

RESISTO:

D3.8_KPIs, QUANTITIES AND METRICS FOR CYBER-PHYSICAL RISK AND RESILIENCE OF TELECOM CIs - final



RESISTO

D3.8 – KPIS, QUANTITIES AND METRICS FOR CYBER-PHYSICAL RISK AND RESILIENCE OF TELECOM CIS - FINAL

Document Manager:	Rodoula Makri	ORG: 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:	EMI - Fraunhofer

Document ID N°:	RESISTO_D3.8_200515_01	Version:	V1.0
Deliverable:	D3.8	Date:	15/05/2020
		Status:	APPROVED

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

Approval Status	
Prepared by:	Rodoula MAKRI (ICCS)
Approved by: (WP Leader)	Mirjam FEHLING-KASCHEK (Fraunhofer)
Approved by: (Coordinator)	Bruno SACCOMANNO (LDO)
Advisory Board Validation (Advisory Board Coordinator)	N.A.
Security Approval (Security Advisory Board Leader)	N.A.

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Rodoula Makri, Panos Karaivazoglou, Apostolos Papafragkakis, Athanasios Panagopoulos, Nikolaos Lyras, Anargyros Roumeliotis, Takis Kelefas	ICCS	Senior Researchers, Electrical Engineers, Telecommunication Experts
Mirjam Fehling-Kaschek, Gael Haab	EMI	Senior Researchers, Risk and Resilience Experts
Ioan Constantin, Octavian Echim, Carmen Patrascu	ORO	Telecommunication experts, 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	26.11.2019	All	All	Table of contents and draft sections
0.7	27.02.2020	All	All	Additions and partners contributions
0.8	06.04.2020	-	3	Corrections to the details of the KPI list
0.8	28.04.2020	All	All	Minor corrections
0.9	05.05.2020	All	All	Ready for review
1.0	15.05.2020	All	All	Final version

COPYRIGHT STATEMENT



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

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

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

PROJECT CONTACT



LEONARDO
Via Puccini 2 – Genova – 16154 – Italy
Tel.: +39 348 6505565
E-Mail: bruno.saccomanno@leonardocompany.com

RESISTO PROJECT – PUBLISHABLE EXTENDED ABSTRACT

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

EXECUTIVE SUMMARY

Deliverable D3.8 is the final version of the report “KPIs, quantities and metrics for cyber-physical risk and resilience of telecom CIs” assigned to Task 3.4. Following the methodology detailed in the first version of the deliverable, i.e. D3.7, it further refines the initial list of KPIs ending up with a short, final list of 9 KPIs, that will be measured and used for the evaluation and validation of the project's results during the field trials scheduled for the last year of the project.

In this document, after a short introduction, a summary of the methodology is presented as a reference and a link to the first deliverable. Then, in section 3, the complete list of the KPIs is presented again and the inclusion or exclusion from the final list is properly justified for each KPI. For those KPIs included in the final list, detailed methods of measurement alongside baseline and target values are presented.

Finally, two tables are included in the document. The first one with all the KPIs of the initial list and the second one with just the 9 KPIs of the final list, summarize the work in this deliverable.

CONTENTS

ABBREVIATIONS	10
1. INTRODUCTION – PURPOSE OF THE DOCUMENT.....	12
2. SUMMARY OF THE METHODOLOGY (LINK TO THE PREVIOUS VERSION).....	13
2.1. Principles and guidelines for the KPI selection- A summary	13
2.1.1. General features	13
2.1.2. Security-specific KPI features.....	14
2.1.3. RESISTO-specific KPI features	14
2.2. Sources and procedures used for selecting indicators and baselines	14
3. SELECTION OF THE FINAL KPI-LIST	15
3.1. Metrics and KPIs related to Detection and Prevention	15
3.1.1. Number of detected physical threats	15
3.1.2. Number of detected cyber threats	16
3.1.3. Number of detected cyber-physical threats (combined)	16
3.1.4. Detection probability	17
3.1.5. False Alarm Rate (false positives)	18
3.1.6. Number of concurrent (managed) threats	18
3.1.7. Awareness of black swan threats	18
3.1.8. Time to Detection (average)	19
3.1.9. Sensitivity of the monitoring system sensors.....	19
3.1.10. Effectiveness of the events generated per service or application	20
3.2. Response, Recovery and Resilience related metrics and KPIs.....	21
3.2.1. Performance loss.....	21
3.2.2. Decision-making time (average)	21
3.2.3. Mitigation Time (average)	22
3.2.4. RESISTO platform Reliability.....	22
3.2.5. Incident Correlation / Propagation Index	23
3.2.6. Downtime	23
3.2.7. Human intervention / automated response.....	24
3.2.8. Decision-making failure rate	24
3.2.9. False Information rate (provided to the operator)	25
3.3. Network performance related metrics.....	26
3.3.1. Network Availability.....	26
3.3.2. Service Utilization	26
3.3.3. Service capacity/inventory	27

3.3.4.	Network Performance	27
3.3.5.	Service Continuity	27
3.3.6.	Service Availability	28
3.3.7.	Service Coverage	28
3.3.8.	Service Speed.....	28
3.4.	General KPIs of the RESISTO platform	30
3.4.1.	Number of validated security modules integrated into the RESISTO platform	30
3.4.2.	Financial Impact.....	30
3.5.	Complete and final KPI list.....	32
4.	CONCLUSIONS – discussion	35
5.	REFERENCES.....	36

LIST OF TABLES

Table 1:	The complete list of RESISTO's KPIs	32
Table 2:	The final KPI list.....	34

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 D3.8 is the final version of the report “KPIs, quantities and metrics for cyber-physical risk and resilience of telecom CIs” assigned to Task 3.4 of WP3.

The WP3 deals mainly with the definition of the “Long Term control Loop” of the RESISTO architecture, and generally the Risk and Resilience Analysis and management process for all types of threats affecting telecommunication CIs. 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). Thus Task 3.4 provides 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 contribute in highlighting the added value of the RESISTO platform as a holistic and integrated approach for enhancing the resilience and security of a telecommunication critical infrastructure against existing security approaches and against a variety of threats and vulnerabilities.

