

RESISTO:

D3.1_Risk and resilience management process for cyber- physical threats of telecom CI



RESISTO

D3.1 – RISK AND RESILIENCE MANAGEMENT PROCESS FOR CYBER-PHYSICAL THREATS OF TELECOM CI

Document Manager:	Mirjam Fehling-Kaschek	Fraunhofer	Editor
--------------------------	------------------------	------------	--------

Project Title:	RESilience enhancement and risk control platform for communication infraSTructure Operators
Project Acronym:	RESISTO
Contract Number:	786409
Project Coordinator:	LEONARDO
WP Leader:	Fraunhofer

Document ID N°:	RESISTO_D3.1_190516_01	Version:	1.0
Deliverable:	D3.1	Date:	16/05/2019
		Status:	APPROVED

Document classification	PUBLIC
--------------------------------	---------------

Approval Status	
Prepared by:	Mirjam Fehling-Kaschek, Katja Faist (Fraunhofer)
Approved by: (WP Leader)	Mirjam Fehling-Kaschek, Katja Faist (Fraunhofer)
Approved by: (Coordinator)	Federico FROSALI (LDO)
Advisory Board Validation (Advisory Board Coordinator)	NA
Security Approval (Security Advisory Board Leader)	Alberto BIANCHI (LDO)

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Mirjam Fehling-Kaschek, Natalie Miller, Ivo Häring, Jörg Finger	Fraunhofer	Scientific Researcher
Maria Belesioti, Evangelos Sfakianakis, Ioannis Chochliouros	OTE	Telecom experts
Rodoula Makri, Panagiotis Karaivazoglou, Apostolos Papafragkakis, Takis Kelefas, Michalis Sofras, Evangelos Groupas, Athanasios Panagopoulos	ICCS	Telecom engineers, senior researchers

DISTRIBUTION LIST

Name	Company / Organization	Role / Title
PMT	RESISTO CONSORTIUM	NA
Markus MULLER	EC DG REA	EC Programme Officer
General Public	NA	NA

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
0.5	20.01.2019	All		First draft version
0.9	26.02.2019		3.1, 4.1.3, 4.1.4	Release for SAB review
1.0	16.05.19	All	All	Final release

COPYRIGHT STATEMENT



© 2018-2021 This document and its content are the property of the RESISTO Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the RESISTO Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the RESISTO Partners. Each RESISTO Partner may use this document in conformity with the RESISTO Consortium Grant Agreement provisions.

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Program, under the Grant Agreement No 786409.

The views and opinions in this document are solely those of the authors and contributors, not those of the European Commission.

PROJECT CONTACT



LEONARDO

Via delle Officine Galileo 1 – Campi Bisenzio (FI) – 50013 – Italy

Tel.: +39 055 5369640, Fax: +39 055 5369640

E-Mail: frederico.frosali@leonardocompany.com

RESISTO PROJECT – PUBLISHABLE EXTENDED ABSTRACT

Communications play a fundamental role in the economic and social well-being of the citizens and on operations of most of the CIs. Thus they are a primary target for criminals having a multiplier effect on the power of attacks and providing enormous resonance and gains. Also extreme weather events and natural disasters represents a challenge due to their increase in frequency and intensity requiring smarter resilience of the Communication CIs, which are extremely vulnerable due to the ever-increasing complexity of the architecture also in light of the evolution towards 5G, the extensive use of programmable platforms and exponential growth of connected devices. The fact that most enterprises still manage physical and cyber security independently represents a further challenge. RESISTO platform is an innovative solution for Communication CIs holistic situation awareness and enhanced resilience (aligned with ECSO objectives). Based on an Integrated Risk and Resilience analysis management and improvement process availing all resilience cycle phases (prepare, prevent, detect, absorb, etc.) and technical resilience capabilities (sense, model, infer, act, adopt), RESISTO implements an innovative Decision Support System to protect communication infrastructures from combined cyber-physical threats exploiting the Software Defined Security model on a suite of state of the art cyber/physical security components (Blockchain, Machine Learning, IoT security, Airborne threat detection, holistic audio-video analytics) and services (Responsible Disclosure Framework) for detection and reaction in presence of attacks or natural disasters. Through RESISTO Communications Operators, will be able to implement a set of mitigation actions and countermeasures that significantly reduce the impact of negative events in terms of performance losses, social consequences, and cascading effects in particular by bouncing efficiently back to original and forward to operational states of operation.

EXECUTIVE SUMMARY

This deliverable summarizes the status of task T3.1. The aim of this task is to define the risk and resilience management process for the long term control loop of the RESISTO platform.

To this end, a resilience based extension of the risk management process, defined by the ISO-31000 standard, is introduced. Specifications for all steps of this extension for the RESISTO project are provided.

Another focus in this report is the coverage of relevant resilience dimensions. Current definitions, found in literature or pre-defined by the objectives of RESISTO, are reviewed.

CONTENTS

1. INTRODUCTION	10
2. EXTENDING ISO-31000 TOWARDS RESILIENCE MANAGEMENT	12
3. RESILIENCE DIMENSIONS	14
3.1. Cyber, physical and cyber-physical disruptions/threats	14
3.2. Resilience cycle phases.....	16
3.3. System domains	18
3.4. Technical resilience capabilities	18
4. RISK AND RESILIENCE MANAGEMENT PROCESS FOR RESISTO	21
4.1. Refinement of the resilience management steps	21
4.1.1. Context analysis	22
4.1.2. System analysis.....	22
4.1.3. System performance function identification.....	23
4.1.4. Disruptions identification.....	24
4.1.5. Pre-assessment of the criticality of combinations of system functions and disruptions.....	28
4.1.6. Overall resilience quantification.....	28
4.1.7. Resilience evaluation.....	29
4.1.8. Selection of options for improving resilience	29
4.1.9. Development and implementation of options for improving resilience	30
4.2. Supporting inputs, tools and methods	30
5. SUMMARY	33
5.1. Next steps	33

List of figures:

Figure 1 - RESISTO logical architecture (see deliverable D2.6 for more information)	10
Figure 2 - Risk and resilience management processes. The risk management process (left) follows the definition of ISO 31000 (2018) Risk management – Principles and guidelines. The resilience management process (right) extends the risk management process to cover resilience specific steps [1].....	12
Figure 3 - The framework designed for cyber-physical security [2]	14
Figure 4 - The holistic resiliency cycle for cyber-physical systems [3].	16
Figure 5 - The resilience cycle as defined by [4].	17
Figure 6 - The resilience cycle as defined by ResiliNets [6].....	17
Figure 7 - Resilience characteristics and their interrelation to each other as defined by [14].	19
Figure 8 - Exemplary screenshot of the System Components table of the Excel file	23
Figure 9 - Exemplary screenshot of the System Functions table of the Excel file.	24
Figure 10 - Exemplary screenshot of the Threats table in the Excel file.	27
Figure 11 - Exemplary correlation matrix of system functions and threats (left) and threat ranking (right top) by a score calculated based on the frequency and economic impact (right bottom). It should be noted, that the entries in the correlation matrix are not normalized but rather refer to a connection strength in arbitrary units.	28
Figure 12 - Exemplary screenshot of the table of improvement measures of the Excel file.	29
Figure 13 - Exemplary screenshot of a visualisation of the inter-connections of the tables in the Excel file.	31
Figure 14 – Input and tools supporting the risk and resilience management process for the long term control loop of RESISTO. The usage of the tabular inputs and graphical network representations is indicated by orange boxes and the support by the Shiny app and simulation tools by blue or green boxes, respectively.	32

ABBREVIATIONS

2G, 3G, 4G	Second, third and fourth generation of mobile phone network systems
CI	Critical Infrastructure
DoW	Document of Work (RESISTO grant agreement)
EU	European Union
GUI	Graphical User Interface
KPI	Key Performance Indicator
LTE	Long Term Evolution (= 4G)
NFV	Network Function Virtualization
T	Task – referring to tasks within the WPs of the RESISTO project
WP	Work Package – referring to other WPs of the RESISTO project

1. INTRODUCTION

The main objective of the RESISTO project is to improve the security and resilience in communication infrastructures. This is achieved by developing an innovative platform for threat detection, an integrated risk and resilience assessment and optimized decision support. The RESISTO platform interfaces to existing communication infrastructures and modularly integrates tools and methods in the integration platform, which consists of two control loops, the short term and the long term control loop. A scheme of the architecture of the integration platform is shown in Figure 1.

