

RESISTO:

D3.7_KPIs, QUANTITIES AND METRICS FOR CYBER-PHYSICAL RISK AND RESILIENCE OF TELECOM CIs - first



RESISTO

D3.7 – KPIS, QUANTITIES AND METRICS FOR CYBER-PHYSICAL RISK AND RESILIENCE OF TELECOM CIS - FIRST

Document Manager:	Rodoula Makri	ICCS	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_D3.7_190423_05	Version:	1.0
Deliverable:	D3.7	Date:	14/05/2019
		Status:	APPROVED

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

Approval Status	
Prepared by:	Rodoula MAKRI (ICCS)
Approved by: (WP Leader)	Mirijam (Fraunhofer)
Approved by: (Coordinator)	Federico FROSALI (LDO)
Advisory Board Validation (Advisory Board Coordinator)	Carmen PATRASCU (ORO)
Security Approval (Security Advisory Board Leader)	NA

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Rodoula Makri, Panos Karaivazoglou, Apostolos Papafragkakis, Athanasios Panagopoulos, Panagiotis Fragkos, Eyangelos Groumpas, Michalis Sofras. Takis Kelefas	ICCS	Senior Researchers, Electrical Engineers, Telecommunication Experts
Mirjam Fehling-Kaschek, Lena Schäffer, Katja Faist	EMI	Senior Researchers, Risk and Resilience Experts
Carmen Patrascu, Ioan Constantin	ORO	Telecommunication experts, telecom providers, security experts
Maria Belesioti, Eyaggelos Sfakianakis, Ioannis Chochliouros	OTE	Telecommunication experts, telecom providers, security experts
Alberto Neri, Annarita Di Lallo	LDO	Senior Researchers, Defence and Security Specialists
Marco Carli, Federica Battisti, Michele Brizzi	RM3	Telecommunications Experts, Senior Researchers
Moisés Valeo, Jose Manuel Sanchez, Javier Valera	INT	Senior Researchers, Electrical Engineers, Defence and Security Specialists

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
0.1	15.02.2019		All	Table of contents and draft sections
0.2	22.03.2019		All	Additions and partners contributions
0.9	23.04.2019		All	Final release for AB validation
1.0	14.05.2019	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

The present Deliverable D3.7 is the first version of the report entitled “KPIs, quantities and metrics for cyber-physical risk and resilience of telecom CIs” of Task 3.4.

The present report provides a first assessment of the actual metrics and KPIs that are going to be validated through the RESISTO platform components and the Risk and Resilience Analysis and Management Process in order to prove the RESISTO’s added value to the telecom CIs.

A full justification of each of the suggested metrics is provided along with discussions on inherent challenging aspects while the main outcome of this feasibility study is a (preliminary) shortlist.

Having set the framework in the present Deliverable D3.7, for defining and measuring the metrics and KPIs, a final list in the form of a “database inventory” will be given in the next final version (D3.8) of this Deliverable, so that a complete set and description of the RESISTO KPIs and metrics to be provided in the end.

CONTENTS

ABBREVIATIONS	11
1. INTRODUCTION – PURPOSE OF THE DOCUMENT.....	13
2. SECURITY metrics, quantities and KPIs – AN OVERVIEW.....	16
2.1. Security Metrics – definitions and challenges	16
2.2. Existing Security Metrics.....	18
2.2.1. Campell's 2007 Metric Review	18
2.3. Metrics by Security Type	19
2.3.1. Physical security metrics	19
2.3.2. Information technology (IT) and cyber security metrics.....	21
2.3.3. Metrics for Critical Infrastructures as CPS systems – TLC use case	23
2.4. Other related classifications of metrics	25
2.4.1. Metrics by Business Function, ROI and Incident Management software	25
2.4.2. Other Classifications	26
2.5. Models for obtaining security metrics	27
2.6. Measuring Resilience.....	28
2.6.1. Resilience in telecom Infrastructure: the ENISA metrics	31
2.7. Discussion and assessment	33
3. KPIs SELECTION – BASIC PRINCIPLES AND METHODOLOY	35
3.1. Why measure KPIs.....	35
3.2. Metrics and KPIs within the RESISTO framework	35
3.3. Principles and guidelines for the selection of the RESISTO metrics and KPIs	37
3.3.1. General features	38
3.3.2. Security-specific KPI features.....	38
3.3.3. RESISTO-specific KPI features	38
3.3.4. Challenges to be tackled	39
3.4. Sources and procedures used for selecting indicators and baselines	40
3.4.1. Contractual indicative list	40
3.4.2. End Users' feedback.....	41
3.4.3. The ENISA framework	41
3.5. Resilience metrics through the RESISTO Long-term Control loop	44
3.5.1. System performance functions identified by the extended threat list	45
3.6. General guidelines for KPIs measurements.....	47
4. The RESISTO Resilience KPIs – SHORTLIST AND JUSTIFICATION.....	48
4.1. Protection and Detection Stages: Metrics and KPIs.....	49
4.1.1. Number of detected physical threats	49
4.1.2. Number of detected cyber threats	50

4.1.3.	Number of detected cyber-physical threats (combined)	50
4.1.4.	Detection probability	51
4.1.5.	False Alarms Rate (false positives)	52
4.1.6.	Number of concurrent (managed) threats	53
4.1.7.	Awareness of black swan threats	53
4.1.8.	Time to Detection	54
4.1.9.	Sensitivity of the monitoring system sensors	55
4.1.10.	Effectiveness of the events generated per service or application	56
4.2.	Response and Recovery Stages: Metrics and KPIs	58
4.2.1.	Performance loss	58
4.2.2.	Decision-making time (average)	59
4.2.3.	Mitigation Time (average)	60
4.2.4.	RESISTO platform Reliability	61
4.2.5.	Incident Correlation / Propagation Index	62
4.2.6.	Down Time during Incident	63
4.2.7.	Human intervention / automated response	63
4.2.8.	Decision-making failure rate	64
4.2.9.	False Information rate (provided to the operator)	65
4.3.	Metrics related to Network Performance (assessed through the Risk and Resilience Analysis)	66
4.3.1.	Network Availability	66
4.3.2.	Service Utilization	68
4.3.3.	Service capacity / Inventory	69
4.3.4.	Network Performance	69
4.3.5.	Service Continuity	70
4.3.6.	Service Availability	70
4.3.7.	Service Coverage	73
4.3.8.	Service Speed	73
4.4.	General KPIs of the RESISTO platform	74
4.4.1.	Number of validated security modules integrated within RESISTO platform	74
4.4.2.	Security Costs	75
4.5.	Short List overview	76
5.	CONCLUSIONS – discussion and next steps	79
6.	REFERENCES	80

LIST OF FIGURES

Figure 1 - Conceptual framework for resilience (Source: A. Madni and S. Jackson, "Towards a Conceptual Framework for Resilience Engineering," IEEE Systems Journal, vol. 3, p. 181, June 2009)	29
Figure 2 - RMI Dashboard Overview Screen (Argonne National Laboratory US).	30
Figure 3 - Resilience Metrics Taxonomy according to ENISA Framework	32
Figure 4 - Risk and resilience management process with supporting inputs and tools for the RESISTO project.	44
Figure 5- Exemplary resilience curves for two different threats.	45
Figure 6 - List of system performance functions provided by the five telecommunication operators (OP1-OP5).	46
Figure 7-Exemplary screenshot of the performance functions table with partial input from one operator.....	46
Figure 8 - Resilience cycle phases.....	48

ABBREVIATIONS

2G, 3G, 4G	Second, third and fourth generation of mobile phone systems
API	Application Programming Interface
APN	Access Point Name
ASIC	Application Specific Integrated Circuit
AV	Antivirus detection
B2B	Back-to-Back gateway
CCA	Critical Communication Application
CCS	Critical Communications System
CPS	Cyber-Physical Systems
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DMO	Direct Mode Operations
ETSI	European Telecommunications Standard Institute
EU	European Union
FIPS	Federal Information Processing Standard
FW	Firewall
GGSN	Gateway GPRS Support Node
GSM	Global System for Mobile communications
GSSI	Group Short Subscriber Identity
HW	HardWare
IDS	Intrusion detection systems
IEC	International Electrotechnical Commission
IPS	Intrusion prevention systems
ISI	Inter System Interface
ISO	International Standardisation Organization
ISSEA	International Systems Security Engineering Association
ISSI	Individual Short Subscriber Identity
ISITEP	Inter System Interfaces for TETRA-TETRAPOL Networks

ITSEC	Information Technology Security Evaluation Criteria
ITSI	Individual TETRA subscriber Identity
LTE	Long Term Evolution (= 4G)
MNO	Mobile Network Operator
NIST	National Institute of Standards and Technology
NIST-SP	NIST – Special Publicaiton
PC	Personal Computer
PPDR	Public Protection and Disaster Relief
PTT	Push To Talk
QoS	Quality of Service
SOC	Security Operation Center
SSE-CMM	System Security Engineering – Capability Maturity Model
SW	SoftWare
TCCE	TETRA and Critical Communications Evolution
TCSEC	Trusted Computer System Evaluation Criteria (TCSEC: a United States Government Department of Defence standard)
TEA2	TETRA Encryption Algorithm #2
TETRA	TErrestrial Trunked Radio
TG	Talk Group
TMO	Trunked Mode Operations
UE	User Equipment
VPN	Virtual Private Network
WP	Work Package

1. INTRODUCTION – PURPOSE OF THE DOCUMENT

The present Deliverable D3.7 is the first report of WP3-Task 3.4 “Risk and resilience quantities and related KPIs for telecommunications infrastructure”.

This WP deals mainly with the definition of the “Long Term control Loop” of the RESISTO architecture. This component is based on the Risk and Resilience Analysis and Methodology in order to provide communication operators with a fast, flexible and tailorable analytical resilience-driven risk analysis and management process for all types of threats (cyber, physical and cyber-physical threats). The outcome of WP3 is the definition of Key Performance Indicators (KPIs) and metrics for the risk and resilience assessment of the infrastructure that will be validated through the Use Cases in the framework of the three main macro-scenarios (in WP7, 8 and 9).

The Task 3.4 is based on this Risk and Resilience Analysis Management process and tool in order to provide metrics and KPIs that should be monitored, computed or generated for the protection and security of the telecommunications infrastructures, to be shared and used by the involved telecom operators, especially within the RESISTO reference architecture. The metrics and KPIs derived within this Task should provide the risk and resilience quantities for effective and efficient overall joint risk and resilience assessment in telecom CIs through the RESISTO platform.

To this respect, the suggested metrics should prove the added value of the holistic RESISTO solution in terms of improving preparation and enhancing risk control and resilience of Communication CIs against existing security approaches and against a variety of threats and vulnerabilities.

It should be noted that a thorough description of the various threats and vulnerabilities for telecom infrastructures including their definition and classification has already provided in detail in the WP2 Deliverables and especially in “**D2.3 Cyber-physical threat/risk scenarios and pre-assessment**” (sections 2.3 and 2.4). To this respect, the respective definitions and classifications will not be repeated herein, while the reader is kindly encouraged to make the relevant references through D2.3. In general terms, the RESISTO project deals with both physical and cyber threats along with the combined physical-cyber threats especially since the telecom infrastructures can be treated as cyber-physical systems (CPS). Based on the above, the metrics and KPIs that are suggested herein will follow the relevant types of threats as these will be processed through the RESISTO platform.

Following the above, the Task 3.4 incorporates 2 versions of the Deliverable entitled “**KPIs, quantities and metrics for cyber-physical risk and resilience of telecom CIs**”: The present report D3.7, which is the first version and the final one through D3.8 (due in M18).

In order to provide a complete inventory of KPIs and metrics for the RESISTO solution towards enhanced resilience and risk control for the telecom CIs, the analysis presupposes the development of the RESISTO platform and its subcomponents along with the definition of the respective use case scenarios that will be used for the platform capabilities validation. However, the main workload concerning these activities is foreseen for the next project period according to the project workplan.

On the other hand, for validating and proving the RESISTO solution added value along with its associated risk and resilience framework, **actual, tangible and quantifiable metrics and KPIs are needed**. Therefore, performance indicators and metrics need to be measurable within RESISTO. This will be accomplished mainly through the end users Test Beds offered to the project, since for obvious reasons the direct use of the commercial telecom networks cannot be exploited. However, the exact definition of the RESISTO Test Beds is again subject of the next reporting period.

Based on the above, it is seen that, despite the fact that the integrated RESISTO platform, the exact Use Case scenarios and the Test Beds may not be fully determined at the current stage of the project, the current knowledge on their capabilities and features along with the Risk and Resilience

Analysis Management process and methodology, enables the RESISTO Consortium to define, at least a first shortlist of the actual metrics and KPIs that will be used and validated within the RESISTO solution.

To this respect, the subject of the first version of this Deliverable D3.7 (the present report) is to provide as an outcome a shortlist of metrics and KPIs for the RESISTO risk and resilience framework. This shortlist, presented also in a tabular format, is defined under the following conditions:

- The metrics and KPIs should represent measurable features and parameters that will be actually validated within the RESISTO framework and are compliant with the end user demands
- They should enable their measurement, validation and assessment during the RESISTO piloting tests through the use case scenarios and (where applicable) through the test beds and within the time frame of the project
- Should act as a pool of parameters and metrics or in other words an inventory that will be monitored and enriched following up the project evolution and its development stages.

Since, as discussed, at the current stage of the project not all the prerequisites for a definite and final analysis are known, the **shortlist provided within this first version of the Deliverable D3.7** includes:

- The most probable metrics and KPIs that it is currently estimated that it is will be feasible to be measured and validated within the RESISTO piloting tests and within the timeframe of the project
- In the case where certain KPIs are not applicable to all use cases they are still included within this shortlist since their validation can be made on a case by case basis or under specific assumptions
- Even if it is already acknowledged that certain metrics are proven to be difficult or even impossible to be measured, attempts will be pursued so that under specific conditions and assumptions a set of probability related metrics to be derived.
- Finally, at the present Deliverable, an assessment of these metrics is made in terms of their measurements and validation; to this respect, estimated methods of measurements are suggested along with ranges of baseline or target values discussing the challenges involved.

At this point, it should be noted that the metrics and KPIs for the risk and resilience framework of the project should be distinguished from the network performance ones. The latter are network KPIs already measured by the telecom providers through software / hardware tools of their network centres and refer to the network parameters that are subject to the commercial operations (i.e. in customer SLAs such as coverage or speed). These metrics and parameters can be used in the present framework however, in order to prove that the RESISTO approach maintains or even improves their current values as set by the operators. Nevertheless, the majority of these network performance metrics are not directly seen as independent or separate KPIs, but rather as an input in the form of system functions for the Risk and Resilience Analysis Management process and tool (long term control loop working offline) that will result in vulnerability analysis in case of disruptions providing suggestions for mitigation methods.

Having set the framework in the present Deliverable D3.7, for defining and measuring the metrics and KPIs, a fully detailed final list in the form of a “database inventory” will be given in the next final version (D3.8) of this Deliverable, which will include:

- Following up of preliminary experiments through the Test Beds that will be conducted to define the exact ways of measurements of the metrics and KPIs, where applicable along with initial sets and analysis of the Risk and Resilience Management process

- Exact definitions of the baselines and the target values for the finally selected KPIs to validate the RESISTO solution along with a complete mapping of the risk and resilience quantities to be inserted as input in the form of system functions within the long-term control loop, after their verification with the Risk and Resilience Analysis Management process
- Presentation of the links between the selected KPIs and the use case scenarios that will be validated and tested (following up the scenarios and use cases included within D2.8 due in M15).

so that a complete set and description of the RESISTO KPIs and metrics to be provided.

Based on all the above and for the sake of providing a complete as possible presentation, starting from this current first version of the metrics and KPIs Deliverable, the structure of the present Deliverable D3.7 is as follows:

In Chapter 2, an overview of the general security and resilience parameters, identifiers, metrics and indicators are provided as found through a literature survey, acting as the current relevant state of the art. This overview starts with security metrics in general, in order to conclude to existing KPIs for telecom infrastructures.

The third chapter defines the basic principles that should govern the selection and definition of the RESISTO metrics and KPIs for the telecom infrastructures. These principles are based on the literature overview, however, are also tailored to the RESISTO project evolution and capabilities.

Finally, in Chapter 4 the description of each metric is provided in terms of estimated ways and types of measurements emphasizing on the challenges involved towards their validation. The Chapter ends with the metrics and KPIs presented in a tabular format with related attributes.

The aim is, from the one hand, to present a complete and overall picture of the current situation identifying and selecting the RESISTO risk and resilience metrics and from the other hand, to adequately explain and highlight the challenges involved along with the basic assumptions and conditions for appropriate KPIs validation so that to be able to adequately prove the added value of the RESISTO project for increased security and protection in modern Communication CIs.

2. SECURITY METRICS, QUANTITIES AND KPIS – AN OVERVIEW

The purpose of this Section is to provide an overview of the related literature concerning security metrics, quantities and performance indicators in order to provide a thorough insight of the recent practices and benchmarks and to identify potential gaps. As it will be seen, the metrics and indicators identified in the literature are directly connected to the various types of threats and vulnerabilities that need to be mitigated. A thorough description of the relevant risks for the telecom infrastructures has already been provided in detail in WP2 Deliverables and especially in D2.3. In this context, the respective definitions and classifications will not be repeated herein again; however, the metrics and KPIs that are suggested herein will be presented in a relevant structure especially in terms of physical, cyber (information technology) and cyber-physical threats classification types. Thus, the aim of this overview is to provide a synthesis on how security metrics and quantifiable indicators are being treated nowadays in literature or commercial life; the variety discovered involves attempts of setting metrics to meet measurement standards and assessing traditional ones. The analysis will start from security metrics in general and will conclude in current approaches for telecommunication networks and CIs.

2.1. Security Metrics – definitions and challenges

The definition of the term “security metrics” is rather old, when seen in light of today’s practices and comes from Carnegie Mellon University in 1995: **“Metrics are quantifiable measurements of some aspect of a system or enterprise.... Security metrics focus on the actions (and results of those actions) that organizations take to reduce and manage the risks of loss of reputation, theft of information or money, and business discontinuities that arise when security defences are breached”**¹ (Carnegie Mellon University, 1995). A more recent definition based on the knowledge gained in the meantime and tailored to the security requirements of an organization can be stated as: **“Security metric is a system of related dimensions (compared against a standard) enabling quantification of the degree of freedom from possibility of suffering damage or loss from malicious attack”** (Abedin, 2006), (Abbadi, 2007). Security metrics are a critical aspect of risk management while in the information security field, metrics are defined in a large variety of ways (Azuwa, 2012):

- a measurement compared to a benchmark in order security results to be derived
- a quantitative and objective basis for security assurance, comparing two or more measurements taken over time with a predetermined baseline
- an indicator, (not an absolute value but i.e. a percentage of increase or decrease) with respect to an external scale or set parameter
- a measurement parameter that can be quantified and reviewed for expressing an improvement in terms of security objectives, while enabling decision making and compliance with standards.

These definitions can be broadened enough to include protection, detection, response and mitigation aspects as well. In this sense, Key Performance Indicators (KPIs) are set to provide a way of measuring the success or failure of a goal, function or objective, and a means of providing actionable information on which decisions can be based. Although goals in other business sectors are clearly

¹ Carnegie Mellon University. (1995). Security metrics. In systems security engineering-capability maturity model. Retrieved from <http://web.archive.org/web/20120423172421/http://www.ssecmm.org/metric/metric.asp>.

defined, and although security aspects may have similar goals as business operations, it is not always clear enough how security aspects can be measured. To this respect, most security operations goals are less finite, while they are more focused on positive or negative trends over time than achieving a specific target².

Many and various attempts for measuring security have been carried out by national and international agencies and organizations such as (Abbadì, 2007): TCSEC (Orange book), ITSEC (Europe's Orange book), CTCPEC (Canada's Orange book), Common Criteria (everyone's Orange book which is rather a framework than a list of requirements), ISSEA's SSE-CMM, NIST FIPS-140 series, NIST SP 800-55 and others. According to ISO/IEC 27002:2005³, information security metrics can be classified in major categories (where each category foresees more specific metrics) providing a large list related to security and overall management as well: Risk management metrics, Security policy metrics, Management / governance metrics (including Information Security Management customer satisfaction rating), Information asset management metrics, Human resources security metrics, Physical & environmental security metrics, IT security metrics, Access control metrics, Software security metrics, Incident management metrics, Business continuity metrics, Compliance & assurance metrics.

As denoted in the ASIS Foundation Report⁴ “the security metrics are vital, but the field offers few tested metrics and benchmarks”⁵. Through the literature review conducted within this report, gaps were identified concerning the existence and evaluation of statistically sound metrics. As acknowledged, **“explicitly defined metric criteria, measurements and evidence that these criteria are met, and example metrics that meet these criteria do not yet exist within the security literature”**.

Historically in the past, it seems that security aspects and related implementations were seen and treated as a separate issue than the core businesses of an organization and were often limited to access control and / or entrance security checks only. However, during the last decades on the one hand the risk environment has radically changed and on the other hand terrorism and malicious actions have dramatically increased. Especially in critical infrastructures the above aspects are amplified since the integration and complexity of their facilities and services turned them into complex and large Cyber-Physical Systems (CPS). To this respect, and when considering the embedded Information Technology systems, security on the cyber domain is a vital parameter in all related implementations.

In this context, security metrics, measurable quantities and performance indicators are essential for assessing and evaluating security systems and they constantly obtain a valuable gain within business operations. The main aim of setting them is to quantify, as possible, the effectiveness of security measures in terms of risk mitigation and through that to enable more reliable and effective decision-making driven by quantitative analysis and grounded on scientific methods or processing data. Thus, in recent years, the perceived value of security metrics is on the rise (Campbell, 2007) to support the added value of an organization's security operation. However, due to the complexity of the operations

² “Key Performance Indicators (KPIs) for Security Operations and Incident Response”, John Moran, Senior Product Manager, DFLabs S.p.A, www.dflabs.com, https://www.dflabs.com/.../KPIs_for_Security_Operations_and_Incident_Response-2.pdf

³ ISO/IEC. (2005b). Information technology — Security techniques — Code of practice for information security management. ISO/IEC 27002. Retrieved from <http://www.iso27001security.com/html/27002.html>

⁴ “Effective, Evaluated Security Metrics - Persuading Senior Management with Effective, Evaluated Security Metrics”, Ohlhausen, Poore, McGarvey and Anderson, Research funded by a grant from the ASIS Foundation, 2014, https://capindex.com/wp-content/uploads/ASIS_Report_Complete1.pdf

⁵ Guidelines and Metrics Working Group, ASIS Defense and Intelligence Council (2012). “Watch us build an effective security performance metric...,” presentation at the ASIS International 58th Annual Seminar and Exhibits, Philadelphia

and the cyber and physical threats, the focus seems more on counting events than creating meaningful, risk-based metrics (Hayes & Kotwica, 2012); the value of their optimization is not widely understood and implemented but is mainly limited on past performance reporting (Davenport & Harris, 2010).

Based on the above, in the following, the main findings of a literature and web-searching surveys will be presented, concerning the existing and currently available security metrics affecting all security aspects in an organization in a broader sense; that is, not directly affecting the telecom CIs. The aspects to be presented provide a general overview of what metrics exist and how are taken into consideration in order to assess their effectiveness and demonstrate their measurable impact on an organization's strategic, organizational, financial and operational risks and profits.

2.2. Existing Security Metrics

Again, the ASIS Foundation Report will act at this point as a good basis to start providing an overview of existing security metrics since it concentrates and assesses the relevant literature findings on this specific subject while it will be further enriched in the following. According to this, multiple attempts have been carried out through scientific literature on examining existing security metrics. As main representative examples of metric categories the following are discussed and assessed by the report:

- Campbell's 2007 Metric review with baseline performance metrics (a brief reference will follow)
- Metrics by Security type i.e. physical security metrics, which will be analysed in a separate paragraph, since they are considered most relevant to the RESISTO project's work
- Metrics by Business functions and return on investment (financial metrics)⁶ along with metrics related to incident management software (degree of automation) or of other type.

2.2.1. Campbell's 2007 Metric Review

The ASIS Report recognizes that perhaps the most thorough treatment of the topic is that by Campbell (2007). In his review, Campbell (2007) provides a description of numerous types of metrics and discusses many of the issues pertaining to their use in organizations. However, organizations are treated in a general manner even though, depending on their type, specific metrics would be more applicable and representative than general ones. Moreover, the suggested security metrics cover a broad range of examples on their impact in services and organisation's business; from examining the causes of increased workplace violence incidents in a specific branch up to employee and customer satisfaction surveys to analyse the impact of the security measures and thus to derive related metrics.

Despite this general manner, Campbell's work was the most representative systematic approach at that time, while specific metrics and parameters were set to drive the analysis: **Key Performance Indicators (KPIs)** were established, by identifying a desired performance level and assessing the progression, or lack thereof, toward that level; **Risk analysis**, was identified as a parameter of measuring assets in terms of cost of loss or loss events, or conducting a cost-benefit analysis; the valuable parameter of **Baseline performance metrics** was also recognized (i.e. emergency service response time) while **Diagnostic metrics** were also used as identifying the root causes of trends.