The previous Deliverable D3.7 described the methodology for the definition and adoption of the KPIs alongside an extended list of metrics and their characteristics as a first preliminary shortlist. In other words, this first list would serve as a pool of metrics so that the final list of KPIs to be evaluated and selected depending on and in relation to the suggested Use Case scenarios described within D2.8. Thus, the selected final KPIs would serve as the means for validation of the RESISTO Use Cases.

As defined within the previous D3.7, 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. Moreover, as the RESISTO Use Cases have been formulated in the meantime, the need of having more or less the same list of KPIs for all the Use Cases validation was also evident; since, by this way, a common basis for validating the Use Cases would be created and thus a common basis for proving the RESISTO added value through various implementation and piloting scenarios.

To this respect, based on the principles and the methodology set in D3.7 for the final selection of the RESISTO metrics and KPIs, the present Deliverable D3.8 further refines the initial list of KPIs ending up with a short, final list of 9 KPIs, that will be measured and used for the evaluation and validation of the projects results during the field trials scheduled for the last year of the project. This deliverable describes how the final list is selected by presenting the complete list including the reasons for inclusion or exclusion from the final list, for each KPI in the original list.

In the beginning, a summary of the methodology is presented as a reference and a link to the first deliverable (D3.7). Then, in section 3, the complete list of the KPIs is presented again and the inclusion or exclusion from the final list is properly justified for each KPI. For those KPIs included in the final list, detailed methods of measurement alongside baseline and target values are presented.

Finally, two tables are included in the document. The first one with all the KPIs of the initial list and the second one with just the 9 KPIs of the final list, summarize the work in this deliverable.

2. SUMMARY OF THE METHODOLOGY (LINK TO THE PREVIOUS VERSION)

As mentioned in the introduction, the current deliverable relates to deliverable D3.7. Both deliverables involve the same topic, the definition of KPIs for the RESISTO system. Deliverable D3.7 described the methodology for the definition and adoption of the KPIs alongside an extended list of metrics and their characteristics from which the final selection of KPIs, that would be used and measured within the project's framework. This deliverable describes how the final list was selected by presenting the complete list including the reasons for inclusion or exclusion from the final list, for each KPI in the original list. In this section, a summary of the methodology detailed in deliverable D3.7 is presented as a reference for the reader, that will facilitate the understanding of the selection process.

2.1. Principles and guidelines for the KPI selection- A summary

In order to select meaningful KPIs in the framework of the RESISTO project, a set of guidelines has been defined and followed. The adopted methodology of the selection starts with an important question: how many KPIs should be measured? According to the literature 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 must be measured, but rather empirical suggestions. Measuring **5 to 9 KPIs in total**, was one of the empirical rules that we followed.

Furthermore, meaningful KPIs should possess certain features that need to be defined prior to the selection process. Accepting or rejecting a KPI in the final list, would be based on the presence or absence of these characteristics. These **features** can be classified into **three groups** from the more general to the more specific. Thus, the KPIs should:

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

2.1.1. General features

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

- **Simple:** 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:** This 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 every KPI.
- **Time-based:** 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 should not 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.

2.1.2. Security-specific KPI features

This group contains the common features of security specific KPIs. Security KPIs should be **relevant** to the security function being assessed and **actionable**. Defining proper security KPIs starts with the identification of the most critical security goals or functions of the system. 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.

2.1.3. 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, the characterization of a KPI as a RESISTO-specific KPI depends on the following assumptions for each potential metric:

- a) **The KPI should be of interest for the end users and relevant to the RESISTO solution.** The KPIs should be compliant with the user requirements and should not duplicate existing KPIs that are already measured by the telecom operators.
- b) The KPIs should **enable their measurement and assessment during the piloting activities**, 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 adoption.

2.2. 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. A summary of the different sources is presented here for reference. For more details, see deliverable D3.7.

- **Contractual indicative list:** KPIs included in the proposal
- **End-users' feedback:** KPIs suggested by the end-users of the consortium
- **The Enisa framework:** KPIs described therein

3. SELECTION OF THE FINAL KPI-LIST

The main section of the deliverable describes how the final, short list of the KPIs was produced from the initial complete list of the KPIs, that was initially described in deliverable D3.7. The methodology, which was summarized in the previous section and detailed in D3.7, has driven the process starting from a variety of sources and ending-up with the list of KPIs, that will be measured during the field trials of RESISTO.

In the next sections the complete list is presented again on a KPI-by-KPI basis. This time apart from a short description of each KPI, the focus is mainly on the reasons of including or excluding a KPI from the final list. This is done again for each KPI. Specifically, for the KPIs that are included in the list, a detailed measurement method is described that ensures reliable and consistent measurement that can be performed within the framework of RESISTO's field trials. Moreover, potential risks and challenges are identified, and possible solutions are proposed.

It should be noted, that although the original grouping of the KPIs was preserved, minor modifications have been made in some occasions to the titles of the groups to better reflect the nature of their elements. This have been done also to the names of certain KPIs of the initial complete list, i.e. their name has been modified to better describe their purpose. For example, "Security Costs" has been changed to "Financial Impact" for reasons that become apparent from the description of the metric.

3.1. Metrics and KPIs related to Detection and Prevention

This section involves metrics and KPIs related to the threat detection phase. The RESISTO system possesses detection capabilities, integrating modules developed during the project, especially for physical threats, along with existing detectors as well.

3.1.1. *Number of detected physical threats*

Description: This numerical-valued KPI 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. This KPI is related to the physical threat detection functions of the RESISTO system and effectively measures its detection capabilities.

Inclusion to the final list justification: This KPI **will** be included in the final list, since it can be easily measured and provides a good measure of the detection capabilities of the RESISTO system. Additionally, it provides an indication on the amount of effort put into the development of the modules integrated into the platform.

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.

Baseline and target values: Since there are no similar systems with automated detection capabilities like the RESISTO platform deployed by the end-users in their infrastructure, the baseline value for this KPI will be **0** and the target value will be **>4**. As the RESISTO platform offers a variety of interfaces to integrate potentially any type of physical threat detector, these values correspond to the specific deployment of the platform that will be used during the piloting activities of the project.