Aim of WP3 is the definition of the long term control loop of the RESISTO platform, which mainly features the risk and resilience analysis and management process.

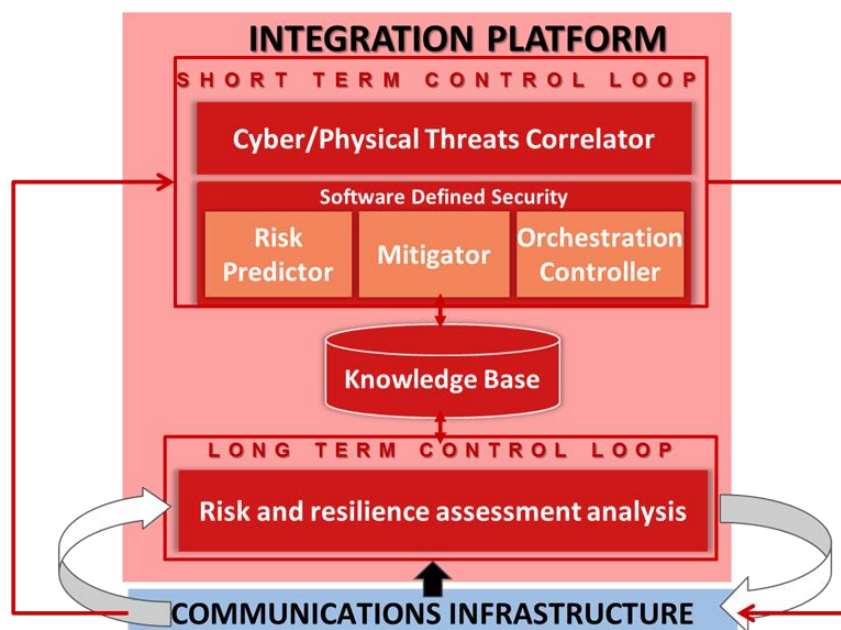


Figure 1 - RESISTO logical architecture (see deliverable D2.6 for more information)

The following tasks are included in WP3:

- T3.1 Long term learning cyber-physical risk and resilience management
- T3.2 Methods/Plans for joint cyber-physical security management process
- T3.3 Physical protection and prevention methods: assessment and cyber-physical interaction
- T3.4 Risk and resilience quantities and related KPIs for telecommunications infrastructure
- T3.5 Desk-top application to use case scenarios for second use cases refinement

This report summarizes the status of T3.1. Main objective of this task is to define the risk and resilience management process for RESISTO, including the specification of all relevant process steps. The process is supported by inputs and modules developed and defined in other tasks of WP2 and WP3. The general mapping of all inputs and tools to the risk and resilience management process is investigated and summarized in this report. Another focus in this report is the definition and election of adequate resilience dimensions, supporting the resilience quantification process.

This report is structured as follows:

Chapter 2 provides a short introduction to the general definition of the extended risk and resilience management process used within RESISTO.

Chapter 3 gives an overview of various definitions of resilience dimensions, as found in literature, relevant for RESISTO.

Chapter 4 contains the specific setup for RESISTO's risk and resilience management process. The meaning of each step of the management process is revised in the context of the RESISTO project, including the identification of necessary inputs and tools.

Chapter 5 provides a summary of the report and an outlook on the next steps to be followed within this task.

2. EXTENDING ISO-31000 TOWARDS RESILIENCE MANAGEMENT

The risk and resilience assessment plays a fundamental role in the RESISTO project. It is performed by following an integrated risk and resilience management process, which is described in [1]. This assessment and improvement process was initially developed based on the ISO 31000 (2009) [2] standard, but still holds for the updated ISO 31000 (2018) version¹.

The ISO 31000 standard provides a systematic and iterative procedure for the risk management process, consisting of five sequential steps, as shown in Figure 2 (left):

1. Context analysis
2. Risk identification
3. Risk analysis
4. Risk evaluation
5. Risk treatment

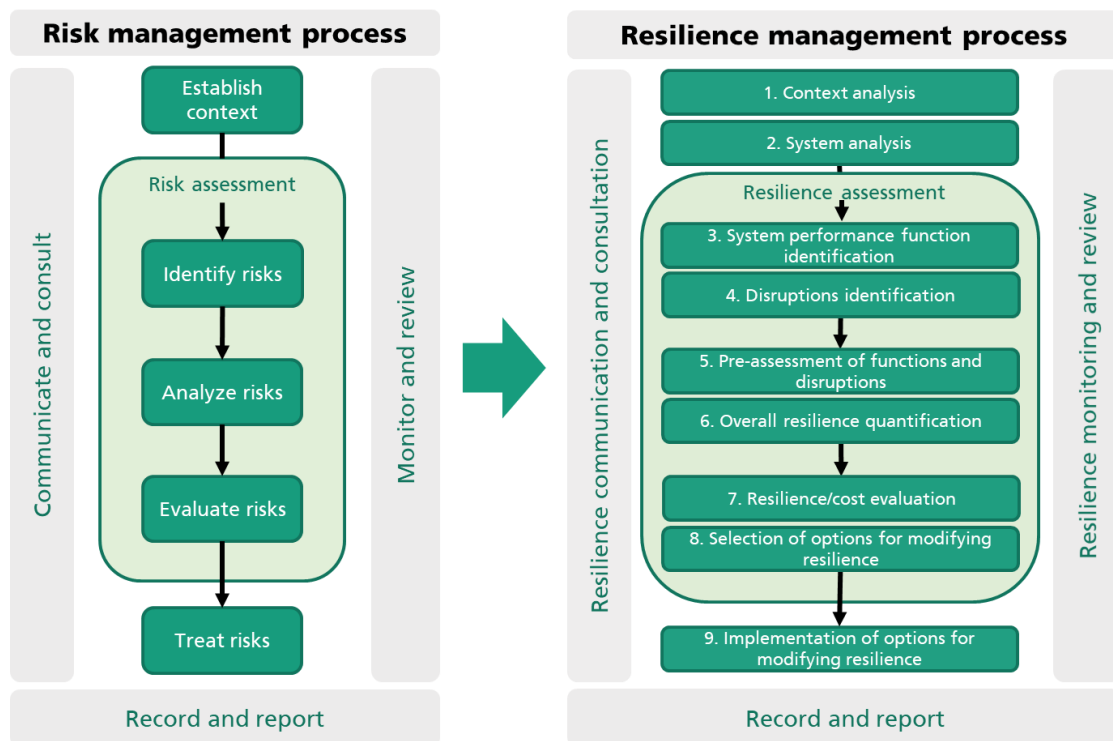


Figure 2 - Risk and resilience management processes. The risk management process (left) follows the definition of ISO 31000 (2018) Risk management – Principles and guidelines. The resilience management process (right) extends the risk management process to cover resilience specific steps [1].

¹ International Standard ISO 31000: Risk management — Principles and guidelines (<https://www.iso.org/iso-31000-risk-management.html>).

