Risk and Resilience Assessment and Improvement in the Telecommunication Industry

Mirjam Fehling-Kaschek, Natalie Miller, Gael Haab, Katja Faist, Alexander Stolz, Ivo Häring
Safety Technology and Protective Structures, Fraunhofer Institute for High-Speed Dynamics, Germany. E-mail: Mirjam.Fehling-Kaschek@emi.fraunhofer.de

Alberto Neri
Electronics Division, Engineering Department, Leonardo Spa, Italy. E-mail: alberto.neri@leonardocompany.com

Giuseppe Celozzi
Ericsson Telecommunicazioni S.p.A., Italy. Email: Giuseppe.celozzi@ericsson.com

Jose Sanchez, Javier Valera
Integrasys S.A., Spain. Email: jose.sanchez@integrasys-sa.com

Rodoula Makri
Institute of Communication and Computer Systems, Greece. Email: rodia@esd.ece.ntua.gr

A growing number of consumer and industrial functionalities, including safety relevant and safety critical functions and services, rely on reliable and resilient telecommunication infrastructures. As telecommunication grids advance virtualization, are designed resembling the internet and are moving towards 5G, the interest to quantify their resilience with respect to major disruptions is increasing. Due to this increasing complexity of the telecom infrastructures, as attack types and often intensities are growing, their potential susceptibility and vulnerability increases. In this context, the main goal of the EU-funded H2020 project RESISTO is to provide an innovative solution for the cyber-physical resilience enhancement and holistic situation awareness for communication infrastructures. The solution consists of two main parts, the short term and the long-term components. While the short term components are designed to respond to events in real time and provide a decision support system, the long term components, mainly described herein, feature a risk and resilience analysis, based on a holistic risk and resilience management process created in previous work. Based on the inputs and a simulation grid approach, first results on the resilience quantification are presented resorting to graphical analyses and distributions for behavioral modeling. Finally, the integration of the long-term tool in the RESISTO solution and its interaction with the short term components is discussed.

Keywords: Resilience quantification, telecommunication, critical infrastructure, network simulation.

1. Introduction

Telecommunication (telecom) infrastructures play a large role in the functioning of society, economy, and industrial production, mainly because of their fundamental role in information distribution and data sharing. Therefore, these critical infrastructures (CIs) need to be able to handle risks and be more resilient against any adverse events. This remains difficult as the interdependencies with other CIs, as well as the complexity of each infrastructure system is increasing.

This work continues building on a tabular risk and resilience assessment method for telecom infrastructures presented in Fehling-Kaschek *et al.* (2019) by adding a resilience quantification method. So far, it has been shown that tabular and matrix assessments are capable of efficiently identifying key threats, related consequences and expected resilient response actions.

The presented assessment process and simulation is currently being used in the H2020 project RESISTO (2020). The project focuses on physical, cyber and physical-cyber threats in the telecom infrastructure domain, with the aim of improving their resilience. The simulation method advances the tool CaESAR (**Ca**scading **E**ffects **S**imulation in urban **A**reas to assess and increase **R**esilience), which has the ability to investigate cascading effects across different CIs, as originally developed within the EU project SnowBall (2017).

The paper is organized as follows: Section 2 discusses the current challenges communication infrastructures are or will be facing in the future. Section 3 shows the adoption and extension of the risk and resilience assessment process to telecom

Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0

infrastructures as defined in Häring *et al*. (2017). This includes a brief summary of previously published steps and detailed information on the most recent project work including simulation and quantification. Section 4 embeds the approach within the overall RESISTO platform and tools currently developed. Section 5 concludes in assessing whether these tools are expected to cover most of end users' needs, mainly regarding flexible and validated risk and resilience control and assessment options.

2. Challenges of current and future communication infrastructures

2.1 5G networks

Private businesses, government agencies and other bodies are dependent on telephone and internet services provided by telecom networks to carry out daily operations, but concerns have been raised in recent years over their security. Concerns include the ever-increasing amount of data that is transported through the telecom infrastructure; consumer services (e.g. video communication, navigation, and mainly only streaming services) and private and business cloud services (e.g. software on demand, storage on demand, etc.).

There is a general increase of potential physical threat modes relevant to all CIs, in particular shifting to more extreme loadings such as human-increased (anthropogenic) loading or severe weather events. Besides this, the increasing (and almost complete) digitalization of telecom networks has already been a versatile field for cyber-attacks, further enabled through the distributed, combined and legacy nature of the telecom CIs.

At the same time, increasing virtualization and abstraction from physical layers is further increased through the intended (and in parts ongoing) move towards 5G. These networks have a larger number of alternative routings as well as a larger amount of redundancies and back-up options, at least for high priority and real time services. 5G networks are critical in ensuring digitization and M2M (machine-to-machine) connectivity for other CIs driving the future of our industries. The data necessary shall be confidentiality protected, as well as its integrity protected hop-by-hop, posing more complex modeling in the network (Teppo und Norrman 2019).