Challenges and risks: Measuring this KPI is rather simple and straightforward depending solely on the effort put in the development of the RESISTO platform. There are neither challenges that should be addressed, nor risks that can be foreseen.

3.1.2. Number of detected cyber threats

Description: This numerical-valued KPI 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.

Inclusion to the final list justification: This KPI **will** be included in the final list, since it can be easily measured and provides a good measure of the detection capabilities of the RESISTO system

Measurement method: As with the previous KPI, the measurement method for this KPI is rather straightforward. Measuring this KPI won't impose to the platform any overhead at all.

Baseline and target values: The deployment of the RESISTO platform, that will be used during the pilot activities, will mainly include already existing cyber detectors provided by the consortium's end-users. Nevertheless, there is no similar platform used by the end-users in their infrastructure with automated detection abilities and thus the existing cyber detectors are deployed as standalone systems involving some kind of human intervention. Thus, the baseline value of this KPI will be **0** and the target value for the specific deployment of the RESISTO platform (see previous KPI) will be **>5**.

Challenges and risks: Measuring this KPI is rather simple and straightforward depending solely on the effort put in the development of the RESISTO platform. There are neither challenges that should be addressed, nor risks that can be foreseen.

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

Description: This numerical valued KPI was defined as an indication of how many different types of cyber-physical threats can be detected by the RESISTO platform. 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. In truth, these are complex threats consisting of different cyber and physical threats that occur at specific timings triggered by different conditions and as such they can better described as sequences of events enabling a specific (physical or cyber) threat. For example, a physical intrusion on a building that hosts points of access to a telecom infrastructure (e.g. servers, routers etc.) and the subsequent cyber-attack by installing malicious software, is a typical example of a cyber-physical scenario.

Inclusion to the final list justification: This KPI **will not** be included in the final list. One of the advantages of the RESISTO platform is its ability to correlate events that are connected and thus enhance the detection capabilities of the individual detectors, while simultaneously reducing the false alarms rate. This is done by a rule-based correlation engine that is part of the platform. Each rule of the correlation engine is defined to address a different situation/scenario, that can be a sequence of connected physical and/or cyber events including cyber-physical cases. Thus, the value of this KPI would be directly related to the number of rules defined within the correlation engine, rendering this practically infinite, especially by considering how simple is to define and implement new rules. Although the piloting activities of the project include cyber-physical scenarios, that will demonstrate RESISTO's ability to handle such cases efficiently, measuring such a KPI, will not provide any useful information especially since it practically comes down to counting the correlator's rules.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.1.4. *Detection probability*

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. Since the RESISTO platform integrates different detectors in order to handle a wide range of complex threats, measuring a single detection probability for the whole system seems meaningless, as different types of threats are detected by different modules or even combinations of modules, exhibiting different detection probabilities. A meaningful KPI of this type should be measured for each type of threat that can be detected by the RESISTO system and is included in the use-cases defined for the piloting activities within the project.

Inclusion to the final list justification: This KPI **will** be included in the final list. As the RESISTO system integrates several detectors (physical or cyber), measuring this KPI will provide insight on the detection capabilities of the platform.

Measurement method: In order to measure the detection probability for a specific threat, scenarios involving that threat will be executed for a number of times. The number of successful detections divided by the total number of the scenario executions will be the estimate of the detection probability. Although for a statistically reliable estimate, the proper number of executions depends on the value range of the quantity under measurement, due to time and resource restrictions during the project's pilots, this number may be lower than required.

Baseline and target values: RESISTO platform will not improve the detection probability of the individual detectors, physical or cyber, but rather provide intelligence able to identify and detect complex events that **cannot be** detected by a single detector. A measurement of the detection probability can be performed for each complex event of the piloting activities of the project, following the measurement method described previously. Since complex events are composed of simpler events, that **can be** detected by the platform's detectors, the **baseline** value(s) of the measurement will be the value(s) of the detection probability for each simple threat comprising the complex event, while the **measured** value will be the detection probability of the complex event. The measured values for all complex events of the scenarios will be averaged and an average detection probability of the platform will be derived. The **target** value of the average detection probability of the RESISTO platform will be 90%. Thus, measurements of this KPI will be a good indication of the augmented detection capabilities provided by RESISTO. For example, this KPI for a complex cyber-attack involving a physical breach to gain access to a router and subsequently attacking the infrastructure by installing malicious software on the router, will have baseline values of 85% and 87%, assuming these are the detection probabilities of the physical detector (physical breach) and the cyber detector (malicious software detection) respectively and will contribute to the average detection probability of the platform that will be compared to the **target** value of 90%.

Challenges and risks: As mentioned above, the only risk associated with this specific measurement is whether enough repetitions of the complex events will be performed during the piloting activities. Regardless of how low the number of repetitions is, a measurement of the KPI will be performed and the number of repetitions will be reported as a measure of reliability of the measurement.

3.1.5. False Alarm Rate (false positives)

Description: This KPI, measured as a percentage, corresponds to the number of detections that are caused not by real events, but rather due to detector imperfections over the total number of detections. For example, a false alarm rate of 5% would mean that 5 out of 100 detections have not been caused by real events/threats. This number usually accompanies the detection probability of a detector, since there is usually a trade-off between detection probability and false alarm rate, i.e. the false alarm rate can be decreased to almost zero by significantly lowering the detection probability.

Inclusion to the final list justification: This KPI **will not** be included in the final list. It is known that false alarm rate is a useful metric, which in conjunction with the detection probability, conveys useful information about the detection capabilities of a system. Nevertheless, in order to properly measure it, the under measurement system needs to be observed in operation for a significant amount of time, far longer than the time required to complete the pilots planned for the project. A realistic approach would dictate an uninterrupted operation spanning a period of several months in order to measure properly the ratio. This is because false alarms are events that cannot be “created” artificially, but rather they occur as random events in unpredicted moments.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.1.6. Number of concurrent (managed) threats

Description: This number valued KPI indicates how many different events can the RESISTO platform handle simultaneously. Its aim is to show how the platform could improve the awareness of concurrent physical, cyber, combined threats in order to optimize reaction and mitigation.