Based on this process an integrated risk and resilience management process was developed [1]. It extends the ISO 31000 standard by adding necessary steps to perform the resilience assessment, as shown in Figure 2 (right):

1. Context analysis: general description of the system, including societal, economic, legal and ethical context. Identification of key stakeholders, resilience objectives, restrictions and evaluation criteria.
2. System analysis: analysis of the system environment and interfaces, including boundary definitions, static and dynamic analysis, and (graphical) modelling / representation.
3. Identification of system performance functions: definition of (non-)performance (service) functions of the system, including qualitative and quantitative descriptions. The system (non-) performance functions in combination should cover the expected system behaviour and its assessment.
4. Identification of disruptions: identification of threats, hazards and disruptions (classical risk events) that might affect system (non-)performance. Identification of potentially affected system functions, system layers and resilience capabilities.
5. Pre-assessment of critical combinations: analysis of all combinations of system functions (step 3) and potential disruptions (step 4), in order to identify critical combinations which need to be further evaluated (in step 6). Step 5 is typically conducted analytically using a semi-quantitative approach. Step 5 and step 6 take account of all resilience cycle phases.
6. Resilience analysis: system modelling and simulation to determine resilience quantities, i.e. quantification of the resilience of the system (non-)performance functions regarding the identified threats based on the criticalities identified in the previous step 5. Step 6 covers advanced (overall) resilience quantification approaches.
7. Resilience evaluation: comparison of resilience performance, illustration of the performance loss and evaluation of the acceptance level for all threats. Step 7 evaluates the results of steps 5 and 6.
8. Selection of mitigation options: selection of improvement options based on the generation of an inventory of resilience improvement options and the selection of a decision making method. Step 8 includes the re-execution of all previous steps that affect the resilience (semi) quantification to assess the resilience gain taking account of the planned improvement methods.
9. Implementation and monitoring of mitigation options: development and implementation of options for improving resilience, based on domain-specific standards as far as possible and efficient methods corresponding to determined resilience levels for all subsystems.

These nine steps are the basis for the risk and resilience management process followed within the RESISTO project. It should be noted, that the steps are processed in a circular iterative mode, allowing to refine and retest the system. For example, the whole process should be restarted after significantly changing the system due to the implementation of a mitigation option, not only for supporting the selection of such improvement methods.

Several specific inputs (e.g. information about the system) and tools (e.g. for resilience quantification) are needed in order to process all nine subsequent steps. The specific setup for the resilience management process for the RESISTO project is described in Chapter 4. For instance, RESISTO provides a tool for the semi-quantitative tabular-analytical implementation of the overall process as well as for the simulative resilience quantification in step 6 (see section 4.2).

3. RESILIENCE DIMENSIONS

When analyzing the resilience of a system it is beneficial to divide resilience into different dimensions. This allows for all the aspects of the system to be investigated for potential resilience improvement measures. This section will look into a RESISTO specific dimension based on the source of disruption (3.1), different resilience cycles proposed in literature (3.2), resilience domains or system layers (3.3) and technical capabilities of resilience (3.4). All will allow for the communication systems in RESISTO to be categorized in a way that can aid in the resilience quantification of the system.

3.1. Cyber, physical and cyber-physical disruptions/threats

An important aim within RESISTO is to cover the full bandwidth of possible threats and disruptions for the communication infrastructures. This includes the two domains of cyber and physical threats, and in particular also possible joint cyber-physical threats. As defined in the WP2 Deliverables (i.e. D2.2 and D2.3) joint cyber-physical threats correspond to physical intrusions that can induce cyber-threats or vice versa and most importantly the correlation between them should be identified. To this respect, joint cyber-physical threats affect complex systems as Cyber-Physical Systems (CPS) and telecom infrastructures can also be seen as such, as well. To this respect, a special focus is therefore set on covering all three categories.

Looking specifically at the cyber-physical domain, [3] created a framework that allows the interconnecting areas of concern to be seen (Figure 3). Ten broad areas of concern are listed like the life cycle, the electronic and physical security and recovery plans. Included in the framework are policies, guidance and governing bodies as the areas of concern may already have their own specific requirements to report or policies to follow.

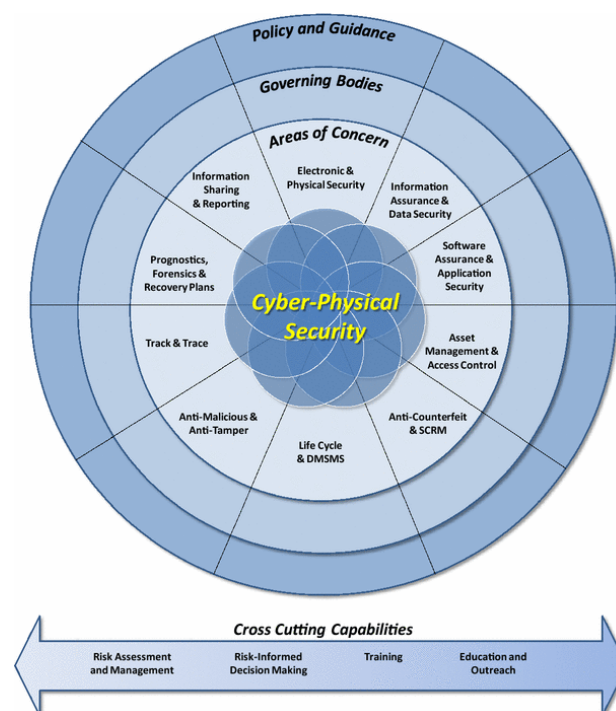


Figure 3 - The framework designed for cyber-physical security [2]

While RESISTO has a focus on communication infrastructure, other CPSs i.e. power grids also have similarities in terms of security. In telecommunication infrastructures, due to the nature of everyday operations affecting the cyber domain in a large extend (when taken into account cloud services or data services in general), the distinction between the three possible threat categories should be more precise. That is, for joint cyber-physical threats it is important the correlation between them to be identified in a more definite manner; otherwise they can be seen as only physical or cyber threats separately (for example when considering a physical threat deliberately made to induce a threat in the cyber domain after a certain period of time).

To this respect, for the sake of simplicity and in order to provide a more comprehensive manner of the risk and resilience mechanisms that can be introduced to complex systems, an example concerning to the power grids is given in the following paragraph, while the comparison to telecommunication CIs will be indicated.

Power system's physical and cyber security, the differences as well as the combination of the two are discussed in [4] (Figure 4). Physical security relates to the equipment and components of the grid and their protection. However, to protect all the components with measures like lighting, fencing or security guards would be costly and impractical. This conclusion was also derived for the telecommunication infrastructures within deliverable D4.1, where this kind of more sophisticated measures are mainly taken for main buildings or headquarters through their existing security management systems. As grid technology gets more advanced, cyber security becomes more difficult. Smart grid technology introduces an influx of data that must be protected from attacks.

Different types of attacks relevant for power systems include [4]:

- Data intrusion
- Non-technical loss fraud
- Time delay
- Replay
- Indirect cyber

Each type of attack targets a different aspect of the grid, but has the potential for major damage. Data intrusion attacks are the most common and include three subcategories: false data inject, load redistribution or denial of services. Each attack changes the data of the power system. Non-technical loss fraud adjusts consumption data, time delay changes the control signal, replay attacks use a false identity and indirect cyber attacks take advantage of the Internet of Things and use the internet to attack the grid. More or less similar threats, in terms of the cyber domain also affect the telecommunication infrastructures as well, although more physical and cyber threats can be identified for the telecommunication ones.

While being similar to the other cycles mentioned in section 3.2, the holistic resiliency cycle created by [4] is specific to cyber-physical security. The goal of this cycle is to improve resiliency of power systems as they become more complex, and vulnerable to equipment failure or external attacks. The four stages of this cycle are:

- Prevent and planning
- Detection
- Mitigation and response
- System recovery

From the above simple example concerning the power grids, it can be harmlessly stated that the same cycles are targeted within RESISTO project for all three main threat categories; it should however be noticed that RESISTO attempts to act complementary to the existing security systems of the telecommunication CIs and do not replace them instead.

