. earthquake
- Description: information about the hazard
- Hazard type: a classifier to identify the event (physical, cyber or cyber-physical)
- Hazard cause: a classifier to identify the general source of the threat (man-made (accidental), man-made (attack), technical/system failure, natural)
- Frequency: a classifier to rank the occurrence of the event from very frequent (>= 10/week) to rare (<=1/year)
- Duration: approximate mean time that the system is affected
- Economic impact: a classifier (high, medium, low, no)
- Impact on society: a classifier (high, medium, low, no)
- SCs affected directly: a drop-down menu to select all system components, from the SC table, directly affected by the threat
- SCs affected indirectly: a drop-down menu to select SCs indirectly affected by the threat
- SFs affected directly: a drop-down menu to select all system functions, from the SF table, directly affected by the threat
- Subsystems affected: a classifier of all subnetworks affected (as in the SC table)
- Impact on other critical infrastructures (CIs): needed to simulate cascading effects (i.e. on power grids) or used as an indicator for the threat impact
- Comments: any additional information.

An exemplary threats table is shown in Table 4.

3.2.6 *Mitigation Options*

The following contents are collected by the table of Improvement Measures (IM) in FRAT:

- ID: a unique identifier for each IM starting with the prefix IM, i.e. IM1, IM2, etc.
- Name: short name of the IM
- Description: general information
- Subsystem: a drop-down menu to select all threats, from the Threats table, that are targeted by the IM
- Component: similarly, a drop-down menu to select all SCs improved or repaired by the IM
- Action Type: a classifier to specify the purpose or type of the IM (preparation, detection, prevention, protection, stabilization, recovery, improve)
- Comments: any additional information.

An example of the IM table is shown in Table 5.

Table 2. FRAT: Exemplary list of System Components (SCs) for the telecommunication infrastructure.

ID	Name	Description	Subsystem	Type	Quantity	Technical characteristics	Interconnections
SC1	Security Equipment	Firewalls, IPs, etc.	Core Network	Hardware Device	10	Firewalls, etc.	SC6
SC2	Internal Security	VLAN, Proxy	Internal Network	Hardware Device	60		
SC3	FO	Fiber optics cables	Optical Network	Interconnection		Buried or overhead	SC5
SC4	Operation	Software utilized for operation	Data Center	Software Tool	1-1000	Windows PC, Linux, etc.	SC1, SC2
SC5	Radio Infrastructure	Connectivity for different services	Radio Network	Hardware Device			SC3
SC6	Servers	Servers and network terminal points	Internal Network	Hardware Device		Windows PC, Linux, etc.	SC1, SC2

Table 3. FRAT: Exemplary list of System Functions (SFs) for the telecommunication infrastructure.

ID	Name	Description	Subsystem	Linked Components	Performance Quantification	Dependence of other SFs
SF1	Voice services	Voice communication services and connections	Radio Network; Optical Network; Core Network; Data Center	SC3: SC5; SC6	Real time	SF2; SF3
SF2	Connectivity (IP)	Connectivity between devices in network	Optical Network; Core Network; Radio Network	SC1; SC2; SC5	Varying matrices: delays, losses, etc.	
SF3	Connectivity (Radio/FO)	Connections between radio, fiber optic links within equipment	Radio Network; Optical Network	SC3; SC5;SC6	Varying matrices: delays, losses, etc.	
SF4	Data center services	Date storage, manipulation, etc.	Data Center	SC1; SC4; SC6	Volume of data and number of requests	SF2; SF3

Table 4. FRAT: Exemplary list of potential threats (Ts) for telecommunication infrastructures.

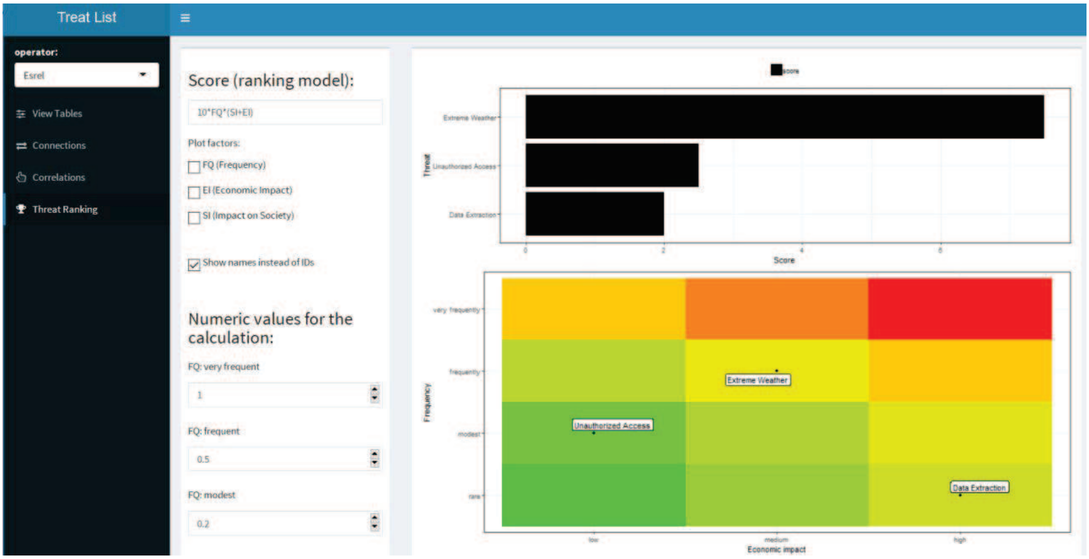
ID	Name	Description	Hazard type	Hazard cause	Frequency	Duration
T1	Extreme Weather	Storms or natural disasters causing physical damage	physical	natural	frequently: several per month	Variable
T2	Data Extraction	Hackers accessing the system and capturing data (including data sniffers)	cyber	man made (attack)	rare: ≤ 1/year	2+ hours
T3	Unauthorized Access	A physical intrusion causing malware on the cyber domain core	cyber-physical	man made (attack)	modest: several per year	Variable

