

RESISTO:

D3.2_Risk and resilience management process for cyber- physical threats of telecom CI



RESISTO

D3.2 – 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_D3.2_200417_01	Version:	1.0
Deliverable:	D3.2	Date:	17/04/2020
		Status:	APPROVED

Document classification	Public
--------------------------------	---------------

Approval Status	
Prepared by:	Gael HAAB (Fraunhofer)
Approved by: (WP Leader)	Mirjam FEHLING-KASCHEK (Fraunhofer)
Approved by: (Coordinator)	Bruno SACCOMANNO (LDO)
Advisory Board Validation (Advisory Board Coordinator)	Carmen PATRASCU (ORO)
Security Approval (Security Advisory Board Leader)	Paolo DI MICHELE (LDO)

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Mirjam Fehling-Kaschek, Natalie Miller, Gael Haab, Andrea Roland, Ivo Häring, Jörg Finger	EMI (Fraunhofer)	Scientific Researcher
Maria Belesiotti, Evangelos Sfakianakis, Ioannis Chochliouros	OTE	Telecom experts
Rodoula Makri, Panagiotis Karaivazoglou, Apostolos Papafragkakis, Takis Kelefas, Michalis Sofras, Evangelos Groumpas, 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
V0.1	15.08.2019	ALL	ALL	First draft (copy of D3.1)
V0.2	20.12.2019	ALL	ALL	Preliminary version for WP3 review
V0.2	21.01.2020	Page 21	4.1	Final version after WP3 review
V0.3	28.01.2020	ALL	ALL	Final Release for AB validation
V0.4	12.03.2020	ALL	ALL	Final Release for SAB assessment
V1.0	17.04.2020	ALL	ALL	Final version

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 Puccini 2 – Genova – 16154 – Italy
Tel.: +39 348 6505565
E-Mail: bruno.saccomanno@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 final status of task T3.1 “Long term learning cyber-physical risk and resilience management”. 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.

The report is based on the first version of the report (D3.1). Updates and modifications made for D3.2 are summarized in the Introduction.

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	19
3.4. Technical resilience capabilities	20
4. RISK AND RESILIENCE MANAGEMENT PROCESS FOR RESISTO	22
4.1. Refinement of the resilience management steps	22
4.1.1. Context analysis	23
4.1.2. System analysis	24
4.1.3. System performance function identification	25
4.1.4. Disruptions identification	27
4.1.5. Pre-assessment of the criticality of combinations of system functions and disruptions	30
4.1.6. Overall resilience quantification	31
4.1.7. Resilience evaluation	32
4.1.8. 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. Selection of options for improving resilience	33
4.1.9. Development and implementation of options for improving resilience	35
4.2. Supporting inputs, tools and methods	35
4.3. Requirements traceability	37
5. SUMMARY	39

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 [4]	14
Figure 4 - The holistic resiliency cycle for cyber-physical systems [5].	16
Figure 5 - The resilience cycle as defined by [6].	17
Figure 6 – A typical performance time curve with the resilience phases added [6]. This system exemplifies adaptive capacity as the final performance is greater than the initial.	18
Figure 7 - The resilience cycle as defined by ResiliNets [8].....	18
Figure 8 - Resilience characteristics and their interrelation to each other as defined by [8].	21
Figure 9 - Exemplary screenshot of the System Components table of the Excel file	24
Figure 10 - Exemplary screenshot of the System Functions table of the Excel file.	25
Figure 11 - Exemplary screenshot of the Threats table in the Excel file.	29
Figure 12 - 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.	30
Figure 13 - A generic performance time curve. The resilience indicators, RI1-RI4, are specified.	31
Figure 14 – Illustration of performance curve computed with CaESAR for two performance functions (Biggest connected component and Percentage working components), and two different threats, with different mean time to repair (200 or 350 minutes).	32
Figure 15: The matrix structure within the knowledge base.....	33
Figure 16 - Exemplary screenshot of the table of improvement measures of the Excel file.	33
Figure 17 – Illustration of resilience curve and expected resilience improvement through the improvement measure.....	34
Figure 18 - Exemplary screenshot of a visualisation of the inter-connections of the tables in the Excel file.	36
Figure 19 – 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.	36

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
LTCL	Long Term Control Loop
LTE	Long Term Evolution (= 4G)
NFV	Network Function Virtualization
RI's	Resilience Indicators
STCL	Short Term Control Loop
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 control loop (STCL) and the long term control loop (LTCL). A scheme of the architecture of the integration platform is shown in Figure 1.

Aim of WP3 “Cyber-physical risk/resilience assessment and improvement process for preparation, prevention and protection” is the definition of the long term control loop of the RESISTO platform.

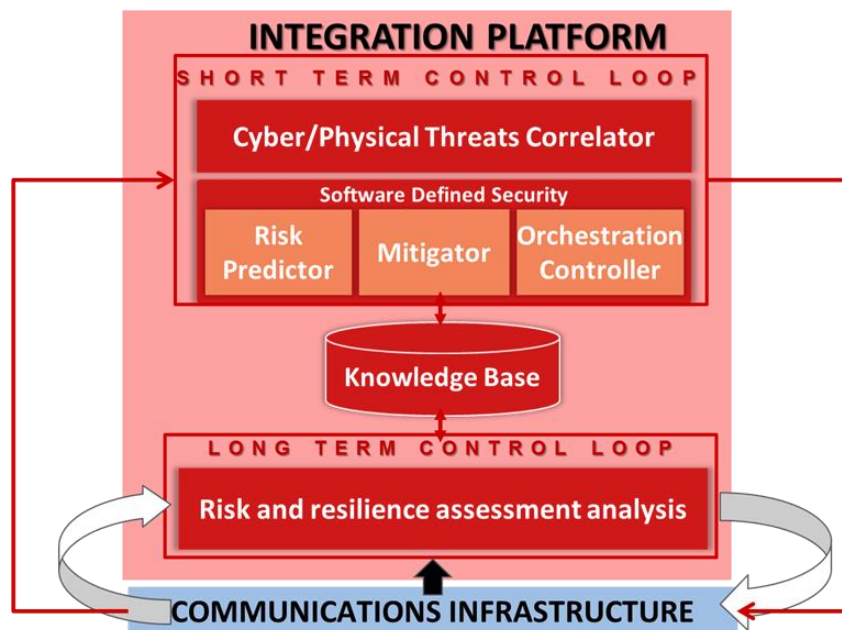


Figure 1 - RESISTO logical architecture (see deliverable D2.6 for more information)

The main feature of the long term control loop is the risk and resilience analysis and management process for telecommunication critical infrastructure (CI). It covers telecommunication specific cyber-physical risk control and resilience analytics. Besides the risk and resilience analysis tool for cyber, physical and cyber-physical threats, a main outcome of the WP is the definition and provision of key performance indicators (KPIs) for the risk and resilience assessment

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 work of T3.1. The 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 selection of adequate resilience dimensions, supporting the resilience quantification process.