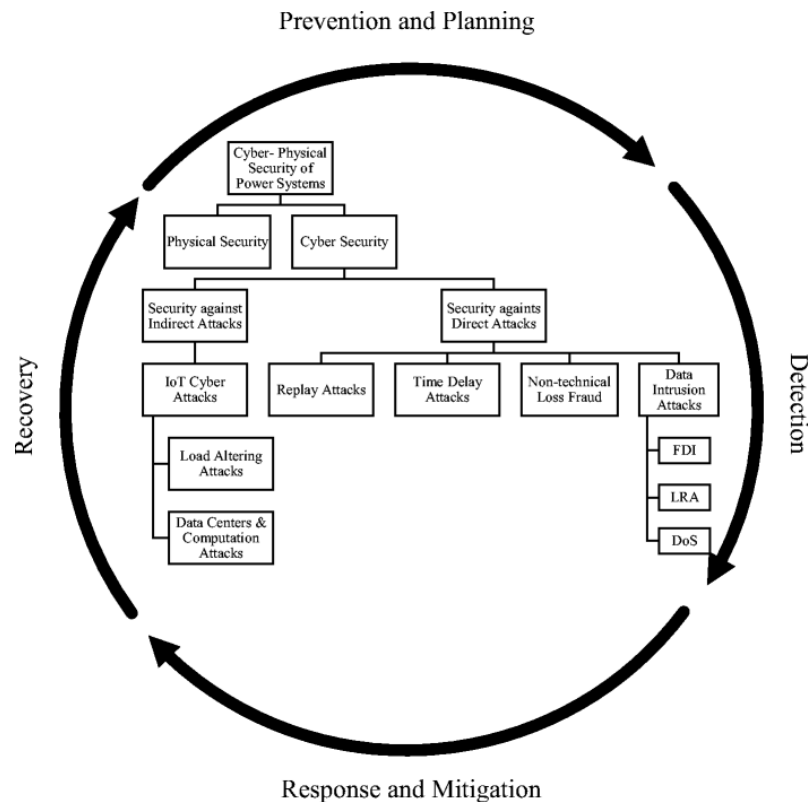


Figure 4 - The holistic resiliency cycle for cyber-physical systems [3].

3.2. Resilience cycle phases

Based on the above, various similar resilience mechanisms are identified within the existing literature as it is provided in the following:

Resilience can be defined with cycles as a way to illustrate the concept. A five phase cycle, as defined by [5], includes the phases: prepare, prevent, protect, respond and recover (Figure 5). The paper mentions that the phases all work together and do not have a simple order in reality, however each has different resilience characteristics. In the prepare phase, preparations for different kinds of disasters are made. During the prevention phase, the occurrence of a disastrous event is prevented. However some events, like natural disasters cannot be prevented. The protection phase then works to minimize the effects felt by the system due to the disaster. The response phase occurs after the event and the main goal is to maintain critical functionality and provide relief. The recover phase works to help the system adapt from the event and learn from it to better the system for future disasters or events that may occur. Other cycles that are similar to this one include the cycle proposed by the National Research Council which includes the four stages: plan, absorb, recover and adapt [6].



Figure 5 - The resilience cycle as defined by [4].

Another cycle is one designed within the ResiliNets initiative. The strategy, or cycle, for ResiliNets has two different loops: a main control loop and a background loop (Figure 6). The phases of the control loop are: defend, detect, remediate and recover while the background loop includes diagnose and refine [7]. These phase definitions are explained through the name, for example, in the defend phase the system defends against events with both passive and active defence. Similar to the prevention phase in [5], the remediate phase minimizes the consequences of the event. The diagnose phase determines the root cause of the fault and the refine phase works to better future behaviour, similar to the recover phase.

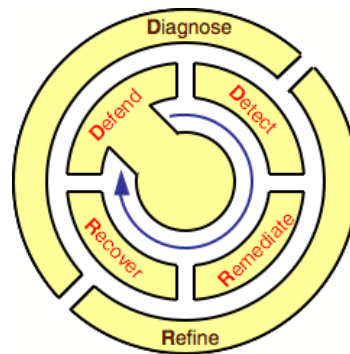


Figure 6 - The resilience cycle as defined by ResiliNets [6].

Other approaches towards a resilience cycle can be done. A general, three phase cycle was created by [8] with a focus on social resilience with disasters. The three phases are: pre-disaster, response and recovery. These phases were simplified from the Australian emergency management phases defined by the Australian government. The pre-disaster phase contains prevention and preparedness. Once the disaster or event occurs, the response phase is initiated and after the disaster, the recovery phase starts. Another cycle, defined by [9], includes three phases for creating resilience: partnering, preparing and providing. In the partnering phase there is shared responsibility between communities and the government to create resilience. During the preparing phase, all threats and hazards are analysed, including ones that are not foreseeable. Threats, hazards, shocks and stresses are differentiated but the preparing phase considers all of them. Lastly, in the provide phase, after an event occurs, the critical services need to be provided to the community with as little interruptions as possible. A four

phase cycle briefly mentioned by [10], is the OODA loop with four steps: observe, orient, decide, and act.

3.3. System domains

When creating resilience for systems, different domains or system layers are defined. These domains help when analyzing the resilience of a system by breaking the system down into different parts. Each part is then analyzed in regards to resilience making sure that no aspects are left out. One way of dividing the domains is done by MCEER [10]. The four domains of a system are defined as:

- Technical
- Organizational
- Social
- Economic

The domains, or subsystems, within community resilience are defined by [11] to be:

- Ecological
- Physical infrastructure
- Civil society
- Economic
- Governance

Within the ecological domain, important features include the natural resources that are present, like water resources, or the climate. A key characteristic of the ecological domain would be the adaptive capacity, or the ability to bounce back. The economic domain is focused on the life cycle of goods and services. Important in this domain is making sure that the critical grids and services can still be delivered and produced. Robustness also plays a large role in this domain. The physical infrastructure domain includes all the structures that support the economic domain. The civil society are organizations that are not the government such as unions or philanthropic organizations. Lastly the governance domain includes all forms of the government and their important characteristics such as robustness and adaptive capacity.

More general commonly used domains are the physical, information, cognitive and social domains [12]. The physical domain includes devices like sensors and the platforms where they work. The information domain includes all the data that is used and stored. The cognitive domain is defined to be the perceptions and biases, etc. of the interpreters of the data. Lastly, the social phase includes individuals and their interactions within the organization. However, [13] warns that as systems become more complex and interdependent resilience should focus on all the domains and their relationships to one another.

3.4. Technical resilience capabilities

There are many different resilience capabilities, or characteristics, systems can have to aid in their resilience efforts. A roadmap can be used to implement resilience and resilience engineering in society [13]. The steps include the need for specific resilience methods, system modeling, implementation of resilience engineering and communicating with the shareholders. Resilience capabilities are defined generally by [10] to be:

1. Observation: being aware of the situation
2. Modeling: completing simulations
3. Inference: making decisions
4. Implementation: taking action
5. Learning and adaption: adapting

Other capabilities that are mentioned include the ability to respond, monitor, anticipate and learn [10]. Within the observation capability there is situation awareness and in inference decision making occurs. One of the biggest characteristics is the “four R’s of resilience”. The goal of these four R’s is to improve the system’s ability to deal with the adverse events and decrease the time to recovery [14]. They are:

- Robustness
- Redundancy
- Resourcefulness
- Rapidity

Different technical capabilities can also be information sharing, the number of service disruptions and how they are managed [9]. Critical functionality, adaptability, independency and flexible response all play a role in creating a more resilient system [13]. More capabilities are tolerance to faults, disruptions or traffic where systems can deal with failures, increased loads or disruptions [15]. Survivability, dependability, security and performability are also important capabilities for resilient systems. The interconnectedness of these different capabilities can be seen in Figure 7.