The services offered by the 5G infrastructure shall carefully consider priority levels (from critical services to consumer ones) and the increasing necessity to ensure the physical (near) real-time backbone capabilities (e.g. actual physical redundancies and fast handshakes).

RESISTO will investigate advanced risk control and resilience assessment of a 5G network as one of the use cases to allow for a better analysis of the challenges posed on 5G infrastructure and cascading effects as a CI. The risk and resilience assessment and quantification will be applied to these use cases. The process is defined and discussed in Section 3.

2.2 *Security challenges of current and future radio infrastructures*

Radio Access Networks (RAN) play a key role in cellular communications as they connect the UE (User Equipment) to the CN (Core Network) for both data and control communications. The services provided by RAN nodes -commonly known as *cellular base stations*- require a high degree of reliability and security in order to guarantee continuous availability and Quality of Service (QoS).

The RAN base station nodes are therefore a critical asset that must be protected from both physical attacks and cyber-attacks. The control channels and synchronization signals, are communication resources provided by the cell nodes which play a fundamental role in connecting to, coordinating and communicating with all the terminals (UEs). Besides, data channels represent a relevant resource as they ultimately carry the user data.

Under this scenario, a set of multiple threats and attacks (intentional or unintentional) emerge which may degrade or completely halt the cell service by targeting the mentioned channels or signals. They could be more generally classified into: i) interference-based issues (barrage) (Marojevic, et al. 2017), ii) user generated issues and rogue base stations issues.

- Full or partial band interference (barrage): These types of attacks are able to affect the whole or a considerable amount of the cell channels with a powerful noise signal. Yet they are highly inefficient in terms of power needed to disrupt the services. They could be intentional interference from a malicious attacker or unintentional from a faulty or uncoordinated RF device.
- Distributed Denial of Service (DDoS) by cell users: These attacks are conducted by botnets, where a master bot instructs the bot nodes (hacked UEs) to upload and download high amounts of useless data to overload a target cell node (Khosroshahy, Qui und Ali 2013).
- Rogue base station: These are usually illegitimate base station nodes that are advertised as valid ones and deceive the user to connect to them without any knowledge from them (IMSI Catchers). IMSI Catchers

pose a serious threat for the privacy and security of the user but also this threat is extended to the infrastructure itself by breaking coordination in SON Radio Access Networks (Shaik, et al. 2018). Into the rogue base station category also can be included the uncoordinated small cells.

Within the RESISTO project a tool named RANMONITOR has been develop which is able to detect and report the above listed RAN threats and attacks. The tool offers multi-operator, multi-band signal monitoring capabilities for live control-channel parameters and spectral analysis of the cell signals. These data are processed and detection events are reported to the RESISTO Short Term Control Loop (STCL) in real time. The RESISTO platform then analyses the event and raises an alarm followed by proper mitigation action by the critical infrastructure end user.

3. Resilience assessment and quantification

Within the RESISTO project, a risk and resilience management process is performed for telecom networks and infrastructures. The method for this procedure is detailed in Häring *et al*. (2017). The procedure bases on the ISO 31000 standard (2018) which was created to aid in the process of classical risk management.

Häring *et al.* (2017) adapted this risk management procedure to fit with and cover resilience. This adaption extends the risk procedure of five steps into a nine-step procedure that investigates and manages resilience of systems. The risk and resilience assessment process has been adapted to the RESISTO project, by collecting relevant inputs and identifying and implementing supporting tools, see Figure 1.

3.1 *Expert inputs for communication infrastructures*

The first part of the risk and resilience management process within RESISTO has been reported in Fehling-Kaschek *et al*. (2019). This part focused on a fast and flexible input collection template to be used for the risk and resilience quantification. The inputs for the analysis were categorized into four tables, including 1. system components, 2. system functions, 3. threats and 4. improvement measures, each covering a different step of the risk and resilience management process (see Figure 1).

The next analysis steps were completed using a web application based on the Shiny package (Chang, et al. 2018) for the computing language R which specializes in statistical analysis. Within the web application, the tables can be browsed interactively, connections between the different tables can be visualized and correlation matrices can be created. This allowed for the qualitative investigation of critical combinations of disruptive events, or threats, and their effect on different performance functions, and helps create the basis for the simulation completed later in the resilience management process.

A short summary on the collected inputs and extracted information is given in the following.

3.1.1 *System attributes and model*

Telecom CI subsystems and components are similar as collected in Fehling-Kaschek *et al*. (2019), see Table 2. Network schemes for testbeds to be used in RESISTO were additionally provided allowing to set up a realistic model for the simulation. For the simulation, these network schemes were converted to node and edge lists that can be read into the program.

The present results in this paper were derived for a testbed setup based on the current 4G networks. The basic information needed for the simulation is a list of all network nodes and their interconnections. Additional information, such as the localization of the nodes or other attributes of the nodes and connections, such as mean time to repair or capacity, is supporting the simulation. An important attribute necessary for the creation of the results shown in section 3.2, is the allocation of services to each node (e.g. voice service, data transmission, etc.). The probability of failure for each node is also an important attribute. The attributes can vary depending on which testbeds, threats and performance measures are selected by the user for investigation.