Table 4. FRAT: Threats, hazards and disruptions (continued)

ID	Name	Economic impact	Impact on society	SCs affected directly	SCs affected indirectly	SFs affected	Subsystems affected	Impact on other CIs
T1	Extreme Weather	medium	medium	SC5	SC3; SC5	SF1; SF2; SF3	Radio Network; Optical Network	Power
T2	Data Extraction	high	high	SC6	SC1; SC2; SC4	SF2	Applications; Internal Network; Data Center	
T3	Unauthorized Access	low	medium	SC1; SC2	SC4; SC6	SF4	Radio Network; Optical Network; Data Center; Internal Network; Core Network; Applications	

Table 5. FRAT: Improvement Measures (IM). Exemplary list of mitigation options for the Table 4 threats.

ID	Name	Description	Threat	Component	Action Type
IM1	Generation	Generators placed in strategic locations for emergency power	T1	SC2; SC4	preparation
IM2	Training	Employee training on variety of topics including security and vulnerability	T2; T3	SC1; SC2; SC4; SC6	prevention
IM3	Physical barriers	Fencing, cameras, and/or locks to protect the infrastructure	T3	SC3; SC5	protection
IM4	Security Review	Review of security proceedings to keep up to date and employees informed	T2; T3	SC1; SC2; SC4; SC6	prevention
IM5	Alerts	An alert system when new accounts are created or accessed form a different location than normal	T2; T3	SC1; SC2; SC4; SC6	prevention
IM6	Redundancy	Increased redundancy to improve response to attack or other adverse event	T1; T2; T3	SC4; SC6	improve



operator: Esrel

Score (ranking model):

10*FQ*(SI+EI)

Plot factors:

□ FQ (Frequency)

□ EI (Economic Impact)

□ SI (Impact on Society)

☑ Show names instead of IDs

Numeric values for the calculation:

FQ: very frequent

1

FQ: frequent

0.5

FQ: modest

0.2

Fig. 2. Screenshot of the web-application. The threat ranking option is selected and the score of the example threats, based on the frequency, economic and social impact, is shown (top right). In addition, the frequency vs economic impact of the threats is visualized in a matrix plot (bottom right).

3.3 *FRAT analysis*

In order to further support the risk and resilience management process a web-application was developed, allowing to interactively browse the tables and to develop first analysis steps based on sophisticated visualizations of FRAT. The application was implemented in the statistical computing language R[2], using the shiny package by Chang et al. (2018). A screenshot of the dashboard is shown in Fig. 2.

3.3.1 *Connections*

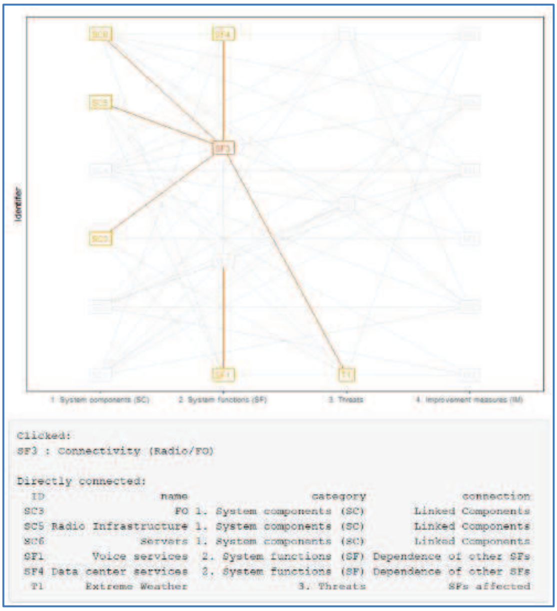
An example for the visualization of the interconnections of the tables is shown in Fig 3. By selecting (clicking on) any item in the graph, those items that are directly connected with it are highlighted and automatically listed below the plot.