⁶ CIS consensus information security metrics (n.d.). Security Benchmarks. Retrieved from <http://benchmarks.cisecurity.org/downloads/metrics>

Examples of Security-related “Measures and Metrics in Corporate Security” (by George K. Campbell)⁷ are given in the following table:

EXAMPLE							
SECURITY MEASURE OR METRIC	BUSINESS DRIVERS						
	COST MGT.	RISK MGT.	ROI, VALUE	LEGAL REQ.	POLICY REQ.	LIFE SAFETY	INTERNAL INFLUENCE
The number of nuisance alarms from corporate facilities monitored by Corporate Security	X	X				X	
Security cost as a percentage of total company revenue	X		X				
The number of safety hazards proactively identified and eliminated annually		X		X	X	X	
Percentage of critical information assets or functions residing on systems that are currently in compliance with approved system architecture		X			X		X
The number of failed or ineffectual business unit responses to issues identified by Security as control weaknesses that result from fraud prevention analysis, investigations or other feedback		X					X

Table 1 - Examples of Security-related “Measures and Metrics in Corporate Security” (by George K. Campbell)

Similar analysis in threat assessment and classification focused on the security demands of the telecom CIs have already been carried out and reported in the framework of other RESISTO Deliverables (WP2) and especially D2.3. To this end, RESISTO follows more or less the principles of Campbell's work. Moreover, a risk and resilience management tool (In WP3) attempts to concentrate and to assess the risk analysis specifically for telecom CIs, while baseline performance and KPIs as quantitative metrics of this analysis in respect to the RESISTO solution are the main subject of the present Deliverable.

2.3. Metrics by Security Type

Security metrics are often categorized based on the type of security (physical security, information and cyber security, personnel security, etc.) or types of threats and form a performance-based approach. To this respect, a brief analysis of each separate segment is given in the following:

2.3.1. Physical security metrics

Physical security metrics are basically connected to threat detection parameters and are also useful in vulnerability assessment. To this respect, external sensors detection and performance estimations

⁷ George K. Campbell, “Measures and Metrics in Corporate Security”, Security Executive Council Publication Series, 2011, <http://www.securityexecutivecouncil.com>

against defined threats are used as metrics while their technical aspects often provide the desired quantities for establishing the baseline performance and the security related goals to maintain this performance or to increase the detection capabilities or even upgrade them if not acceptable in case of performance degradation; in this case false acceptance ratios or nuisance alarm rates are considered and how easy would be to bypass or spoof the sensor.

Estimates of the probability of assessment or combinations in case of various detection parameters have to be used in the analysis resulting in identifying vulnerabilities. The performance measures for physical protection functions include probability of detection; probability of and time for alarm communication and assessment; frequency of nuisance alarms; time to defeat obstacles; probability of and time for accurate communication to the response floor; probability of response force deployment to adversary location; time to deploy to a location; and response force effectiveness after deployment (Garcia, 2008). In the case of CCTV for example the combined effects of video image quality and resolution, speed of capture and camera field-of-view coverage in detection zones should be taken into account. Similar examples include measurable issues surrounding alarms, protective barriers, theft, etc. Other examples of a physical security metrics include;

- a) the number of door alarm annunciations to explore the cause of false alarms so that all alarms do not have to be treated as emergency security situations (Treece & Freadman, 2010);
- b) the number of persons who voluntarily show identification badges versus those who do not (Scaglione, 2012);
- c) flier threat-level calculations are pursued, to determine whom to screen at security checks (Sternstein, 2013).

It is seen that these particular metrics are mainly related to human resources / personnel security where compliance, cost controls and efficiency, and continuous evaluation are rather easier to be measured or to be connected to financial aspects of the organisation such as the rate of turnover, i.e., staff retention, (Campbell, 2012) and the average time needed to conduct background checks⁸. In a similar context security reviews and workforce factors can be measurable events within industrial security, i.e. the number of deficiencies reported or the number of classified contracts and their potential breaches. Relevant examples in this manner are those considered in performance measures such as: input / process measures (asset Inventory, number of countermeasures in use, Resource Requirements) or output measures (security assessments completed versus planned, countermeasures deployed, countermeasures tested, Incident Response Time) which are more generic and focus on a more strategic level as well as the impact on an organization's operation⁹.

According to (Kovacich & Halibozek, 2006) when setting a metric to assess a given security function, the following should be encountered: What specific data are to be collected, how and when these will be gathered, at what point in the function's process, and what will be the targeted result in order to be appropriately displayed. Actions for setting related standards have been attempted, as by the Interagency Security Committee of the U.S. Department of Homeland Security¹⁰, where the relevant standard recognizes security metrics as an important component of risk management and establishes policies for the security of all buildings and facilities in the U.S. occupied by Federal employees.

However, the complexity of nowadays critical infrastructures and organizations' operations along with the advanced technologies used for physical intrusions and exploiting vulnerabilities by the attackers

⁸ How metrics can link security to the business (2011). Security Director's Report, 11(4), 10-12.

⁹ "Use of Physical Security Performance Measures", Interagency Security Committee, US Homeland Security 2009

¹⁰ The risk management process for federal facilities: An Interagency Security Committee standard (2013). Retrieved from http://www.dhs.gov/sites/default/files/publications/ISC_Risk-Management-Process_Aug_2013.pdf.

indicate that physical security metrics have to involve additional security technological solutions for threats detection than only access control and personnel security metrics. Thus, as it will be seen later on, this is one of the objectives of the RESISTO project. To this respect, the aforementioned security metrics have to be enriched and expanded in order to include also the physical detection and cyber security aspects tackled by the project.

2.3.2. Information technology (IT) and cyber security metrics

Information technology (IT) and cyber security is on the other hand the domain where a large metrics literature is already present both in the standardization, academic and commercial / web fields. The International Organization for Standardization (ISO) / International Electro-technical Commission (IEC) 27001 certification is widely used as best practice and outlines IT security standard requirements for a broad range of threats and vulnerabilities. As it has already been noted, a thorough description of the various threats and vulnerabilities, especially for cyber (information technology) threats, has already provided in detail in the WP2 Deliverables and especially in D2.3 (sections 2.3 and 2.4). To this respect, the respective definitions and classifications will not be repeated herein; however, the metrics and KPIs that are suggested from the literature search follow more or less the same relevant types.

The ISO/IEC 27001 standard mandates the measurement of information security as a requirement to measure the effectiveness of controls to verify that security requirements have been met¹¹ while the ISO/IEC 27002 standard additionally dictates security techniques for managing information security¹². Information and cyber security as well as related metrics are of critical importance according to the aforementioned standards and should focus on analysing data in real-time so to result in immediate response¹³; the measurable issues within information security include inspection, incident management, change management, and classification measurement (Rathbun, 2009) along with identification, authentication, audit and accountability, etc.

As indicative examples of information security and cyber security metrics the following are reported in literature; the percentage of security incidents caused by improper access control configuration; the number of new viruses identified on the internet as a metric of active security; the viruses / trojans received and internal incidents; the viruses detected in user files; the interoperability problems associated with certification authorities and public key infrastructure; the time needed to encrypt a sensitive document; the percentage of information systems with annual testing focused on contingency planning; the number of weak password breaches reported [(Chew, 2006), (Pironti, 2007), (Collins, 2004), (Doinea & Pavel 2010), (Whitman & Mattord 2012), (Aleem et al, 2013)].

Cyber security plays a very important role in today's business. According to a KPMG survey ("Consumer Loss Barometer"), cyber-attacks and hacking are widely recognized as threats to small and large businesses alike, but many of them are still slow to adopt security practices resulting in being left vulnerable; over 80% of executives companies admit they have been exposed in cybersecurity events over a 24-month period while almost half of them haven't invested in IT security in the past. When discussing on cyber-security KPIs, it is often recognized that the ability to identify and measure cybersecurity KPIs or measuring the performance of a cyber security strategy is

¹¹ ISO/IEC. (2005a). Information technology — Security techniques — Information security management systems — Requirements. ISO/IEC 27001. Retrieved from <http://www.iso27001security.com/html/27001.html>.

¹² ISO/IEC. (2005b). Information technology — Security techniques — Code of practice for information security management. ISO/IEC 27002. Retrieved from <http://www.iso27001security.com/html/27002.html>.

¹³ Embracing big data can lead to greater security (2013). COMPUTERWEEKLY.

essential for improving its efficiency and resilience; however, when identifying KPIs, critical risks must be identified before solutions can be outlined; thus the whole process becomes a risk assessment aspect tailored to and reflecting each organisation's priorities, goals and objectives. In this context, many IT security metrics can be found in bibliography or by surfing through the web, as examples of cyber security KPIs that can be applied to the majority of organisations or infrastructures¹⁴:

- (Increase or decrease in the) **number of devices being monitored**; to evaluate the workload.
- (Increase or decrease in the) **total number of events**; in order to assess the incidents detection, response and recovery processes, to identify patterns and key risks as well as related costs. Variations or prioritizations are seen such as: (increase or decrease in) reported Incidents; number of major or of small security incidents, in order either to focus on the incidents that make the biggest impact on the organization's business or that may be easily deflected.
- **Number of events per device or host that are more prone to security issues** than others; in order to evaluate the detection success rates and key risks per component.
- (Increase or decrease in the) **time to detect security events**; in order to assess and evaluate the detection success rates and the performance of the processes used.
- **Time needed to resolve an actual security event (often found as "time to resolution")**; considering also the time taken away from other tasks within the organisation; this time can be reduced with additional equipment and thus to assess the mitigation processes.
- **Meeting Regulatory Requirements**; failing to abide to national or local regulations affecting cybersecurity incidents may have important financial impact in the organization (i.e. fines, public fallout etc.). The regulations may also require to officially report data breaches over time.
- **Uptime or Downtime during an Incident**; the main aim is to estimate the business impact of a downtime during a security incident (from lost sales and revenue to loss of customers) with crosschecks of historical financial data (volume of sales or revenue). Insights and estimations through server logs of cyber threats (i.e. hacking incidents) in order to identify data and traffic.
- **Cost Per Incident**; the effort herein is not only to estimate the expenses for resolving an attack, but also to calculate the cost for the overall incident and the individual resources involved.
- **Management of Customer Impact**; this KPI may be difficult to be measured since affected customers' records or accounts need to look at and managed after an attack along with the relevant data collected on the impact on customers during the attack. Usually this KPI is related to brand and revenue impact or consecutive damage.

In the same manner and context, a variety of similar metrics and KPIs are reported¹⁵, ¹⁶ when applying management techniques (such as Earned Value Management - EVM), to the cybersecurity

¹⁴ As Cyber Security KPI examples from the <https://cyberseries.io/2019/01/14/cyber-security-kpis/> to support the forthcoming UKSec Summit 2019 (<https://cyberseries.io/uksec/>) and Nordic Cyber Series 2020 (<https://cyberseries.io/nordic/>) and NordiX, the Nordic region's Cyber Security Summit events powered by Catalyst Global.

¹⁵ "8 Cybersecurity KPIs and How to Track Them", by Venkatesh Sundar, Founder & Chief Marketing Officer, Indusface, <https://www.indusface.com/blog/8-cybersecurity-kpis-track/>, September 14, 2017

performance. This way, the actual performance (in terms of schedule and cost) against planned performance across a project's scope, schedule, budget, and expenses can be calculated in monetary values in order to measure organizational cybersecurity performance over a given time frame. The dimensions needed to be taken into account are: the cybersecurity expenditures invested (in the technical and non-technical domains i.e. hardware, software, personnel, policies etc.), the actual events and activities that occurred, the planned scope of cybersecurity events and activities that the investments were intended to address and the successful handling of events or activities, among others.

Although the above KPIs are too important for an organisation's monetary justification in order to upgrade, adjust or install security programs, it has to be noted that they are too closely related with the financial aspects of the enterprise. In other words, it may be difficult to assess and measure unless a profound insight in the organization's economic matters is taken. To this respect, commercial relevant tools may be needed to monitor this kind of metrics.

As it is seen, a vast literature is present for all security domains and even more on information and cyber security metrics. However, since the related security metrics are on the rise, the need of more, better-defined and empirically tested or proven metrics for all security domains is more than essential nowadays than ever, since valid and reliable metrics are vital for accurate conclusions and effective decisions on organisations' policies and threats responses and mitigation.

2.3.3. Metrics for Critical Infrastructures as CPS systems – TLC use case

As denoted in D2.3, Cyber-physical systems (CPS) are context-aware, autonomous systems that extract data from the physical world using embedded sensors, process it with distributed computational power and employ this information to drive actuators on the physical domain, supporting or entirely taking over the decision process. There are several works that survey different aspects of security in CPS from different domains. Examples include smart grid, pervasive medical monitoring, robot-mediated industrial systems, autonomous driving systems, and unmanned avionics.

Smart grids result from the integration of existing physical power infrastructures with cyber systems providing advanced computing and communication capabilities, real-time monitoring and control applications through sensor networks. On the one hand, the adoption of this framework promotes numerous benefits, improving reliability, scalability, interoperability and lowering maintenance costs of the power system. On the other hand, as the separation between cyber and physical domains vanishes, the security surface of a system that was initially built to be isolated and self-dependent grows.

Moreover, attracted by the possibility of a much higher gain, adversaries too are getting smarter, coming up with new integrative cyber-physical attacks to strike such systems and cause business interruptions, financial loss, reputation damage and, more importantly, threaten life-critical applications. Thus, it is of utmost importance to understand how physical and cyber-related threats interplay. In fact, due to the entangled relation between the physical and cyber domain of CPSs, the same vulnerabilities associated with a cyber system could potentially have much more disruptive effects if exploited.

To this aim, (He et al, 2016) conduct an in-depth investigation of joint cyber-physical attack schemes targeting different aspects of the power systems and the appropriate defence strategies to adopt in

¹⁶ "Cybersecurity Performance: 8 Indicators", by Summer Fowler, Insider Threat Blog, Publications of Software Engineering Institute, Carnegie Mellon University, <https://insights.sei.cmu.edu/insider-threat/2018/03/cybersecurity-performance-8-indicators.html>, March 15, 2018

case of a breach. More specifically, they analyse attacks targeting the Remote Terminal Units (RTUs) deployed in the Supervisory Control and Data Acquisition (SCADA) system, which collect information on the system behaviour to monitor system status and dynamics. In (Tan et al, 2017) the cyber security of CPSs is studied from a data-driven point-of-view, systematically decomposing the entire lifecycle of Big Data inside smart grids in generation, acquisition, processing and storage. For each of these phases, security aspects are thoroughly analysed.

Considering the amount of data that is collected by power equipment (e.g. smart meters readings, billing information), privacy is another major concern in smart grid operations and CPSs in general. In fact, that data could potentially reveal sensitive information and ultimately be used to infer behaviours, activities and preferences of the final users. This problem is addressed in (Jawurek et al, 2012), where strength and weaknesses of commonly used policy tools and proposed Privacy Enhancing Technologies (PETs) are reviewed. An analysis of cyber security and privacy issues in the smart grid can also be found in (Liu et al, 2012). Since CPS depend so much on communication and networking infrastructures, they are prone to be vulnerable to almost all IT-related threats.

In (Komninos et al, 2014), a comprehensive review of cyber-attacks whose objective is the smart home environment and its interaction with the smart grid is provided. To assess the impact that threats menacing the Smart Grid/Smart Home joined environment could have, the FIPS 199 (NIST, 2004)¹⁷ impact level assessment criteria are used. Then, possible countermeasures for those attacks are also devised and organized by security goal (ensuring confidentiality, privacy, authentication, availability, integrity and repudiation). Relevant use-cases and ongoing activities in industry are also presented.

To plan future advances on metering, monitoring, operation, automation and markets, real-world validation should be conducted. The same holds for CPS protection, detection and mitigation strategies, which shouldn't be based solely on simulated scenarios. To this aim, dedicated cyber-physical testbeds exist. However, most of them are developed to assess the security of a specific component of the CPS infrastructure, whether it is the communication protocols, the power infrastructure or the security and privacy requirements. Security-oriented testbeds are surveyed in (Cintuglu et al, 2017), where they are evaluated according to the presence of a heterogeneous communication backbone supporting both wireless and legacy protocols, security and privacy awareness, multiple protocol support of the devices in the grid and remote connection access.

Other surveys, like (Tawy et al, 2016), investigate the trade-off between innovative features and the security of CPS, with a special attention to implantable medical devices (IMD). It is particularly important to ensure the security of telemetry interfaces, software, and hardware of this kind of devices, since the health and sometimes the life of patients depends on them. Different types of attacks and vulnerabilities for several IMD-specific authentication protocols are identified, and safety and privacy trade-offs are presented for the case of emergency access specifically. In addition to that, IMD typically are resource-constrained devices (with energy, communication and processing limitations), so there is a need for appropriate solutions. As an example, in (Wang et al, 2016) three types of cyber-attacks (denial-of-service, replay and deception) under security and resource constraints are discussed.

The problem of securing storage, data sharing and cloud processing of medical CPS is tackled in (Kocabas et al, 2016) by evaluating both conventional and emerging encryption schemes, while emerging threats related to the exploitation of previously considered private body signals are identified in (Rushanan et al, 2014). Another important field of complex interaction between cyber and

¹⁷ National Institute of Standards and Technology. 2004. FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems. [Online] Available: <https://doi.org/10.6028/NIST.FIPS.199>

physical frameworks is represented by IoT-based manufacturing systems. Thanks to connected supply chains, flow of inventory and production cycles can be optimized, greatly reducing costs. At the same time, however, a malicious entity could attack it and jeopardize the production (He et al, 2016). Recently, there has been an increasing attention to the risks of including more sophisticated communication capabilities in industrial equipment, due to the danger of them getting compromised.

The modification of the manufacturing processes could lead to parts whose physical characteristics have been altered, for example by introducing fine internal defects (Zeltmann et al, 2016), to be more susceptible to fail with hazardous results. The problem gets more serious if we consider that, as exemplified in (Wells et al, 2014), the current workforce is not educated to deal with this kind of security challenges, so corruptions could easily pass unnoticed. Important insights on this matter are provided in (Pan et al, 2014), where cyber-physical attacks targeting manufacturing processes are classified together with quality control measures for counteracting them.

Approaches that do not focus on a specific domain but instead address security and privacy issues in a general CPS context are included in References [(Combata et al, 2015), (Han et al, 2014), (How, 2015), (Lun et al, 2016), (Mitchell et al, 2014), (Wang et al, 2016)]. A comparison and classification framework for comparing research on CPS security methods is proposed in (Lun et al, 2016), and used to build a systematic review of the state-of-the-art approaches. In (Combata et al, 2015), defence against cyber-physical attacks is considered. Two main approaches are found: a preventive protection, which identifies the vulnerabilities in the system and try to increase its resilience by acting on the control parameters or installing redundant devices; a reactive protection, which tries to mitigate the impact of the attack through real-time detection and response.

Given their strict requirement on availability, fault-tolerance and security, the automatic detection, classification and mitigation of abnormal events is of major importance in CPS. In (Mitchell et al, 2014), Intrusion Detection Systems (IDS) for CPS are compared to traditional IDS for ICT infrastructures, grouped by application domain and classified according to design principles and audit material used. Then, main advantages and drawbacks of existing IDS techniques are considered. Intrusion detection performance metrics are also reported: false positive (FP) and false negative (FN) rates being the most common, but also detection latency, communication overhead and power consumption. Based on the peculiarities of the architecture, anomaly-based (also known as outlier detection) IDS are suggested in (Han et al, 2014) as preferred for CPS. Some requirements are also outlined to facilitate their design. More specifically, the detection mechanism should be distributed (because control and management services are also distributed), online (to react in a timely manner), effective against cyber-attacks and random failures, fault tolerant and respectful of the users' privacy.

Even though there is a wide number of surveys from different venues that address several aspects of security in CPS, the RESISTO approach focuses instead directly on physics-based anomaly detection and in proposing a unified taxonomy that includes the vast amount of research in this field.

2.4. Other related classifications of metrics

2.4.1. Metrics by Business Function, ROI and Incident Management software

These metrics are strongly related to financial metrics or management ones. Indicative examples are; average recovery time and time / latency for compliance with policies coverage for vulnerabilities (incident and vulnerability management function metrics), (Berinato, 2005); the security cost per employee and annual security costs in relation to annual revenue (financial metrics), (McIlravey & Ohlhausen, 2012); and average time for change completion (change management metric). Additionally, Return On Investment (ROI) metrics can serve as a framework for classifying and

identifying metrics; in other words, the savings gained in the security or overall organizations' budget when implementing specific changes or actions in the security system (i.e. better allocation of security resources). Examples of ROI metrics are often used through the Cisco Cybercrime Return on Investment Matrix, which is used to predict successful cybercrime techniques¹⁸.

Some metrics are captured instantaneously through incident management software (IMS), such as the IMS used in emergency preparedness (McIlravey & Ohlhausen, 2013); the software can be configured based on business rules, and notifications can be set up based on specific rule violations (Huff, 2013), to document and share data, to track compliance issues, accidents, emergencies, employee access to networks or to identify anomalies. The related metrics then lead to policy recommendations or to a more standardized setup of security ROI.

It is clear that in order to accurately measure the above kinds of metrics, internal accurate information is needed on the organisations' financial data and performance along with profound knowledge on the organisations; management functions. This kind of knowledge is not always subject to public information but rather remains confidential while specific assumptions should be made on the core of businesses and operations in relation to economic values. To this end, these types of metrics are not always easy to be measured unless information on the corporate level is obtained.

2.4.2. Other Classifications

Similar to that by security type, however more specific, classifications of metrics can be found as in (Abbadi Z. 2007) under OWASP auspice. In this context the security metrics are classified as follows:

- **Process Security Metrics:** herein the aim is to measure processes and procedures which dictate that security policies and processes are already been implemented within an organization such as: the number of policy violations, the number of identified risks and their significance, the percentage of systems with tested security controls, the percentage of systems with contingency plans etc.
- **Network Security Metrics:** these are metrics related to the organization's IT network and its vulnerabilities: Successful and unsuccessful logons, number of IT incidents and viruses' infections, number of viruses or spam blocked, or patches applied, traffic analysis etc.
- **Software Security Metrics:** such as the number of defects or attacks, along with their severity and type over time, either in the lines of code or in the interfaces or design flaws and the relevant cost.
- **People Security Metrics:** these have to do with human behavior which is again difficult to be modeled. On the other hand, the risk perception differs from person to person while bias aspects cannot be neglected. These are similar to personnel security described previously while they imply a continuous training and awareness.

Certain of the above metrics are already known and implemented as described in the previous sections. It is again recognized that measurements of risk are the most common security metrics while reliability is not always identical to security. Risk identification is dynamic in nature since it varies a lot depending on the organizations' core business and services while models have to be taken into account concerning the data to be collected and the respective processes used.

¹⁸ Cisco 2010 annual security report: Highlighting global security threats and trends. (2010). Retrieved from <http://www.cisco.com/go/securityreport>.

2.5. Models for obtaining security metrics

Especially for Information Security a regular and constant effort has been carried out in recent years in order to provide relevant metrics in a more systematic way. This dictates the use of models which often classify threats and attacks and prioritize the related risks in a form of risk scores. To this respect, various models can be found in literature for information security metrics. Highlighting some of them, the following can be stated:

An ISP 10×10 Model for Holistic State Evaluation has been developed in (Bernik, 2016) to measure information security performance through 100 variables, each of which has its own weight (the dependent variable is composed of 10 critical success factors, which are further measured by 10 different key performance indicators). The process is based on survey questionnaire at the organization to evaluate the extent to which the organization meets a certain criterion. Immediate measures are prioritised against long-term ones. This way, a multi-dimensional approach with a multilevel model enabling an inherent measuring of the organizations by themselves. However, despite of the practical application the model has certain limitations which mainly lie on its qualitative nature since it relies on personal evaluations and thus the result depends on subjective assessments whereas a larger experts' validation should be in order. Nevertheless, it is seen that information security performance is strongly influenced by operational and technical measures, and thus high-quality technological and physical protection should be first implemented prior to any upgrades in security aspects (social, user-related, environmental etc.) in order to achieve maximum effects and to result in effective decisions. Furthermore, it is showed that the organization's capabilities towards an information risk management system have the strongest impact on IT security efficiency in comparison to other measured factors.

Another recent approach is introduced by (Brotby and Hinson, 2013) describing a rational process to score, rank and shortlist candidate information security metrics, to cover the complexities of designing, using and maintaining a metrics system. The approach is called "PRAGMATIC" because it attempts to result in scoring the information security metrics based on specific Predictive, relevant, Actionable, Genuine, Meaningful, Accurate, Timely, Independent and Cheap criteria (the acronym "pragmatic" is formed by the first letters of each criterion). The authors describe a structured method for identifying potential metrics, assessing them rationally, ranking them, and selecting the few that have the most value according to the prioritization of scores. The method presupposes a profound insight of all the organisations' processes and can be also applied to the ISO/IEC 27002:2005 security metrics as well.

The above mentioned examples, indicate tabular (excel) based formats for providing information security measurements. Naturally, there are also mathematical models based on theoretical modelling of the system itself or of the attacks or even the investment with functions, theorems, conditions and equations. In this context, the modelling exploits benchmarking of the Smart Grid Infrastructure (Kim et al, 2012), or focuses on calculating the vulnerability measures (existing, historical), the policy security scores and the network factors (Abedin et al, 2006), or even calculates attacks models for cyber-physical systems which in certain cases resemble the fault detection or automatic control theories (networked control systems with adversary models, attack space, Input Observability and Detectability, Attack and Disturbance Models aiming to derive security indexes)¹⁹.