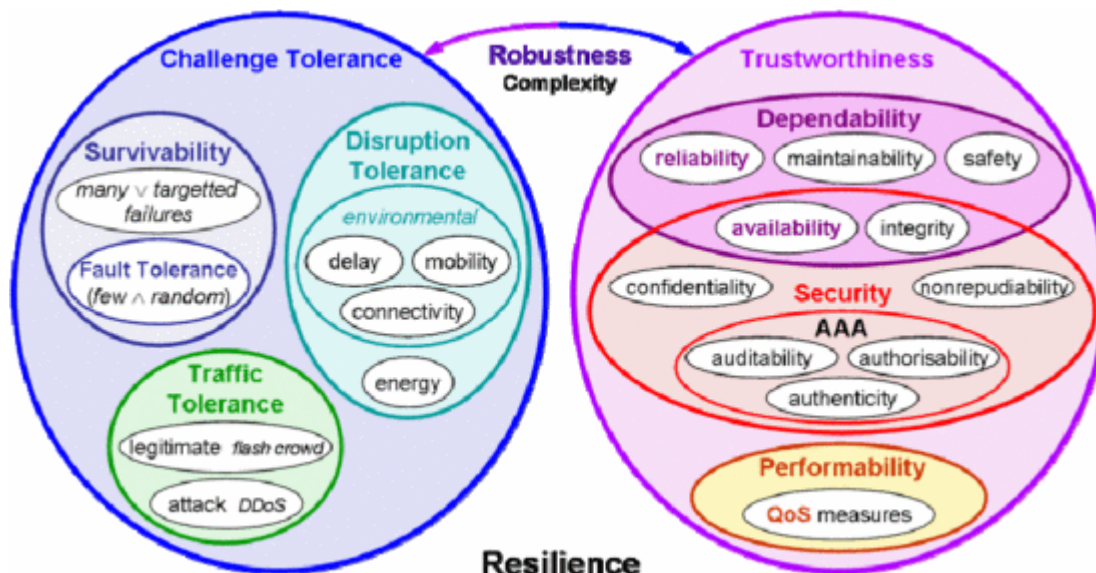


Figure 7 - Resilience characteristics and their interrelation to each other as defined by [14].

Resilience engineering is a method of implementing resilience measures using engineering tools. Technical capabilities and objectives are defined by [16] to include extending risk assessment and management approaches to have more flexibility and include “black swan” events. Like the resilience

capabilities mentioned above, extending maintainability and reliability are also important for resilience engineering. Other resilience engineering objectives are ensuring different domains like societal and organizational are included in resilience analysis as well as physical and IT security.

4. RISK AND RESILIENCE MANAGEMENT PROCESS FOR RESISTO

The risk and resilience management process was generally introduced in Chapter 2. In this chapter the meaning and implications for the RESISTO project are highlighted. First, a specification for each resilience management process step is given in subsection 4.1. It is followed in Section 4.2 by a summary of inputs and tools needed to support the management process.

4.1. Refinement of the resilience management steps

This section provides an overview how each process step is addressed by the RESISTO project. A special focus is set on the collection of relevant information from the telecommunication operators.

Since tabular information is needed as input at several steps, a combined Excel file, referred to as Excel file or input in the following, was constructed containing each table in a separate sheet. This way, it is possible to directly link the items of one list to the items of another list, allowing e.g. to extract the information which system components contribute to a system function or are affected by a given threat.

A summary of the relevant tasks, deliverables, inputs and tools is given in Table 1. Please refer to the DoW [17] and the following corresponding subsections for further information. The first and the last two columns of Table 1 are relevant for any telecommunication infrastructure. They can be understood as a major extension, tailoring and operationalization of the specifications provided for the steps in [1].

Process step		Tasks	Relevant Deliverables	Inputs by end users	Software tools
1.	Context analysis	2.1	D2.1	Questionnaire: data and inputs / requirements	
2.	System analysis	2.3	D2.4, D3.5	Excel: System Components; Network schemes	
3.	System performance function identification	3.4	D2.1, D3.7	Excel: System Functions	App: matrix assessment to act also as input for the RESISTO platform KPIs definition
4.	Disruptions identification	2.2	D2.2	Excel: Threats	App: threat ranking and matrix assessment
5.	Pre-assessment of the criticality of combinations of system functions				App: matrix assessment of correlations

	and disruptions				
6.	Overall resilience quantification	3.3, 2.3, 3.2	D2.4, D2.6, D3.5	Network schemes (technical and spatial data)	App: matrix assessment Simulator: CisiaPro, Caesar
7.	Resilience evaluation	2.4	D2.6	Risk and resilience criteria	App: matrix assessment and visualization
8.	Selection of options for improving resilience	3.2, 3.3		Excel: Improvement Measures	App: matrix assessment Simulator: CisiaPro, Caesar
9.	Development and implementation of options for improving resilience	2.4	D2.6		App or other: matrix and visualization (top level status tracking)

Table 1 - Summary of specifications of the resilience management process steps within RESISTO, comprising relevant tasks and deliverables, collected inputs and tools and methods planned to be integrated.

4.1.1. Context analysis

The socio-technical environment of RESISTO is generally described in the project DoW [17]. It also contains context information regarding the timeline, economic background, stakeholder identification, resilience objectives and resilience management domains.

In addition, a more precise context analysis is performed in task T2.1. A questionnaire was constructed to collect relevant inputs from the end-users. The questions were structured according to the resilience management process steps to ensure that all process phases are covered. The results of the questionnaire are presented in deliverable D2.1. This deliverable also contains a chapter with further requirement specifications by the end-users.

4.1.2. System analysis

The system analysis is mainly performed in T2.3, which has the aim to generate a social-technical model of the telecommunication infrastructure. This model is needed as input for any simulation of the telecommunication network, e.g. for quantifying the resilience. For this purpose the relevant system components and their connections need to be known. Two issues are identified in this context:

- Level of complexity: It needs to be addressed up to which technical layer system components need to be included, e.g. separation of components in sub-components.

- Realistic model: A realistic model of the system is needed, including details and geo-locations for all components. However, this information cannot be provided easily by the operators due to security reasons.

Deliverable D2.4 contains a summary of general network schemes that were provided by the operators. An additional evaluation of the network schemes is provided in D3.5 of T3.3. Regarding the second issue, a focus will be set on the testbeds which the operators will use for the use case scenarios. More information can be provided for the testbeds, which is currently collected for D2.5 of T2.3.

More information is provided by the Excel input. A list of all relevant system components is collected in its first table. An exemplary screenshot of this table is shown in Figure 8.

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	
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	

Figure 8 - Exemplary screenshot of the System Components table of the Excel file

The following contents are collected by the System Components table:

- ID: a unique identifier for each component
- Name: 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
- Technical characteristics: information on the component relevant for its functioning and/or assessment of disruption impacts e.g. data rate, physical dimensions, energy consumption
- Interconnections: possible direct linkages to other components of the system
- Comments: any additional information

4.1.3. System performance function identification

The system performance and non-performance functions serve as basis for resilience measures. Furthermore, they can partially be identified through the procedure for defining the RESISTO platform key performance indicators (KPIs); the preliminary background for identifying the RESISTO solution

KPIs is provided from the project DoW [17] while it will further be refined in the framework of T3.4. Shortlists of the RESISTO platform KPIs will be reported within deliverables D3.7 and D3.8 (first and final versions) of T3.4.

However, it should be noted that the system performance functions for the telecom infrastructures are not exactly the same with the RESISTO platform KPIs as it will be seen within the above-mentioned relevant Deliverables D3.7 and D3.8; the system performance functions rather serve as the parameters upon which certain KPIs of the RESISTO platform will be extracted as far as resilience mechanisms are concerned. An important aspect to be taken into account is the relevant validation measurements of the RESISTO solution KPIs within the project duration in order to act as values of the RESISTO success. To this end, it is initially foreseen that the RESISTO platform KPIs are to be validated through the telecom end users' test beds, and in this sense certain telecom system performance functions especially related to resilience factors will be validated through this manner as well.

The Excel file assigns one sheet to the table of system functions. An exemplary screenshot is shown in Figure 9.

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	
SF2	L1 Connectivity	Provides L1 Radio and FO links between equipment	Radio Network; Optical Network	SC4; SC9; SC10		Security Functions and Policies	

Figure 9 - Exemplary screenshot of the System Functions table of the Excel file.