In the following, the structure of the report is summarized and updates with respect to the first version of the report (D3.1) are highlighted for each chapter.

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

- ➔ Updates: No updates were added in the text since this chapter contains only a short summary of the risk and resilience management process which is described in detail in the context of the RESISTO project in chapter 4.

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

- ➔ Updates: All information provided in this chapter was reviewed and updated. In particular, information about the resilience cycle phases and the performance time curve ("resilience curve") were added in section 3.2. In section 3.4, information about the "four R's of resilience" were detailed and linked to the resilience indicators (RI's) used in 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.

- ➔ Updates: Minor updates in section 4.1, i.e. relevant tasks, deliverables and methodologies (developed in the deliverable D3.4 "Methods for cyber-physical security management for telecom CI") were added to Table 1. An explanation of the system performance function quantification in the context of the RESISTO project was added to section 4.1.3. The different assessment methods and tools collected in deliverable D3.4 to improve the knowledge about the hazards threatening the CI's were added in the section 4.1.4. In section 4.1.6, the performance time curve used to quantify resilience in the context of the RESISTO project was described and illustrated. The resilience matrix and resilience indicators (RI's) which enable to evaluate the resilience are presented in section 4.1.7. In the section 4.1.8 the link between resilience improvement and RI's were added. In section 4.2 methods and tools developed in deliverable D3.4 were added. Finally, section 4.3 was added to trace the requirements collected in deliverable D2.1 "End user requirements for integrated cyberphysical risk and resilience management".

Chapter 5 provides a summary of the report and an outlook on the LTCL implementation followed in the other ongoing and future tasks and WPs.

- ➔ Updates: The summary was updated to take into account that this is the final version of the report from T3.1.

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) version [3].

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

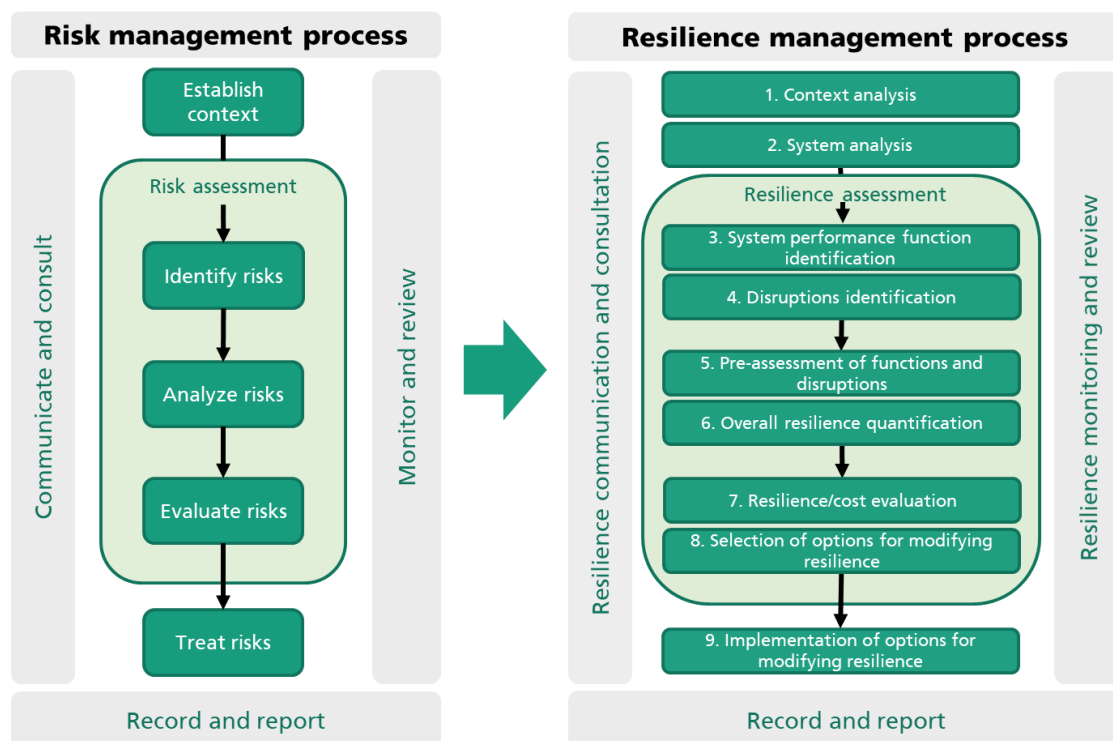


Figure 2 - Risk and resilience management processes. The risk management process (left) follows the definition of ISO 31000 (2018) Risk management – Principles and guidelines. The resilience management process (right) extends the risk management process to cover resilience specific steps [1].

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 analysing 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, [4] 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.

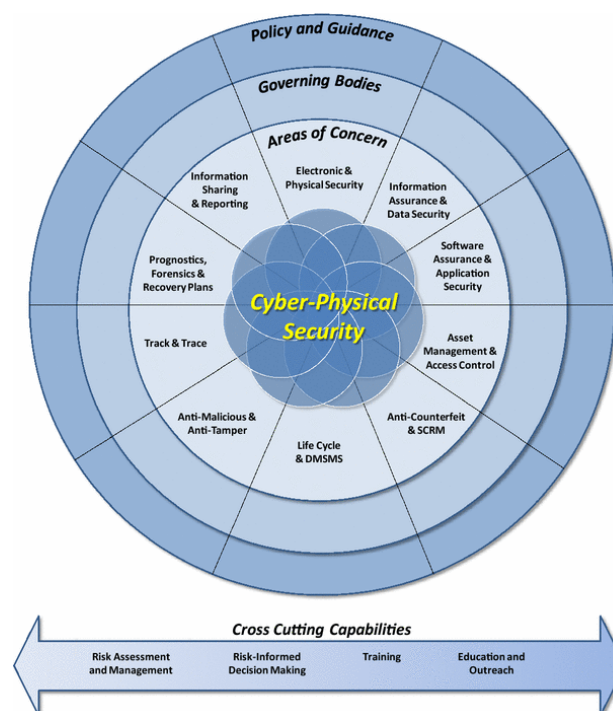


Figure 3 - The framework designed for cyber-physical security [4]

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 [5] (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 [5]:

- 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 [5] 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. Indeed, the RESISTO platform will use the information delivered from the existing security system of the telecommunication CIs in order to improve the response to the threats and therefore the resilience of the telecommunication CIs. (See deliverable D2.7 section 2.2)