It is certain that more complex systems require dramatically more effort to analyse, especially when considering combinations of events. Cyber-physical systems security demands additional security requirements, which are difficult to address by information security alone. The physical component of

¹⁹ Henrik Sandberg, "Security of Cyber-Physical Systems", KTH, Stockholm, Sweden, 7th oCPS PhD School on Cyber-Physical Systems, Lucca, Italy

cyber–physical infrastructures adds significant complexity that greatly complicates security metrics, requiring more effort to understand the system and to elicit meaningful security metrics. On the other hand, model-based approaches lie on approximations of the physical world which is subject to noise, and deviations from the reality. Therefore, system-theoretic approaches are rather nondeterministic as compared to information security more realistic tabular models.

2.6. Measuring Resilience

Resilience is the capacity to adapt to changing conditions and to maintain or regain functionality and vitality in the face of stress or disturbance. It is the capacity to bounce back after a disturbance or interruption²⁰. In other words, resilience is the ability of the system to both absorb the impact as well as to recover rapidly from a disruption so that it can return back to its original service delivery levels or close to it (Omer et al, 2009). For infrastructures' resilience, a resilient system is defined to have a reduced failure probability, reduced consequences from failures and reduced recovery time. Similarly, resilient systems have the ability to maintain a constant output value level when the system suffers from a perturbation (Pavard et al, 2006). Resilience, in the context of critical infrastructure, is defined as the ability of a facility or asset to anticipate, resist, absorb, respond to, adapt to, and recover from a disturbance (Carlson et al, 2012).

In order to evaluate and enhance the infrastructure resilience and the effectiveness of related strategies, metrics are needed to assess the current resilience of the system and allow the decision makers to monitor it under various threat scenarios. However, it is generally admitted that it is difficult to measure resilience since it not directly observable per se but must be placed in relation to a given outcome²¹. Related metrics should be specific to the contexts of the systems under consideration and this precludes generic resilience indicators. It is also difficult to relate resilience to thresholds therefore comparisons to benchmarks or baselines are rather difficult; thus a spectrum of resilience factors (for the specific system) is more meaningful than formative definitions, due to the dynamic and multi-dimensional nature of resilience and the fact that it is not always easy to obtain reliable but comprehensive data.

In light of this, resilience and business continuity standards have been developed from: the US National Infrastructure Advisory Council (NIAC, 2009)²²; the British Standards Institute 25999 Standard on Business Continuity (BSI, 2010)²³; the NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs (NFPA, 2010)²⁴; the ANSI/ASIS SPC.1-2009

²⁰ Resilient Design Institute, <https://www.resilientdesign.org/what-is-resilience/>

²¹ “Measuring resilience”, Food Security Information Network, May 2016, Crown Copyright, DOI: http://dx.doi.org/10.12774/eod_tg.may2016.sturgess2 .

²² NIAC, 2009, Critical Infrastructure Resilience, Final Report and Recommendations, U.S. Department of Homeland Security, Washington, D.C., available at http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

²³ BSI, 2010, BS 25999 Business Continuity, available at <http://www.bsiamerica.com/en-us/Assessment-and-Certification-Services/Management-systems/Standards-and-Schemes/BS-25999/>.

²⁴ NFPA, 2010, NFPA 1600-Standard on Disaster/Emergency Management and Business Continuity Programs-2010 Edition, NFPA, Quincy, MA, USA, 52 p., available at <http://www.nfpa.org/assets/files/pdf/nfpa16002010.pdf>.

Standard on Organizational Resilience (ASIS, 2009)²⁵; and ISO 22301 Societal Security – Business Continuity Management Systems – Requirements 06-15-2012 (ISO, 2012)²⁶.

In specific reference to infrastructure systems, (Bruneau et al, 2007) proposed a metric for measuring the infrastructure resilience in natural hazards as the expected degradation of the quality of the infrastructure over time. Additionally, they identified the 4 Rs dimensions of a resilient system; robustness, redundancy, resourcefulness and rapidity.

(Reed et al, 2009), expanded more and identified the infrastructure capacity to be the measure of the infrastructure's quality. Robustness was defined as the ratio of the lost capacity of the system as a result of a disruptive event over the capacity of a fully functioning structural system. Rapidity was then defined to be the measure of rapidity of recovery. (Reed et al, 2009) captured the interdependencies between the infrastructures through a linear function, although they state that a second order trend might be more appropriate. A resiliency index was suggested by (Attoh-Okine et al, 2009), which propose the use of belief functions for measuring the resiliency index of interdependent urban infrastructure systems.

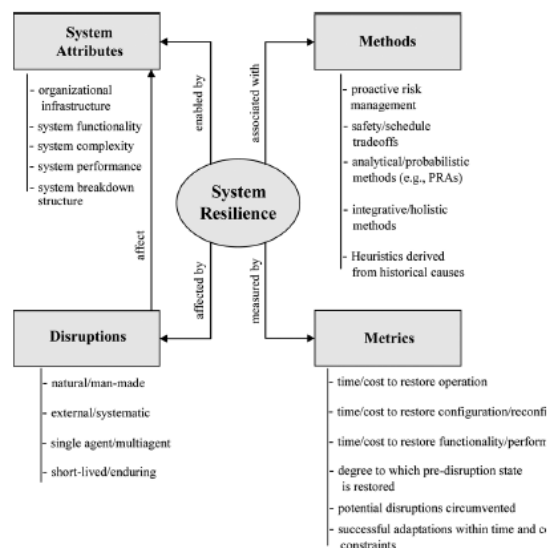


Fig.2. Conceptual framework for resilience engineering
Source: Madni and Jackson (2009)

Figure 1 - Conceptual framework for resilience (Source: A. Madni and S. Jackson, "Towards a Conceptual Framework for Resilience Engineering," IEEE Systems Journal, vol. 3, p. 181, June 2009)

Attempts to derive a resilience measurement index specifically for critical infrastructures were carried out in the US especially after major and devastating natural disasters (such as Hurricane Katrina in 2005 and Superstorm Sandy in 2012). To this respect, the Infrastructure Assurance Center at Argonne National Laboratory, with the Protective Security Coordination Division of the U.S.

²⁵ ASIS, 2009, The Organizational Resilience Standard [ASIS SPC.1-2009], available at <http://organizational-resilience.com/OrganizationalResilienceStandard.htm>.

²⁶ ISO, 2012, ISO 22301:2012 – Societal Security – Business Continuity Management Systems – Requirements, available at http://www.iso.org/iso/catalogue_detail?csnumber=50038.

Department of Homeland Security, developed an index, the Resilience Measurement Index (RMI), to characterize the resilience of critical infrastructure²⁷. The main objective is to measure the ability of a critical infrastructure to reduce the magnitude and/or duration of impacts from disruptive events, capturing fundamental aspects for critical infrastructure with respect to all hazards. The RMI methodology supports decision-making related to risk management, disaster response and maintenance of business continuity and it is based on multi-attribute utility theory and decision analysis principles.

The RMI methodology foresees four major components: preparedness, mitigation measures, response capabilities, and recovery mechanisms. Each component of resilience is decomposed into its individual subcomponents, which are then organized into five levels of information where data that need to be collected are grouped together to calculate the RMI. Data are collected via the DHS Enhanced Critical Infrastructure Protection Program's Infrastructure Survey Tool. The methodology uses a numerical representation of a value pattern by comparing different elements of a facility and each of the components is weighted by subject matter experts to indicate its relative importance to a facility's resilience. The RMI is defined by the aggregation (roll-up) of several indices characterizing the components and subcomponents and its value ranges between 0 (low resilience) and 100 (high resilience). However, the developers of the method note that the RMI is a relative measure; a high RMI does not mean that a specific event will have minimal consequences. Conversely, a low RMI does not mean that a disruptive event will automatically lead to severe failures. The RMI instead allows comparison of different levels of resilience of the critical infrastructure. Determining how different options affect the RMI leads to select the most effective ways to improve the overall resilience.

By that way, this approach produces a relational representation of a facility's protection alternatives by providing a numerical value assignment for each of its components. Thus, the process characterizes a facility with respect to its component properties (e.g., content of the business continuity plan; presence of alternatives and backup in case of loss of a critical resource), which results in possible decisions and proposals for different alternatives or measures to increase resilience.

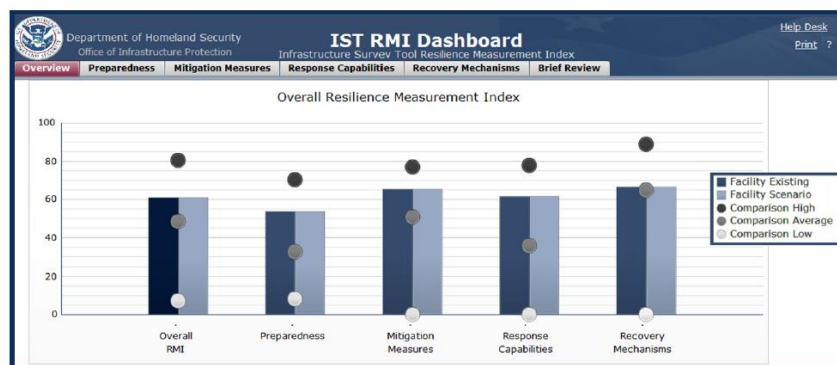


Figure 2 - RMI Dashboard Overview Screen (Argonne National Laboratory US).

Despite of the RMI method's advantages, there are also certain limitations related to the interpretation or use of the collected data and associated indices. Since data collection relies on a voluntary program, the time taken to answer and collect the data along with the degree of the assessor's

²⁷ "Resilience Measurement Index – An Indicator of critical infrastructures resilience", ANL/DIS-13-01, Decision and Information Sciences Division, Argonne National Laboratory, US Department of Energy, April 2013.

knowledge of a specific facility's technical and operational functions are always key factors. However, the most important issue is that the RMI characterizes resilience at a specific facility and thus the data are always collected towards this context and thus RMI values for different facilities cannot directly be used to determine the resilience of a specific region or a given sector since additional elements (e.g., personnel, financial aspects, environment, institutional services) need to be taken into account²⁸.

In networked infrastructure systems, other efforts in defining resiliency metrics refer to the methodology set by (Garbin and Shortle 2007) where the resilience metrics are defined as the percentage of nodes or links damaged in the network versus the network performance. (Omer et al. 2009) proposed a metric for networked infrastructure systems as the ratio of the value delivery of a network after a disruption to the value delivery before. They also propose to measure the node to node resilience of the network. Other efforts (Mostashari et al, 2013) refer to power and water infrastructures, measured resilience in terms of economic loss (Chang & Chamberlin, 2005), while (Shinozuka et al, 2004) suggest measuring the resilience of power systems in terms of speed of restoration and repair efficiency.

In telecommunication infrastructure, on the other hand, (Cohen et al, 2001) studied the tolerance of the internet to intentional attack, and the suggested resilience metric is to be a measurement of the number of sites needed for the disintegration of the network. Recent works on the subject, such as (Smith et al, 2011) introduce more systematic approach with graphical tools and the design of a distributed multilevel architecture that lets the network defend itself against, detect and dynamically respond to challenges.

2.6.1. Resilience in telecom Infrastructure: the ENISA metrics

The European Network and Information Security Agency (ENISA) fully recognizing the large importance and the need for reliable communications networks devised a Multi-annual Thematic Program (MTP) with the ultimate objective to collectively evaluate and improve the resiliency of public communication Network and Services in Europe. As a part of that program, a study was done with a group of ENISA stakeholders on resilience measurements²⁹. It was soon becoming apparent that there is lack of a standardised framework or relevant good metrics and this was considered to be one of the main challenges due to the not well-defined term of resilience and the fact that sources of consolidated information on resilience metrics were not readily available. These challenges were recognised as serious obstacles towards the adoption of resilience metrics. Addressing these concerns, the **“Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report”**³⁰ was created by ENISA, tackling the open issues on resilience metrics, in the areas of security, dependability and specific taxonomy research under the term of resilience. The report provides definitions regarding the important terms of resilience, metrics and KPIs, along with an overview of different initiatives, regulations, works from research projects and frameworks related to resilience metrics and measurements or related taxonomies available in the literature. Based on the above, the report identifies a number of metrics, presented in a detailed and consistent way, to be used as a useful and reliable set of baseline resilience metrics tailored to communications networks and as a starting point for further implementation in telecom and information security aspects.

²⁸ Argonne National Laboratory, 2013, Restore©: Modelling Interdependent Repair/Restoration Processes, available at <http://www.dis.anl.gov/projects/restore.html>.

²⁹ ‘Measurement Frameworks and Metrics for Resilient Networks and Services: Challenges and Recommendations’, ENISA, www.enisa.europa.eu

³⁰ “Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report”, resilience study, February 2011, <http://www.enisa.europa.eu/act/res>

Following a thorough study towards a unified taxonomy of resilience metrics, ENISA's report brings together different taxonomies in single unified model, by presenting a two-dimensional approach to categorising resilience metrics. The model includes an incident- and a domain-/discipline-based dimension along with the current open issues when trying to apply these metrics on a larger scale. This two-dimensional classification provides a flexible model.

The one dimension of the classification model, called incident-based dimension, lies on the principle that resilience metrics can be categorized according to a temporal dimension related to the incident; it takes the incident-based view of classifying resilience metrics before an 'event' happens that is preparing for resilience and delivering the intended service, and after the 'event', while trying to respond and recover to normal operation. Thus, resilience is expressed over the 3 different time phases with respect to challenges and faults (events) that threaten the normal level of service: preparedness, service delivery and recovery phases.

The second dimension of the ENISA taxonomy is based on the parts of different disciplines (domains) which collectively constitute the notion of resilience. A metrics domain is a group of metrics which are measuring different aspects of the same resilience property. This model recognises the multi-disciplinary and multi-domain nature of resilience, covering for example areas from disciplines / domains, such as: security, dependability, performability etc.

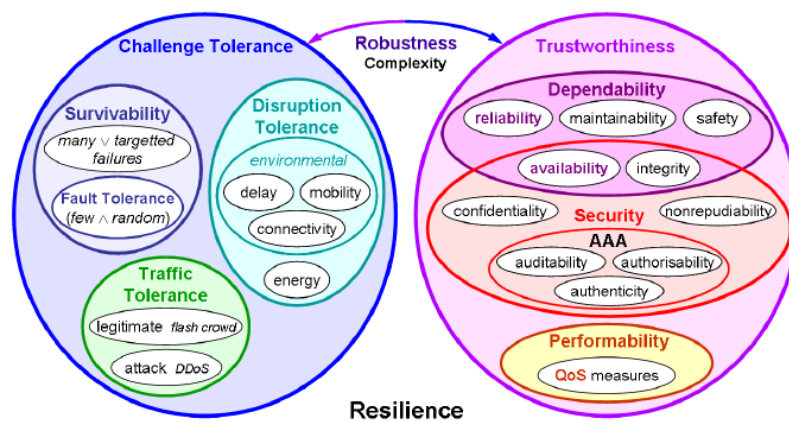


Figure 3 - Resilience Metrics Taxonomy according to ENISA Framework

The ENISA Report recognizes that up to that point the taxonomies that were proposed in the literature mainly referred to the domain dimension of this classification (discipline-/domain-based grouping of the various metrics) and differed in their levels of details. During the same study it became apparent that there was another dimension in the classification of resilience metrics which is related to the temporal view of an event/incident. It was also acknowledged that there was a lack of a standardised framework or good metrics especially for telecommunication networks; related organisations have their own specific approaches and means of measuring resilience, if they actually have any at all. Major hurdles in the identification and implementation of relevant measurement frameworks, are either because the metrics do not exist or because the organisations are unaware of their existence.

During the discussion with experts initiated by ENISA it was found out that even though this approach was not heavily represented in the literature, it had wider acceptance mainly because it relates directly with the definition of resilience; to this end, meaningful examples of metrics categories can contribute to a systematic and comprehensive practical approach when metrics need to be

considered and base the resilience and security metrics on existing business requirements and to start out with a small set of metrics which gradually expands.

The ENISA Measurement Framework for Resilient Networks and Services is too important for the RESISTO project since it refers to the project's actual objectives. To this respect, the way that ENISA framework will be exploited within the RESISTO project and its identifications of KPIs and metrics will be also subject of the next Chapter of the present Deliverable as well.

2.7. Discussion and assessment

From the thorough and overview concerning the existing security and resilience metrics, presented in the previous sections, following assessment can be derived:

It is seen that there is a vast and extended literature attempting to identify and classify existing security metrics, quantities and KPIs in general; however, the descriptions are often vague, making it difficult to adopt them. Only few examples of empirically sound metrics (with statistical justification and evidence) are present within the security literature. As it is derived, many metrics are presented only at a conceptual level or through a theoretical formulation; it is difficult to ascertain what exactly is being measured and how and when the measurement can be obtained or implemented. Definitions that yield specific measurements are not equally provided; the evidence needed to show that these factors are met is not discussed; examples of metrics that illustrate the desired measurement criteria are not provided. In addition, the current focus of security metrics remains more on summative indicators rather than meaningful, risk-based metrics in order to determine the effectiveness of a metric (Hayes & Kotwica, 2012).

Within the security literature many factors are discussed as potential metrics and KPIs, including internal financial aspects of the organisation in order estimate the investment costs needed for security and to relate them with the security metrics. This way, criteria relevant to organizational objectives and procedures or return of investment and benchmarking, are general guidelines often tailoring metrics to the audience; the implementation of these guidelines would likely not be straightforward since they are difficult to be measured and presented in an objective sense. They would presuppose inside information from the organisation and a thorough and profound overview of all operating internal components and systems related to cost figures.

Furthermore, the evaluative factors presented within the security literature (including metric type, relevance to organizational objectives, etc.) are again provided at a conceptual level. Reliability and validity seem not meaningfully explored within the security literature; explicit empirical evidence regarding validity and reliability of the metrics is not always present within the literature in order to derive conclusions concerning their accuracy. It must be noted that this is often a subjective aspect. For example, if a metric increases dramatically often a time period, it is not certain if this happens due to increased attacks or if this is the consequence of a malfunction of the system component behind used to measure the parameter (i.e. door alarm systems). Thus, the reliability and validity of metrics have to be subject of evidence in order to lead to accurate conclusions; otherwise it would jeopardize the attempts of improving security, leading to underestimations of the metrics importance. Moreover, strategies for communicating metrics are general and may be hard to implement.

Based on the above, the overall conclusion of the literature overview, as this is also recognized by the ASIS Report³¹ is that crucial gaps are identified regarding the existence and evaluation of (statistically

³¹ "Effective, Evaluated Security Metrics - Persuading Senior Management with Effective, Evaluated Security Metrics", Ohlhausen, Poore, McGarvey and Anderson, Research funded by a grant from the ASIS Foundation, 2014, https://capindex.com/wp-content/uploads/ASIS_Report_Complete1.pdf

or with other manner) sound metrics in a general manner. The same stands for metrics that illustrate the desired evaluation and measurable criteria for obtaining them in a reliable manner.

However, it is also recognized that physical security and information security appear to have more metrics in use than other security fields, especially when the respective critical infrastructures are concerned. Nevertheless, in the majority of the literature the metrics are tailored to the specific characteristics of the kinds of networks or infrastructure systems that the metrics are applied instead of a more generally applied approaches. And this is reasonable since each network (power grid, gas or telecom networks) has its own features, procedures and technical sub-systems.

The common grounds therefore, when assessing the relevant literature, is the attempt to provide a detailed mapping of all processes affecting security and resilience in all the several stages (prevention and preparedness, detection, response, mitigation and recovery) and through risk assessment to assign a risk-based score, taking into consideration the specific characteristics of the facility / infrastructure / network under consideration both in terms of operational, service provision and technical components point of view. Thus, to implement a specific methodology to each specific case.

This is often being held through evaluation and risk assessment tools and environments (such as the RMI framework of the Argonne National Institute or the PRAGMATIC approach). Thus the above gaps can be addressed; however on a case-by-case basis. As it has been seen these kinds of tools provide a framework with explicit statistical and business criteria through which metrics can be grounded in risk assessment, key objectives and measurement approaches. In the framework of the RESISTO project this kind of tool lies within the resilience and risk-assessment management tool that formulates to Long-Term Control Loop of the RESISTO platform.

Especially for the telecom infrastructures, the ENISA Resilience measurement framework would be a good basis to start with when implementing a solution like the RESISTO one specifically in the telecom CIs. The specific ENISA report recognizes similar gaps in the whole process including the lack of a common communication platform for all telecom providers. Nevertheless, ENISA report tackles the relevant resilience and security metrics specifically for telecom networks as an overall model and successfully addresses the weaknesses found in literature for the specific telecom network cases. However, it should be noted that the ENISA Resilience measurement framework is meant for the existing commercial telecommunication networks. To this end, not all parameters and metrics can be used and above all measured within the RESISTO framework, since certain of them may require inside information from the telecom operators or their measurements might be not feasible to be held within the time frame of the RESISTO project.

To this respect, in order to provide the metrics and KPIs for the RESISTO solution, a methodology should be elicited tailored to the specific cases, requirements and approaches that will be tackled within the framework of the project following specific principles that will need to be defined. Thus, all these will be the subject of the next sections of the present report.

3. KPIs SELECTION – BASIC PRINCIPLES AND METHODOLOGY

As denoted in the previous Chapter the basic outcome of the extended literature review is that there is a lack of overall generic metrics or directly implemented methodologies in order to derive meaningful metrics, quantities and indicators for critical infrastructures; the suggested concepts foresee insights of each system parameters and dimensions and context specific methods and tools. To this respect, the purpose of this Section is to define the main principles that will lead to adequate KPIs selection and to provide guidelines for their measurements as a tailored methodology for the RESISTO solution needs.

3.1. Why measure KPIs

The importance of using KPIs is widely recognized and properly accepted in the literature as denoted in the previous Chapter. The reasons for this are diverse ranging from general e.g. what is measurable is manageable, to specific in relation to the application at hand, e.g. in security the information conveyed in proper metrics, is of paramount importance for both assessment and mitigation. It's out of scope of this document to list all the possible reasons for deriving and using appropriate KPIs even if we limit ourselves within the context of the RESISTO project. Still it is worth mentioning two aspects of the use of KPIs that demonstrate their importance in the context of security operations.

It is well established in the literature³² and easily understood even by the non-expert, that the information obtained by measuring well thought KPIs has a tremendous impact in both tactical and strategic function of security operations. For the RESISTO case, this means that both the short-term and long-term control loops can benefit from this. Additionally, good KPIs can serve as an enabler and driver for continuous improvement thus increasing the added value of the system and strengthening its prospects in achieving such a mature technological level that will naturally lead to commercial exploitation.

3.2. Metrics and KPIs within the RESISTO framework

The RESISTO project will provide a holistic solution aiming to provide situation awareness and enhanced resilience at telecom critical infrastructures. For this reason, a risk-based control platform will be implemented incorporating innovative security models, methodologies and technologies.

It should herein be highlighted the fact that the RESISTO solution does not attempt to replace the existing security systems that the telecom operators possess and have already implemented to their facilities. The aim of the RESISTO solution is rather to act as a complementary tool, interacting with pre-existent security components of a communication Infrastructure, so that to increase the overall level of cyber-physical security providing a quantifiable benefit and thus an added value in terms of resilience improvement and enhanced protection.

In order to result in a tangible benefit, metrics and KPIs need to be set so that this added value to be quantified and provide adequate proof of concept. To this respect, the metrics that will be set need to address the basic aspects and components of the overall RESISTO solution. The main aspects that need to be addressed by the suggested metrics are the following:

³² “Key Performance Indicators (KPIs) for Security Operations and Incident Response”, John Moran, Senior Product Manager, DFLabs S.p.A., www.dflabs.com [KPIs\) for Security Operations and Incident Response-2.pdf](#)

- RESISTO covers **all phases of security** for telecom infrastructures, that is: prevention and preparedness, detection, response and mitigation. Therefore, metrics have to be set for all these stages in a meaningful way that enables tangible quantifications. Detection is an important dimension of the RESISTO project since it proposes and implements additional innovative features to confront the new emerging kind of threats (such as airborne ones, terrorist attacks etc.). This means that setting metrics for personnel or access control in telecom CIs are not a target per se since it is assumed that already the telecom operators tackle these aspects through their existing security systems. On the other hand, the fact that additional detection capabilities are foreseen, dictates that these should be represented in the RESISTO metrics since they would contribute in proving the project's added value to telecom CIs security and resilience.
- Another important aspect is that RESISTO addresses **all kind of threats** (physical, cyber and combined cyber-physical threats), therefore the proposed metrics should focus towards these objectives. Especially, the combined cyber-physical threats are a key issue since nowadays threats and attacks are more complex with advanced characteristics involving both the physical and cyber domains. Especially in the telecom CIs where cybersecurity is a critical issue due to the technological advancements (cloud, Internet of things etc.) there might be a time interval before an actual cyber-physical threat is detected. For example, let us imagine a physical intruder at the telecom premises who implements a virus to the cyber system of servers that will be activated after a period of time; the most common approach would be these two threats to be detected separately. However, if the RESISTO platform manages to perform the proper correlations between these two events then the combined cyber-physical threat could be identified earlier and lead to appropriate mitigation measures.
- RESISTO incorporates a **resilience assessment and risk-management tool** which formulates the Long-term control loop; this tool is the core of the prevention / preparedness and mitigation phases since the long-term control loop can initiate prevention mechanisms and aftermath assessment for adequate mitigation actions. The tool is a tabular-formatted web-based application that can process important system functions and result in a risk assessment in terms of the impact to the various sub-systems or services of the telecom networks, while it is user-centric and tailored to the specific telecom CI aspects.
- Finally, another significant dimension is the **interconnections** of the telecom CIs with other critical infrastructures (such as power grids) in the vicinity or impacting social parameters. This implies a measure of the propagation of the associated risk as a metric of the impact through the interactions between interconnected CIs. A more detailed description of the interconnections' functionality of the RESISTO platform can be found within the rest of WP3 Deliverables as well as the WP5 ones, where the relevant parameters identifying interactions between telecom infrastructures and other critical ones are derived through the corresponding software tools. However, specific metrics and KPIs should be identified herein in order to represent the value of the metrics on the interconnections of the critical infrastructures and how they could be useful to prevent "cascading effects".