The following contents are collected by the System Functions table:

- ID: a unique identifier for each function
- Name: 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 System Components table, needed for a full performance of the function
- Performance Quantification: definition of a minimal/critical performance rate
- Dependence of other SFs: a drop-down menu to select possible other system functions on which this system function depends
- Comments: any additional information

4.1.4. Disruptions identification

Understanding the vulnerabilities of essential communication networks is key to supporting response during and recovery following a natural disaster or a cyber/physical attack. Additionally, it is also important to be able to correlate a threat with a specific impact or disruption and in this sense to be able to correlate physical and cyber threats that initially are regarded as separate incidents.

There already exist a number of standards and guidelines for critical infrastructure information security risk assessment and management². These standards and guidelines can form the basis of understanding the risks associated with communication networks, especially nowadays, where a new transformation is happening in the communication infrastructures as they start to merge with cloud infrastructures and with the trend that communication equipment is also becoming virtualized along with its services with network function virtualization (NFV). Network function virtualization is a network architecture concept that uses the technologies of IT virtualization to virtualize entire classes of network node functions into building blocks that may connect, or chain together, to create communication services³.

Root cause analysis: Root cause analysis (RCA) is a systematic process for identifying “root causes” of problems or events and an approach for responding to them. RCA is based on the basic idea that effective management requires more than merely “putting out fires” for problems that develop, but finding a way to prevent them⁴. For telecommunication CIs on a high level the impact of identified threats is in general known and identified as partially listed below:

- Loss of service/connectivity
- Service Disruptions
- Degradation of quality
- Data loss
- Data leakage

However, depending on the extent of the disaster or attack and the system affected, the result may vary. Localization is an important aspect, especially with regard to whether the affected system is a connection or service platform, or a datacenter hosting several services.

Link Problems

Regarding telecommunication networks, there usually are redundant links between locations and service platforms, but if a link is for some reason down, if a redundant link exists, there may be some momentary disruption. However, if the capacity of the affected link cannot be properly compensated, then congestion will occur and users could suffer various of the above problems. This case usually refers to connections that are providing internet connectivity to users, where capacity is an important factor. Also, the closer to the core network a link problem may occur, the more users are probably affected, as links are aggregated into fewer and larger capacity connections when going from the last mile to the core network.

² threat and vulnerability catalogue[secrit]

³ https://en.wikipedia.org/wiki/Network_function_virtualization

⁴ <https://des.wa.gov/services/risk-management/about-risk-management/enterprise-risk-management/root-cause-analysis>

The situation may vary if the link problem is within a datacenter, where usually, it is easier to fix the link, so the problems or downtime caused, is shorter.

A list of potential disruptions is shown in Table 2. It is an extraction from the Excel sheet discussed below (see Figure 10).

Name	Subsystems affected	Impact on other CIs
DDoS Attack	Core Network; Data Center	
Data exfiltration	Applications, ; Applications, Internal Network, Data Center	
Physical Connectivity Cuts	Optical Network, Radio Network	May impact other Telco CIs that share infrastructure with OTE. May impact similar SFs
Weather Hazard	Optical Network, Radio Network	May impact other Telco CIs that share infrastructure with OTE. May impact similar SFs
Fire	all	May impact other Telco CIs that share infrastructure with OTE. May impact colocated SFs
Earthquake	all	May impact other Telco CIs that share infrastructure with OTE. May impact colocated SFs
Power Shortage	all except physical connections	May impact other Telco CIs that share infrastructure with OTE. May impact colocated SFs

Table 2 – List of potential disruptions, stating its name (cause/event), affected subsystems and impact on other CIs.

Service problems

- Access
- Authentication/Authorization
- Internal Business Systems
- End user services Systems

The generation of a threat list for the telecommunication infrastructures is the aim of task T2.2. A first review is given in deliverable D2.2, which is currently updated. The Excel file contains a table for collecting input for the threat list. An exemplary screenshot of the table is shown in Figure 10.

ID	Name	Description	Hazard type	Hazard cause	Frequency	Duration	Economic impact	Impact on society	SCs affected directly	SCs affected indirectly	SFs affected	Subsystems affected	Impact on other CIs	Comments
T1	DDoS Attack	Botnets scan and often attack visible (i.e. – Public IPs) targets such as public-facing servers and networking equipment that are accessible from the internet, such as web servers, authentication servers, routers, firewalls.	cyber	man made (attack)	very frequently: ≥ 10 /week	Variable: minutes to tens of hours	low	high	SC5	SC1	SF5; SF6	Core Network; Data Center		
T2	Data exfiltration		cyber	man made (attack)	rare: ≤ 1 /year	Several hours	high	high	SC6	SC5; SC7; SC8	SF5; SF6	Applications; Applications, Internal Network, Data Center		

Figure 10 - Exemplary screenshot of the Threats table in the Excel file.

The threats table contains the following information:

- ID: a unique identifier per hazard
- Name: a short name related to the hazard cause, e.g. earthquake
- Description: further information about the hazard
- Hazard type: a classifier to identify the event as *physical*, *cyber* or *cyber-physical*
- Hazard cause: a classifier to identify the general source as either *man-made (accidental)*, *man-made (attack)*, *technical/system failure*, or *natural*
- Frequency: a classifier to rank the occurrence of the event from *very frequent* (≥ 10 /week) to *rare* (≤ 1 /year)
- Duration: approximate mean time the system is affected
- Economic impact: classifier (*high*, *medium*, *low*, *no*)
- Impact on society: list observed and possible impacts on the society
- SCs affected directly: a drop-down menu to select all system components, from the System Components table, directly affected by the threat
- SCs affected indirectly: a drop-down menu to select all system components, from the System Components table, indirectly affected by the threat
- SFs affected directly: a drop-down menu to select all system functions, from the System Functions table, directly affected by the threat
- Subsystems affected: classifier (*radio network*, *optical network*, *satellite network*, *core network*, *data center*, *applications*, *internal network*)
- Impact on other CIs: can be needed to simulate cascading effects or as another indicator for the threat impact

- Comments: any additional information

4.1.5. Pre-assessment of the criticality of combinations of system functions and disruptions

Aim of this step is to identify the critical pairs of system functions and threats that need to be further investigated. Inputs to both, the system functions and the threats, are collected in the Excel file (see sections 4.1.3 and 4.1.4). The direct linkage of the tables in the Excel file allows to estimate the correlation of system functions and threats. One contribution comes from the directly affected system functions given in the Threats table. In addition, the threats may affect system components that are needed for the system function to work properly. The example of a resulting correlation matrix is shown in Figure 11. It was produced using an interactive tool, which is further described in section 4.2.