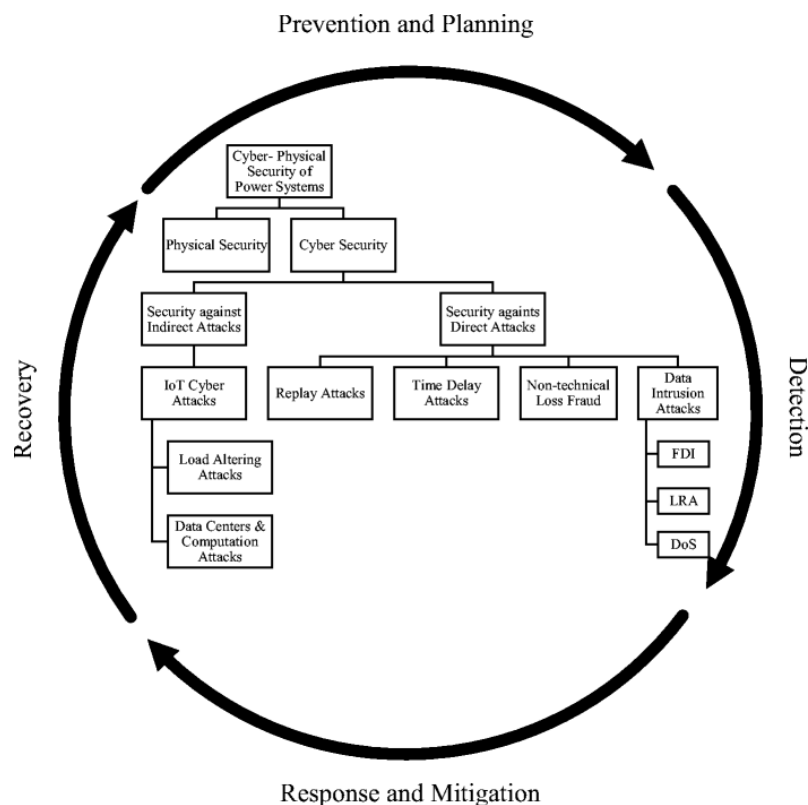


Figure 4 - The holistic resiliency cycle for cyber-physical systems [5].

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. The cycle describes that the work toward building a resilient system is a continuous process. A five phase cycle, as defined by [6], 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, now known as the National Academies of Sciences, Engineering, and Medicine (NASEM), which includes the four stages: plan, absorb, recover and adapt [7]. The absorb phase in the NASEM definition is similar to the protection phase and works to absorb shocks and reduce disasters. The NASEM definition splits recovery and adaption into two separate categories, whereas adaption is a part of the recovery phase in the cycle proposed by [6]. New threats to the system will always be present, as its environment will change over time. Hence, the system will continue to learn from harmful events, improve and adapt to new conditions.



Figure 5 - The resilience cycle as defined by [6].

To better illustrate the resilience cycle phases, Figure 6 shows a system's performance P over time t . This curve is also referred to as "resilience curve" and illustrates the quantification of the performance loss due to a disruptive event. The diagram displays the five resilience cycle phases before, during and after the occurrence of the disruptive event. The phases have different characteristics, as mentioned before, and are applied at different stages regarding a disturbance in the system performance. The preparation phase occurs before the disruptive event. The prevention measures work to stop the disruptive event from occurring (if possible). If the event occurs, the protection measures work to reduce damages and performance loss. During the responding phase, the performance stays relatively constant as the focus is on evacuating or calls for help. Finally, the recovery phase works to build back the system. All the phases are applied to minimize the performance loss in the system when being exposed to a disruption. It can be noted that during the recovery phase for this example, the level of system performance has increased to a higher degree than initial system performance. This indicates that the system has learned and adapted from the disruptive event and increased its capability to deal with future disturbance. Additionally, the system needs to sustain critical functionality over time in adverse conditions. The duration of the different phases varies dependently on the system capabilities and type of disruption, and is used when quantifying the resilience [5]. Further information on performance time curves and how they can be used for quantification of resilience is given in Section 4.1.6.

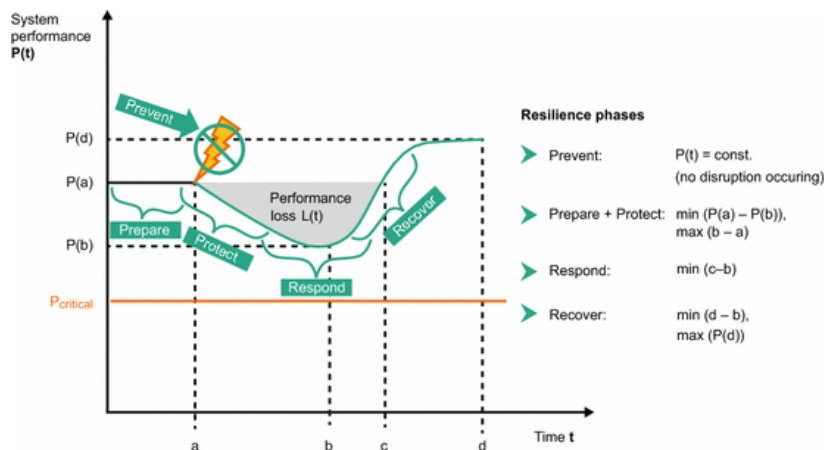


Figure 6 – A typical performance time curve with the resilience phases added [6]. This system exemplifies adaptive capacity as the final performance is greater than the initial.

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 7). The phases of the control loop are: defend, detect, remediate and recover while the background loop includes diagnose and refine [8]. 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 [6], 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.

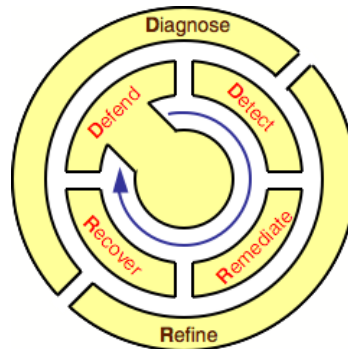


Figure 7 - The resilience cycle as defined by ResiliNets [8].

Other approaches towards a resilience cycle can be done. A general, three phase cycle was created by [9] 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 [10], 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 [11], is the OODA loop with four steps: observe, orient, decide, and act.

For the RESISTO project, based on the further described resilience cycle one model has been developed in order to take the resilience cycle and the system architecture into account. . The logical architecture from RESISTO is composed of two loops, the Long Term Control Loop and the Short Term Control Loop. The Long Term Control Loop is responsible for the identification and the protection phase and the Short Term Control Loop for the detection, reaction and mitigation phase (See deliverable D2.7 section 2).