From all the above it is seen that metrics and KPIs would provide a proof of concept of all the above main dimensions of the RESISTO project. The aim is that these enhanced capabilities would give an advanced feedback to the existing security systems of the telecom operators providing an added value. However, the fact that RESISTO is an innovation action (IA) research project lasting for a certain period of time imposes certain limitations and constraints which would be considered as challenges when setting metrics and KPIs. These limitations pose certain considerations which are briefly the following:

- For obvious reasons, RESISTO does not attempt to use the commercially available telecom networks of the telecom operators since this would imply in many cases loss of the delivered service to the consumers and customers. **Test beds emulating the telecom networks** will be used instead, provided by the telecom operators. However, although this is a good and realistic representation, the fact that the real communications networks will not be used will affect the measurement of KPIs in certain cases, since these depend on the capabilities of the test beds.
- In a similar context, **the piloting will be held through Use Cases** defined accordingly; their number is adequate enough for an IA research project, however a narrower overall testing of the real conditions in a telecom network will be held.
- Finally in combination to the previous restrictions, **the time duration of the project is finite** which implies that perhaps there would not be adequate time to be able to measure overall performance KPIs in a large period of time (e.g. in order to measure the network's availability, often a large period of time i.e. over a year is needed).

Based on the above it is seen that the above limitations may in turn provide relevant constraints to the testing and measurements of the metrics and KPIs that will be set. In other words, care should be taken not to set KPIs risking being proven that it would be very difficult or even impossible to be measured through the test beds in the framework of the use cases and for a specific time constraint. And that is important since baseline values should be checked before measuring the KPIs in order to prove the impact and added value of the RESISTO solution. Consequently, and based on the above discussion, the basic principles that will govern the selection of the RESISTO KPIs along with the suggested guidelines and methodology that is going to be used, are presented in the following paragraphs.

3.3. Principles and guidelines for the selection of the RESISTO metrics and KPIs

It is obvious from the above, that even the definition of KPIs and metrics is not an easy and straightforward task. Still the usefulness of using KPIs and suitable metrics to assess the success (or failure) of a system and obtain information on which decisions can be based, is regardless of how someone defines KPIs and metrics, undisputable. In order to select meaningful KPIs in the framework of the RESISTO project, a set of guidelines has been defined and followed.

First of all, an important question should be thought carefully: of how many KPIs should be measured. According to the sources and the best common practices, measuring too many KPIs can put an excessive overhead to both the analysts that track the KPIs and/or the system itself, while at the same time render the decision process based on the information obtained from the measurements, overly complicated and suboptimal. Still there are no golden rules or formulas that can accurately estimate the optimal number of KPIs that we should measure, but rather empirical suggestions that can be found in the literature as denoted in the previous Chapter. One suggestion is 3 per goal/system function, while another is 5 to 9 in total. Keeping that in mind, we didn't follow any of these suggestions from the beginning, but rather at the end, after the list was refined and all the other guidelines herein were applied. Our choice will be explained and justified in the next chapter, where the first complete, at the moment, list of suggested KPIs is presented.

Furthermore, meaningful KPIs should possess certain features that are needed to be defined prior to the selection process. This would enable accepting or rejecting a KPI in the final list based on whether these characteristics are obtained or not. These features, that all KPIs should possess, can be classified into three groups from the more general to the more specific.

The idea behind this approach is that the selected KPIs should, above all:

- be meaningful KPIs and metrics (general group),
- they should qualify as proper security KPIs (security-specific group)
- and finally, should be suitable for the RESISTO project (RESISTO-specific group).

3.3.1. General features

There are certain features that all meaningful KPIs share, regardless of the application domain. These comprise the most general group of features and the first thing to check when determine the eligibility of potential KPIs. According to the sources, there are three (3) characteristics, that are deemed as necessary for any KPI. Specifically, all KPIs should be:

- **Simple:** By simple is meant that a KPI should be clearly defined and not complicated to measure. Moreover, its purpose and impact should be clear. An overly complicated KPI could be misinterpreted and potentially mess-up the decision process.
- **Measurable:** Measurable is self-explanatory and can be attributed to both quantitative and qualitative KPIs. It stresses the need for a clearly-defined and consistent method of measurement for each and every KPI, and
- **Time-based:** Finally, proper KPIs should be used to demonstrate changes over time. An effective KPI should be able to be measured and grouped by various time intervals to show variations and patterns. Time is an important dimension that it shouldn't be overlooked when selecting suitable KPIs. Being able to assess the system's success or failure over time periods of various lengths is extremely useful and can provide invaluable information to the decision process.

3.3.2. Security-specific KPI features

This group contains the common features of security-specific KPIs. To this respect, Security KPIs should be **relevant** (to the security function being assessed) and **actionable**.

To understand relevant and actionable let us first consider the proper approach to deriving security KPIs. Instead of trying to devise a KPI from scratch based on common sense and insight on what would constitute a good metric, it would be better to start by first identifying which security goals or functions of the system are the most critical ones.

Then a KPI should be a measure of the success or failure of such a goal or function and a means of providing actionable information in order to improve the system. Thus, relevant means that the KPI should be clearly related to the function/goal under assessment, while actionable means that the measurement should provide useful information that will facilitate the decision process.

3.3.3. RESISTO-specific KPI features

Finally, this group contains the features of KPIs that are suitable and meaningful for the RESISTO project. A different approach is being followed to assert whether a KPI possess these features. Instead of clearly defining this list of features, so someone can verify the eligibility of a specific KPI by checking whether it possess the items on the list or not (which is what was done for the previous groups), the approach is simplified by defining the process itself and not the features, since in this specific case defining the features is not an easy task. Thus, for the specific case the selection of a KPI depends on the following assumptions for each candidate KPI:

- a) **The KPI should be under the end users' interest while simultaneously be relevant to the RESISTO solution.** The KPIs should be compliant with the user requirements and should not

duplicate existing KPIs that already are measured from the telecom operators for i.e. contracting SLAs on network performance or through their existing security systems (i.e. access control).

- b) The KPIs should enable their measurement and assessment during the pilot cases, within the project's time framework, the special conditions and the available resources. Although there are certain generally meaningful KPIs, that would be interesting to be measured, time restrictions and resource limitations common to research projects, even IA ones as RESISTO, might prohibit their relevant conductance. Unfortunately, to this respect, certain KPIs of this kind should be rejected and removed from the final list.

3.3.4. *Challenges to be tackled*

Based on the above certain challenges are imposed when justifying the selection of the RESISTO solution KPIs. These are briefly discussed in the following:

- **Targeting ACTUAL KPIs to be addressed within RESISTO:** in order to comply with the above principles and criteria and provide meaningful results the best option should be that the KPIs are measured / validated through the test beds of the telecom providers and within the time frame of the project. Due to the limitations discussed in the previous sections it is rather that representative KPIs can be evaluated on a case by case basis (i.e. per test bed or pilot case); in other words there may be the challenge and risk that unified KPIs for the overall RESISTO solution might not be able to be validated or measured. An important aspect for that is how baselines will be set and if realistic targets can be defined. Furthermore, the baselines must be checked through the test beds and the pilot cases and in this context time constraints may play significant role especially when long time periods are inherently needed for certain KPIs to be calculated and validated.
- **Resilience related metrics and KPIs:** The ideal situation would be to derive an overall unified indicator for the whole RESISTO solution. However, as it seems both from the literature overview and the principles discussed above, this might be very difficult or rather impossible due to the variety of performance characteristics that would need to be involved. To this respect a set of resilience relevant indicators is more likely to be derived. Furthermore, all stages of resilience such as prevention / preparedness, response and mitigation should be addressed which adds to that aspect. As it will be discussed in the following, the resilience related metrics will be held especially through the implementation of the long-term control loop (the risk and resilience management tool).
- **Metrics and KPIs should be related with the RESISTO platform and the relevant risk assessment:** This challenge dictates the fact that the KPIs should be validated through the RESISTO pilot cases as discussed previously. However, certain parameters should be underlined herein affecting the quantification of the RESISTO impact on the telecom CIs security. On the one hand representative pilot use cases should be defined (i.e. in the framework of D2.8) so that the metrics comply with the end users requirements and expectations KPIs and on the other hand the KPIs should be connected to the RESISTO platform and risk assessment outcomes in order to show the positive impact of RESISTO solution to the existing security systems or tools at telecom CIs. In this sense, telecom network performance indicators, metrics and KPIs are not considered as exactly the same with the RESISTO KPIs; moreover, it is assumed that these indicators (traffic, packet loss, denial of Service, availability, response time in failures etc.) are already assessed by the telecom providers (i.e. through technical assessment or under compliance to standards). When threats, attacks, or exploited vulnerabilities happen, the RESISTO solution is applied resulting in risk-assessment outcomes that can be used by the telecom providers (i.e. providing input to existing security systems). However, certain network performance indicators can be used for setting the baselines, since they are or can be tangible, or can be used up to level that they

contribute to measure the added value and the impact of the RESISTO platform in maintaining or improving these goals. Thus, the “impact” of the RESISTO solution needs to lead to a potential improvement of the related security (and even of the network performance, or at least NOT to affect certain indicators).

In the following paragraphs of this Chapter we will attempt to respond to the above challenges through the sources of mining indicators and the available tools of the RESISTO solution itself.

3.4. Sources and procedures used for selecting indicators and baselines

The KPI selection process started with a rather large list of KPIs originating from various sources and proceeded with the refinement of the list using the principles and guidelines defined in the previous section. Herein the different sources are presented with some details on the refinement process, while the actual list with the KPIs is described in detail in the next Chapter of the present report.

3.4.1. Contractual indicative list

An initial acknowledgment of indicative KPIs are presented in the RESISTO DoW in Table 1 of Section B1.1. In this Table the KPIs for the progress of the RESISTO project are listed including the administrative ones. However, certain technical KPIs related to the performance of the RESISTO solution were gleaned and were initially shortlisted as preliminary indicators towards the potential targeted performance. These preliminary indicators are given in the following in priority listing:

KPI Name	KPI Description and Examples	Target Value
TLC system technical/ organizational (non) performance quantities; (Time-dependent functions, all resilience cycle phases)	false alerts; detected physical or cyber-attacks (independently); detected cyber-physical attacks (combined); human interventions/ automated response;	20 % reduction; 10 % increase; 20 % increase; 15 % decrease/ increase;
Threat/ Disruption/ awareness index	awareness of unexampled/ black swan threats; awareness of concurrent/ongoing threats;	25 % increase; 15 % increase;
Quantitative metrics for all resilience cycle phases/steps (Resilience cycle dimension)	Prevention, protection and detection indices; Preparation, response and recovery indices; Improvement ratio indices;	5 -10 % average improvement; 15 % average improvement; 25 % average improvement;
Quantitative metrics for TLC system layers coverage; (Resilience system layer dimension)	Physical layer indices; Cyber/ Protocol/ Software layer indices; Technical/ Hardware layer indices; Organizational, Economical, Ecological indices;	30 % improvement; 15 % improvement; 10 % improvement;
Innovative Technology performance indices, addressed by each technology	Resilience dimension indices; contribution to overall cyber-physical security & CI resilience improvement, in terms of overall KPIs	At least 4 improved by 30 %; At least 5% to overall risk control or resilience;
Risk control and resilience improvement methods awareness index;	Ranging from known, already implemented efficient up to ineffective and/or not efficient methods;	10 % - 30% increase; case dependent
TLC Level of Service (LoS) Quantities; Top level system performance functions; (Time-dependent functions, all resilience cycle phases)	emergency connections available on (continuous) demand, including LEA and private communications, fast industrial/ automotive internet); Security costs: physical/ cyber/ cyber-physical;	2 -10 % increase; case dependent 3 %, 5 %, 15 % decrease;
Residual overall risk due to cyber-physical events Residual overall resilience	Expected monetary loss and casualties per annum; Performance loss triangle area, multiplicative or additive resilience measures and metrics;	10 % improvement average; 20 % improvement;

Table 2 – Indicative Indicators in the RESISTO DoW

Through a qualitative assessment of the above list, it is seen that detection and resilience (prevention / preparedness) related KPIs were formulated in general with desired target values. These metrics were then assessed in terms of context and measurement capabilities through the RESISTO tools and test beds and the list was prioritized. To this end, it is acknowledged that cost related KPIs may be quite more difficult to be validated; however, they are still considered in case the relevant information can be indeed provided by the telecom providers (if not confidential).

3.4.2. End Users' feedback

An important source of desired metrics and KPIs for the initial pool of indicators was the input of RESISTO's end-users and technical partners. Following the proper approach suggested in the sources and literature, instead of devising new KPIs from scratch, the contributing partners first identified, based on their expertise and interests, which security goals or functions of the RESISTO system were the most critical; thus, relevant KPIs were derived that could, as metrics, assess the corresponding goal or function and provide actionable information for the decision making process.

The end users / telecom providers and the technical partners contributed in every step of the selection process and refined the pool of potential KPIs based on the guidelines defined above so that the preliminary, at this point, shortlist to be derived. Thus, no other restriction was imposed to the KPIs initial list at this stage than the end users' feedback.

3.4.3. The ENISA framework

Already from the literature overview in the previous Chapter the importance of the ENISA metrics and resilience measurements framework for the setting of KPIs in security initiatives related to telecom infrastructures like the RESISTO project. The significant importance of the ENISA framework is that it provides the ability to set out the baselines for the measurements of KPIs, especially in the case where baseline metrics are not possible to be provided by the telecom operators or variations should be encountered when using the test beds as emulators of the telecom networks. And this is critical, since the ENISA Report³³ suggests specific calculations for the metrics along with a set of indicators for the resilience stages in general. As discussed in the previous Chapter, a two-dimensional approach is followed to categorising resilience metrics.

The incident-based dimension classifies resilience metrics before an 'event' happens (that is preparing for resilience and delivering the intended service), and after the 'event', while trying to respond and recover to normal operation. Thus, resilience is expressed over the 3 different time phases (preparedness, service delivery and recovery), much alike those intended by the RESISTO project.

In Preparation phase, it is assumed that resilience provisions are implemented in order to prepare the network/service for coping with faults and challenges. Metrics in this dimension measure how well systems and services are prepared to cope with challenges/faults. A high preparedness metric indicates a reduced failure or threat probability to critical infrastructure, systems and components.

In the Service Delivery phase, the network is operational and detects occurrences of faults and threats. Metrics in this dimension measure the difference in service level before, during and after the threat or challenge. A low metric (a high difference in service level) indicates that the consequences on the network are reduced. The specification of the level of a network service typically consists of

³³ "Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report", resilience study, February 2011, <http://www.enisa.europa.eu/act/res>

defined minimum thresholds for all relevant, quantitative properties of that service. The measured properties are monitored and compared to the defined service level thresholds, to assess whether the level of service is met. Network service levels depend on the operational quantitative parameters of the network that supports the service, (as in SLAs or specs) such as service availability, throughput (bandwidth), latency (average round trip time), packet loss, jitter (packet delay variation), etc. These availability and service quality elements express whether the network service is actually delivered and can be measured as a function of time. Therefore, the objective of pursuing network service resilience is to lower the impact of operational network degradation on the network service parameters. In the recovery phase, actions are taken to restore normal operations and the metrics indicate how fast a service/network can recover from faults/challenges. A low metric indicates reduced time to recovery (the time required to restore a network or a service to the normal level of functionality).

The second dimension of the ENISA taxonomy is based on the different domains which collectively constitute the notion of resilience, thus measuring different aspects of the same resilience property. These domains are security, dependability and performability and are defined as follows: Dependability as a property is defined within the report to generally include the measures of availability (ability to use a system or service) and reliability (continuous operation of a system or service), as well as integrity, maintainability, and safety. Security is the property of a system or network of being protected from unauthorised access or change, subject to policy and includes auditability, authentication and accountability, confidentiality, and non-repudiation. Security shares with dependability the properties of availability and integrity. Performability is the property of a system such that it delivers performance required by the service specification, as described by QoS (quality of service) measures.

The result of this two-dimensional model concerning the identified resilience metrics using the suggested by ENISA taxonomy is given in the following table:

Incident-based classification	Domain-based classification		
	Dependability	Security	Performability
	Preparedness <ul style="list-style-type: none"> • Mean time to Incident Discovery • Mean time to Patch • Patch management coverage • Vulnerability scanning coverage 	<ul style="list-style-type: none"> • Risk assessment coverage • Risk treatment plan coverage • Security testing coverage • Security audit deficiencies • Percent of ICT systems with BC plans 	<ul style="list-style-type: none"> • Tolerance
	Service Delivery <ul style="list-style-type: none"> • Operational mean time between failures • Operational availability • Operational reliability • Fault report rate 	<ul style="list-style-type: none"> • Incident rate • Illegitimate network traffic • Percent of systems without known severe vulnerabilities 	<ul style="list-style-type: none"> • Delay variation • Packet loss • Bandwidth utilization
	Recovery <ul style="list-style-type: none"> • Mean down time • Mean time to repair • Maintainability 	<ul style="list-style-type: none"> • Mean time to incident recovery 	

Table 3 – The ENISA suggested taxonomy

Despite the fact that, where possible, each metric is associated with target values, (as thresholds for an acceptable value of the metric, it is admitted by the report that due to the specific nature of different network services existing, it is very difficult to include target values for all metrics.

A generic template is used to describe the resilience metrics in detail, including the following parameters: description of the metric, source from literature, objective targeted goal, measurement method, frequency of appearance (times per period that the data will be collected), target values and reporting format. An indicative example of the description of a resilience metric i.e. the incident rate (the service delivery phase) as presented in the ENISA report is given in the table below:

Metric name	Incident Rate
Source	This metric is adopted from 'The CIS security metrics - Consensus Metric Definitions v1.0.0' [5].
Description	The incident rate metric measures the number of security incidents that occur in a given time period from selected incident categories.
Objective	The incident rate indicates the number of detected security incidents the organisation has experienced during the metric time period. In combination with other metrics, this can indicate the level of threats, the effectiveness of security controls and/or incident detection capabilities.
Measurement method	<p>To calculate the incident rate metric, the number of security incidents in a given time period are counted, additional grouping could occur per incident category or organisational departments for example.</p> $\text{Incident_Rate} = \frac{\text{Amount_of_incidents_per_category}}{\text{Length_of_time_window}}$ <p>The time window is expressed as an absolute unit of time (e.g. hours or days) while the number of incidents is an absolute number, indicating how many incidents have occurred in the past time window.</p> <p>Note: In a network of ICT security systems, it is possible that each security device reports an attack at the very same time, although only one attack is ongoing (for example: an incident on the outer firewall and an incident on the IDS system can indicate the very same event). This can result in a skewed view of the amount of incidents that occurs on the network.</p>
Frequency	The incident management and follow-up should happen on a continuous basis and at least daily.
Target values	<p>No specific target can be set, as the metric will also depend on the categories of incidents that are taken into account in this measure.</p> <p>A target should be set the variation of incidents that occur (to trigger alarms).</p> <p>Incident rate values should trend lower over time – assuming perfect detection capabilities. The value of "0" indicates hypothetical perfect security since there were no security incidents. Because of the lack of experiential data from the field, no consensus on range of acceptable goal values for Incident Rate exists.</p>
Reporting	Reporting of the incident rate should be per category and in a time-series plot.

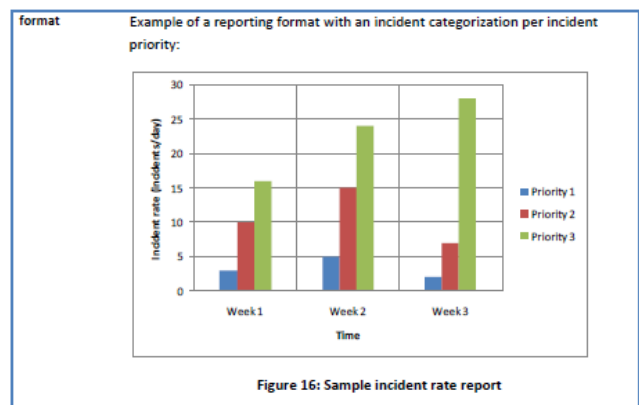


Table 4 – An indicative example of the description of a resilience metric

It is clear that the ENISA resilience metrics refer to the operation of a telecommunications network and in this sense, it involves metrics and KPIs for the network performance itself. It is stated within the report that depending of the criticality of a certain network service for an organisation, (additional) application-specific resilience metrics can be set and is proven to be very useful. For examples, for applications such as Voice-over-IP, HTTP traffic or E-mail, a metric for speech quality in Voice-over-IP environments can be defined e.g. as 'Speech Quality'; to measure the instantaneous voice quality

when Voice-over-IP traffic is sent over networks (ITU-T uses the term “Mean Opinion Score” / MOS in a similar procedure to indicate the resilience of the voice traffic to degraded network conditions)³⁴.

Based on the above the ENISA resilience metrics could act either as baselines for the RESISTO KPIs or selected of them could be used independently as indicators as it will be seen in the next Chapter. Especially for the metrics of the service delivery phase these can act as the service functions for the Risk and resilience management tool (long-term control loop) of the RESISTO platform. To this respect, in the following an insight of the use of the Risk and resilience tool in relation to the resilience metrics will be given along with specific attention to the measurements’ guidelines for the RESISTO KPIs.

3.5. Resilience metrics through the RESISTO Long-term Control loop

As discussed previously special emphasis should be made of the resilience-related KPIs. An integrated risk and resilience management process, based on the ISO-31000 standard for risk management, is performed by the long-term control loop of the RESISTO platform. This process uses suitable metrics and resilience-related KPIs to assess system performance and decides upon mitigation options based on the obtained information. In a similar manner to the procedure described previously, it first identifies the system functions and derives proper and relevant KPIs that will provide the required information that will facilitate the decision make process. Although the complete process is described in detail in deliverable D3.1 of task T3.1, a short description is included herein to show how the resilience KPIs are derived and used within the framework of the RESISTO project.

A schematic representation of the joint risk and resilience management process is shown below.

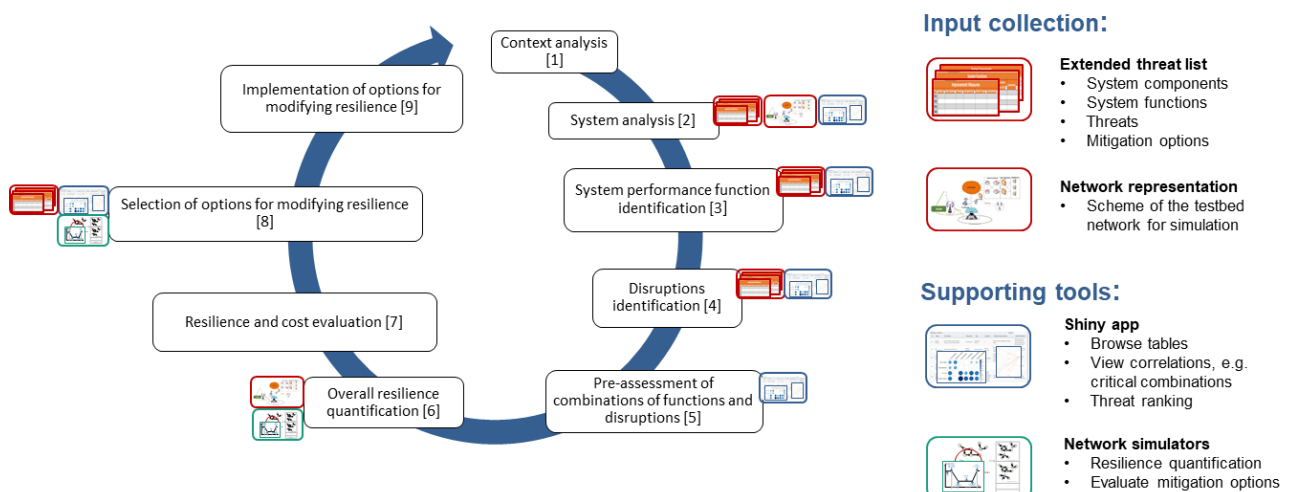


Figure 4 - Risk and resilience management process with supporting inputs and tools for the RESISTO project.