3.3.2 *Threat ranking*

A score for ranking the threats can be calculated based on the frequency of occurrence (FQ), economic impact (EI) and social impact (SI).

$$Score = FQ \cdot (EI + SI) \qquad (1)$$

In the web-application the score formula Eq. (1) and the mapping of numeric values (e.g. high=1,



```
Clicked:
SF3 : Connectivity (Radio/FO)

Directly connected:
  ID                   name                   category              connection
 SC3                     FO 1. System components (SC)      Linked Components
 SC5 Radio Infrastructure 1. System components (SC)      Linked Components
 SC6                Servers 1. System components (SC)      Linked Components
 SF1         Voice services  2. System functions (SF) Dependence of other SFs
 SF4 Data center services  2. System functions (SF) Dependence of other SFs
  T1        Extreme Weather                 3. Threats            SFs affected
```

Fig. 3. Exemplary visualization of the connections of the tables in FRAT. Here, the SF2 was selected and the linked SCs and threats from the other tables are highlighted and listed below the plot.

[2] https://www.R-project.org/

medium = 0.5, low = 0.1) can be modified by the user. The threat ranking is illustrated for the example in Fig. 2. The highest risk is assigned to the extreme weather threat, due to its high frequency in combination with medium economic and social impact.

3.3.3 *Correlation matrices*

The connections among the tables can also be visualized by a correlation matrix, as shown in Fig. 4 for the combinations of threats and system functions. This supports the semi-quantitative pre-assessment of critical combinations of the resilience management process step 5. Direct effects on SFs, as well as indirect effects created via the SCs needed for the specific SF, are considered and the user can modify the strength of each contribution. Our example demonstrates that not all performance measures are affected by the threats equally. Only the strongly correlated pairs of SFs and threats need to be considered for the more sophisticated resilience quantification process, i.e. Voice Services and/or Connectivity for the Extreme Weather and Data center services in case of Data Extraction or Unauthorized Access events.

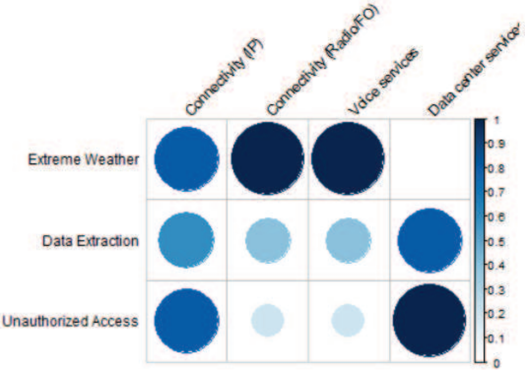


Fig. 4. Assessment of combinations of threats and system functions for the telecommunication example. It should be noted that the entries are not normalized.

4. Summary and Conclusions

A fast and flexible tabular tool for semi-quantitative resilience analysis and resilience improvement was introduced in this paper. FRAT method is derived from ISO 31000, aiming to enrich its implementation. The idea of combining different kinds of tabular inputs needed at the nine resilience management steps allows to directly draw first semi-quantitative and qualitative analysis results, such as the allocation of system elements to system (service) functions, the pre-assessment of critical combinations of system functions and threats, and assigning mitigation measures.

The approach can be applied in various systems and infrastructures. The example used as case study in this paper is a telecommunication network, seen as a complex cyber-physical system. Considering telecommunication networks as holistic critical infrastructures is important due to their large current expansion and in light of the emerging use of 5G; thus related security aspects both in the physical and the cyber domain will be of major significance.

The approach will be further revised in the framework of the ongoing RESISTO project, which deals with threat detection and mitigation aspects in the current and future telecommunication infrastructures. A possible enhancement of FRAT would be the extension of the existing tables as well as the addition of new input and processing tables where necessary, depending on the system's complexity. In particular, a table containing information about experts and stakeholders when contacting each other in case of problems or for the decision making steps would be added in the future version of the described approach.

Acknowledgement

This work is supported by the H2020 RESISTO project, which has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 786409.

References

Häring, I., G. Sansavini, E. Bellini, N. Martyn, T. Kovalenko, M. Kitsak, G. Vogelbacher, K. Ross, U. Bergerhausen, K. Barker, and I. Linkov (2017). Towards a Generic Resilience Management, Quantification and Development Process: General Definitions, Requirements, Methods, Techniques and Measures and Case Studies. *Resilience and Risk*, 21-80.

Scharte, B., D. Hiller, T. Leismann, and K. Thoma (2014). Introduction. In K. Thoma (Ed.), *"Resilience by Design": a strategy for the technology issues of the future*, pp. 9-17. Herbert Utz Verlag.

Winston Chang, Joe Cheng, JJ Allaire, Yihui Xie and Jonathan McPherson (2018). shiny: Web Application Framework for R. URL https://CRAN.R-project.org/package=shiny