3.3. System domains

When creating resilience for systems, different domains or system layers are defined. These domains help when analysing the resilience of a system by breaking the system down into different parts. Each part is then analysed in regards to resilience making sure that no aspects are left out. One way of dividing the domains is done by MCEER [11]. The four domains of a system are defined as:

- Technical
- Organizational
- Social
- Economic

The resilience of each domain mentioned can differ significantly in comparison to the others domains. For example, it is possible for a system to have great technical capabilities, but very low organizational capabilities. Additionally, the quantification of resilience may be more complicated in some of the domains than others. For instance, measuring resilience in the technical domain is straightforward compared to the social domain, when regarding performance losses and recovery.

The domains, or subsystems, within community resilience are defined by [12] 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 [13]. 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, [14] 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. With the use of resilience engineering, complex systems are able to maintain critical functionality, exhibit graceful degradation and achieve fast recovery under disruption, with the help of technical resilience capabilities. These capabilities have to be utilized when the system is in a harmful situation. By only implementing case-specific capabilities, the system is not able to cope with unexpected events that are not predefined. Therefore, a resilient system must have generic resilience capabilities. This way the system is able to withstand stress, recover and adapt to predicted and unpredicted events [5]. A roadmap can be used to implement resilience and resilience engineering in society [14]. The steps include the need for specific resilience methods, system modelling, implementation of resilience engineering and communicating with the shareholders. Resilience capabilities are defined generally by [11] to be:

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

In RESISTO these resilience capabilities are present in the two loop from the system architecture. The Long Term Control Loop is responsible for the steps Observation, Modelling and Learning and adaption, and the Short Term Control Loop for the steps Inference and Implementation.

Other capabilities that are mentioned include the ability to respond, monitor, anticipate and learn [11]. 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” [15]. 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 [16]. They are:

- Robustness
- Redundancy
- Resourcefulness
- Rapidity

A robust system has the strength to withstand stress, without compromising functions or the system itself. Redundancy is about being capable of maintaining functional requirements during the disruption. Resourcefulness is the ability to still be able to identify problems and apply resources under the event. The capacity to restore the desired performance of the system efficiently and within a short period of time is called rapidity. When these “four R’s of Resilience” are optimized, so is the global resilience of a system.

In RESISTO, resilience indicators (RI’s) were defined (see section 4.1.6). These RI’s are correlated with the four R’s of Resilience. The maximal performance loss (RI1) is correlated with the Robustness

and the Redundancy, the time it takes for the recovery process to begin after an event occurs (RI2) is correlated with the Resourcefulness, and the time it takes for the system to reach full performance again after the recovery actions have started (RI3) is correlated to Rapidity (see Deliverable D3.6 section 5.3). Different technical capabilities can also be information sharing, the number of service disruptions and how they are managed [10]. Critical functionality, adaptability, independency and flexible response all play a role in creating a more resilient system [14]. More capabilities are tolerance to faults, disruptions or traffic where systems can deal with failures, increased loads or disruptions [17]. Survivability, dependability, security and performability are also important capabilities for resilient systems. The interconnectedness of these different capabilities can be seen in Figure 8. The specific taxonomy shown in Figure 8 is used as a basis by ENISA for defining its Resilience Metrics Framework for the telecom networks and communication infrastructures, see D3.7 “KPIS, QUANTITIES AND METRICS FOR CYBER-PHYSICAL RISK AND RESILIENCE OF TELECOM CIS” for more details.

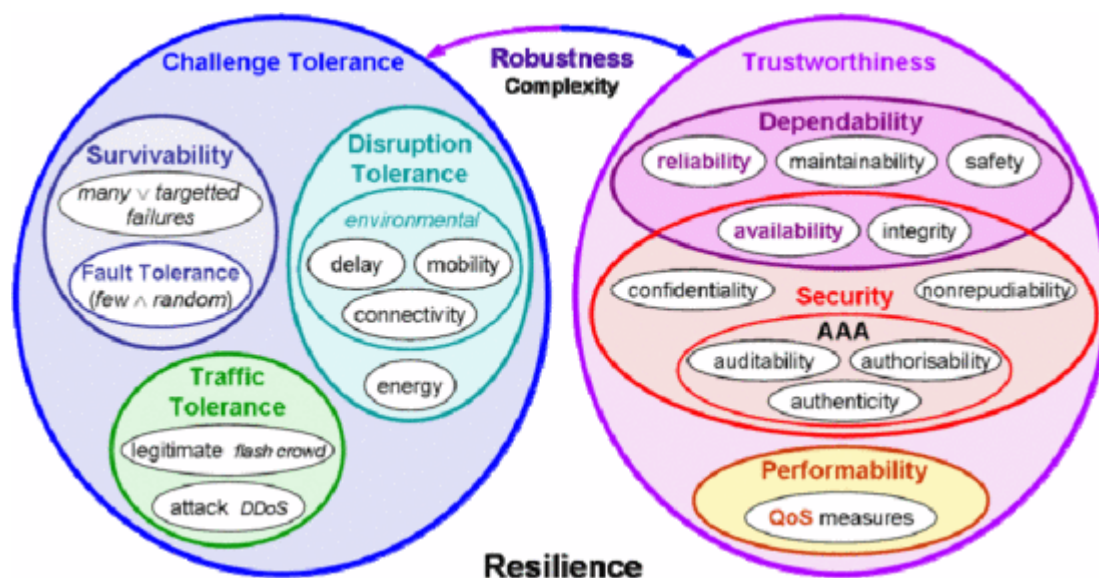


Figure 8 - Resilience characteristics and their interrelation to each other as defined by [8].

Resilience engineering is a method of implementing resilience measures using engineering tools. Technical capabilities and objectives are defined by [18] 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.

During the RESISTO implementation framework and piloting, a whole cycle of the LTCL will be made, where system performance functions and other necessary components of the Risk and Resilience tool will be specifically collected through the use cases and depending on the use case scenario. Thus, the exact functionalities and mitigation actions will be refined and demonstrated. This means that the contents of the Excel inputs will be revised and refined for each Use Case piloting in WP7, 8 and 9.

A summary of the relevant tasks, deliverables, inputs and tools is given in Table 1. Please refer to the DoW [19] 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

Process step		Tasks	Relevant Deliverables	Inputs by end users	Software tools
4.	Disruptions identification	2.2, 3.2	D2.2, D3.4	Excel: Threats Methodologies to discover weakness: Pentest, Attack trees, Honeypots, Mitre Att&ck	App: threat ranking and matrix assessment
5.	Pre-assessment of the criticality of combinations of system functions and disruptions	3.1	D3.1		App: matrix assessment of correlations
6.	Overall resilience quantification	3.3, 2.3, 3.2	D2.4, D2.6, D3.5, D3.6	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 [19]. 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 and D3.6 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 9.

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 9 - 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 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 [19] while it is further refined in the framework of T3.4. Shortlists of the RESISTO platform KPIs are 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 10.