Several input tables were gathered in the extended threat list. In total, dedicated information for four process steps is collected:

³⁴ ITU-T P.800: Methods for objective and subjective assessment of quality (<http://www.itu.int/rec/T-REC-P.800-199608-I/en>)

1. System components → Step 2: System analysis
2. System functions → Step 3: System performance function identification
3. Threats → Step 4: Disruptions identification
4. Mitigation options → Step 8: Selection of options for modifying resilience

The system performance functions identified in step 2 constitute resilience quantities that need to be monitored, computed or generated in order to follow the joint risk and resilience management process of RESISTO. In particular, they are a necessary input for the pre-assessment of critical combinations of system functions and disruptions (step 5) and the following resilience quantification (step 6).

The resilience quantification is based on a computation of the performance loss due to the disruption by means of network simulations (see D3.5 of task T3.3). Exemplary resilience curves are shown in the following figure. The y-axis values are defined by a pre-defined performance measure. A general class of performance measures can be taken directly from network/graph theory, e.g. connectivity or centrality measures. However, more detailed results can be obtained by using the identified system performance functions e.g. a certain failure might only affect specific services while other functions are still working.

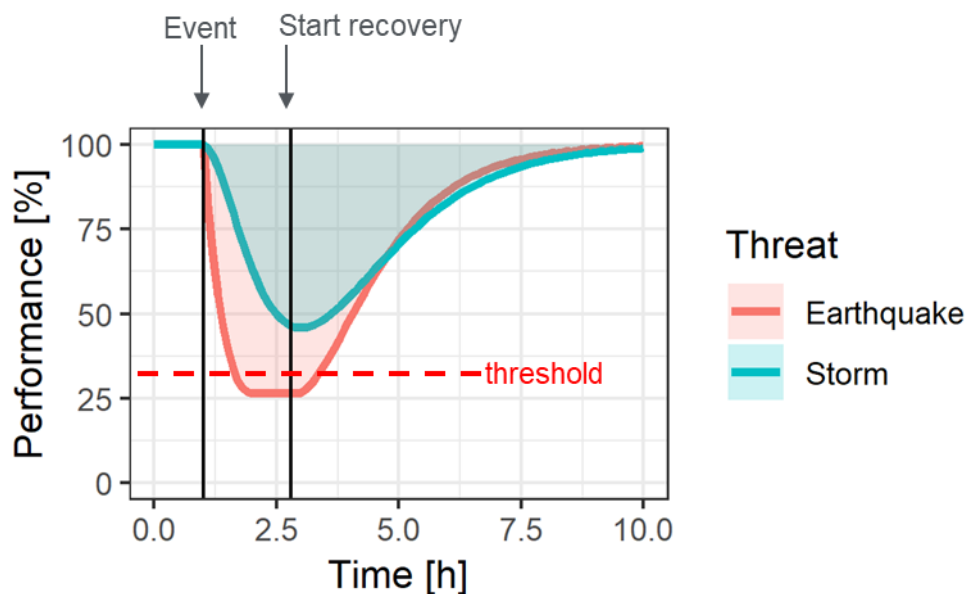


Figure 5- Exemplary resilience curves for two different threats.

3.5.1. System performance functions identified by the extended threat list

All telecommunication partners in the RESISTO collaboration were asked to provide input for the extended threat list (see also D2.3 of task T2.2). A list of all system performance functions (SFs) provided by the partners is shown in Figure 6. For each SF, several input fields were contained in the template, as shown in the exemplary screenshot of one SF table in Figure 7. An important feature of the template is the linkage between the tables, in this case the identification of system components needed for the SF to perform properly (*Linked Components*). This enables the propagation of the malfunctioning of a specific device (*System Component*) due to a disruption (*Threat*) to the performance loss of a specific service (*System Function*).

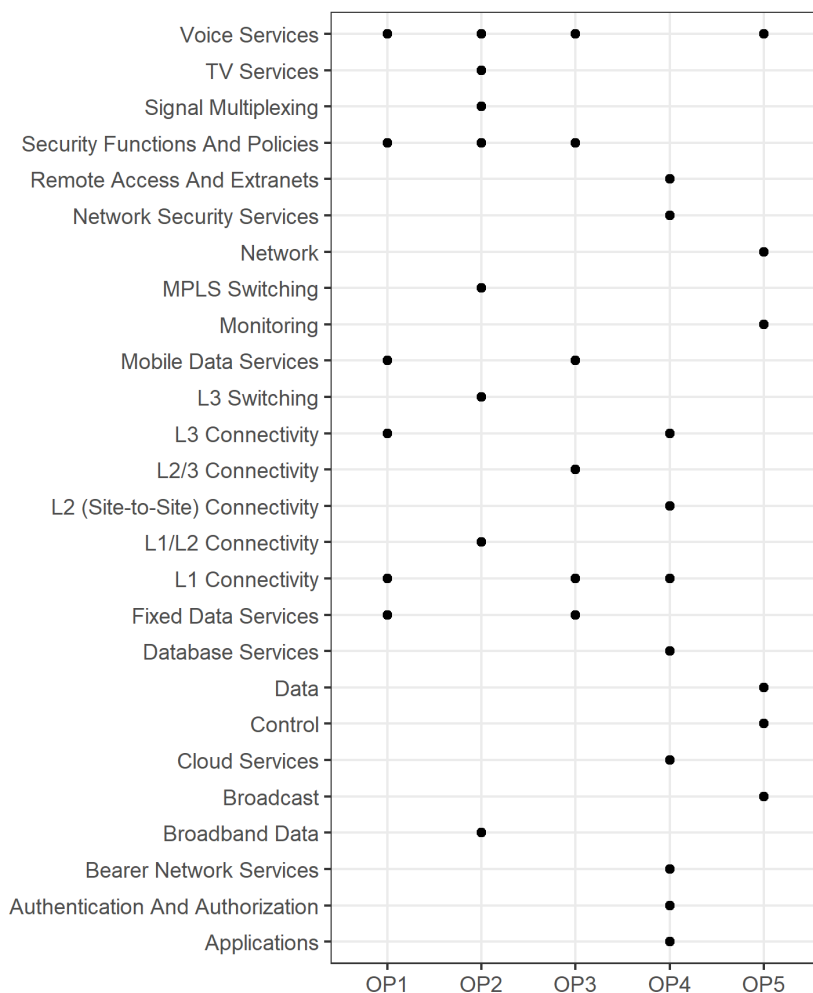


Figure 6 - List of system performance functions provided by the five telecommunication operators (OP1-OP5).

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 7-Exemplary screenshot of the performance functions table with partial input from one operator.

3.6. General guidelines for KPIs measurements

Although specific principles were mentioned before on how to properly measure the KPI values, an insight of these guidelines in relation to measurements and validation processes is being held herein to act as a reference that will be useful, especially for the comprehension of the decisions taken on which KPI to keep and which to reject, that will be described in the chapter that follows.

Additionally, this will be used as a guide during the actual measurements of the final KPIs during the RESISTO project. And this is too important for two reasons:

- They should be encountered when using the test beds as emulators of the telecom networks for the validation of baseline values and the measurement of the KPIs. The test beds are directly connected to the piloting through the macro-scenarios and the RESISRO Use Cases which are to be fully defined in the framework of the relevant Deliverables due within the next project period.
- Furthermore, it is important to define how baselines are going to be validated and measured by the telecom operators through their test beds. To this respect, baseline values have to be checked first through the test beds and then the measurements of the actual KPIs will be held. This way, and through the related comparisons a proof of concept of the RESISTO added value will be derived.

The measurement method for each KPI should thus be rather simple, repeatable, consistent and reliable.

- Simple in the sense that it shouldn't be overly complicated requiring a large overhead that would potentially hinder the system operation and/or compromise the overall system performance.
- It should be repeatable so it doesn't require special conditions and expensive resources to be performed as we should obtain different measurements of the same KPI and track its evolution in time (see 3.3.1).
- The time dimension is of the essence, as it offers additional information, critical to the decision-making process.
- Additionally, the measurement method must be consistent and not being affected by unknown and uncontrollable factors, yielding the same values under the same conditions.
- Finally, a reliable measurement method is needed for each KPI, as the obtained information will drive the decision-making process, a critical process in all security related systems. Unreliable measurements could lead to degradation in performance even to total failure of the system.

Having then defined all the necessary guidelines as described in this section, checks whether any KPI in the preliminary shortlist possesses **all** the required features, i.e. being **simple, measurable, time-based, relevant, actionable, of interest for the end-users** and **suitable for the RESISTO project** are going to take place in the next Chapter. A description of each selected KPIs in this initial pool takes place along with the challenges in their measurements and validation in terms of whether it would be feasible to reliably measure it, given the time and resource restrictions inherent in an IA project.

Following this procedure, as it will be seen in the next chapter a preliminary shortlist of metrics and KPIs is defined which will be finally selected within the framework of the final version (D3.8) of this Deliverable during the next period, where both the Test Beds and the pilot use cases will have been finalized and thus the KPIs measurement methods will have been verified. As it will be denoted in the next Section, certain KPIs were left as a reserve list or even discarded at this point based on the above assumptions. In the next chapter, this list along with KPIs that were rejected will be presented along with explaining the reasons for each KPI separately.

4. THE RESISTO RESILIENCE KPIs – SHORTLIST AND JUSTIFICATION

Following the principles and guidelines, described in the previous Chapter, that would govern the selection of the metrics and KPIs for validating the RESISTO solution and its Risk and resilience framework, the description of the suggested indicators takes place in the following. The aim in this first Deliverable version is, to result in a shortlist of the metrics and KPIs that will be further examined and assessed through preliminary experiments in the next final version of this Deliverable in order to derive actual measurable indicators for the validation of the RESISTO added value. This shortlist will act as a pool of parameters and metrics or in other words an inventory that will be monitored and enriched following up the project evolution and its development stages.

The main aim of RESISTO is to enhance the resilience of telecommunication infrastructures. In this context this chapter provides metrics and KPIs to quantify resilience for the telecommunication infrastructures and in particular, to measure the resilience enhancement and improvement by the implementation of the RESISTO platform and overall solution. As already discussed in the previous Chapter, the resilience improvement should be targeting all resilience cycle phases as shown in the following figure (as these were also defined in Deliverable D3.1 section 3.2, where the reader may seek more information on the details of implementation). In general terms, the resilience cycle phases can be sorted into two categories: before and after the event.

The phases before the event (before-event phases) include the stages: **“prepare, prevent and protect”** (as in Figure 8, left) or **“defend and detect”** (as in Figure 8, right). To this respect, metrics and KPIs related to these stages are provided in section 4.1. The phases after the event (after-event phases) include the stages: **“respond”** or **“remediate and recover”**, in Figure 8 (left/right) respectively. So, metrics and KPIs related to these stages are provided in the subsequent section 4.2.

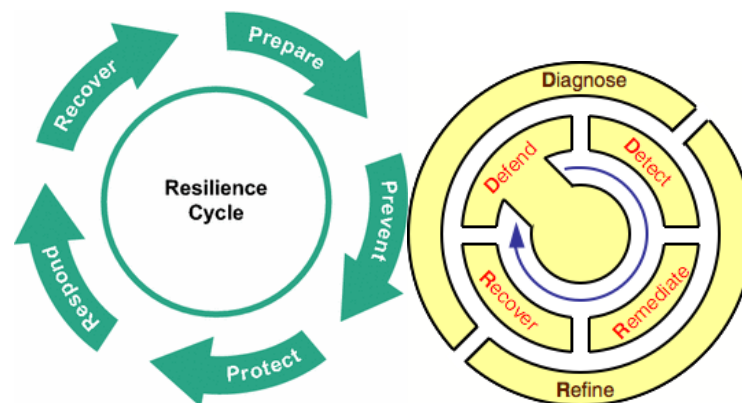


Figure 8 - Resilience cycle phases

Furthermore, (sub-) metrics are needed especially for the quantification of specific resilience KPIs, such as the performance loss during an event being an important indicator. These metrics are provided in section 4.3 and they basically refer to telecom network performance metrics. However, these resilience quantities are needed for the integrated Risk and Resilience Analysis Management process, (as explained in section 3.5) and will be used as input in the form of system functions. Finally, the Chapter ends with certain general KPIs (given in section 4.4) contributing to the performance validation of the RESISTO platform and the presentation of the suggested KPIs shortlist in a tabular format.

4.1. Protection and Detection Stages: Metrics and KPIs

This section covers metrics and KPIs related to the resilience phases before the event, for example protection and most importantly detection. The RESISTO solution incorporates a strong detection dimension especially for physical threats, while the identification of cyber-physical ones through respective correlation can be enabled. It should be noted that specific KPIs are closely related in order to provide an overall overview of the detection process.

4.1.1. Number of detected physical threats

Objective: The number of detected physical threats metric indicates the number of different types of physical threats that can be detected by the RESISTO system. This KPI is related to the physical threat detection functions of the RESISTO system and effectively measures its detection capabilities.

Description: This KPI is a number that indicates how many different types of physical threats can be detected by the system, e.g. a system that could detect hostile drones and perimeter breaches by unauthorized people, would have a measurement of 2 for this specific KPI. Since a single physical security module integrated into the RESISTO platform can detect more than one type of physical threat, this number is a good indicator of the overall system (physical) detection capabilities and it differs from the number of distinct (physical) security modules integrated into the platform. This differentiation is augmented by the fact that in some cases two or more physical security modules can work together to detect a type of threat that would be impossible to detect with just one of them.

Estimated measurement method: The measurement method for this KPI is rather straightforward. Since, the scenarios and use cases will demonstrate during the pilots the detection capabilities of the overall system under almost real-life conditions, measuring this KPI does not seem to impose any overhead at all. Moreover, even before that, during the testing following the development period, a measurement of this KPI would be rather easy and would give an indication of the system's detection capabilities and possibly a motive for further improvement.

Time window and estimated frequency of measurement: This KPI is a single number and it is not time dependent. Thus, it doesn't involve a time window parameter. It can be easily estimated and measured during different phases of the project (see previous section).

Baseline and target values: Probably it may be proven difficult to have baseline values of existing telecom infrastructure, taking also into account that the pilots will not be running on the real commercial network but in an emulated one through the test beds. To this respect, downtime approaches could be used. However, relevant indicators of similar (in functionality) systems can also be sought in the literature and from the existing physical security systems used by the telecom operators to provide a realistic baseline. On the other hand, certain threats (i.e. airborne ones with UAV), probably are not faced (yet). During the development and the post development testing phase a good realistic estimate of the target value for this KPI will be also possible in order these baseline and target values to be finalized in the final (next) version on this Deliverable (D3.8). Absolute values (i.e. zero) could be used as starting points or, depending on the availability of the relevant information, target values can be expressed as percentage of improvement (as suggested also in the RESISTO DoW (section B1.1)).

Challenges, discussion and suggestion for inclusion: There are no other challenges that can be identified at this point, as this seems a well-defined and measurable KPI. To this respect, **it is suggested that the number of detected physical threats KPI is included in the present shortlist.** As discussed previously, it is feasible to measure it in the project's framework without any severe overhead and it provides a good indication of the overall detection capabilities of the system. In a commercial version of the system it would be probably one of the key marketing points.

4.1.2. Number of detected cyber threats

Objective: As in the case of the previous KPI, the number of detected cyber threats metric indicates the number of different types of cyber threats that can be detected by the RESISTO system.

Description: This KPI is a number that indicates how many different types of cyber threats can be detected by the system, e.g. a system that could detect Denial-of-service attacks, Man-in-the-middle attacks and SQL injection attacks, would have a measurement of 3 for this specific KPI.

Estimated measurement method: The measurement method for this KPI is rather straightforward and basically identical to the measurement method of the previous KPI.

Time window and estimated frequency of measurement: This KPI is a single number and it is not time dependent. Thus, it doesn't involve a time window parameter.

Baseline and target values: Since the RESISTO system does not include many "new" cyber threat-detectors, it will rely on the existing detection capabilities of the infrastructure; thus, it is possible that baseline and target values would not be significantly different. To this respect, this KPI differs from the previous physical threats case. It is generally assumed that the detection phase for cyber-attacks should happen at the telco's SOC/CSOC/CSIRT level (Security Operation Center as well as through the Network Security monitoring system), by specialized equipment (i.e. - Anti-DDoS – Distributed Denial of Service, IPS/IDS - Intrusion Prevention / Detection Systems, AV - antivirus, FW - firewalls etc.) and can be reported to the RESISTO platform.

Challenges, discussion and suggestion for inclusion: Although the definition and measurement of this KPI is rather straightforward and normally it would be a good indicator of the cyber-detection capabilities of the system, certain assumptions should be considered in the RESISTO case. Since the RESISTO system does not augment considerably the cyber-detection capabilities of the infrastructure but utilizes the existing ones as an additional source of information that facilitates the decision-making process, this may not result to an absolutely representative KPI. However, since it is generally feasible, this **KPI is suggested for inclusion in the shortlist** while a final decision will be taken and reported in the next version of this deliverable (D3.8).

4.1.3. Number of detected cyber-physical threats (combined)

Objective: Similarly to the previous KPIs, this metric indicates the number of different types of combined (cyber-physical) threats that can be detected by the RESISTO system.

Description: This KPI is a number that indicates how many different types of cyber-physical threats can be detected by the system. The difference from the previous two KPIs is that cyber-physical threats are usually very specific in their characteristics and conditions and cannot be described with simple terms. They usually have the form of specific scenario cases and are more complicated in timing and conditions to either physical or cyber threats. For example, a physical intrusion on the premises that host access to an infrastructure and the subsequent cyber-attack by installing malicious software is a typical example of a cyber-physical threat. However, the correlation between these two actions needs to be identified, otherwise it would be considered as separate threats of each kind.

Estimated measurement method: The measurement method for this KPI is rather straightforward and basically identical to the measurement method of the previous KPI.

Time window and estimated frequency of measurement: This KPI is a single number and it is not time dependent. Thus, it doesn't involve a time window parameter.

Baseline and target values: Relevant indicators of similar (in functionality) systems can be sought in the literature, rather not from the existing security systems used by the telecom operators, since the

cyber-physical security is a rather new approach that in most cases is not covered by the operators' existing security systems. This is planned to be held through the correlator engine and the Risk and Resilience Analysis Tool. To this end, through these components and during the development and the post development testing phase, estimates of the target value for this KPI are expected to be possible and in any case the relevant values will be finalized in the final (next) version of this Deliverable (D3.8).

Challenges, discussion and suggestion for inclusion: The main difficulty in measuring this KPI, stemming from the complicated nature of the cyber-physical threats (see description above), is the thin line between detection success and failure of seemingly similar threats that are only different in specific details, e.g. timing. This makes the actual measurement of the KPI rather tricky despite the straightforward, in principle, measurement method. Thus, the specific KPI **is suggested for the present shortlist**; however the final assessment will be reported in the final (next) version of D3.8.

4.1.4. Detection probability

Objective: The detection probability metric indicates the success rate of the system in detecting potential threats. This KPI corresponds to the threat detection function of the RESISTO system in order to effectively measure the added value on its detection capabilities.

Description: This KPI can be expressed as a percentage that indicates the success rate of the system in detecting potential threats, e.g. a detection probability of 95% would mean that 95 out of the 100 threats, attacking an infrastructure protected by the RESISTO platform, will be successfully detected. It can be based on calculating the number of trials required for an accurate detection estimation. In combination with other metrics, this can indicate the level of detected threats and the effectiveness of security controls and/or incident detection capabilities of the RESISTO solution.

Since the RESISTO platform integrates different security modules in order to handle a wide range of threats of physical, cyber or combined nature, it could be proven to be impossible to define a single detection accuracy for the whole system, as different types of threats are detected by different modules or even combinations of modules. Even the same module, if it can detect different types of threats, may achieve different detection rates, depending on the type of threat. Thus, a meaningful KPI of this type should include different measurements for different types of threats, i.e. a measurement for detecting hostile drones (physical) e.g. 85% probability, another one for perimeter breach (physical) e.g. 90%, another one for detecting eavesdropping attacks (cyber) etc.

Estimated measurement method: Keeping in mind the restrictions imposed by an IA research project, the detection probability can be measured for a small number of different threats with at least one representative, if possible, of all three threat-groups, i.e. physical, cyber and cyber-physical ones. In this sense, it is considered that the Detection probability metric can effectively be measured during the pilots. Similarly, the detection cases must be of physical, cyber or combined type with at least one representative from each type.

Depending on the scenarios and use cases that will be finally selected to be implemented during the RESISTO piloting phase, it is suggested that this KPI is measured on a case by case basis and at least for some specific detection cases; since different cases can have different accuracy baseline values.

Time window and estimated frequency of measurement: A detection probability can be measured for each type of threat by simulating the same type of attack against the system as many times as needed to obtain reliable measurements for the target value of the KPI. The total number of successful detections divided by the total number of attacks will be the detection probability estimate

for each type of threat. Since this KPI is not time dependent, it doesn't involve a time window parameter.

Baseline and target values: An adequate number of cyber and physical attacks can be successfully emulated through the test beds or through the use-case scenarios. Relevant benchmarks can also be sought either in literature or from the telecom operators and end-users. A high value of "detection probability" indicates almost perfect detection since all security incidents are detected. Because of the lack of experiential data from the field so far, a consensus on range of acceptable baseline and target values will be sought and decided in the final (next) version on this Deliverable (D3.8).

Challenges, discussion and suggestion for inclusion: Apart from the aspects discussed in the previous paragraphs, no other major challenges can be identified at this point. To this respect, **it is suggested that the Detection probability KPI will be included in the present preliminary shortlist.** As discussed previously, it is feasible to measure it in the project's framework despite the restrictions posed. Moreover, it provides useful and actionable information that can be used in the decision-making process, e.g. a rather low detection probability for a specific threat type can impose the use of alternative technologies for the specific detection (strategic decisions) or as redundancy solutions.

4.1.5. False Alarms Rate (false positives)

Objective: The False alarm rate metric aims to provide an indication about how many false alarms are raised with respect to the total amount of raised alarms.

Description: The main part of a detection system or equipment, as well as human, provides with each detection a confidence probability, while defining the alert raising threshold is always a problem. A very low threshold would produce too many alarms including some false alarms, while a very high threshold would greatly reduce the detection probability of real alarms. Measuring the false alarm rate can provide, for each detector, a fundamental indication about the threshold's calibration as well as about the benefits of using the specific detector. The RESISTO platform provides different attack detectors to face very different threats (UAVs, jammers, etc.) as well as a correlator of events that can raise alarms by combining related events. So, this KPI should be measured for each attack detector provided by the RESISTO platform.

Estimated measurement method: For each detector a significant set of detector specific positive and negative events should be produced and fed into the system in order to measure the false alarm rate on a case by case basis. The time period where the expected number of false alerts will be produced can be estimated so to measure the actual false alerts during the uninterrupted system operation for the specified period.

Time window and estimated frequency of measurement: For each detector a measurement must be performed corresponding to a specific Detection Probability. So, this KPI can be measured for each type of threat by simulating the same type of attack against the system as many times as needed to obtain reliable measurements for the target value of the KPI. The total number of false detections divided by the total number of detections will be the false alarm estimate for each type of threat.

Baseline and target values: As this depends greatly on the specific detector, an extensive literature search along with some insight from the detectors' developers will provide information that will be used to define the baseline and target values. These will be finalized in the next and final version of this deliverable.

Challenges, discussion and suggestion for inclusion: The KPI is strictly related to the previous Detection Probability KPI; thus the same discussion and suggestions are applicable here as well and

the KPI is **suggested for inclusion in the present shortlist**. It is worth noted that this KPI is more suitable for the physical detectors. For the cyber threats, false positives are mainly handled by the cyber-security equipment of the systems or related infrastructure in place.

4.1.6. Number of concurrent (managed) threats

Objective: The aim of this KPI is to measure how the platform could improve the awareness of concurrent physical, cyber, combined threats in order to optimize reaction and mitigation.

Description: Aim of an Innovation Action (IA) as the RESISTO project, is to put in place and tune a methodology and a set of tools to help CI managers to face different kind of threats, physical, cyber and combined optimizing the reaction and then the effects mitigation. So, in principle, this KPI aims to provide a measure that could show how much the RESISTO solution improves awareness and management of concurrent attacks.

Estimated measurement method: The KPI aims to measure the improvement between the number of concurrent attacks faced by the same team (operators) with and without the RESISTO platform. Since the measurement is based on counting, depending on the desired target values, it may be difficult to create the conditions for a proper measurement during the pilots. One issue is the definition of the baseline where the end users may be able to define the relevant baseline from their existing systems. However, even if this could be accomplished, it would be difficult to emulate the baseline through the pilot cases test beds and the RESISTO platform in order to measure the advancement. And this also depends on the desired target value. Furthermore, more parameters should be encountered especially for cyberthreat types, for example in terms of the number of devices/services/OS currently in use that could be affected.

Time window and estimated frequency of measurement: Different scenarios with concurrent attacks should be run with and without the RESISTO platform in the framework of the foreseen Use Cases. However, this metric does not seem to be time dependent unless the specific scenario to be implemented dictates so.

Baseline and target values: Measures without the platform will be considered as baseline. As expressed in the RESISTO DoW, an improvement of at least 15% is expected as the number of concurrent attacks faced by the same team using the RESISTO platform. However, the feasibility of obtaining this kind of target value remains to be assessed through preliminary experiments with the Test Beds (for i.e. emulating baseline values) in the framework of the next version of this Deliverable (D3.8) where the above values will be finally determined.