Inclusion to the final list justification: This KPI **will not** be included in the final list. Although this could potentially be a useful KPI, to measure it properly, a deployment on an extensive scale would be needed, something that cannot be done during the project’s piloting activities given the time and resource restrictions that apply. This metric is directly connected to the ability of the RESISTO platform to scale and handle increased numbers of event and at least theoretically, has no upper limit.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.1.7. Awareness of black swan threats

Description: Black swan events are large-impact, highly unpredictable and rare events. This KPI measures the system’s awareness of the likelihood of black swan threats occurring and their impact.

Inclusion to the final list justification: This KPI **will not** be included in the final list. By definition, a black swan threat cannot be predicted and/or controlled. This renders any attempt to measure it during the project’s pilots impossible and eventually meaningless.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.1.8. Time to Detection (average)

Description: This metric expresses the duration between the time instant an event of interest happens and the time instant RESISTO issues a detection alert. Since the platform integrates several detection modules based on different technologies that require different times for detection, an average of the measurements will be taken (see measurement method).

Inclusion to the final list justification: This KPI **will be** included in the final list. This is an undoubtedly a useful and well-defined metric, that can be measured within the framework of the piloting activities of the project. Moreover, as a time related quantity, it is critical for the operation of a security system protecting critical infrastructure.

Measurement method: Although, this is a well-defined metric with a rather obvious measurement method, care should be taken to certain details that will ensure its correct and consistent measurement. First, all the subsystems/modules along the processing chain of the platform should be synchronised in a reliable and unified manner. This can be achieved using a time server that will periodically synchronise the modules' individual clocks. Secondly, a time stamp should be assigned to each event, regardless of the source, by the relevant subsystem, e.g. a "time of detection" by the relevant detector, a "time of alert" by the correlator module etc. Finally, a handheld device (e.g. an android smartphone) should be connected to the RESISTO platform, as a special kind of "sensor". Its purpose will be to generate and send to the RESISTO platform a special type of events. These events will correspond and have the same names as events of interest detected by the RESISTO's detectors but will have a "manual" valued instead of "automatic" value in the type of event field. These events will be sent to and processed by the RESISTO platform. The purpose of these special events is to measure the timings of the system, as these events will be created manually by the user of the handheld device, who will observing the piloting activities and will create a manual event the instant a "real-life" event of interest is happening and it is expected to be detected at some point by the RESISTO platform. Comparing the time stamps of the "manual" events with the timestamps of the corresponding detection alerts, will provide the measurements. This procedure will be performed for all types of events defined within the use cases of the piloting activities and different time measurements for different types of detection will be acquired. The final value of this KPI will be the average value of these measurements.

Baseline and target values: Since there are no similar, automated systems like RESISTO already deployed on the telecom providers' infrastructure, no baseline values exist. Additionally, it is rather difficult to define target values since the propagation time from the detector to the platform over the Internet is included in every measurement. Despite that, measuring this metric will provide significant insight into the platform's value and capabilities. The expected target value of this metric will be less than three minutes (**<180 secs**).

Challenges and risks: No real challenges or issues are expected related to measuring this well-defined metric. Nevertheless, the value of this KPI may fluctuate as the unpredictable communication times over the Internet are included in the measurement.

3.1.9. Sensitivity of the monitoring system sensors

Description: This number valued KPI is an indication of the sensitivity of the monitoring system's sensors depending on the minimum signal strength that the sensors are able to detect and therefore, determines the number of detected devices.

Inclusion to the final list justification: This KPI **will not** be included in the final list. This metric applies only to specific sensors integrated into the RESISTO system and although it can help assess the performance of the specific monitoring system, that uses these sensors, it has limited impact to

the overall detection capabilities of the platform. It will not be included in the final KPI list of RESISTO, but measurements of the specific quantity may be performed during the pilot activities to characterize the detection capabilities of the related sensors.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.1.10. Effectiveness of the events generated per service or application

Description: The effectiveness of the events generated per service or application metric measures the total number of events that the security system can detect. This depends on a variety of assumptions: how many events can be handled, how effective are certain technologies at detecting security events and why; how often users or analysts are manually detecting an event, before it is detected by a detection technology.

Inclusion to the final list justification: This KPI **will not be** included in the final list. It is not possible to obtain a reliable, unbiased measurement of this metric considering that during the pilots, the security related events will be produced in a predefined manner in order to demonstrate the RESISTO's capabilities. Modelling and generating random, i.e. "real-life" events and conditions is beyond the scope of the project and would require additional effort and resources that are not available.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.2. Response, Recovery and Resilience related metrics and KPIs

This section covers metrics and KPIs related to the response and recovery phases or are connected to the resilience of the infrastructure.

3.2.1. Performance loss

Description: The aim is 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. This is an overly complicated metric directly connected to various individual metrics that measure specific aspects of the performance.

Inclusion to the final list justification: This KPI **will not** be included in the final list. As this metric is a multi-parametric one, that requires several assumptions for its definition, there is a significant number of definitions of this KPI depending on the performance aspects that will be included. At the same time, it is very tedious if not impossible to find a proper definition including all involved parameters and aspects. Instead more specific KPIs connected to performance will be measured during the piloting activities of the project. These KPIs will be described in the following paragraphs.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

NOTE: A metric with same title, “Performance loss” has been described in several deliverables, including D3.2, as input to the LTCL (Long Term Control Loop). Generally, performance related metrics are required as input and although this specific KPI will not be measured for the above reasons during the field trials, another, more specific, performance related KPI will be used (see Downtime below).

3.2.2. Decision-making time (average)

Description: This metric expresses the duration between the time instant a detection alert is issued and the time instant RESISTO produces a decision for potential actions in response to the event. Since the platform can handle several types of events with the decision process following different paths, an average of the measurements will be taken (see measurement method).