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 10 - 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

The resilience is defined as how a network reacts to a disruption, and the resilience quantification is based on a computation of the performance loss due to the disruption (see deliverable D3.6 “Damage/Vulnerability models for physical and cyber threats of telecom CI”, section 3.3.1). In order to calculate resilience, it is therefore necessary to be able to quantify the loss of performance. Here some example of quantifying some system performance function used in RESISTO.

- L1 connectivity: This performance function indicates if the system is connected (L1 layer), i.e. if each component communicates with the others. We can quantify this performance as follows:

$$\frac{\text{Size of the giant component}}{\text{Size of the network}}$$

- L2 connectivity: this performance function says if the system is congested. In fact, there are some cases where the network is still physically connected, but the communication between some nodes is not possible because of the congestion. A system is congested when a large number of packets are stuck in the nodes, but never reach their destination. This happens when the network is not able to transport the requested flow in the network any more. The capacity of the nodes or arcs from the network is exceeded. In a network where the capacity of the nodes is characterized by the time needed from the node to serve one packet and where this time follow an exponential distribution with mean $1/\mu$ and where the packets in the network are created in each node following a Poisson distribution with mean ρ . We have the following critical value ρ_c , value for which the network will congest ([20] page 98):

$\rho_c = \frac{\mu(S-1)}{B^*}$; Where S is the number of steps the packets performs in the network before disappearing and B^* is the highest algorithm betweenness from network.

- Mobile Data Services/ Fixed Data Services/ Voice Services: this performance function quantifies if the various services are delivered in an acceptable manner. We could have an indication of the quality of those mentioned services by measuring the percentage of needed components for these services, which are not damaged or congested. To have a better image of the loss of performance of these services, it would be necessary to measure some more specific metrics corresponding to each offered service (see D3.6 section 2.3.2 and D3.7 section 4.3.6). We plan to integrate the network performance metric measured from the operators on their testbeds into our model.

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 management¹. 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 services².

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 them [21]. 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 datacentre 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.

¹ threat and vulnerability catalogue[secrit]

² https://en.wikipedia.org/wiki/Network_function_virtualization

The situation may vary if the link problem is within a datacentre, 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 11).

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 collocated SFs
Earthquake	all	May impact other Telco CIs that share infrastructure with OTE. May impact collocated SFs
Power Shortage	all except physical connections	May impact other Telco CIs that share infrastructure with OTE. May impact collocated 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 in deliverable D2.3. The Excel file contains a table for collecting input for the threat list. An exemplary screenshot of the table is shown in Figure 11.

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 11 - 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* ($\geq 10/\text{week}$) to *rare* ($\leq 1/\text{year}$)
- 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

Once the threats have been identified, there are different assessment methods and tools completed in RESISTO. These assessment methods are completed in the long term control loop and include attack trees, MITRE ATT&CK, penetration tests and Honeypots. Each of these methods have their own strength. MITRE ATT&CK is an information base of attacker behavior. Penetration tests, also called PenTests, are utilized when testing new software and hardware are introduced into the system. PenTests can determine any additional or new weaknesses these new modules introduce in the system. Honeypots are modules in the system that collect information during attacks or intrusions. Attack trees can be used to determine the step by step actions during an attack, to show which measures best mitigate the attack phases.

More information on these methods can be found in deliverable D3.4. The outputs of these methods and how they will be used in the RESISTO project will be detailed in T3.5 in deliverable D3.9.

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 0). 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 12. It was produced using an interactive tool, which is further described in section 4.2.

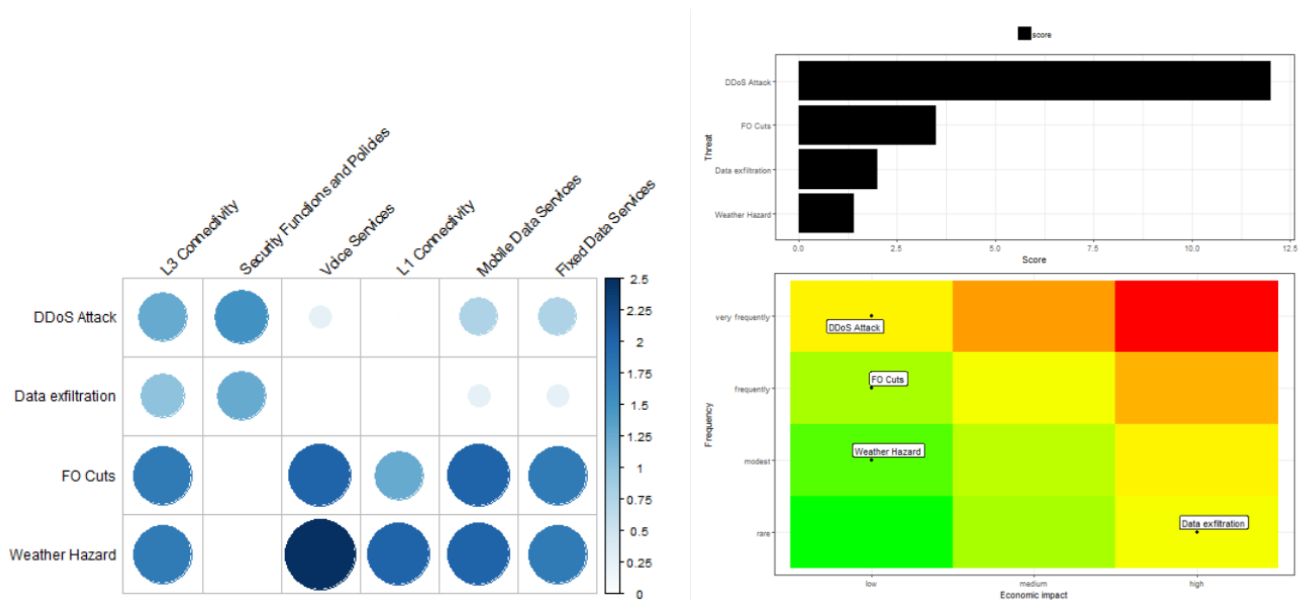


Figure 12 - Exemplary correlation matrix of system functions and threats (left) and threat ranking (right top) by a score calculated based on the frequency and economic impact (right bottom). It should be noted, that the entries in the correlation matrix are not normalized but rather refer to a connection 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 12.

4.1.6. Overall resilience quantification

The performance time curve (“resilience curve”) of a system can describe the system's resilience in different phases, see Figure 6 in Section 3.2. This curve can give a general sense of the resilience of a system, such as if it has adaptive capacity, or ever full recovers after a disruptive event. However, this curve can be used more specifically to quantify resilience. If the performance time curve is created specific to an event and a system, the quantification of resilience can be completed with different resilience indicators (RI) as shown in Figure 13. Four distinct RIs are currently defined. The maximum performance loss (as a percentage) is RI1. The buffer time between when the recovery starts and the event occurs in RI2. RI3 is defined as the recovery time from start to finish. RI4 is the area above the curve. This area indicates the total performance loss throughout the entire process.