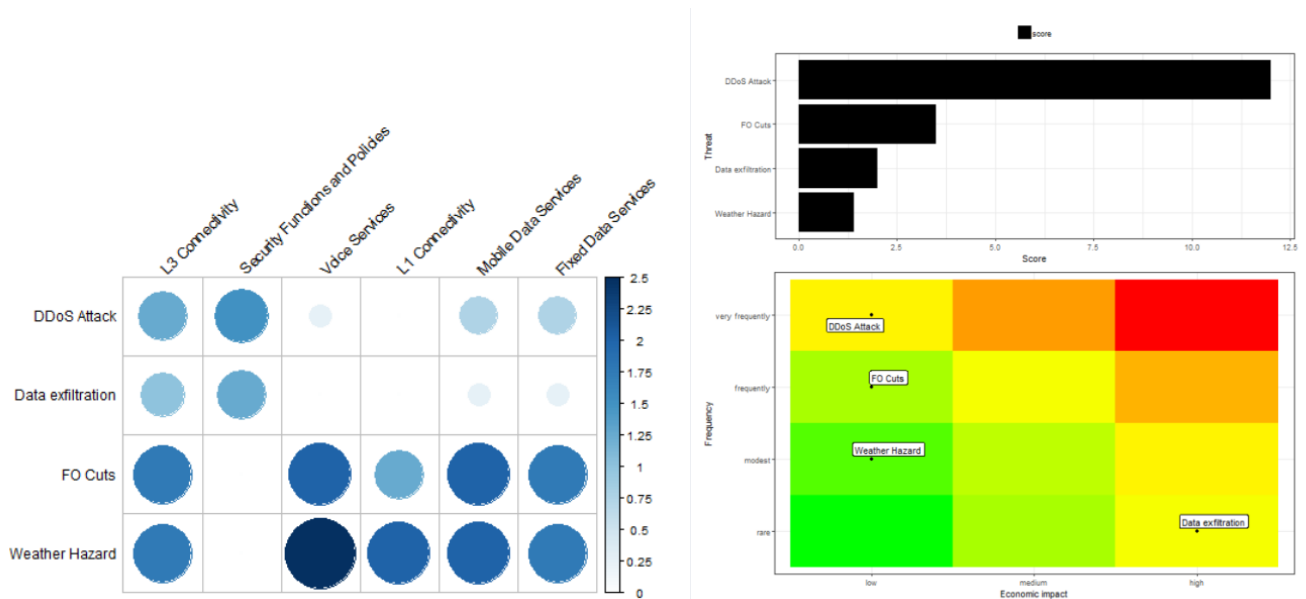


Figure 11 - Exemplary correlation matrix of system functions and threats (left) and threat ranking (right top) by a score calculated based on the frequency and economic impact (right bottom). It should be noted, that the entries in the correlation matrix are not normalized but rather refer to a connection strength in arbitrary units.

A major point for further investigation is the identification of concrete selection criteria for the criticalities. This could partially rely on the strongest connections found. However, also other criteria should be taken into account. For example, an important additional indicator would be a risk assessment based score for the threats, since threats with major impact not necessarily show the strongest connections to system function, as shown in Figure 11.

4.1.6. Overall resilience quantification

The resilience quantification is based on the resilience quantities of interest, e.g. selected system functions, and a realistic model of the system. For RESISTO, the resilience computation will be based

on network simulations carried out using the tools CisiaPro (short term and long term control loop) and Caesar (long term control loop).

The underlying network models are primarily evaluated as described in section 4.1.2 for the system components. The tasks and deliverables mentioned in that subsection also contain descriptions for the simulation tools. In addition, further information is provided in deliverable D2.6 of T2.4, introducing the RESISTO architecture.

4.1.7. Resilience evaluation

The resilience evaluation is mainly based by the outputs of the previous steps, the resilience pre-assessment (step 5) and resilience quantification (step 6). Different tabular and graphical visualisations will be implemented in the cockpit of the RESISTO platform. The architecture of the platform is refined within T2.4 and its deliverable D2.6.

Resilience evaluation depends on risk and resilience criteria (risk of resilience loss criteria) as specified by the end-users on top level in step 1.

4.1.8. Selection of options for improving resilience

For threats that are evaluated as non-acceptable in the previous step, adequate improvement measures need to be implemented. As starting point, a list of possible improvement options is generated or provided. A table with improvement options is included in the Excel file, thus providing a primary input for the threats given in the threats table of the Excel file. An exemplary screenshot is shown in Figure 12.

ID	Name	Description	Threat	Component	Action Type	Comments
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; SC4	protection	
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; SC4	preparation	

Figure 12 - Exemplary screenshot of the table of improvement measures of the Excel file.

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

- ID: a unique identifier for each IM
- Name: name of the IM
- Description: general information about the IM
- Subsystem: a drop-down menu to select all threats, from the Threats table, that are targeted by the IM
- Component: a drop-down menu to select all system components, from the System Components table, that are 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

The options provided by the list are compared by re-assessing the resilience of the system via simulations, as described in section 4.1.6 Resilience quantification.

In T3.2 additional methods and tools are reviewed for their use within RESISTO, which could possibly also support the selection of improvement measures.

4.1.9. Development and implementation of options for improving resilience

The development and implementation of improvement options will be based on the results obtained in the previous step. To facilitate the decision making, appropriate visualisation tools (tabular, graphical) need to be implemented in the cockpit of the RESISTO platform. The platform architecture is refined in T2.4 and its deliverable D2.6.

Step 9 resorts as much as possible to existing (domain) development standards and comprises only top level monitoring.

4.2. Supporting inputs, tools and methods

A successful application of the resilience management process requires specific and realistic inputs from the end-users and appropriate tools to further process the inputs and generate outputs.

The inputs per resilience management process step are discussed in the previous section. A major contribution is provided by the Excel file, containing four interlinked tables. The inter-dependencies of the tables are summarized in Table 3.

Name	Abbreviation	Step	Linkage			
			SC	SF	T	IM
System Components	SC	2				
System Functions	SF	3	•			
Threats	T	4	•	•		
Improvement Measures	IM	8	•		•	

Table 3 - Interlinkages of the tables in the Excel file. The linkage states if the elements from one table affect, depend on or target elements from another table.

The rich information content of the tables and their linkage led to the development of a web-application to easier access and visualize the contents. The application is based on the Shiny package⁵ in the statistical programming language R. Screenshots of the app are shown in Figure 8 - Figure 12. An additional exemplary screenshot of an implemented visualisation option of the tabular inter-connections is shown in Figure 13. More information about the Shiny-app is provided in chapter 5 of deliverable D3.3.

The main software tools for quantifying resilience in telecommunication infrastructures are the network simulators CisiaPro and Caesar (see section 4.1.6).

⁵ <https://shiny.rstudio.com/>

In addition, further possible methods and tools to be used are evaluated in T3.2. It still needs to be further investigated if and how they will be implemented. With respect to T3.1 it also needs to be specified which resilience management step is supported.

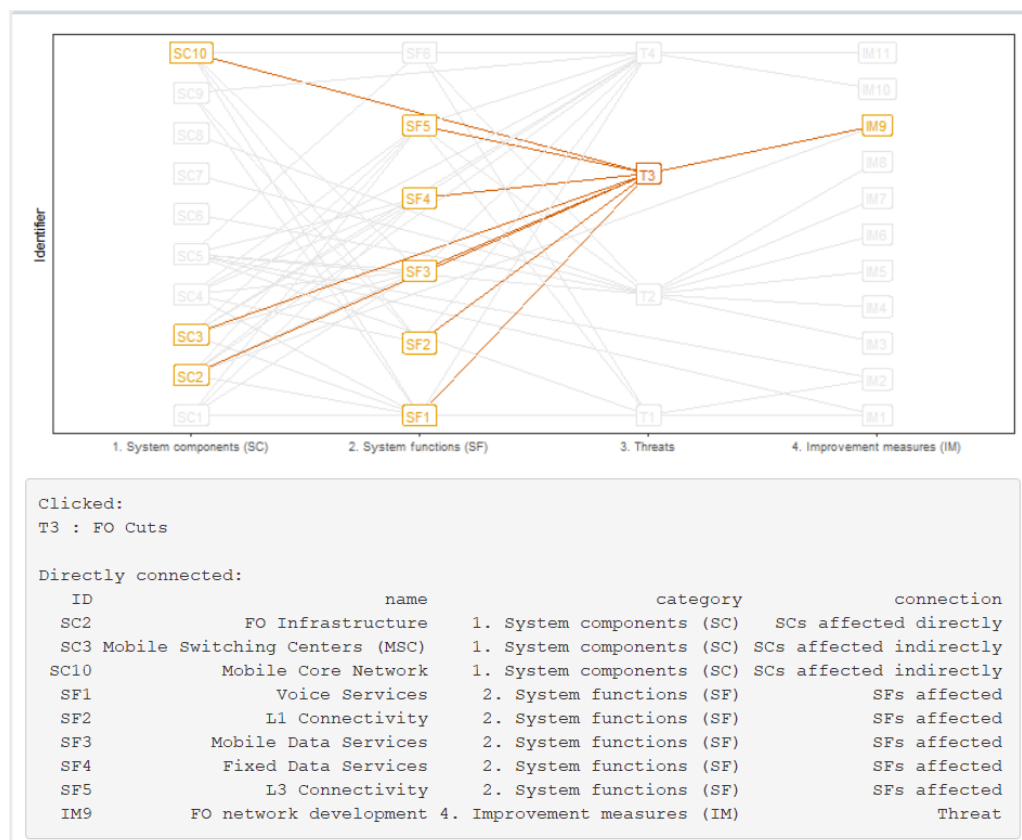


Figure 13 - Exemplary screenshot of a visualisation of the inter-connections of the tables in the Excel file.