Inclusion to the final list justification: This KPI **will be** included in the final list. This is an undoubtedly a useful and well-defined metric, that can be measured within the framework of the piloting activities of the project. Moreover, as a time related quantity, it is critical for the operation of a security system protecting critical infrastructure.

Measurement method: As with the “Time to detection” KPI (3.1.8), care should be taken to certain details that will ensure its correct and consistent measurement. First, all the involved subsystems/modules should be synchronised in a reliable and unified manner. Secondly, a time stamp should be assigned to the alert and the decision, by the relevant subsystem. Comparing the timestamp of the alert with the timestamp of the corresponding decision, the measurement for each case will be obtained. This procedure will be performed for all types of alerts that invoke decisions defined within the use cases of the piloting activities and different time measurements for different types of alerts will be acquired. The final value of this KPI will be the average value of these measurements.

Baseline and target values: Since there are no similar, automated decision-making systems like RESISTO, already deployed on the telecom providers’ infrastructure, no baseline values exist.

Fortunately, compared to the “*Time to detection*” KPI (3.1.8), this metric involves measurements without unpredictable components as the communication between the relevant modules happens internally at the core of the platform. The target value of this metric will be less than two minutes (<120 secs).

Challenges and risks: No real challenges or issues are expected related to measuring this well-defined metric.

3.2.3. *Mitigation Time (average)*

Description: This metric expresses the duration between the time instant a response decision is produced and the time instant RESISTO suggests a mitigation action related to the decision. Since the platform can suggest several mitigation measures, an average of the measurements will be taken (see measurement method).

Inclusion to the final list justification: This KPI **will be** included in the final list. This is an undoubtedly a useful and well-defined metric, that can be measured within the framework of the piloting activities of the project. Moreover, as a time related quantity, it is critical for the operation of a security system protecting critical infrastructure.

Measurement method: As with the “*Decision-making time*” KPI (3.2.2), care should be taken to certain details that will ensure its correct and consistent measurement. First, all the involved subsystems/modules should be synchronised in a reliable and unified manner. Secondly, a time stamp should be assigned to the decision and the mitigation suggestion, by the relevant subsystem. Comparing the timestamp of the decision with the timestamp of the corresponding mitigation action, the measurement for each case will be obtained. This procedure will be performed for all types of decisions that lead to mitigation actions defined within the use cases of the piloting activities and different time measurements for different types of decisions will be acquired. The final value of this KPI will be the average value of these measurements.

Baseline and target values: Since there are no similar, automated decision-making systems like RESISTO, already deployed on the telecom providers’ infrastructure, no baseline values exist. Fortunately, compared to the “*Time to detection*” KPI (3.1.8), this metric involves measurements without unpredictable components as the communication between the relevant modules happens internally at the core of the platform. The target value of this metric will be less than one minute (<60 secs).

Challenges and risks: No real challenges or issues are expected related to measuring this well-defined metric.

3.2.4. *RESISTO platform Reliability*

Description: The 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.

Inclusion to the final list justification: This KPI **will not** be included in the final list. Measuring it within the framework of the piloting activities of the project, a biased value will be obtained, since the correlation rules are specially designed for the use-cases. A reliable estimate would be obtained if random conditions were applied and measurements were performed spanning several months of continuous operation. Modelling these random conditions and performing the measurements is not feasible during the pilots considering their resource and timing restrictions.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.2.5. *Incident Correlation / Propagation Index*

Description: This metric is an indication of the correlation between separate events. It is related to the combined cyber-physical complex events occurrence and attempts to measure the dependency between them. This KPI is related to the impact of the threats on the network, their propagation dynamics and could be useful for driving the system's response.

Inclusion to the final list justification: This KPI **will not** be included in the final list. This is a very difficult KPI to define and measure. Even if an accurate propagation and correlation model(s) could be defined, deriving a single, measurable KPI would be rather impossible. A potential strategy would be to define one KPI of the specific type, for each combined event. Following this approach, a significant overhead would be imposed on the piloting activities, considering the limited resources and time available, while at the same time subjectivity would be introduced into the definition of the KPI, which is highly undesirable.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.2.6. *Downtime*

Description: This metric indicates the time duration of the disruption in the availability of any system component affected by an incident. Formally, a period of downtime starts at the moment of the last registered activity of the affected component (this can be identified by time-stamped logs, for example) and ends at the moment of the next registered activity of the affected component. Unfortunately, this definition is not very useful within the framework of RESISTO, as the measurements will be performed during the field trials on the end-users' testbeds. Since the events of interest will be generated artificially and will be under the system's control for the whole duration of the trials, measuring the downtime of single components or even the overall infrastructure (testbed), would provide false, biased values. Instead the downtime will be defined and measured normally on the whole testbed and it will be compared with the expected downtime caused by the same event of interest under the assumption that **the RESISTO system is not** deployed on the testbed. As it will be explained later on (see 3.4.2), this will enable the connection with the *Financial Impact* metric. Moreover, this KPI will be used as input to the LTCL since it is a performance related metric. Although in several prior deliverables, including D3.2, a "Performance Loss" metric was described as input, for the reasons explained in 3.2.1, such a general KPI will not be measured during the field trials.

Inclusion to the final list justification: This KPI **will be** included in the final list. Although special care will be taken in order to properly measure this metric (see description and method of measurement), it will enable the estimation of the financial impact of the RESISTO system and as such, it is a very useful and significant KPI that will be measured during the pilot activities of the project.

Measurement method: Following the ideas presented in the description, the effect of "downtime" will be simulated during the field trials based on the experience of past real events provided by the end-users. This is necessary since the field trials will be performed on the testbeds and not on the actual

telecom network of the telecom providers. The modelling of the downtime effect will be performed separately for each scenario using information from the end-users that will be integrated into the execution of the scenarios. The details will be decided and finalised during the field trials and the details will be included in the description of the piloting activities. The measurement of the downtime will then be straightforward. Moreover, for each measurement, another value for the case that no RESISTO system is deployed on the testbed, will be extrapolated. The difference of the two values will be an indication on the reduction of the downtime caused by various events due to the usage of the RESISTO solution. It is obvious from the assumptions taken, that averaging the derived values would be meaningless and thus one value for each case will be provided.