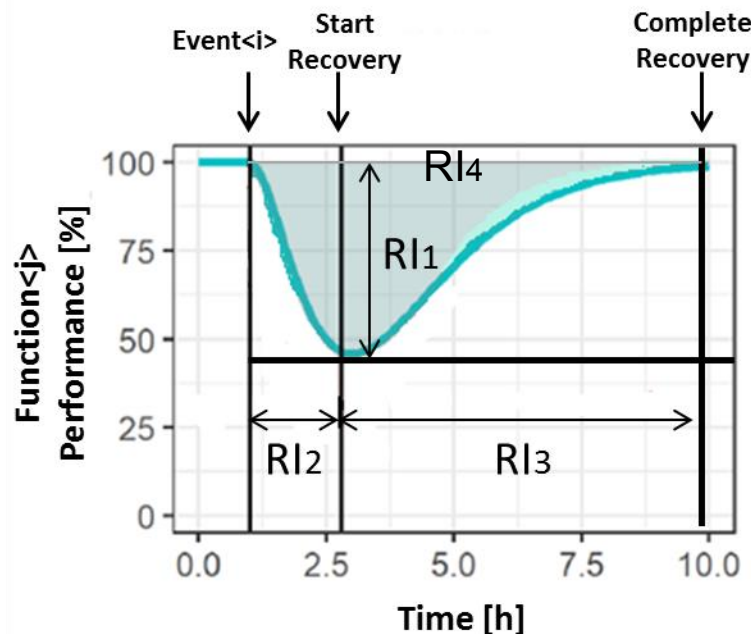


Figure 13 - A generic performance time curve. The resilience indicators, RI1-RI4, are specified.

Each of these indicators can be used to determine the overall resilience of a system against a disruptive event. Another important aspect of the performance time curves besides the RIs is the performance measure that is selected. The resilience quantification is based on the resilience quantities of interest, e.g. selected system functions, and a realistic model of the system. Therefore, the performance measure can differ between systems, depending on what information is available and what the focus is (see Figure 14). In RESISTO, a matrix approach is planned to cover a combination of different threats (first dimension) and different performance functions (second dimension).

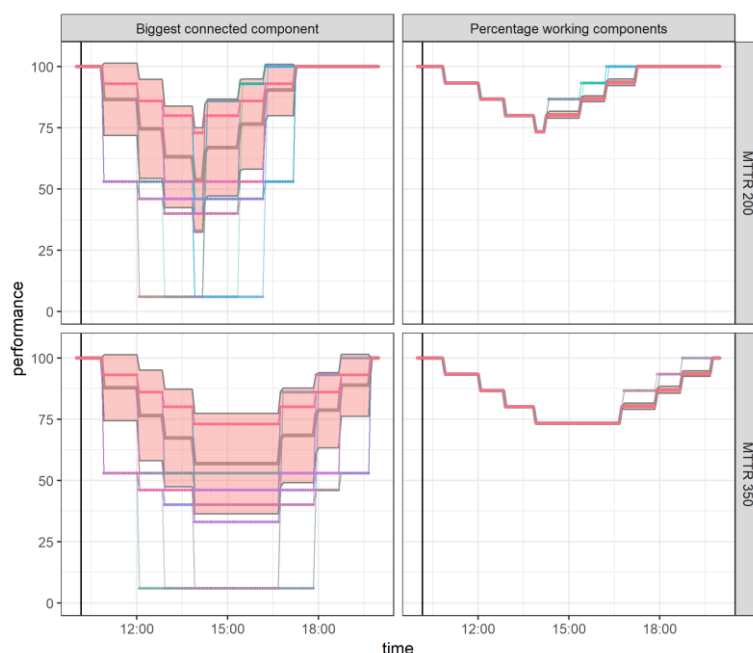


Figure 14 – Illustration of performance curve computed with CaESAR for two performance functions (Biggest connected component and Percentage working components), and two different threats, with different mean time to repair (200 or 350 minutes).

For service based systems, the performance measure is often the availability of the services. For example, the performance measure of a power grid with a blackout as a disruptive event, the performance measure could be the number of customers with power, or the power available. 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/D2.7 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 “RESISTO platform and tools reference architecture”.

The resilience indicators, as defined in the previous section, play an important role in the evaluation of resilience, as the indicators are what links the two control loops of the RESISTO platform together: The Long Term Control Loop (LTCL) estimates the indicators and store the estimates in the knowledge base. The Short Term Control Loop (STCL) actually measures the indicators and then also stores them in the knowledge base. A comparison of the estimates and measurements allows to

validate the simulation approach. Deviations from the real measurements can be used for refinements and calibration of the LTCL simulation results.

The indicators are stored in the knowledge base in a matrix structure. This matrix has two dimensions, the performance function and the potential events. Therefore, each cell answers the question “What are the resilience indicators for this particular event with this specific performance function?” Each cell is filled with the estimated resilience indicators as a result of the execution of the LTCL. The estimated values can be validated with data from real events that were monitored by the STCL and are also stored in the knowledge base. Besides the validation of the simulation results, deviations from the real data allow to improve the model and simulation approach.

	Event<1>	...	Event<i>	...	Event<M>
Funct<1>					
...					
Funct<j>			Estimated RI(1;i;j) RI(2;i;j) RI(3;i;j)		
...					
Funct<N>					

Figure 15: The matrix structure within the knowledge base.

4.1.8. 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. 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 16.

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 16 - 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. Indeed, the new resilience of the CI will be evaluated, taking in account the chosen improvement measure. This will enable an analysis of the potential resilience improvement from these strategies. After the new resilience evaluation, the new RI's will be stored in the knowledge base.

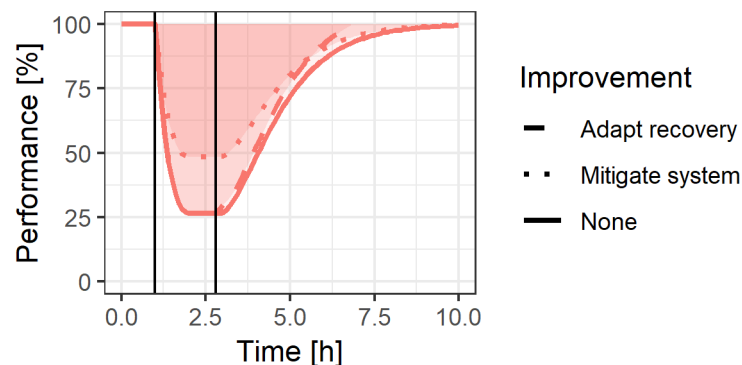


Figure 17 – Illustration of resilience curve and expected resilience improvement through the improvement measure.