Challenges, discussion and suggestion for inclusion: Despite the challenges discussed above, the KPI focuses on one of the main aspects of Innovation Action projects. So, the KPI definition, as well as the measurement method for validation could be refined after a detailed Use Cases and test beds definition that will be finalised in the next period according to the workplan. Based on the above and due to its importance, this type of KPI **should be included in the present shortlist**.

4.1.7. Awareness of black swan threats

Objective: this KPI measures the system's awareness of the likelihood of black swan threats occurring and their impact. It is related to the RESISTO objective of improving CIs resiliency and preparedness.

Description: Black swan events are large-impact, highly unpredictable and rare events. Basically, black swan events can be considered as occurrences which deviate beyond what is normally expected of a situation and which are extremely difficult to predict. An event can be classified as Black Swan if:

- The event is a surprise (to the observer).
- The event has a major effect.
- After the first recorded instance of the event, it is recognized that it could have been expected; that is, the relevant data were available but unaccounted for in risk mitigation programs. The same is true for the personal perception by individuals.

As an example, the existence of a single point of failure is a highly undesirable condition that might expose the system to a catastrophic collapse.

Estimated measurement method: The specific metric is mentioned in Table 1.1 of the RESISTO project Description of Work. However, it is argued whether this metric can be measured, since as it seems this might be impossible. Most professionals are aware that black-swan type of events might very well happen within the organization's operation. Thus, it seems that if an organization is able to manage a black swan, then it not a black swan any more. To this respect, a possible baseline would be the number of black-swans handled already by the end users' existing systems; however, on the other hand it would be impossible to emulate this baseline within the framework of the RESISTO project, due to the element of surprise, inherent in black swans and due to the limited timeframe.

Baseline and target values: As discussed above, these parameters remain undefined.

Time window and estimated frequency of measurement: Similarly, these remain undefined too.

Challenges, discussion and suggestion for inclusion: As was previously mentioned, black swan threats are, by definition, impossible to predict. On the other hand, it is important to manage their awareness; however, a clear measurement (i.e. in terms of percentage) of the (added) awareness provided by RESISTO solution would be again impossible due to the previously described reasons.

To this respect, this metric would probably be related to resilience, in order to determine how the CI can assure a core reduced service also in a "catastrophic" situation. Thus, it is necessary to increase the real situational awareness since, especially cyber situational awareness and information sharing are mandatory. Even if difficult to be achieved, associated tools can be available for automatically monitoring tasks and alert security teams to any anomalous activity that may indicate a breach across a network. Situational awareness processes and systems are being used in concert with other, more traditional cyber security measures to enhance the effectiveness. A black swan event cannot be predicted; however, the probability that it will occur could be estimated as well as its potential impact.

Therefore, as it seems, the probability of this type of event ever to happen is more related to the long-term control loop of the RESISTO platform and especially the Risk and Resilience Management Tool. Through the specific methodology already described, involving an offline pre-processing of the system functions and their impact, an estimation of the likelihood that a black swan event might occur could be derived. In this context, the resilience analysis could derive important results, even in this rather qualitative manner, which would contribute significantly to increasing the awareness on the probability of occurrence of such black swan events. In this sense and under the specific assumptions discussed above, **this metric is kept within the preliminary shortlist.**

4.1.8. Time to Detection

Objective: This metric indicates the duration (expressed as a time value - length) of all the processes needed and used by the RESISTO solution to detect an incident and provide a detection alert.

Description: This KPI can be expressed as a time value measured, starting with the timestamp of the first action or activity registered by any of the RESISTO components as pertinent to (or part of) an Incident and ending with the timestamp of the recording of said incident as an entry in the incident databases. As incident, any type of threats (physical, cyber or combined) can be considered, as long as it is registered to the RESISTO platform databases as such. An incident may also include system failures, which could indicate vulnerabilities; to this respect, it is assumed that the pre-processing of the long-term control loop could lead to proper identification of the incident's type.

Estimated measurement method: Based on the above description, it is seen that the method to measure this KPI could be straight forward; the events could very well be generated through the RESISTO Test Beds. Thus, logs can be observed, as generated by the equipment / software used for simulation of the event through the Test Beds, while these (their timestamps) can be compared to the logs and events as they are recorded in RESISTO platform. The process can therefore be automated to some extent. Keeping in mind the restrictions imposed by an IA research project, as discussed previously, the generated events can vary in type with at least one representative, if possible, of all threat-groups or vulnerabilities. Depending on the scenarios and use cases that will be finally selected during the RESISTO piloting phase, it is suggested that this KPI is measured on a case by case basis and at least for some specific detection cases. In this sense, it is considered that the time to detection metric can effectively be measured during the pilots.

Time window and estimated frequency of measurement: The emulations used in the test scenarios can be re-run as many times as needed through the Test Beds to obtain reliable measurements for the target value of this KPI; thus generating enough data in the form of time stamps in order to normalize the resulted measurement. The exact equipment / software / technique to generate the incidents and the desired type of threat events to be detected by RESISTO, will be defined during the test pilots. To this respect, a specific time window of observing the metric is not needed to be specifically set since the measurements for this metric can be done within the whole piloting period.

Baseline and target values: In order to derive reliable results the end users tools through the Test Beds along with the RESISTO platform tools will be used; for example, ORO's use case and test scenario will make use of both SOC/SIEM configurations and PSIM tools. Although the exact kind of simulations / emulations will be decided during the testing of the scenarios, a target value for this KPI can be approximated as an overall value at this point; as being at least as good (or better) than the baseline, which is assumed as the time to detection needed by the individual monitoring and management systems, for both cyber and physical events (the SIEM and the PSIM).

Challenges, discussion and suggestion for inclusion: As discussed previously this type of metric it is feasible to be implemented and measured within the framework of the RESISTO test pilots, even taking into account the limitations of the project. **To this respect, it is suggested that the Time to Detection will be included in the present preliminary shortlist.** However, the main challenge herein, is to emulate representative threat incidents both in the physical and cyber domain, which on the other hand is the main objective of the piloting use case scenarios of the next project period. Thus, this KPI is considered very important since it is directly connected to the relevant time-related KPIs that govern the decision-making process, as these will be defined in the following paragraphs.

4.1.9. Sensitivity of the monitoring system sensors

Objective: Sensitivity of the monitoring system sensors metric indicates the minimum signal strength that the sensors are able to detect and, therefore, will determine to a great extent the number of

detected devices. This KPI corresponds to the threat detection function of the RESISTO system in order to effectively measure the added value on its detection capabilities.

Description: This KPI is a number that indicates the capability of the system, the number of devices that the sensor or the sensors which make up the monitoring system is able to analyse. This is useful to evaluate the coverage that could handle the monitoring system. The different values that this KPI can have could be for example, a system which is capable of receiving low signal strength, would have a KPI value of 3 (good coverage), a system which is capable of receiving medium signal strength, would have a KPI value of 2 (medium coverage) and a system which is capable of receiving only high signal strength, would have a KPI value of 1 (low coverage).

Estimated measurement method: The measurement method for this KPI is rather straightforward. Since, the scenarios and use cases will be evaluated during the pilots the detection capabilities of the overall system under almost real-life conditions, measuring this KPI won't impose any overhead at all. Moreover, even before that, during the testing following the development period, a measurement of this KPI would be rather easy and will give an indication to the platform what critical infrastructure could be assigned to the monitoring system for the detection of potential threats. Large critical infrastructure could be assigned to system monitoring with high value of this KPI. It would be convenient to decide a standard for the definition of the different values of this KPI taking account the signal strength of the sensors.

Time window and estimated frequency of measurement: This KPI is a single number and it is not time dependent. Thus, it doesn't involve a time window parameter. It can be easily estimated and measured during different phases of the project (see above).

Baseline and target values: An adequate number of sensors with good signal strength could be included to the monitoring system through the test beds or through the use-case scenarios to improve benefits. Relevant benchmarks can also be sought either in literature or from the telecom operators and end-users. These baseline and target values will be finalized in the final (next) version on this Deliverable (D3.8).

Challenges, discussion and suggestion for inclusion: There are no challenges that can be identified at this point, as this is a well-defined and easily measurable KPI. To this respect, **it is suggested that the sensitivity of the monitoring system sensor KPI will be included in the present preliminary shortlist.** As discussed previously, it is feasible to measure it in the project's framework without any overhead and it provides a good indication of the overall detection capabilities of the system. In a commercial version of the system it would probably one of the key marketing points.

4.1.10. Effectiveness of the events generated per service or application

Objective: The effectiveness of the events generated per service or application metric measures the total number of events that the security systems are able to detect. This, for example, could depend on a variety of assumptions; on how many events can be handled; if certain detection technologies are more or less effective at detecting security events and why; on how often users or analysts are manually detecting an event before it is detected by a detection technology. To this respect, this KPI corresponds to the threat detection function of the RESISTO system in order to effectively measure the added value on its detection capabilities.

Description: The intrusion-detection systems within RESISTO could integrate security event management that includes the real-time monitoring and correlation of security events, including notifications and console views for security teams. These systems could provide real-time analysis of

security alerts generated by operational systems, applications, network hardware, databases and basically any other piece of technology that produces collectable logs. Some functions that the intrusion-detection system should include are: data aggregation, event correlation and alerting, creating dashboards... This KPI is a measure of how effective the generation of alerts is and the total number of alerts sent when the threats are detected. This KPI can be expressed as a percentage that indicates the success rate of the system in prompt an alert or event for each detected potential threat, e.g. an effectiveness of 95% would mean that the system will prompt 95 alerts or events out of 100 detected threats attacking an infrastructure protected by the RESISTO platform. It can be based on calculating the number of trials required for an estimation of effectiveness as for the number of events generated.

Since the RESISTO platform integrates different security modules in order to handle a wide range of threats of physical, cyber or combined nature, it is possible to define a single effectiveness of the events generated for the whole system since the events will be generated regardless of the type of detected potential threat.

Estimated measurement method: The measurement method for this KPI is rather straightforward. Since, the scenarios and use cases will be evaluated during the pilots the detection capabilities of the overall system under almost real-life conditions, measuring this KPI will not impose any overhead at all. Some possible measurements would be the number of events/hour, the number of events/day, the number of events/month, the number events/year among others. It would be convenient to decide a standard for the definition of the different values of this KPI.

Time window and estimated frequency of measurement: This KPI is a single number and it is not time dependent. Thus, it does not involve a time window parameter. It can be easily estimated and measured during different phases of the project (see above).

Baseline and target values: An adequate number of events could be included to the detection system through the test beds or through the use-case scenarios to improve benefits. Relevant benchmarks can also be sought either in literature or from the telecom operators and end-users. These baseline and target values will be finalized in the final (next) version on this Deliverable (D3.8).

Challenges, discussion and suggestion for inclusion: There are no challenges that can be identified at this point, as this is a well-defined and easily measurable KPI. To this respect, **it is suggested that the effectiveness of the events generated per service or application KPI will be included in the present preliminary shortlist.** As discussed previously, it is feasible to measure it in the project's framework without any overhead and it provides a good indication of the overall detection capabilities of the system. In a commercial version of the system it would probably one of the key marketing points.

4.2. Response and Recovery Stages: Metrics and KPIs

This section covers metrics and KPIs related to the resilience phases after the event, i.e. response and recovery. The main component involved is the Risk and Resilience Analysis and Management Tool through the Long-term Control Loop of the RESISTO platform.

4.2.1. Performance loss

The performance loss due to a disruptive event is a prominent quantifier to allow a resilience assessment of the system. However, there is also a variety of network performance metrics that are basically considered as sub-KPIs which on the one hand can provide the system functions of the Risk and Resilience Management Tool and on the other hand can be considered as the components of the performance loss as a quantifier KPI. These network performance metrics as sub-KPIs are sorted out with more detailed metrics in Section 4.3.

Objective: the aim is to measure the time-dependent system performance and to quantify resilience for the risk and resilience management process in two levels: a) the total performance loss (as the integral of the performance curve) and b) the maximal performance loss. In other words, to measure the effectiveness of the RESISTO platform in improving the telecom CIs resilience, while guaranteeing that certain performance quantities would not go under a predefined threshold.

Description: This KPI is related to network measures (e.g. connectivity, centrality) considering which components and connections between network nodes are functional. Furthermore, it is related to specific system performance functions which are defined by the end users (as in Section 4.3) taking into account the linkage of system functions with the system components (as presented in Section 3.5).

One of the main aims of the RESISTO platform is to provide a methodology and a set of tools able to improve a Communication CI resilience. This will be accomplished through two main elements: The first one is the identification, (conducted off-line through the Risk and Resilience Analysis), of some disruptions or interventions on the CIs, in order to guarantee that, facing human-driven or natural events, certain CI performances will not be under a predefined threshold. In the second one, at run-time, when an event is detected, the RESISTO platform mitigates the effects in order to maintain the sufficient performance; thus, it reacts in order to recover to the level of complete performance. So, this KPI aims to identify a set of couples (function; event), by applying a complete Risk and Resilience Assessment cycle (Long-Term Control Loop), in order to estimate the permissible performance loss. Then, during the run-time validation phase (Short-Term Control Loop), the events are tackled and thus, the KPI basically measures the real performance loss and the difference with the estimated one.

Estimated measurement method: The measurement is based on the relation between disrupted system functionalities or system components and fully functional components. Thus, the maximal performance loss can be seen as the indicator of the degree of interruption and the number of connectives and centralities which are affected. Furthermore, the total loss, as well as the leak time until the full recovery of the systems, are measured as the ratio of non-functional components against time. Using this information, the total loss can be calculated and compared for different event scenarios, system setups and potential mitigation options.

Time window and estimated frequency of measurement: As part of the RESISTO long-term Control Loop, the performance loss should be computed after the network has been modified in addition to the regular review (offline) cycles of the long-term control loop. The time window which is needed to examine the performance loss as a single KPI depends on the test scenario (use-case) as well as the complexity and size of the network which is analysed. In addition, the performance loss should be measured by the platform for real events (see section 4.3).

Desired results and target values: The positive outcome of the analysis will be a better understanding of how a disruptive event affects the network performance and how the network is recovering, highlighting the specific interrupted system functions vs. leak time. And thus, a **straightforward indicator** is provided to compare the character and impact that different threats, scenarios and mitigation options will have towards the tested network.

Challenges, discussion and suggestion for inclusion: This KPI is too important and **is to be included within the present shortlist**. The main challenge for the validation of the simulated resilience curve is this to be held with real performance data from the end users / telecom operators. Comparing the simulated resilience curves with real performance data under similar distress of the network will enhance the performance of the RESISTO tool and ultimately lead to a better understanding, response and mitigation of the network performance and to this end improved resilience.

4.2.2. Decision-making time (average)

Objective: This KPI aims to measure the degree of reduction of the decision-making time.

Description: The RESISTO platform aims to provide a Decision Support System to assist the telecom operators in their Decision-Making process. Thus, a decrease of the Decision-Making time could be too important for evaluating the added value of the RESISTO solution.

Estimated measurement method: The KPI aims to measure the improvement with and without the RESISTO platform. This can be accomplished during the piloting test trials in order to compare the reaction to the same attack scenarios with and without the platform's intervention. Due to this reason, and the fact that the process may be proven too complex, it is suggested either to focus on one representative case where the majority (if not all) of the RESISTO security modules would be included or to conduct the validation per use-case basis. The starting point in time where this metric should be measured would be directly after the detection phase.

Time window and estimated frequency of measurement: Based on the above, a specific time window for this metric's validation seems irrelevant. Nevertheless, for each scenario a set of measures should be evaluated, to take also into account the operators' experience using the RESISTO platform.

Baseline and target values: Measure without the platform should be considered as baseline. As expressed in the RESISTO DoW, at least a 20% decrease is expected. However, the feasibility of obtaining this kind of target value remains to be assessed through preliminary experiments with the Test Beds since it depends on each scenario's details. This will be subject of the next version of this Deliverable (D3.8) where the above values will be finally determined.

Challenges, discussion and suggestion for inclusion: A lot of different scenarios and threats could be faced so it would be rather difficult to define specific related measures and target values. Moreover, a subjective component must be considered in terms of the operator's familiarization and experience when using the RESISTO platform. Based on the above discussion, **the KPI could be included in the shortlist**; however, through conductance of certain fixed scenario cases and taking into account the subjective component.

4.2.3. Mitigation Time (average)

Objective: The aim is to measure the effectiveness of the RESISTO platform in improving telecom CI resilience, guaranteeing that certain CI performances loss could be recovered in a short time.

Description: As discussed previously, a main objective of the RESISTO platform is to provide a methodology and a set of tools to improve the Communication CI resilience. In order to accomplish that and linked to the Performance loss metric, two main elements will be provided; the first aspect is the identification (conducted off-line through the Risk and Resilience Analysis) of the CI vulnerabilities, in order to guarantee that, at least certain CI performances loss could be recovered in a shorter acceptable time, in case of disruptions or human / natural events. Then, at run-time, when an event is detected, the RESISTO platform mitigates the effects in order to maintain sufficient performance; thus, it reacts in order to recover to the level of complete performance.

To this respect, through this KPI, a set of couples (function; event) is aimed to be identified, by applying a complete Risk and Resilience Assessment cycle (Long-Term Control Loop) in order to estimate the permissible recovery time. Then, during the run-time and validation phase (Short-Term Control Loop), when the events (real or simulated) will be faced, the aim of this KPI is to measure the real recovery time and the difference with the estimated one.

Estimated measurement method: Based on the above, it is suggested for each selected couple (function; event) to validate the estimated recovery time during the Long-Term Control Loop against the measured recovery time during the Short-Term Control Loop.

Time window and estimated frequency of measurement: Similarly, to the previous KPI (decision-making time) a specific time window for this metric's validation seems irrelevant. However, due to the above justification and the fact that the process may be proven too complex, it is again suggested either to focus on one representative case where the majority (if not all) of the RESISTO security modules would be included or to conduct the validation per use-case basis. Thus, specific trials for some selected couples (function; event) could be encountered and a case by case approach is very probable.

Baseline and target values: From the above it is concluded that it would not be possible to fix a baseline. However, it is possible to fix a target value as the difference between estimated and measured recovery time; meeting the target value demonstrates the appropriate methodology approach.

Challenges, discussion and suggestion for inclusion: This KPI is strictly related with the Performance loss one, since both aim to measure resilience indicators' improvements. So, **this KPI should be included in the shortlist** because it characterizes the overall RESISTO approach. It is important to note that certain couples (function; event) should be fixed in order to be able to validate this metric without unnecessary overhead.

NOTE:

It should be noted at this point that, the **"Mitigation time"** and the **"Decision-making time"** KPIs are quite important and, despite the difficulties in assessing and validating them, they could indicate the average "response time" of the RESISTO solution towards either the decision process or the mitigation one for a telecom CI. To this end, in conjunction with the **"Performance loss"** metric, they could be considered as the **"Quality of Service of the RESISTO solution"**.

Thus, apart from the apparent assistance to the telecom operators towards the increasing of their CIs resilience, the RESISTO platform Quality of Service, as defined above, could provide a high exploitation advantage to the RESISTO project.

4.2.4. RESISTO platform Reliability

Objective: The RESISTO platform Reliability metric indicates the success rate in processing the ingested logs and alarms related to cyber-physical security incidents. This metric is related to overall RESISTO platform performance and response while specific modules (data integration layer, threats detector) can be validated simultaneously by this metric.

Description: Reliability is the ability of the system to perform its required functions at normal level service for a specified period of time. This indicator will be calculated taking into account that the number of alerts/events sent to the platform should be the same with the number of alerts/events processed by the platform. Thus, two aspects are involved: the alarms that are produced in respect to the physical and cyber security incidents, which in turn is subject to other KPIs (i.e. the detection ones) and most importantly the fact that all alerts that are generated by the RESISTO platform are also processed. This way, the overall capabilities of the RESISTO platform along with those of internal platform sub-systems are assessed. Moreover, this metric presupposes the proper function of the detection sub-systems of the RESISTO platform (i.e. PSIM) and thus can be evaluated against their relevant KPIs.

Estimated measurement method: The estimated method for measuring this KPI is by counting the alerts/events generated by the systems integrated into RESISTO platform (SOC/PSIM) and the events processed indicated by specific RESISTO modules. The result can be expressed as the percentage of the above ratio. Reliability will be measured in respect to “mean time between failure” (MTBF). The measurement can be carried out through the Use Case piloting process that will be initiated in the next project period and will indicate an overall outcome of the RESISTO platform proving the appropriate operation of all subsystems.

Time window and estimated frequency of measurement: the measurement can be carried out within the whole period of the Use Cases piloting at regular times i.e. quarterly. An adequate time interval can be established as time window of observation (for example 6 hours) in which generated and processed events will be counted. This measurement can be repeated several times during the use-case tests and can be independent of the scenarios tested since it assesses the overall platform performance.

Baseline and target values: As discussed previously, the RESISTO Platform Reliability will be measured in respect to “mean time between failure” (MTBF). As a result, the higher the MTBF value, the higher the platform reliability. As a target value it will be verified that the number of ingested events is equal with the processed events. Nevertheless, the exact type and nature of the incidents will be detailed during the Use case scenarios definition due on the next project period and they will be presented within the final (next) version on this Deliverable (D3.8).

Challenges, discussion and suggestion for inclusion: While reliability is an important KPI, emphasis should be on resiliency and fault tolerance due to the fact that this is an important goal of the project. This means that the RESISTO system design should expect faults and disasters and compensate for them rather than trying to design them out. Thus, apart from the aspects discussed in the previous paragraphs, no other major challenges can be identified at this point. To this respect, **it is suggested that the RESISTO Platform reliability metric will be included in the present preliminary shortlist**, since it is feasible to measure it within the project’s framework.

4.2.5. Incident Correlation / Propagation Index

Objective: This metric identifies critical events and which parts of the network are in particular a target for combined cyber-physical threats. Consequently, this KPI is related to measuring the impact of the threat on the network and its propagation likelihood and thus it relates to the system's response.

Description: Critical components have a cascading and therefore severe impact on the performance of the network in case of a failure or threat incident. Identifying these components is also part of the risk analysis of the risk and resilience management goals of this project. It should be noted, that an incident is characterised as a cyber-physical threat when the physical and cyber events are correlated; otherwise, these would be regarded as separate incidents. Thus, this metric depends on the Risk and Resilience Management Tool (the long-term Control Loop) to investigate this correlation. Moreover, the impact of these incidents, even if these are identified as separate kinds of threats, may propagate within the same organisation or towards other interconnected CIs i.e. in the vicinity. In this context, the Risk Predictor component of the RESISTO platform performs an interdependency analysis, gathering data from the cyber and physical domains to evaluate the impact of exploitations and countermeasures, to simulate the effects of detected anomalies and security attacks while accounting for interconnections between CIs in terms of fault and performance propagation and for preventing and investigating the impact of an event in relation to "cascading effects".

Estimated measurement method: Based on the above, the specific index is feasible to be assessed and measured within the RESISTO framework. Depending on the scenarios and use cases that will be finally selected to be implemented during the RESISTO piloting phase, it is suggested that this KPI is measured at least once, in the framework of the related scenario. Initially the degree of disruption and redundancy of the network components and infrastructure is analysed. On a further step, this information is used to investigate the cascading effect of a single localized event impacts the neighbouring components, respectively to the incident correlation of cyber-physical threats. Simultaneously the Risk Predictor component performs the interdependency analysis and the overall results are correlated together to provide the relevant index.

Time window and estimated frequency of measurement: As part of the long-term control loop the propagation index should be measured after the network has been modified in addition to the regular review cycles of the long-term control loop. Additionally, the exact time frame of measurements depends on the risk predictor's parameters set each time to obtain reliable values.

Baseline and target values: Enhanced knowledge about the inherent weaknesses of the system is needed and will be sought by identifying critical components. This knowledge is important to increase the overall resilience of the system as measures can be undertaken to reduce the vulnerability of such components. Of particular interest is identifying which events and system components are highlighted during this analysis, if considering the combination and propagation of cyber-physical threats in comparison to their sole investigation. Thus, this metric could map out the importance of combined investigation of cyber-physical threats and therefore also highlight the importance of the RESISTO. Thus, a high value of the relevant KPI indicates a high degree of correlated or propagated events.

Challenges, discussion and suggestion for inclusion: Therefore, the measurement of this index is feasible within the RESISTO framework and thus **it is included in the present shortlist**. Information obtained from the short- and long-term control loop should be exchanged and integrated in the reciprocal analysis to allow for an integrational and holistic approach as provided by the RESISTO platform. Due to the involvement of main system components and the absence of experiential data from the field so far (since these are planned to be obtained within the next project period), a consensus on range of acceptable baseline and target values will be sought and decided in the final

(next) version of this Deliverable (D3.8), whereas the WP5 activities and related results will also be more mature.

4.2.6. Down Time during Incident

Objective: This metric indicates the duration (length of time) for the disruption of availability of any system component affected by a threat and thus it is related to the system's response.

Description: This KPI is related to the periods of time that a System Component is 'down'; i.e. it cannot provide functionality to other System Components or to its own processes. A period of down time during an incident will start at the moment of the last registered activity of the affected component (this can be time stamped logs, for example), but only after the detection of an incident, and will end at the moment of the next registered activity of the affected component.