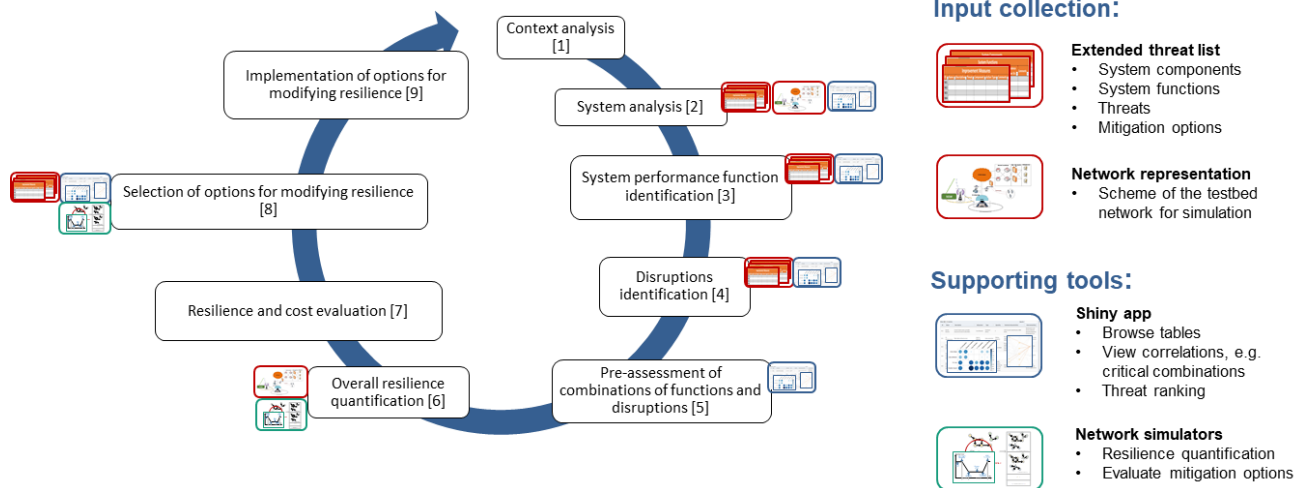


Figure 14 – Input and tools supporting the risk and resilience management process for the long term control loop of RESISTO. The usage of the tabular inputs and graphical network representations is indicated by orange boxes and the support by the Shiny app and simulation tools by blue or green boxes, respectively.

5. SUMMARY

This deliverable reports the status of T3.1 of WP3 at intermediate runtime. The main focus of this document was the introduction and first specification of the risk and resilience management process for the long term control loop. The specifications for RESISTO depend on the input from various other tasks and WPs. They therefore need to be updated and further defined with the progress of the other tasks and WPs.

Another focus was set on identifying relevant resilience dimensions, which need to be covered by RESISTO. In this report, a literature based review of resilience dimensions is included. The usage and coverage by RESISTO needs to be further specified.

The task is ongoing and an outlook to the next steps is recapped in the following subsection.

5.1. Next steps

The identification and specification of inputs, tools and methods for each of the risk and resilience management process steps, as primarily done in Table 1, is an ongoing process. For example, tools and methods collected in task T3.2 should be associated with the corresponding process step. It might also be necessary to consider the work done in other WPs, as only inputs from WP2 and WP3 were considered at this stage. In addition, the linkage to existing domain specific standards (technical safety, IT-Security, physical security and perimeter protection) needs to be addressed.

An important quality feature is to ensure the coverage of all relevant resilience dimensions. The importance and usability for RESISTO needs to be further evaluated, including a direct association with the resilience management process.

References

- [1] I. Häring et al., „Towards a Generic Resilience Management, Quantification and Development Process: General Definitions, Requirements, Methods, Techniques and Measures, and Case Studies Resilience and Risk,“ in *Resilience and Risk*, Bd. 6, I. Linkov und J. M. Palma-Oliveira, Hrsg., Dordrecht, Springer Netherlands, 2017, pp. 21-80.
- [2] International Organization for Standardization, „ISO 31000 Risk management - Principles and guidelines,“ Genf, 2009.
- [3] D. DiMase, Z. A. Collier, K. Heffner und I. Linkov, „Systems engineering framework for cyber physical security and resilience,“ *Environment Systems and Decisions*, pp. 291-300, June 2015.
- [4] S. Mehrdad, S. Mousavian, G. Madraki und Y. Dvorkin, „Cyber-Physical Resilience of Electric Power Systems Against Malicious Attacks: a Review,“ *Current Sustainable/Renewable Energy Reports*, pp. 14-22, March 2018.
- [5] K. Thoma, B. Scharte, D. Hiller und T. Leismann, „Resilience Engineering as Part of Security Research: Definitions, Concepts and Science Approaches,“ *European Journal for Security Research*, pp. 3-19, April 2016.
- [6] National Research Council, „Disaster Resilience: A National Imperative,“ The National Academies Press, 2012.
- [7] J. Sterbenz und D. Hutchison, „ResiliNets: Multilevel Resilient and Survivable Networking Initiative,“ 2006. [Online]. Available: <https://www.ittc.ku.edu/resilinet/>.
- [8] S. Khalili, M. Harre und P. Morley, „A temporal Social resilience framework of communities to disasters in Australia,“ *Geoenvironmental Disasters*, 2018.
- [9] NSW Department of Justice | Office of Emergency Management, „NSW Critical Infrastructure Resilience Strategy,“ State of New South Wales, Sydney NSW, 2018.
- [10] I. Häring, S. Ebenhöch und A. Stolz, „Quantifying Resilience for Resilience Engineering of Socio Technical Systems,“ *European Journal for Security Research*, pp. 21-58, 2016.
- [11] P. H. Longstaff et al., „Building Resilient Communities: A Preliminary Framework for Assessment,“ *Homeland Security Affairs*, September 2010 <https://www.hsaj.org/articles/81>.
- [12] D. Alberts und R. Hayes, „Power to the Edge. Command...Control...in the Information Age,“ Information Age Transformation Series, Washington, DC, 2003 http://www.dodccrp.org/files/Alberts_Power.pdf.
- [13] I. Linkov, T. Bridges, F. Creutzig, J. Decker, C. Fox-Lent, W. Kröger, J. H. Lambert, A. Levermann, B. Montreuil, J. Nathwani, R. Nyer, O. Renn, B. Scharte, A. Scheffler, M. Schreurs und T. Theil-Clemen, „Changing the resilience paradigm,“ *Nature Climate Change*, pp. 407-409, 2014.
- [14] P. Tamvakis und Y. Xenidis, „Comparative Evaluation of Resilience Quantification Methods for Infrastructure Systems,“ *Procedia - Social and Behavioral Sciences*, pp. 339-348, 2013.
- [15] Y. Hamida, B. Amine und B. Mostafa, „Toward resilience management in critical information infrastructure,“ in *2015 5th World Congress on Information and Communication Technologies (WICT)*, Morocco, 2015.
- [16] I. Häring, B. Scharte, A. Stolz, T. Leismann und S. Hiermaier, „Resilience Engineering and Quantification for Sustainable Systems Development and Assessment: Socio-technical Systems and Critical Infrastructure,“ in *IRGC Resource Guide on Resilience*, Lausanne: EPFL International Risk Governance Center, IRGC, 2016.
- [17] RESISTO, „Grant Agreement. Project Starting Date: May, 1st 2018“.
- [18] I. e. a. Häring, „Towards a Generic Resilience Management, Quantification and Development Process: General Definitions, Requirements, Methods, Techniques and Measures, and Case Studies Resilience and Risk,“ in *Resilience and Risk*, Bd. 6, I. Linkov und J. M. Palma-Oliveira, Hrsg., Dordrecht, Springer Netherlands, 2017, pp. 21-80.