The improvement methods can be separated into different categories depending on which aspects of resilience they are improving. There are four main methods to improving resilience, related to the RI's and the “four R's of resilience”, as described in Section 3.4. This allows for the improvement methods to be implemented in different phases of the system, including the defend, remediate and recover phase. For example, when the system is absorbing the attack, improvement methods could be put into place to minimize the maximum performance loss or RI1. This would mean that system is able to absorb the attack, or disruptive event, better, or that the disruptive event has less of an influence. Improvement methods that influence RI1 would fall into the defend phase of the system. RI2 relates to the time it takes to begin the recovery process, and improvement methods would make this time smaller. This then influence the remediate phase of the system. Also related to time, is RI4 which is

the total time required for the recovery process. Shortening this time could be completed with improvement methods. Lastly, RI4 is the area above the curve and improvement methods would minimize this area. Overall, the improvement methods work to reduce the timing, and reduce impacts on the system. Example of mitigation measures can be found in D3.6 Section 5.1.1.

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 appreciate 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 package [22] in the statistical programming language R. Screenshots of the app are shown in Figure 9 - Figure 16. An additional exemplary screenshot of an implemented visualisation option of the tabular inter-connections is shown in Figure 18. More information about the Shiny-app is provided in chapter 5 of deliverable D3.3/D3.4 “Methods for cyber-physical security management for telecom CI”.

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

The tools used for assessment include Penetration tests, MITRE ATT&CK methodology, attack trees and Honeypots, see Section 0 and D3.4 for more details. These tools are utilized in the long term control loop to investigate steps that can be taken when an attack occurs to improve the resilience, this will be explained in detail in deliverable D3.9 of Task 3.5.

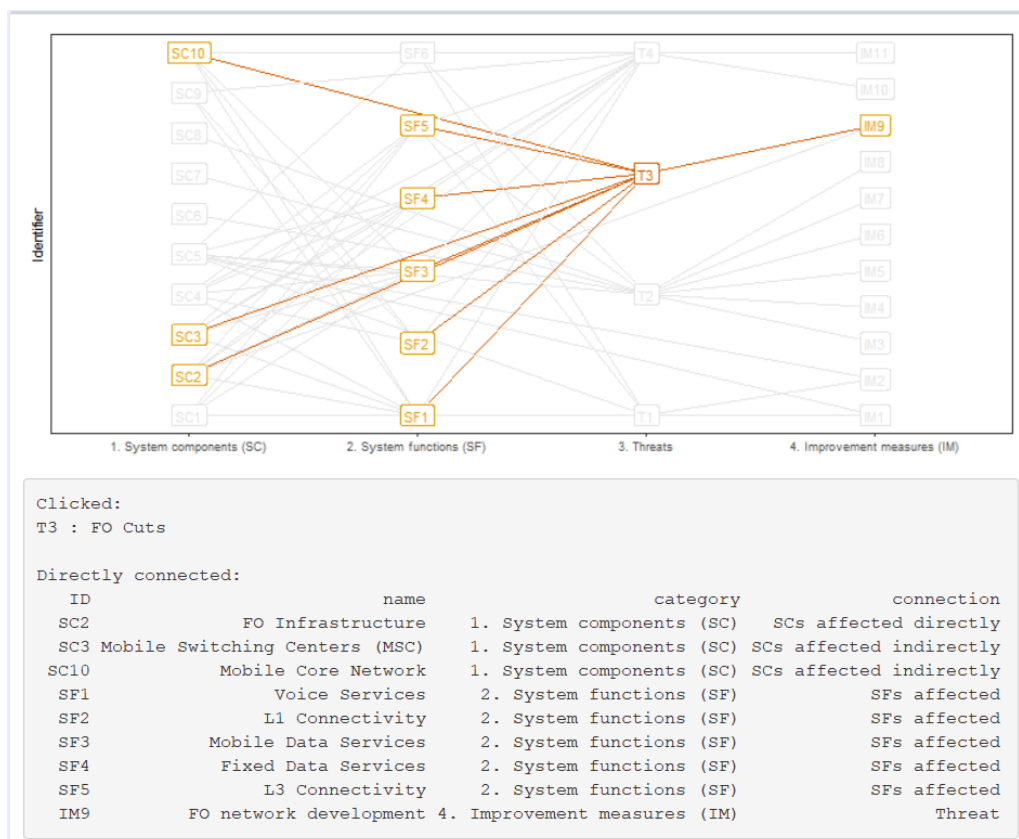


Figure 18 - Exemplary screenshot of a visualisation of the inter-connections of the tables in the Excel file.

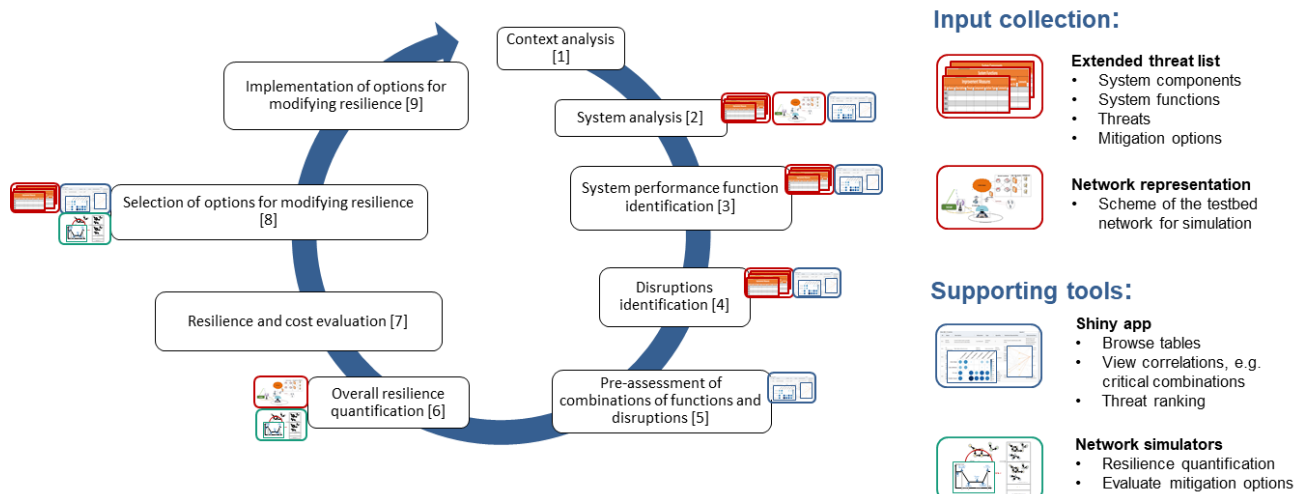


Figure 19 – Input and tools supporting the risk and resilience management process for the long term control loop of RESISTO. The usage of the tabular inputs and graphical network representations is indicated by orange boxes and the support by the Shiny app and simulation tools by blue or green boxes, respectively.