Estimated measurement method: Based on the above, the estimated method for measuring this KPI is by simply counting the "down time" by comparing evidence (i.e. – equipment logs, operating system logs, user logs) pertinent to the former and current activity of the affected component(s). It is assumed that this or similar metrics are already assessed by the telecom end users. To this respect, the RESISTO platform through its additional security and resilience enhancement features would "intervene" positively to reduce the down time during incidents. A reduction expressed as a percentage of the currently measured down time could be also an alternative way of assessment. Furthermore, depending on the scenarios that will be used through the piloting use cases, emulations of specific threat incidents can be implemented through the Test Beds; it is suggested that at least one index of this kind is to be measured per use case.

Time window and estimated frequency of measurement: In order to measure the down time of system components, the incidents leading to down time can be simulated in different time frames as to cover as many usage patterns as possible (i.e. for a border router, different time intervals during a 24-hour timeframe poses different loads as per the traffic patterns and data volumes of the users). Thus, simulations and testing can take place for different system components within these time windows. A frequency of measurement, however, is not a requirement for accuracy when measuring this KPI.

Baseline and target values: The exact baseline value can be assessed and emulated during the simulation tests through the Test Beds, through example incidents, in order to resemble actual values within an organization. The aim is to target improvement over current measurements as the scope of RESISTO is to result in improvements on Resilience. To this respect, a low value (reduced down time) compared to current organization's benchmarks would be targeted. Since obtaining experiential data from the field is subject of the Use Cases in the next project period, a consensus on acceptable baseline and target values will be sought and decided in the final (next D3.8) version of this Deliverable.

Challenges, discussion and suggestion for inclusion: Apart from the aspects discussed in the previous paragraphs, no other major challenges can be identified at this point. To this respect, it is suggested that the Down Time during incident metric **is included in the present preliminary shortlist** and as it seems, it is feasible to measure it in the project's framework.

4.2.7. Human intervention / automated response

Objective: This KPI aims to evaluate how much the platform could enable the reaction and mitigation phases while automating some of the actions and decreasing the human intervention time.

Description: The RESISTO platform aims to assist operators to increase their organization's awareness concerning threats and attacks involving the telecom CIs. Cyber, as well as physical, attacks are evolving, so the target of the RESISTO solution is to provide to the operators a decision support system able to improve their awareness with respect to known and unknown attacks and to suggest certain "preset" options (actions) to face different attacks. In this sense, this metric aims to validate a decrease in human single actions and an increase in automated response actions.

Estimated measurement method: In principle, this metric seems very difficult to quantify and measure since it implies a subjective (qualitative) manner. For example, questions could be raised, if hypothetically a single human intervention happens during an automated response cycle; how then the whole process would be classified, as human intervention or as automated response. Moreover, the impact of the attack to functionalities, components and accessed devices should be considered. However, it is estimated that through the Risk and Resilience Analysis and Management process an off-line procedure could be enabled by analysis of the reaction workflows; thus, for each orchestrator's complex action the number of individual actions (usually performed singularly) would be evaluated as an increase.

Time window and estimated frequency of measurement: This metric does not seem to be time dependent. However, it could be implemented on a case by case basis, where applicable; for each trial in each testbed, also comparing different communication services or technologies (i.e. 4G, 5G, etc.).

Baseline and target values: The number of usual individual actions can be set as the baseline. As expressed in the RESISTO DoW, an (automated actions) increase of at least 15% is expected. However, the feasibility of obtaining this kind of target value remains to be assessed through preliminary experiments with the Test Beds and also through offline related processes of the Risk and Resilience Analysis and Management methodology conducted in the framework of the next version of this Deliverable (D3.8) where the above values will be finally determined. As a preliminary assessment, it could be considered that this KPI could be an improvement towards facing the same threat set, and not the indicator per se.

Challenges, discussion and suggestion for inclusion: The threats evolving scenarios suggest a Decision Support System approach based on risk assessment; the man-in-the loop is provided with recommendations which are derived, based on complete automated, but not too rigid, response approaches. Since through the RESISTO solution, predefined set of actions to be executed singularly is suggested and enabled, it seems that generally the relevant improvement could be measured. In this sense, this specific KPI is **suggested to be included in the shortlist**, despite the issues posed and the challenges to be tackled. In this context, a comparison of results on traditional communication technologies test bed and/or 5G ones would be very interesting.

4.2.8. *Decision-making failure rate*

Objective: The aim of this metric is to measure if the platform has any "side effect" and how this could be improved.

Description: The KPI aims to measure if and how frequently the platform is not able to provide adequate response elements to the telecom operators or if it provides even erroneous elements inducing operators to fail on their decision-making process.

Estimated measurement method: Although this metric could be very interesting to measure, it seems that there is not a deterministic counter to evaluate correct and failure decisions. To this end, the KPI has a subjective qualitative component. It seems that it would be difficult to provide the

conditions for accurately measuring this index within the time framework of the project and the pilots. However, the use of one representative case where the majority (if not all) of the RESISTO security modules would be included or validation per use-case basis would be probable and it will be examined within the next final version of this Deliverable.

Time window and estimated frequency of measurement: As stated above, these features are to be evaluated at the end of the complete validation period on the base of complete trials results.

Baseline and target values: Defining a baseline could be too hard and perhaps useless. On the other hand, the target value seems to vary within a minimal percentage (i.e. < 1%) with respect to total decisions, and this is another reason for making this metric completely challenging.

Challenges, discussion and suggestion for inclusion: Despite the many challenges imposed, this KPI could provide feedback to improve the RESISTO platform i.e. upgrading to higher TRLs or providing information data to improve operators training. Based on the above, this KPIs was **included in the metrics shortlist** and will be re-assessed again in the framework of the next final version of this Deliverable (D3.8) depending on the approach that will be followed.

4.2.9. False Information rate (provided to the operator)

Objective: The aim of this KPI is to measure the amount of erroneous information provided by the platform. In this sense, it is quite similar to the previous one concerning the decision-making failure rate.

Description: The KPI aims to measure if and how frequently the platform provides erroneous elements to the operators inducing them to fail on their decision-making process.

Estimated measurement method: Again, there is no deterministic counter to evaluate correct and failure decisions. Thus, this KPI has a subjective qualitative component too. In this context, the overall approach for its validation would be similar to the previous KPI for the decision-making failure rate.

Time window and estimated frequency of measurement: Similarly, the KPI is meant to be evaluated at the end of the complete validation period on the base of complete trials results.

Baseline and target values: Once more, defining a baseline seems impossible, while the target value would be of a minimal percentage (i.e. < 0.1%) with respect to total decisions.

Challenges, discussion and suggestion for inclusion: This metric could provide an indication of some problematic reports, for example CI modelling mistakes, bugs, and similar cases. Due to the interesting manner of both this and the decision-making failure rate KPI, **the suggestion is twofold:**

- Either not to include this KPI as such in the short list but instead to collect false information events in order to address potential evolution of the RESISTO platform.
- Or to examine both these KPIs (the false information rate – provided to the operator and the decision-making failure rate) in the framework of the next final version of Deliverable D3.8 and to keep the one that is more prone to be measured, providing that adequate data processes can be implemented and nevertheless taking into account all the assumptions discussed herein.

4.3. Metrics related to Network Performance (assessed through the Risk and Resilience Analysis)

Independent metrics or inputs to system functions are needed for the Risk and Resilience Management Tool (see section 3.5). Within the tool they are used to evaluate the network “performance loss” due to disruptive events via network simulation methods in order to identify criticalities. The measurement of these performance functions allows to the retrospective resilience assessment. In addition, it is also important in two ways:

- First, data of real events can be used to validate the outcome of the tool.
- Second, the online monitoring of the same performance indicators in the short-term loop, as evaluated in the long-term loop, allows to directly link appropriate results from the long-term loop in case of an event.

4.3.1. Network Availability

Objective: The network availability is characterized by its availability rate X, defined as follows: the network is available for the targeted communication in X% of the locations where the network is deployed and X% of the time (see Table 8 below for different levels of availability).

Description: Network availability is the average percentage of time during which the network is performing its intended function. In another definition it can be considered as the reachability between the regional points of presence (POP).

Availability %	Downtime per year	Downtime per month*	Downtime per week
90%	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
98%	7.30 days	14.4 hours	3.36 hours
99%	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes
99.9% (“three nines”)	8.76 hours	43.2 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% (“four nines”)	52.6 minutes	4.32 minutes	1.01 minutes
99.999% (“five nines”)	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% (“six nines”)	31.5 seconds	2.59 seconds	0.605 seconds

*month = 30 days

Operator’s measurement method: In case an operator uses a full mesh of measurement points, where every POP measures the availability to every other POP, the total availability of the service provider’s network can be calculated. This KPI can also be used to help monitor the service level of the network and can be used by the service provider and its customers to determine if they are operating within the terms of their service-level agreement (SLA).

Operator’s Time window and estimated frequency of measurement: The network availability is measured by the operators on a 24/7 basis.

Operator's Baseline and target values: Similarly, the usual baseline and target values of a telecom operator (depending on the readiness of the service providers' network) is to have a network availability of 99.999% (five nines) in order to adequately tackle all potential disruptions even in major events.

Challenges, discussion and suggestion for inclusion in the RESISTO framework: Although the specific parameter is a very important metric to provide the network's availability and readiness to all kinds of events, its inclusion within the RESISTO Resilience framework as a separate KPI faces certain key difficulties. Assuming that the commercial network of the telecom provider cannot be used directly for obvious reasons, the possibilities that this KPI can be included within the RESISTO framework are the following:

The aim of the RESISTO solution, in order to prove its added value through its introduced Resilience framework and the rest of its sophisticated components (i.e. detection features, risk predictor, correlator engine etc.) would be to provide improvements on existing security systems and tools. Since, network availability (five nines) might be reduced in specific time spots due to i.e. catastrophic disasters especially when redundancy networks have not been appropriately foreseen for all the components and dimensions of a commercial network, it is reasonable to consider that the target value of the network availability, as a KPI of the RESISTO framework, should be increased.

However, in order to measure the improved (increased) network availability as independent metric within the RESISTO solution, the time basis of reference through the available Test Beds of the project should be defined. In this context, the baseline value should first be validated in order to measure the targeted, by RESISTO, value and prove the improved resilience obtained. In this context, the time basis of reference may be too difficult or even proven impossible to be obtained, since very long periods of continuous operation are required for the overall platform. This is rather not feasible due to the limited timeframe of the project and the setting up of the various Use cases and related scenarios. For example, if 5/9s (five nines) are set as the usual baseline then the estimated downtime over a month is around 26 seconds; within this time interval is impossible to consider threat incidents and provide an overall resilience assessment that could lead to improved network availability (i.e. six nines).

To this respect and taking into account the above restrictions, suggestions can be considered, as possible solutions for deriving the desired outcome. A possible suggestion would be to measure the targeted network availability with an indirect manner. For example, to consider various lower levels of network availability as baselines where the downtime could be feasible in Test Bed terms and to measure the (increased) availability of the RESISTO solution each time. Similarly, this to be implemented in specific Use Case scenarios and threat cases (case by case basis) and to consider only specific services for the network availability measurement so that to emulate the metric for a certain well-defined period of time. Then, through mathematical calculation models including interpolation, it would be feasible to uptime the measured results with, of course, a certain degree of probability within acceptable ranges.

Apart from being regarded as independent metrics (through the online monitoring in the short-term loop), the specific KPI could very well act as an input to system functions for the Risk and Resilience Tool (long-term control loop, see section 3.5). This way, predefined baseline values of network availability provided by the RESISTO end users (telecom operators) for specific network services or slices can feed the Risk and Resilience Management Tool in order to contribute to the evaluation of the network performance in the presence of disruptive events allowing for the resilience assessment.

Based on all the above, it is suggested that the network availability is to be included in the present preliminary shortlist, either as independent metric or through the long-term Control Loop provided that all the assumptions discussed in the previous section are met.

4.3.2. Service Utilization

Objective: The metrics representing service utilization are used for service dimensioning and technology migration.

Description: Service Utilization KPI can be composed of other sub-KPIs, the most relevant being *percentage of specific traffic out of total*. The definition of the respective sub-KPI is a ratio between a specific traffic over the total traffic (example: 3G mobile voice from total mobile voice). Other sub-KPIs that are related with the Service Utilisation are the following:

- a) Traffic: this refers to the traffic volume transferred on the network, during the measurement period. This sub-KPI can be assessed for a specific service or technology etc. (voice/data, 2G/3G/4G, fixed/mobile, geographic area etc.) or for the assessment of the overall services.
- b) number of active customers: this refers to the total number of customers that used a specific service at least once during the measurement period
- c) average traffic per customer: in a similar way this refers to the average traffic consumption per active customer over the measurement period.

Although the above four sub-KPIs are already assessed by the telecom organizations, it is evident that in the framework of RESISTO, those sub-KPIs related to customers will be too difficult or even impossible to be evaluated within the project, unless specific inherent knowledge is known independently of the project and its related Test Beds.

Estimated measurement method: As discussed, the sub-KPIs “traffic” and most importantly “the percentage of specific traffic out of total” are feasible to be measured within the framework of the RESISTO project through the Test Beds. The metric is calculated using specific traffic network counters that are continuously measured and reported by network elements and are supported by the project Test Beds. Also, during the Use case testing and piloting, specific services (i.e. voice, data, 2G/3G/4G or fixed / mobile) can be attributed according to the scenarios involved and the Test Beds capabilities.

Time window and estimated frequency of measurement: As it seems the traffic related metrics are not time dependent. Specific counters from the Test Beds can be used to measure continuously these parameters and the metric can be reported on a regular basis i.e. monthly.

Baseline and target values: It has to be noted that, as expected, the values for the above KPIs refer usually to internal and confidential information of the telecom end-users. Thus, it would be rather impossible to obtain the relevant values from the commercial network to be used as baselines to determine the target values. However, as discussed previously, traffic aspects can be emulated through the Test Beds both for determining the baselines values (without the RESISTO platform) and the target values (with the RESISTO platform) for a specific set of services. To this respect, the exact type of services and the traffic baseline values will be extracted through preliminary experiments with the Test beds during the Use cases in the next project period. Thus, the target values will be presented within the final (next) version on this Deliverable (D3.8).

Challenges, discussion and suggestion for inclusion: The above metrics for the set of services can be regarded as independent metrics (through the online monitoring in the short term loop) and / or as inputs to system functions for the Risk and Resilience Tool (long-term control loop, see section 3.5). This way they contribute to the evaluation of the network performance due to disruptive events allowing for a direct link from the long-term loop in case of an event and thus the resilience

assessment. To this respect, **it is suggested that the service utilisation KPIs are included in the present preliminary shortlist**, either as independent metrics or through the long-term Control Loop.

4.3.3. Service capacity / Inventory

Objective: The metric under service capacity is used for service dimensioning and network elements inventory.

Description: This metric refers to the number of Similar Network elements, used for a specific service; as examples could be seen the shared sites, 4Gcells, Backbone routers and / or security equipment. The metric is similar to the Service Utilization (traffic sub-KPIs) discussed previously.

Estimated measurement method: This KPI is usually indicated by network inventory tools counting the number of Similar Network elements used for a specific service. This metric can be measured and assessed through the RESISTO Test Beds in a similar way as described previously for the Service Utilisation KPIs.

Time window and estimated frequency of measurement: Again, this metric can be continuously updated and reported monthly as well.

Baseline and target values: N/A. Similar aspects as for the Service Utilisation KPIs, discussed previously are tackled in this type of metric.

Challenges, discussion and suggestion for inclusion: The above metric is considered as input to system functions for the Risk and Resilience Tool (long-term control loop). Thus, the metric can be used to evaluate the network performance due to disruptive events as these may affect a specific number or set of network elements for a specific service. To this respect, it will act as an input to the Risk and Resilience Management Tool in order to assess the overall resilience of the telecom network through the RESISTO platform, and as such **it is suggested to be included in the preliminary shortlist**.

4.3.4. Network Performance

Objective: Networks performance expressed by Congested Network Elements metric is used in order to assure customer satisfaction, network improvements and revenue loss prevention.

Description: The metric is used to estimate the limitation of access to a specific network element due to congestion, for example the HSDPA congested cells. Congested Network elements is expressed by the ratio between the Number of Congested Network elements related to a specific service over the total Number of Network elements used for the specified service. However, for each situation, a more exact definition of "congested Network element" should be given.

This metric is similar to the Service capacity/Inventory in terms of number of network elements that was described previously. To this respect, the **estimated measurement method** refers to counting the congested network elements during busy hours and regarding the **time window and estimated frequency of measurement** these can be determined using network counters for congestion, continuously measured.

Challenges, discussion and suggestion for inclusion: The above metric is considered as input to system functions for the Risk and Resilience Tool (long-term control loop) and as such **it is suggested to be included in the preliminary shortlist**. To this end, the baseline and target values will be determined upon emulations through the Test Beds during the next period in order to evaluate the network performance due to congested network elements for a specific service. To this respect, it

will act as an input to the Risk and Resilience Management Tool in order to assess the overall resilience of the telecom network through the RESISTO platform.

4.3.5. Service Continuity

Objective: This metric is related to the Drop-call rate. This metric monitoring is performed in order to improve customer satisfaction and network performance.

Description: The Drop-call rate is a very important metric that measures the performance of a telecommunication network, specifically related to the radio coverage, radio interference, network malfunctioning and overload of the different elements of the network for the situations that can be related to a "call". The metric indicates the network quality of service in terms of call completion. Drop-call rate is defined as the ratio of abnormally released (dropped) calls, from user perspective:

Drop Call Rate = Total dropped calls / Total established calls.

The metric is similar to the Service Utilization and service capacity KPIs discussed previously.

Estimated measurement method: This KPI can be calculated using specific call related counters that are continuously measured and reported by network elements. Thus, as in the previous similar metrics, it is feasible to be measured within the framework of the RESISTO project through the Test Beds. Also, during the Use case testing and piloting, specific parameters (i.e. radio coverage, interference, network malfunctioning) can be attributed according to the scenarios involved and the Test Beds capabilities.

Time window and estimated frequency of measurement: This KPI can be measured with Call related counters through the Test Beds and can be continuously assessed and monthly reported.

Baseline and target values: It has to be noted that, as expected, the values for the Drop Call rate refer usually to internal and confidential information of the telecom end-users. However, in a similar way with the previous metrics, drop call aspects can be emulated through the Test Beds for determining the baselines and the target values. To this respect, the exact types will be extracted through preliminary experiments with the Test beds during the Use cases in the next project period.

Challenges, discussion and suggestion for inclusion: Again, this metric is considered as input to system functions for the Risk and Resilience Tool (long-term control loop). Thus, it can be used to evaluate the network performance due to disruptive events as these may affect the user perspective. To this respect, it will act as an input to the Risk and Resilience Management Tool in order to assess the overall resilience of the telecom network through the RESISTO platform, and as such **it is suggested to be included in the preliminary shortlist.**

4.3.6. Service Availability

Objective: As service availability is denoted the characteristic of a service to be available, in a state to perform a required (by the user) function at a given instant of time, or at any instant of time within a time interval, assuming that the external resources, if required, are correctly provided. It very important for the network performance in order to assure customer satisfaction and provide network improvements.

Description: This metric measures end to end service availability or unavailability in terms of capacity to provide the service. Such a ratio can be evaluated (for a service or technology) starting from the

time during which the service was not available for (some) customers, during the measurement period.

If the specified service relies on several similar elements, the ratio should take into account all these elements by using a pondered value.

The Service Availability is a very general term and under its “umbrella” quite many network performance KPIs are often included in a holistic manner. To this respect, depending on the service or technology incorporated, a list of sub-metrics (sub-KPIs) can be defined. Indicative examples are given below.

As general customer related sub-metrics used by the telecom providers the following are given:

- **Call Setup Success Rate:** it refers to the percentage of established calls/sessions over the requested ones, for a service or technology (voice/data, 2G/3G/4G, fixed/mobile, geographic area etc.) or overall, for the situations that can be related to a "call".
- **Service Availability/ Unavailability (in terms of capacity):** The meter end to end service availability or unavailability in terms of capacity to provide the service. Such a ratio can be evaluated (for a service, technology, etc) starting from the time during which the service was not available for (some) customers, during the measurement period. If the specified service relies on several similar elements, the ratio should take into account all these elements by using a ponderated value.
- **Customer Service Calls Ratio:** The ratio between the Number of calls to the Customer Service related to a specific service and the total Number of customers that use the specified service.

For specific service or technology, more specific metrics are defined per telecom end user. Indicatively, for Video Streaming service availability, the corresponding KPIs are listed below:

- **Retainability:** it is defined as the E-UTRAN Radio Access Bearer (E-RAB) release/loss rate during the total usage of the E-RAB.
- **Quality of service:** It is the most important KPI for Video Streaming service. It is defined as the ability and immediacy of the end user to understand the service requested (eg the video content and/or service audio). It is measured during the Active Session service.
- **Delay:** it is defined as the total time takes from a packet to travel from source to destination.
- **Jitter:** it is defined as the delay variation.
- **Packet Loss Rate:** it is defined as the number of packets that are successful received, or not, at the destination
- **Utilization:** it is defined for the EPC side like the EPC bearer utilization
- **Connect Time:** it is defined as the service time necessary to its use by the end user. It represents the time perceived before the service becomes active. It must be measured during the Setup Session service, in which it is significant to measure and represent the network Attach Phase.
- **Response Time:** defines how fast the system is able to respond to an internal or external stimulus. In the **Video Streaming service**, it can be interpreted as the system speed in responding to repeat requests or rewind request of the entire or video parts. It is measured during the Active Session service. It depends on Jitter, delay and retainability.
- **Mobility:** it is defined as the mobility success rate in terms of handover performance of the service (for mobile networks).

And for VoLTE (voice over LTE):

- **E-UTRAN Cell Availability³⁵**: it that shows Availability of E-UTRAN Cell.
- **EPS Attach Setup Success Rate**: it is calculated as the ratio of the number of successfully performed EPS attach procedures to the number of attempted EPS attach procedures for EPC network, and it is used to evaluate accessibility provided by EPS and network performance. It refers to the Attach Phase during the Session Setup
- **Handover Success Rate³⁶**: it has many types of indicators such as: E-UTRAN Mobility KPI, Tracking Area, Update Success Rate KPI, Outgoing Intra-System Hard Handover Success Rate.
- Each one of these metrics measures performances related to Handover procedures during VoLTE Setup and Session Active.
- **Speech Quality**: is a subjective evaluation made by the user about the end-to-end performances of a VoLTE session. It is influenced by network load conditions, interactions between network elements, environmental scenario in which user operates, and also by end user behaviour and psychological conditions.

As it seems the above metrics can vary a lot both in number and in type depending on the service or technology under assessment.

Estimated measurement method: This kind of metrics is measured using incident tickets or availability counters. However, it is evident that it could not be possible to use and include all the above metrics for all the relevant kind of services under the holistic Service Availability. To this respect, a selection is to be made in order to incorporate representative cases for the network performance functions depending on the capabilities and specific preliminary experiments that will be held through the Test Beds. Based on that the measurement methodology will be the same for all the metrics described under this Section.

Time window and estimated frequency of measurement: These metrics can also be continuously assessed and monthly reported, as for the other metrics of this Section.

Baseline and target values: The availability metrics are usually established by each National Authorities for Management and Regulation in Communications. To this respect, the relevant values will be followed for each selected metric, depending on the capabilities of the Test Beds and the final values will be presented in the final (next) version on this Deliverable (D3.8).

Challenges, discussion and suggestion for inclusion: The above metrics **are considered to be included in the preliminary shortlist** as input to system functions for the Risk and Resilience Tool (long-term control loop) through the assumptions and restrictions discussed already above. To this respect, a selected set it will act as input to the Risk and Resilience Management Tool in order to assess the overall resilience of the telecom network through the RESISTO platform.

³⁵ 3GPP TS 32.450 version 8.0.0 Release 8 “Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Key Performance Indicators (KPI) for Evolved Universal Terrestrial Radio Access Network (E-UTRAN): Definitions

³⁶ 3GPP TS 32.455 version 10.0.0 Release 10 “LTE; Telecommunication management; Key Performance Indicators (KPI) for the Evolved Packet Core (EPC)

4.3.7. Service Coverage

Objective: The Service Coverage metric is used in order to improve customer satisfaction and to increase the customer base.

Description: This metric refers to the ratio between the covered zone and the maximum possible in terms of geographic, population or service.

For example, the geographic service coverage is expressed by the ratio between: Coverage for a specific technology or conditions (Km²) over the Total Country Surface (Km²).

Estimated measurement method: The service coverage is determined using a specific GIS coverage tool. The coverage for some services is established also by each National Authority for Management and Regulation in Communications. It is clear that this metric cannot be used by the RESISTO project Test beds and Use Cases as such. To this respect, it is estimated that only through the use of predefined values obtained by the telecom end users as indicative examples, the specific metric will be incorporated mostly within the Risk and Resilience Management tool (long-term Control Loop). To this respect, other parameters such as **time window and frequency of measurement or baseline and target values** are pointless to be defined within the KPIs framework of the RESISTO project.

Challenges, discussion and suggestion for inclusion: Due to the above limitations the coverage metric can **only be considered as input to system functions for the Risk and Resilience Tool** (long-term control loop) through the assumptions and restrictions discussed already above. To this respect, selected predefined values will act as input to the Risk and Resilience Management Tool in order to assess the overall resilience of the telecom network through the RESISTO platform.

4.3.8. Service Speed

Objective: The service speed metric is related to the customer satisfaction, network improvements and revenue loss prevention.