Baseline and target values: The required assumptions for the measurements of this metric that was described above render the definition of any baseline or target value for the metric, impossible. Thus, the values will be revealed during the pilots, when the details of the measurements will be finalised on a case-by-case basis.

Challenges and risks: Apart from the aspects discussed in the previous paragraphs, no other major challenges or risks are expected in relation to the measurement of this metric.

3.2.7. Human intervention / automated response

Description: This metric will measure the level of human intervention involved in the response and mitigation phases of the RESISTO platform operation or alternatively the level of automation of the specific phases. The objective is to indicate how the RESISTO platform enables the automation of these phases and decreases the human involvement.

Inclusion to the final list justification: This KPI **will not** be included in the final list. Under real-life conditions the security protocols of the telecom providers forbid the use of fully automated procedures for the response and mitigation phases. A fully automated platform like RESISTO can only provide suggestions to facilitate the decision-making process, which is performed by professionally trained humans. Thus, there is always some kind of human intervention in the operation cycle, ensuring that the critical decisions are man-made. Moreover since there are no complete security systems, similar to RESISTO, that cover all the phases of the security and resilience enhancement procedure, already deployed and operating on the end-users telecom infrastructure, it would be impossible to define meaningful baseline values for the specific KPI.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.2.8. Decision-making failure rate

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 whether it provides erroneous elements driving the operator's decision-making process to failure. This would identify any "side effects" caused using the platform and provide insight on how this could be avoided.

Inclusion to the final list justification: This KPI **will not** be included in the final list. There is an inherent subjective element in the definition of this metric. Even though it is easy to identify failure, it is exceedingly difficult to determine the cause of this failure in many cases, which renders the actual measurement of this metric rather infeasible. Moreover, it would be impossible to define meaningful baseline values for this KPI as this baseline values would depend on the actual failure cases covered by a specific system. Thus, a fair comparison between different systems would not be possible.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.2.9. False Information rate (provided to the operator)

Description: Similar to the previous KPI, this metric measures the amount of erroneous information provided by the platform. Since there is no universally acceptable way to rate such a quantity, a consistent method for defining it, should be considered first.

Inclusion to the final list justification: This KPI **will not** be included in the final list. There are several reasons for not including this metric in the final list. The argumentation follows the same path with the previous KPI, focusing on the inherent subjectivity, the unclear definition of rating and the inability to obtain baseline values (see 3.2.8).

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.3. Network performance related metrics

Network performance related metrics are usually adopted by the telecom providers to assess the business aspect of their operations and in many cases are connected to the Service Level Agreements (SLAs) with their customers. As such they play an especially important role in the operations of telecom companies, but at the same time, the details of their usage are often protected by business secrecy.

3.3.1. Network 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). The network availability is expressed as a 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. For example, a 99.999% availability, a.k.a. five nines, implies a downtime of 5.26 minutes per year, including the downtime due to maintenance activities.

Inclusion to the final list justification: This KPI **will not** be included in the final list. The main reason behind this decision is that even though it is rather straightforward to define a measurement method for this metric, in order to obtain a reliable measurement, system operation over extended (at least a couple of months long) periods of time, is required. This is not feasible within the time restricted framework of the piloting activities of the project. Moreover, since only testbeds and not the real infrastructure will be used for the piloting activities, measuring this metric properly would require an initial estimation of the baseline values, which may be different from the ones that correspond to the real infrastructure. Finally, there is no guarantee whatsoever, that an unbiased measurement could be performed.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.3.2. Service Utilization

Description: This is in fact a complex metric comprised of several other simpler metrics. A common practice is to measure percentages of specific traffic over total traffic, e.g. 3G mobile voice over total mobile voice traffic, etc. Other examples are number of active customers and average traffic per customer.

Inclusion to the final list justification: This KPI **will not** be included in the final list. The main reason for the exclusion from the final list, is the fact that the piloting activities will be carried on testbeds and not the actual networks of the end-users. In order to properly measure such a metric, even under simplifying assumptions, an extensive simulation framework would have been developed, that would simulate “real-life” traffic on the piloting testbed, something that is not feasible and completely out of scope for the project. Even if such a framework was available, it would be extremely difficult to define a proper unbiased measurement method for this metric and even more difficult to obtain baseline and target values.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.3.3. *Service capacity/inventory*

Description: This metric refers to the number of similar network elements, used for a specific service; examples include *shared sites, 4G cells, backbone routers and security equipment*. The metric is similar to the service utilization KPI, discussed previously.

Inclusion to the final list justification: This KPI **will not** be included in the final list. Although related to the previous KPI, it involves a different aspect of the service concept. By definition, this is a metric that will not be affected by the use of a security system, such as RESISTO and thus measuring it, will not provide any information or even insight on the effect of the involvement of the RESISTO system in the operational activities of a telecom provider.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.3.4. *Network Performance*

Description: This is a very general metric that can be addressed from several different angles. For example, it can be expressed as the ratio of the number of congested network elements related to a specific service to the total number of network elements used by the service. Even with this definition, the term “congested” must be properly and uniquely defined.

Inclusion to the final list justification: This KPI **will not** be included in the final list. Even if the issue of several different definitions of this metric is overcome, the fact that testbeds and not the actual telecom network will be used, renders the measurement of such a metric unreliable and the definition of proper baseline values impossible. Too many assumptions should be made with unpredicted effects on the actual information carried by the measurement. Instead of having such a general and “vague” metric in the final list, more specific performance related metrics have been chosen. No single metric can cover all the performance aspects of a telecom provider’s network, but a properly chosen metric can provide useful information on the actual performance.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.3.5. *Service Continuity*

Description: This metric indicates the network quality of service in terms of call completion. It can be expressed as the drop-call rate, which is defined as the ratio of abnormally released (dropped) calls, from user perspective: $\text{Drop Call Rate} = \frac{\text{Total dropped calls}}{\text{Total established calls}}$. The drop-call rate is a very important metric, that measures the performance of a telecommunication network. It depends on the radio coverage, radio interference, network malfunctioning and overload of the different elements of the network in situations related to a “call”.