4.3. Requirements traceability

In task 2.1 (D2.1 “End user requirements for integrated cyberphysical risk and resilience management”), the operators and technical experts of the consortium collected a large number of requirements that the RESISTO platform shall, should or could comply with – the modal verb stating the level of technical readiness of the platform. 38 of them have been labelled “SHALL”, which means the implementation of those requirements is mandatory for a TRL7 prototype. “SHOULD” requirements are mandatory for TRL 8/9 and “COULD” requirements are not mandatory at any level but could improve performance and functions of the platform.

During the design and development phase of the RESISTO platform, all “SHALL” requirements have been and will be traced and monitored. If a requirement cannot be covered, the reason for that will be analysed and appropriate recovery actions will be identified.

The goal is a traceability matrix at the end of the project, where the completeness of the implementation of the requirements can be demonstrated together with the information about why, where and how they were implemented.

To ease the complexity of that task, the tracing of requirements will be carried out in each relevant deliverable to come, where the “SHALL”-requirements will be matched with the methods, tools, cases etc. described in that document.

In general, the main requirements for the LTCL are given by RES_FUN_0570 and RES_FUN_0070, but there are contributions as well to other requirements such as RES_FUN_0700 or RES_FUN_0005 (see also D3.4 of T3.2).

A matching to corresponding requirements to the steps of the resilience management process and specific tools/methods is shown in Table 4.

Mandatory Requirements (D2.1, chapter 6.3)		
Requirement Identity Code	Requirement Description	Related to step /method
RES_FUN_0005	RESISTO shall exploit the outcomes of the cyber security and the physical security systems of the TLC infrastructures (if existing).	Step 4/ Honeypots
RES_FUN_0070	RESISTO shall suggest to the operator the necessary steps to mitigate the effect of a cyber/physical attack.	Step 8
RES_FUN_0570	The <i>Risk and resilience assessment analysis</i> shall also take into consideration network single point of failure nodes, using network metrics such as: <ul style="list-style-type: none"> ✓ Link state protocol databases for alternative IGP routes ✓ BGP secondary paths for EGP routes HSRP/VRRP/GLBP statuses for gateway redundancy.	Step 2, step 4 and Step 6
RES_FUN_0670	The <i>Vulnerability Disclosure Framework</i> shall be able to provide users with functionalities to define the scope for testing, rewards for different types of threats.	Step 4/ Penetration test assessment
RES_FUN_0700	The <i>Vulnerability Disclosure Framework</i> shall be able to help Security Researchers and users to monitor vulnerabilities reported through the whole cycle: <ul style="list-style-type: none"> ✓ report the finding, ✓ confirm/reject/request additional information from the security researcher, ✓ notify the stakeholders, ✓ patch the finding, ✓ confirm from the security researcher that the issue was fixed, reward the security researcher, if appropriate.	Step 4/ Penetration Test , Attack trees
RES_FUN_0870	The RESISTO platform shall be able to produce a report for each attack/mitigation action set containing relevant elements such as duration of the attack, types of traffic or sensors that triggered the attack for security insight, etc.	Step 7/ Resilience Indicator Matrix

Table 4 - Mandatory requirements related to the Long Term Control Loop.

5. SUMMARY

This deliverable reports the final status of T3.1 of WP3. The main focus of this document was the introduction and specification of the risk and resilience management process for the long term control loop. Another focus of this task was set on identifying relevant resilience dimensions, which need to be covered by RESISTO.

This report was based on the intermediate version, D3.1, and was updated with new results from other tasks and WPs, in particular D3.4 of T3.2. The main modifications of D3.2 with respect to D3.1 are noted in the introduction

An outlook to the use of the LTCL in RESISTO is recapped in the following.

The exact definitions of all relevant inputs (e.g. set of performance measures and potential threats) and applicable tools (e.g. penetrations tests) will depend on the testbeds implementations and use case scenarios. Therefore, 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 were collected in task T3.2. How the outputs of these tools and the outputs from the Long Term Control Loop will be stored in the Knowledge Base and used from other partners from the RESISTO project have to be organized. This is currently performed in the ongoing Task T3.5 and will be presented in deliverable D3.9 “Analytical security assessment application to use cases and their refinement”.

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 for the specific use case scenarios. This will be done during the implementation phase in WP7, WP8 and WP9.

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] International Organization for Standardization, "ISO 31000 Risk management" Genf, 2018.
- [4] 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.
- [5] 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.
- [6] 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.
- [7] National Research Council, "Disaster Resilience: A National Imperative" The National Academies Press, 2012.
- [8] J. Sterbenz und D. Hutchison, "ResiliNets: Multilevel Resilient and Survivable Networking Initiative" 2006. [Online]. Available: <https://www.ittc.ku.edu/resilinet/>.
- [9] S. Khalili, M. Harre und P. Morley, "A temporal Social resilience framework of communities to disasters in Australia" *Geoenvironmental Disasters*, 2018.
- [10] NSW Department of Justice | Office of Emergency Management, "NSW Critical Infrastructure Resilience Strategy" State of New South Wales, Sydney NSW, 2018.
- [11] 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.
- [12] P. H. Longstaff et al., "Building Resilient Communities: A Preliminary Framework for Assessment" *Homeland Security Affairs*, September 2010 <https://www.hsaj.org/articles/81>.
- [13] 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.
- [14] 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.
- [15] "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities" *Earthquake Spectra*, pp. 733-752, November 2003.

- [16] P. Tamvakis und Y. Xenidis, "Comparative Evaluation of Resilience Quantification Methods for Infrastructure Systems" *Procedia - Social and Behavioral Sciences*, pp. 339-348, 2013.
- [17] 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.
- [18] 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.
- [19] RESISTO, "Grant Agreement. Project Starting Date: May, 1st 2018".
- [20] J. D. i. Gavalda, "Structure and traffice on complex networks" Universitat de Barcelona, 2008.
- [21] Washington State Department of Enterprise Services, "Root Cause Analysis" [Online]. Available: <https://des.wa.gov/services/risk-management/about-risk-management/enterprise-risk-management/root-cause-analysis>. [Zugriff am 12 12 2019].
- [22] RStudio, "Shiny" [Online]. Available: <https://shiny.rstudio.com/>. [Zugriff am 12 12 2019].
- [23] 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.