Description: The metric is expressed as the average user throughput (speed), only for services related to speed (data services). To this respect is quite similar in process to the Service Coverage metric discussed previously.

Estimated measurement method: This metric is usually measured by the average time needed to download specific web pages.

Challenges, discussion and suggestion for inclusion: Similarly to the service coverage, it is clear that this metric cannot be used by the RESISTO project Test beds and Use Cases as such since it cannot directly prove the added value of the RESISTO platform in terms of resilience and security.

To this respect, it is estimated that the service speed metric **can only be considered as input to system functions for the Risk and Resilience Tool** (long-term control loop). To this respect, indicative examples of baseline values as average throughput will be inserted and assessed through the Test Beds in order to provide adequate input for the extraction of criticalities and retaining resilience through the risk and resilience tool. The examples will be representative per service case in order to check if the average throughput is sustained so that the long-term control loop to provide mitigation and response suggestions.

4.4. General KPIs of the RESISTO platform

In this Section, certain general metrics and KPIs for the RESISTO solution are identified, which are related with the integration and piloting process and the security costs; the latter metric seems to be accounted for by the majority of the security consultants. However, these metrics should be tailored to the RESISTO solution being the outcome of an Innovation Action project.

4.4.1. *Number of validated security modules integrated within RESISTO platform*

Objective: this metric indicates the number of security modules that have been integrated within the current implementation of the RESISTO platform.

Description: To be able to handle a wide range of physical, cyber, and cyber-physical threats, the RESISTO platform integrates different security modules (e.g. the Airborne threat detection module, the holistic audio-video analytics module, blockchain-based network threats detection module, the correlator engine and risk predictor, the integrated Risk and Resilience Management Tool etc.). Those modules concurrently improve risk control and resilience by supporting the RESISTO functionalities. As already noted, the overall RESISTO platform provides a solution to be regarded as complementary to the existing security systems of the telecom operators, and so to enhance their resilience and protection capabilities. Thus, greater overall security is associated with a greater value of this KPI.

Estimated measurement method: for this metric, the expected measurement method is counting the security modules added and implemented by the RESISTO solution. However, in order these modules to be included in this metric, their validation is required on the field in order to prove their reliability and their contribution to the overall solution. In other words, this validation will be accomplished through the piloting tests within the 3 main macro-scenarios foreseen and the respective Use Cases which is among the main objectives of the RESISTO project. The focus of the project is therefore to be able to appropriately demonstrate and easily measure this metric during the different phases of the project showing their added value; this KPI will be finalized when the platform will be fully deployed.

Time window and estimated frequency of measurement: the metric is a single number and it is not time dependent. Thus, it doesn't involve a time window parameter nor a frequency of measurement.

Baseline and target values: The baseline value of this KPI, accounting for the core functionalities of the RESISTO platform, is the number (which and how many) of the existing security systems in telecom CIs that can be used for reference, comparison or potential interaction with the RESISTO platform; these should be identified during the development and the post development testing phase of the project in order to check the added value of the RESISTO solution upon them. At the same time, the number of the on-field validated (additional) security modules offered by RESISTO, through the piloting tests, will provide the ability to come up with a final estimate of the target value of this KPI. Following the conductance of initial tests and integrated attempts of the overall solution during the next period, the baseline and target values will be presented in the final (next) version on this Deliverable (D3.8).

Challenges, discussion and suggestion for inclusion: It could be useful to account as well for any existing security system in telecom CIs that can be used for the same purpose. Nevertheless, since this is a well-defined and easily measurable KPI, challenges are not foreseen at this point. To this respect, **the number of validated security modules integrated within RESISTO platform is a very important KPI and thus is included in the shortlist.** As discussed previously, it can be measured in the project's framework and it provides a good indication of the overall capabilities of the

RESISTO system. In a potential future commercial version of the system it would probably be one of the key exploitation assets and advantages.

4.4.2. Security Costs

Objective: The Security costs KPI is used to account for the costs incurred by the end user telecom operator for the implementation of security systems. Thus, the security costs for implementing the RESISTO solution should be also taken into account.

Description: As discussed in Chapter 2 of the present report, metrics and KPIs related to the security costs and return on investment figures are usually considered when implementing security systems. The relevant financial metrics are also the main focus of security consultants. In the framework of RESISTO project, this metric was also mentioned at table 1 - B1.1 of the DoW. When assessing this KPI for the present report, it should be taken into account that RESISTO, being an IA research project, encounters development costs and resources in order to come up with an overall integrated solution. In other words, the RESISTO solution is not a commercial product; however, estimations of the relevant economic values can be considered through the project's exploitation and foreseen market penetration plans. Furthermore, it should also be taken into account that RESISTO aims to provide a holistic platform that incorporates all types of threats (physical, cyber and combined cyber-physical) which may be different from the current approaches where physical and cyber threats are tackled with separate respective security systems, even within the same organization.

Estimated measurement method – Baseline and Target values: in order to be able to measure the security or investment costs related with a future commercial implementation of the RESISTO solution, baselines should be set. These are directly related with the security costs invested already by the telecom operators for their existing security systems. However, in almost all cases this is a confidential information which cannot be shared. On the other hand, this KPI cannot be measured or demonstrated during the pilots or during the development and the post development testing phase. Based on that, this metric, seems difficult or even impossible at this point to find an accurate way of measurement since it would be very difficult to define accurate baseline values, which on the other hand should be somehow normalized for fair comparison among the RESISTO end users.

However, good estimates can be approximated through a variety of resources: suggested methods by the end users or through the literature, information available in relevant commercial web sites of relevant consulting companies, market estimation studies and reviews or even benchmarks through published financial results of the telecom operator companies. Moreover, the target value, representing the RESISTO solution impact and added value, could also be assessed through similar methods and through exploitation analysis.

To this respect, the targeted percentage of additional security costs induced by the RESISTO approach could be set in relation to the resilience improvement and impact offered by the RESISTO solution to provide an adequate analysis and demonstration of this KPI. Thus, the corresponding trade-off can be estimated and assessed. Since these aspects lie more on the RESISTO exploitation activities, it is expected that the final values for this metric will be finally determined towards the end of the project.

Time window and estimated frequency of measurement: Not relevant for this metric.

Challenges, discussion and suggestion for inclusion: The main challenges and assumptions for the inclusion of this general metric have already been discussed. To this respect, the security costs metric is still **included in the present preliminary shortlist**, provided that a thorough relevant analysis is made within the project's exploitation framework and adequate information can be derived to set realistic baseline value estimates.

4.5. Short List overview

Following the justification and the discussion concerning each suggested metric held in the previous Sections, the KPIs (preliminary) shortlist is presented herein in a tabular format for facilitation.

Within the following Table only the key elements per KPI along with the main assumptions from the previous discussion are presented, in order to provide a quick overview of the main outcomes of the first version of the present Deliverable. The reader is, therefore, encouraged to seek more detailed justification, especially concerning the inherent challenges, within each KPI description paragraph in the previous Sections.

No	KPI / Metric Title	Justification / measurement method	Suggestion for final list / assumptions and conditions / comments
Protection and Detection Stages			
1.1	Number of detected physical threats	Counting	Generally feasible
1.2	Number of detected cyber threats	Counting	Generally feasible
1.3	Number of detected cyber-physical threats (combined)	Counting	Generally feasible
1.4	Detection probability	percentage indicating the success rate of the system in detecting potential threats	Feasible, different measurements for different types of threats, with at least one representative
1.5	False Alarms Rate (false positives)	total number of false detections over the total number of detections	Feasible, should be measured for each attack detector (each type of threat) Related to Detection Probability
1.6	Number of concurrent (managed) threats	The degree in which RESISTO improves awareness and management of concurrent attacks	Difficult to define values. Different scenarios with concurrent attacks should be run
1.7	Awareness of black swan threats	Rare and surprising events - difficult to measure	Under assumptions: Assess the probability of their occurrence, where applicable
1.8	Time to Detection	time value measure – period through timestamps	Feasible under conditions To be measured on a case by case basis and at least for some specific detection cases.
1.9	Sensitivity of the monitoring system sensors	the number of devices that the sensor monitoring system is able to analyse	Generally feasible

1.10	Effectiveness of the events generated per service or application	measures the total number of events that the security systems are able to detect	Generally feasible
Response and Recovery Stages			
2.1	Performance loss	to measure the time-dependent system performance and to quantify resilience	Feasible Through the Risk and Resilience Management Tool
2.2	Decision-making time (average)	To measure the degree on reducing the decision-making time	Under assumptions: focus on one representative case or on a case by case approach includes subjective parameters
2.3	Mitigation Time (average)	To measure the effectiveness of the RESISTO platform so that performances loss could be recovered in a short time	Under assumptions: focus on one representative case or on a case by case approach
2.4	RESISTO platform Reliability	indicates the success rate in processing the ingested alarms the number of alerts/events sent to the platform should be the same with the number of alerts/events processed	Generally feasible
2.5	Incident Correlation / Propagation Index	measuring the impact of the threat on the network and its propagation likelihood (cyber-physical threats and interconnected CIs)	Generally feasible through the modules incorporated within the RESISTO platform
2.6	Down Time during Incident	duration of the disruption (time period that the system is "down" / not available)	Generally feasible
2.7	Human intervention / automated response	The degree that the platform could enables the reaction and mitigation by automating some of the actions and decreasing the human intervention time	Under assumptions: Difficult to measure, could be made feasible through the Risk and Resilience Management Tool
2.8	Decision-making failure rate	measure if the platform is not able to provide adequate response elements to the telecom operators or if it provides even erroneous elements	Although an interesting metric, it would be very difficult to define baselines and target values might be impossible to assess it
2.9	False Information rate (provided to the operator)	to define if the platform provides erroneous information	Although an interesting metric, it would be impossible to define baselines and target values might be impossible to assess it
Related to Network Performance (will be assessed through the Risk and Resilience Analysis)			

3.1	Network Availability	the average percentage of time during which the network is performing its intended function Difficult to measure	Only under assumptions – also as system function in the Risk and Resilience Analysis
3.2	Service Utilization	composed of other sub-KPIs mainly related to traffic	Generally feasible through the through the online monitoring of the short term loop also as system function in the Risk and Resilience Analysis
3.3	Service capacity / Inventory	number of Similar Network elements, used for a specific service	only as system function in the Risk and Resilience Analysis
3.4	Network Performance	expressed as Congested Network Elements	only as system function in the Risk and Resilience Analysis
3.5	Service Continuity	related to the Drop-call rate	only as system function in the Risk and Resilience Analysis
3.6	Service Availability	Quite many sub-metrics indicating the various services (also per technology)	only as system function in the Risk and Resilience Analysis
3.7	Service Coverage	ratio between the covered zone and the maximum possible in terms of geographic, population or service	only as system function in the Risk and Resilience Analysis
3.8	Service Speed	average user throughput (speed), only for services related to speed (data services)	only as system function in the Risk and Resilience Analysis
General			
4.1	Number of validated security modules integrated within RESISTO platform	Counting of validated modules	feasible
4.2	Security Costs	Under exploitation analysis	Under assumptions

Table 5 – The RESISTO metrics and KPIs Shortlist

5. CONCLUSIONS – DISCUSSION AND NEXT STEPS

The present Deliverable D3.7 is the first version of the report entitled “KPIs, quantities and metrics for cyber-physical risk and resilience of telecom CIs” of Task 3.4.

The present report provides a first assessment of the actual metrics and KPIs that are going to be validated through the RESISTO platform components and the Risk and Resilience Analysis and Management Process in order to prove the RESISTO’s added value to the telecom CIs.

A full justification of each of the suggested metrics is provided along with discussions on inherent challenging aspects. The main outcome of this feasibility study is a (preliminary) shortlist while the assumptions and challenges imposed will be further examined in a more detailed technical manner in the framework of the next final version of this Deliverable (D3.8) due in the next period. The present analysis is based on a thorough related literature review and on defined principles and guidelines tailored to the needs and characteristics of the RESISTO project.

Having set the framework in the present Deliverable D3.7, for defining and measuring the metrics and KPIs, a fully detailed final list in the form of a “database inventory” will be given in the next final version (D3.8) of this Deliverable, which will include:

- Following up of preliminary experiments through the Test Beds that will be conducted to define the exact ways of measurements of the metrics and KPIs, where applicable along with initial sets and analysis of the Risk and Resilience Management process
- Exact definitions of the baselines and the target values for the finally selected KPIs to validate the RESISTO solution along with a complete mapping of the risk and resilience quantities to be inserted as input in the form of system functions within the long-term control loop, after their verification with the Risk and Resilience Analysis Management process
- More detailed definition of the propagation indices to identify the interconnections and potential cascading effects between the telecom infrastructures and other critical ones in the vicinity. This will be made possible through the evolution of the Risk Predictor component in the framework of WP5 which will be in a more mature stage during the next period, enabling the proper measurement of the relevant metrics and KPIs.
- Presentation of the links between the selected KPIs and the use case scenarios that will be validated and tested (following up the scenarios and use cases included within D2.8 due in M15).

so that a complete set and description of the RESISTO KPIs and metrics to be provided in the end.

6. REFERENCES

REFERENCE
RESISTO – Grant Agreement. Project Starting Date: May, 1 st 2018
M. Abedin, et al, "Vulnerability analysis for evaluating quality of protection of security policies", Procds of the 2nd ACM Workshop on Quality of Protection, QoP 2006, Alexandria, VA, USA, October 30, 2006, ISBN 1-59593-553-3, pp 49-52
Abbadi, Z., 2007, 'Security metrics: What can we measure', Open Web Application Security Project (OWASP), Nova Chapter meeting presentation on security metrics, viewed 02 July 2011, from http://www.owasp.org/index.php/ File:Security_metrics-_what_can_we_measure-Zed_Abbadi.pdf
Azuwa, M., Ahmad, R., Sahib, S., & Shamsuddin, S. (2012). Technical security metrics model in compliance with ISO/IEC 27001 standard. International Journal of Cyber-Security and Digital Forensics, 1(4), 280-288
Campbell, G. (2007). Measures and metrics in corporate security: Communicating business value. Framingham, MA: CSO Executive Council
Hayes, B., & Kotwica, K. (2012). Advances and stalemates in security. Security Magazine, 34
Davenport, T., & Harris, J. (2010). Analytics and the bottom line: How organizations build success. Key Learning Summary published by Harvard Business Review.
Garcia, M. L. (2008). The design and evaluation of physical protection systems (2d ed). Boston, MA: Butterworth-Heinemann.
Treece, D. & Freadman, M. (2010). Metrics is not a four-letter word. Security Magazine, 90-94.
Scaglione, B. (2012). Metrics: The evaluation of access control and identification. Security Magazine. Retrieved from http://www.securitymagazine.com/articles/83134-metrics--the-evaluation-ofaccess-control-and-identification .
Sternstein, A. (2013). Taking a flier on big data. Government Executive, 45(3), 24-26.
Campbell, G. (2012). Metrics for success: Security operations control center metrics. Securityinfowatch. Retrieved from http://www.securityinfowatch.com/article/10840065/metricsfor-success-security-operations-control-center-metrics .
Kovacich, G., & Halibozek, E. (2006). Security Metrics Management. Boston, MA: Butterworth-Heinemann.
Rathbun, D. (2009). Gathering security metrics and reaping the rewards [White Paper]. Retrieved from http://www.sans.org/reading_room/whitepapers/leadership/gathering-security-metricsreaping-rewards_33234 .

Chew, E., et al. (2006). Guide for Developing Performance Metrics for Information Security. NIST Special Publication 800-80 Revision 1. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf .
Pironti, J. (2007). Developing metrics for effective information security governance, ISACA 2. Retrieved from http://www.isaca.org/Journal/Past-Issues/2007/Volume-2/Pages/Developing-Metrics-for-Effective-Information-Security-Governance1.aspx .
Collins, B. (2004). Information security program metrics. In Security Business Practices Reference 6, 20-21. Alexandria, VA: ASIS International.
Doinea, M., & Pavel, S. (2010). Security optimization for distributed applications oriented on very large data sets. Informatica Economică, 14(2), 72-85.
Whitman, M. & Mattord, H. (2012). Information security governance for the non-security business executive.
Aleem, A., Wakefield, A., & Button, M. (2013). Addressing the weakest link: Implementing converged security. Security Journal, 26, 236-248.
H. He and J. Yan. 2016. Cyber-physical attacks and defences in the smart grid: a survey. IET Cyber-Phys. Syst.: Theory Appl. 1, 1 (2016), 13–27.
S. Tan, D. De, W. Z. Song, J. Yang, and S. K. Das. 2017. Survey of security advances in smart grid: A data driven approach. IEEE Commun. Surveys Tutor. 19, 1 (Firstquarter 2017), 397–422.
M. Jawurek, F. Kerschbaum, and G. Danezis. 2012. Privacy Technologies for Smart Grids: A Survey of Options. Technical Report MSR-TR-2012-119. Retrieved from http://research.microsoft.com/apps/pubs/default.aspx?id=178055
J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen. 2012. Cyber security and privacy issues in smart grids. IEEE Commun. Surveys Tutor. 14, 4 (2012), 981–997.
N. Komninos, E. Philippou, and A. Pitsillides. 2014. Survey in smart grid and smart home security: Issues, challenges and countermeasures. IEEE Commun. Surveys Tutor. 16, 4 (2014), 1933–1954.
M.H. Cintuglu and O.A. Mohammed and K. Akkaya and A.S. Uluagac. 2017. A survey on smart grid cyber-physical system testbeds. IEEE Commun. Surveys Tutor. 19, 1 (2017), 446–464.
R. Al Tawy and A.M. Youssef. 2016. Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. IEEE Access 4 (2016), 959–979
D. Wang, Z. Wang, Bo. Shen, F. E. Alsaadi, and T. Hayat. 2016. Recent advances on filtering and control for cyber-physical systems under security and resource constraints. J. Franklin Inst. 353, 11 (2016), 2451–2466.
O. Kocabas, T. Soyata, and M. K. Aktas. 2016. Emerging security mechanisms for medical cyber physical systems. IEEE/ACM Trans. Comput. Biol. Bioinformat. 13, 3 (May 2016), 401–416.

M. Rushanan, A. D. Rubin, D. Foo Kune, and C. M. Swanson. 2014. SoK: Security and privacy in implantable medical devices and body area networks. In Proceedings of the IEEE Symposium on Security and Privacy (SP'14). IEEE, 524–539.
H. He, C. Maple, T. Watson, A. Tiwari, J. Mehnen, Y. Jin, and B. Gabrys. 2016. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In Proceedings of the IEEE Congress on Evolutionary Computation (CEC'16). IEEE, 1015–1021.
S. E. Zeltmann, N. Gupta, N. G. Tsoutsos, M. Maniatakos, J. Rajendran, and R. Karri. 2016. Manufacturing and security challenges in 3D printing. J. Miner. Metals Mater. 68, 7 (2016), 1872–1881.
L.J. Wells, J.A. Camelio, C.B. Williams, and J. White. 2014. Cyber-physical security challenges in manufacturing systems. Manufact. Lett. 2, 2 (2014), 74–77. https://doi.org/10.1016/j.mfglet.2014.01.005
Y. Pan, J. White, D.C. Schmidt, A. Elhabashy, L. Sturm, J. Camelio, and C. Williams. 2017. Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems. Int. J. Interact. Multimedia Arti c. Intel. 4, Special Issue on Advances and Applications in the Internet of Things and Cloud Computing
L. F. Cómbita, J. Giraldo, A. A. Cárdenas, and N. Quijano. 2015. Response and reconfiguration of cyber-physical control systems: A survey. In Proceedings of the IEEE 2nd Colombian Conference on Automatic Control (CCAC'15). IEEE, 1–6.
S. Han, M. Xie, H. H. Chen, and Y. Ling. 2014. Intrusion Detection in Cyber-Physical Systems: Techniques and Challenges. IEEE Syst. J. 8, 4 (Dec. 2014), 1052–1062.3
J. How. 2015. Cyberphysical security in networked control systems [about this issue]. IEEE Control Syst. 35, 1 (Feb. 2015), 8–12. Retrieved from DOI: https://doi.org/10.1109/MCS.2014.2364693
Y.Z. Lun, A. D'Innocenzo, I. Malavolta, and M.D. Di Benedetto. 2016. Cyber- physical systems security: A systematic mapping study. arXiv preprint arXiv:1605.09641 (2016).
R. Mitchell and I.-R. Chen. 2014. A survey of intrusion detection techniques for cyber-physical systems. ACM Comput. Surv. 46, 4, Article 55 (Mar. 2014), 29 pages.
Berinato, S. (2005). A few good information security metrics. CSO Online. Retrieved from http://www.csoonline.com/article/220462/a-few-good-information-security-metrics .
McIlravey, B., & Ohlhausen, P. (2012). Metrics and analysis in security management [White Paper]. Retrieved from http://www.ppm2000.com/resources/white_papers.asp .
McIlravey, B., & Ohlhausen, P. (2013). Strengthening intelligence and investigations with incident management software [White Paper]. Retrieved from http://www.ppm2000.com/resources/white_papers.asp .
Huff, A. (2013). Big data I: Exception monitoring. Commercial Carrier Journal. Retrieved from http://www.highbeam.com/doc/1G1-324762775.html .

I. Bernik, K. Prislan, "Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation", PLoS ONE 11(9): e0163050. doi:10.1371/journal., Editor: Houbing Song, West Virginia University, US, September 2016
W. Krag Brotby, Gary Hinson, "PRAGMATIC Security Metrics - Applying Metametrics to Information Security", Book, CRC Press, Taylor & Francis Group, Auerbach Publications, USA, First Published 2013, eBook Published 19 April 2016, DOI https://doi.org/10.1201/b14047
Mo, Kim et al, "Cyber-Physical Security of a Smart Grid Infrastructure", Invited Paper, Proceedings of the IEEE, Volume: 100 , Issue: 1 , Jan. 2012, pp 195-209, DOI: 10.1109/JPROC.2011.2161428
Mayada Omer, Roshanak Nilchiani, and Ali Mostashari, "Measuring the Resilience of the Trans-Oceanic Telecommunication Cable System", IEEE Systems Journal, Vol. 3, No 3, pp 295-303, September 2009.
Pavard, B., et al. 2006, "The Design of Robust Socio-Technical Systems", Paper read at 2nd Symposium on Resilience Engineering, 8-10 November, at Juanles-Pin, France.
Carlson, L., G. Bassett, W. Buehring, M. Collins, S. Folga, B. Haffenden, F. Petit, J. Phillips, D. Verner, and R. Whitfield, 2012, Resilience Theory and Applications, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-12-1, Argonne, IL, USA.
Bruneau, M., and A. Reinhorn. 2007, "Exploring the Concept of Seismic Resilience for Acute Care Facilities", Earthquake Spectra 23 (1):41-62.
D. Reed, K. Kapur, and R. Christie, "Methodology for Assessing the Resilience of Networked Infrastructure," IEEE Systems Journal, vol. 3, pp. 174-180, 2009.
N. Attoh-Okine, A. T. Cooper, and S. A. Mensah, "Formulation of Resilience Index of Urban Infrastructure Using Belief Functions," IEEE Systems Journal, vol. 3, pp. 147-153, June 2009.
D. A. Garbin and J. F. Shortle, "Measuring Resilience in Network-Based Infrastructures," in Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resiliency, J. A. McCarthy, Ed., 2007.
M. Omer, R. Nilchiani, and A. Mostashari, "Measuring the Resilience of the Global Internet Infrastructure System," IEEE Systems Journal, vol. 3, pp. 295-303, September 2009.
S. E. Chang and C. Chamberlain, "Assessing the role of lifeline systems in community disaster resilience," Research Progress and Accomplishments 2003-2004, 2005.
Ali Mostashari, Mayada Omer and Roshanak Nilchiani, "Assessing Resilience in a Regional Road-based Transportation Network" in International Journal of Industrial and Systems Engineering, 2013, Volume 13, Issue 4, pp 389-408, Inderscience on Line, https://doi.org/10.1504/IJISE.2013.052605

M. Shinozuka and S. E. Chang, "Evaluating the Disaster Resilience of Power Networks and Grids," in Modeling Spatial Economic Impacts of Disasters Berlin: SpringerVerlag, 2004, pp. 289-310.
R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, "Breakdown of the internet under intentional attack," Phy Rev Lett, vol. 86, pp. 3682-3685, Apr. 2001.
Smith et al, "Network Resilience: A Systematic approach," Topics in Network and Service Management, IEEE Communications Magazine, pp. 88-97, July 2011, EC FP7 ResumeNet project.
Wailgum, T. (2005). Metrics for corporate and physical security programs. CSO Online. Retrieved from http://www.csoonline.com/article/220023/metrics-for-corporate-and-physical-security-programs .
Mayor, T. (2006). Ideas you can steal from Six Sigma: Tips for improving the effectiveness and efficiency of physical and information security. CSO Online. http://www.csoonline.com/article/221094/ideas-you-can-steal-from-six-sigma
Garigue, R., & Stefaniu, M. (2003). Information security governance reporting. Security Management, 36-40.
Ravenel, J. (2006). Effective operational security metrics. Security Management, 10-17.
Casola, V., Mazzeo, A., Mazzocca, N., & Vittorini, V. (2007). A policy-based methodology for security evaluation: A security metric for public key infrastructures. Journal of Computer Security, 15, 197-229.