Inclusion to the final list justification: This KPI **will not** be included in the final list. In order to properly measure such a metric on a testbed as the ones that will be used during the pilots, conditions related to the abnormal termination of calls must be reproduced following a realistic, random model, even at a simulation level. Such a task would require time and resources not available within the project’s framework.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.3.6. *Service Availability*

Description: Service availability is a service's capacity 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 is an especially important performance metric with significant impact on customer satisfaction. Service Availability is a very general term and cover under its "umbrella" quite many, more specific KPIs. These include *Call Setup Success Rate*, *Customer Service Calls Ration* or even more service specific metrics, as *Connect Time*, *Response Time*, *Retainability etc.*

Inclusion to the final list justification: This KPI **will not** be included in the final list. Even if an individual KPI from the ones described above was chosen as an indication of service availability, measuring it would involve the reproduction of the appropriate "real-life", random conditions that usually apply in practice. Such a task, even at a simulation level, would require time and resources not available within the project's framework. Moreover, defining proper baseline values would still be a tedious task with uncertain results.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.3.7. *Service Coverage*

Description: This metric is expressed as the ratio of the size of the covered zone to the maximum possible size in terms of geographic region, population or service. For example, the geographic service coverage is expressed by the ratio of the coverage region for a specific technology or conditions in Km² to the total country surface (in Km²). The service coverage is usually determined using GIS coverage tools and for some services, it is regulated by the corresponding national authority for management and regulation in communications.

Inclusion to the final list justification: This KPI **will not** be included in the final list. By its definition this metric is impossible to measure within the framework of the project.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.3.8. *Service Speed*

Description: The metric is expressed as the average user throughput, for services related to speed (data services). This metric has a significant impact on the customer satisfaction, and it is a driving indicator for revenue loss prevention

Inclusion to the final list justification: This KPI **will not** be included in the final list. Even though a system as RESISTO may affect such a metric, there are more suitable metrics that can be measured in order to assess the impact of security on a telecom network. Measuring it, will not add any new

information or provide any additional insight on the effects of the RESISTO system. If a useful and reliable measurement of such a KPI was to be made, a time window of several months would be required, since this should involve unbiased averaging.

Measurement method: Non-applicable

Baseline and target values: Non-applicable

Challenges and risks: Non-applicable

3.4. General KPIs of the RESISTO platform

In this section, general metrics and KPIs, that do not fall into any of the above categories, are described.

3.4.1. *Number of validated security modules integrated into the RESISTO platform*

Description: This metric expresses the number of security modules that have been integrated into the current implementation of the RESISTO platform. The value of this KPI is a good indication on the effort put into the development of the platform and provides a general idea on the number of diverse technologies integrated into the proposed solution.

Inclusion to the final list justification: This KPI **will** be included in the final list. This metric corresponds to the overall RESISTO system and its measurement is not connected to the piloting activities of the project.

Measurement method: Measuring this KPI is straightforward and does not require a specific method. Moreover, this could be performed independently from the piloting activities, that will be performed within the project's framework.

Baseline and target values: This KPI is related to the RESISTO system specifically or to similar systems that integrate different technologies and address security and resilience in a holistic manner. Since such systems are not currently deployed on the providers' infrastructure, there are no baseline values for this KPI. Nevertheless, a target value of **8** is the expected value of this metric.

Challenges and risks: No real challenges or issues are expected related to measuring this well-defined metric.

3.4.2. *Financial Impact*

Description: Although initially the name of this KPI was "Security Costs", a more realistic approach in addressing the financial aspect of the RESISTO solution, has led to looking "the problem" from a different angle. The only realistic and feasible way to connect costs with the use of an automated security system, like RESISTO, was to assess its impact on the reduction of the financial losses that security events could cause on the business of telecom operators. Based on the literature and the feedback from the end-user partners of the consortium, the only way to achieve this was by connecting it with a performance related KPI, i.e. downtime (see Measurement Method).

Inclusion to the final list justification: This KPI **will** be included in the final list. Measuring any financial related KPI is overly complicated and would involve the development of complex financial models under certain assumptions, based on numerous parameters with varying levels of accuracy. Still, including at least one financial KPI in the final list would be useful and valuable for the end-users and could provide valuable input for the exploitation activities of the project.

Measurement method: This is not a common KPI in the sense that there will be no direct measurement of this metric. Instead, the reduction of the downtime due to the use of the RESISTO solution will be measured as described in 3.2.6. Then this reduction (in minutes) will be multiplied by the average financial cost per minute of downtime, which will provide the value of this metric. As for the downtime measurement, this will be done on a case-by-case basis. A thorough literature research and the feedback from the end-users of the consortium, that was based on past real-life events, has revealed the average financial cost per minute of downtime for a company to range from \$2.3K to

\$9K¹. A value in this range will be used for the financial impact calculations following the downtime measurements during the field trials of the project.

Baseline and Target values: As this is a special KPI directly connected to the “*downtime*” KPI, no baseline or target values will be provided. This is because it will not be measured as a normal KPI, but it will be used to estimate, the impact of the RESISTO system on the financial losses caused by events that can be handled by the platform. For example, for a specific cyber-attack and under certain assumptions, an average reduction on the financial losses caused by the attack, due to the use of the RESISTO system, will be calculated.

Challenges and risks: Considering the peculiarity of this metric, the required assumptions and its connection to the “*downtime*” metric, an approximation of the actual value should be expected.

¹ <https://www.atlassian.com/incident-management/kpis/cost-of-downtime>

3.5. Complete and final KPI list

Following the discussion concerning each suggested metric of the previous sections, the KPIs complete list is presented herein in a tabular format for convenience.

Finally, a smaller table summarizes the final list, i.e. the KPIs that will be measured during the piloting activities that will be performed within the project's framework.

Table 1: The complete list of RESISTO's KPIs

No	KPI / Metric Title	Value	Inclusion in the final list
Detection and Prevention			
1.1	Number of detected physical threats	Number	YES
1.2	Number of detected cyber threats	Number	YES
1.3	Number of detected cyber-physical threats (combined)	Number	NO
1.4	Detection probability	Percentage	YES
1.5	False Alarms Rate (false positives)	Percentage	NO
1.6	Number of concurrent (managed) threats	Number	NO
1.7	Awareness of black swan threats	Binary	NO
1.8	Time to Detection (average)	Number (in seconds)	YES
1.9	Sensitivity of the monitoring system sensors	Percentage	NO
1.10	Effectiveness of the events generated per service or application	Number	NO
Response, Recovery and Resilience			

2.1	Performance loss	Percentage	NO
2.2	Decision-making time (average)	Number (in seconds)	YES
2.3	Mitigation Time (average)	Number (in seconds)	YES
2.4	RESISTO platform Reliability	Percentage	NO
2.5	Incident Correlation / Propagation Index	Number	NO
2.6	Downtime	Number (in seconds)	YES
2.7	Human intervention / automated response	Binary	NO
2.8	Decision-making failure rate	Percentage	NO
2.9	False Information rate (provided to the operator)	Percentage	NO
Network Performance			
3.1	Network Availability	Percentage	NO
3.2	Service Utilization	Percentage	NO
3.3	Service capacity / Inventory	Number	NO
3.4	Network Performance	Number	NO
3.5	Service Continuity	Percentage	NO
3.6	Service Availability	Percentage	NO
3.7	Service Coverage	Percentage	NO
3.8	Service Speed	Number	NO
General			
4.1	Number of validated security modules integrated into the RESISTO platform	Number	YES
4.2	Financial Impact	Number	YES

Table 2: The final KPI list

#	KPI	section
1	Number of detected physical threats	3.1.1
2	Number of detected cyber threats	3.1.2
3	Detection probability	3.1.4
4	Time to Detection (average)	3.1.8
5	Decision-making time (average)	3.2.2
6	Mitigation Time (average)	3.2.3
7	Downtime	3.2.6
8	Number of validated security modules integrated into the RESISTO platform	3.4.1
9	Financial Impact	Errore. L'origine riferimento non è stata trovata.

4. CONCLUSIONS – DISCUSSION

Deliverable D3.8 is the continuation of deliverable D3.7 involving the selection of a list of KPIs from the complete list of KPIs presented in D3.7, that will be measured during the piloting activities scheduled for the final year of the RESISTO project. Following the methodology detailed in the initial deliverable, a rather long list of KPIs was selected, originating from different sources, that could be potentially useful as key performance indicators for the assessment of the proposed solution's technical aspects and its impact on the application domain.

Further refinement of the list, following the principles presented in the current deliverable, led to the adoption of a shorter list of 9 KPIs. These KPIs were described, justified and their corresponding measurement methods were properly defined in the current document. The output of this deliverable and the corresponding task of WP3, will be used as input to the work-packages dealing with the piloting activities of the project, i.e. WP7 & WP8, since the selected KPIs will be measured during the pilots and will drive the evaluation and validation process of the RESISTO approach.

5. REFERENCES

[1]	RESISTO – Grant Agreement. Project Starting Date: May, 1 st 2018
[2]	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
[3]	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
[4]	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
[5]	Campbell, G. (2007). Measures and metrics in corporate security: Communicating business value. Framingham, MA: CSO Executive Council
[6]	Hayes, B., & Kotwica, K. (2012). Advances and stalemates in security. Security Magazine, 34
[7]	Davenport, T., & Harris, J. (2010). Analytics and the bottom line: How organizations build success. Key Learning Summary published by Harvard Business Review.
[8]	Garcia, M. L. (2008). The design and evaluation of physical protection systems (2d ed). Boston, MA: Butterworth-Heinemann.
[9]	Treece, D. & Freadman, M. (2010). Metrics is not a four-letter word. Security Magazine, 90-94.
[10]	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 .
[11]	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 .
[12]	Kovacich, G., & Halibozek, E. (2006). Security Metrics Management. Boston, MA: Butterworth-Heinemann.
[13]	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 .
[14]	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 .
[15]	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 .

[16]	Collins, B. (2004). Information security program metrics. In Security Business Practices Reference 6, 20-21. Alexandria, VA: ASIS International.
[17]	Doinea, M., & Pavel, S. (2010). Security optimization for distributed applications oriented on very large data sets. Informatica Economică, 14(2), 72-85.
[18]	Whitman, M. & Mattord, H. (2012). Information security governance for the non-security business executive.
[19]	Aleem, A., Wakefield, A., & Button, M. (2013). Addressing the weakest link: Implementing converged security. Security Journal, 26, 236-248.
[20]	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.
[21]	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.
[22]	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
[23]	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.
[24]	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
[25]	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.
[26]	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.
[27]	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.
[28]	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.
[29]	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

[30]	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
[31]	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.
[32]	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
[33]	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
[34]	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).
[35]	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.
[36]	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 .
[37]	McIlravey, B., & Ohlhausen, P. (2012). Metrics and analysis in security management [White Paper]. Retrieved from http://www.ppm2000.com/resources/white_papers.asp .
[38]	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 .
[39]	Huff, A. (2013). Big data I: Exception monitoring. Commercial Carrier Journal. Retrieved from http://www.highbeam.com/doc/1G1-324762775.html .
[40]	I. Bernik, K. Prislán, “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
[41]	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
[42]	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
[43]	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.
[44]	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.

[45]	Bruneau, M., and A. Reinhorn. 2007, "Exploring the Concept of Seismic Resilience for Acute Care Facilities", Earthquake Spectra 23 (1):41-62.
[46]	D. Reed, K. Kapur, and R. Christie, "Methodology for Assessing the Resilience of Networked Infrastructure," IEEE Systems Journal, vol. 3, pp. 174-180, 2009.
[47]	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.
[48]	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.
[49]	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.
[50]	S. E. Chang and C. Chamberlain, "Assessing the role of lifeline systems in community disaster resilience," Research Progress and Accomplishments 2003-2004, 2005.
[51]	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