Regarding the modeling of 5G telecom CI, the following grid elements should be modeled: virtual infrastructure to support the core network functions, virtual infrastructure to support the MEC network functions and access terminals to connect IoT devices used to support new 5G enabled use cases.

3.1.2 *Performance functions*

System performance functions defined by the partners in RESISTO include voice services, L1 Connectivity, Mobile Data Services, Fixed Data Services, L3 Connectivity and security functions and policies (see Kaschek *et al*. (2019) Table 3 for examples). The measures need to be calculated for the implemented network model during the simulation. Therefore, a focus was set on measures that can be linked to graph theory based measures, like connectivity.

3.1.3 *Threats*

The final list of threats collected from different telecom partners in RESISTO covered cyber,

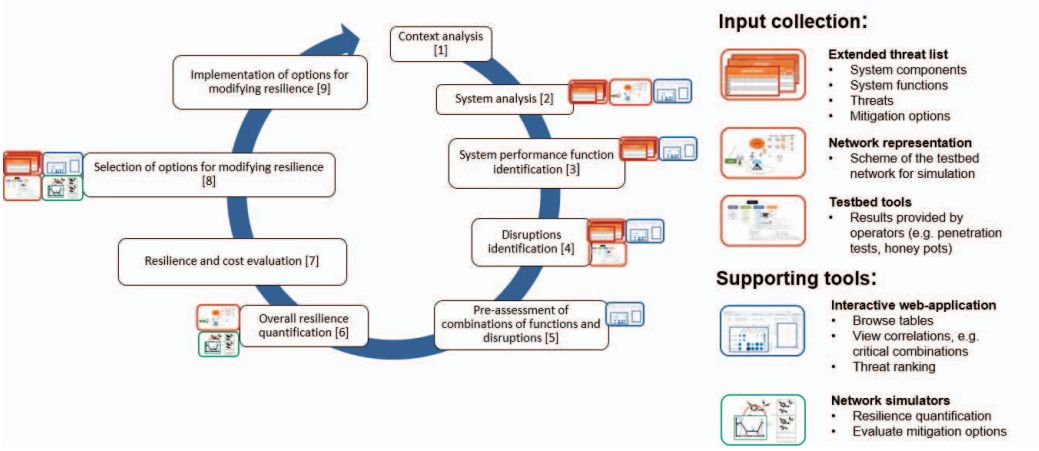

Figure 1. The adapted risk and resilience management process used in RESISTO, adapted from (Faist and Fehling-Kaschek 2019).

physical and cyber-physical threats (see Kaschek *et al*. (2019) Table 4 for examples). Popular threats submitted included distributed denial of service (DDoS) attacks, as well as weather hazards. Radio and mobile network threats remain challenging, as the coverage of mobile communication will further increase, see (GSMA 2019) and references therein. The focus for the results in this paper was set on physical attacks, which lead to a temporary removal of nodes from the system. If the threat is one that effects the arcs instead of the nodes, the arcs can also be removed from the system. At each simulation step during the damage phase, nodes are removed from the network based on the specific threat defined.

3.1.4 *Risk and Resilience Improvement Methods*

Partners also defined different improvement methods, see Kaschek *et al*. (2019), Table 5, as an initial starting point.

Improvement methods were collected for every threat listed and for all resilience cycle phases with the aim to cover all aspects of resilience. Depending on the improvement method, quantification ranges from relatively easily accessible approximations (e.g. increase of probability to prevent a threat) to more difficult ways of actually measuring the resilience benefit (e.g. addition of redundancies to the network via new nodes or connections). This again confirmed the need for a simulative assessment capability for CIs in order to assess the effect of improvement measures in case of disruptions during and post such events.

3.2 *Simulation approach*

The simulation tool used in RESISTO for the resilience assessment analysis is CaESAR. CaESAR investigates cascading effects within a critical network; see Hiermaier, Hasenstein and Faist (2017). It can simulate disruptive event types at base network levels, the resulting damage of the overall network including cascading effects as well as model the network recovery. Resilience improvements and strategies can be tested and optimized to determine their effectiveness. After the damage simulation is completed, the infrastructure is recovered by adding the nodes back online. At this phase, the improvement measures or mitigation measures that are implemented can be evaluated.

An output of the CaESAR simulation is a set of performance time curves, computed for a list of dedicated performance measures and the most relevant threats. These curves illustrate and quantify the performance loss due to an adverse event, highlighting the different phases of resilience including the response (absorption, immediate response, stabilization) and the recovery phase. These curves can be used to determine the effectiveness of the different improvement measures, and allows this comparison to include all phases of resilience.

3.3 *Simulation results for RESISTO*

Results presented in this section are based on the testbed implementation of a RESISTO end user. The testbed is composed of 11 routers (core, distribution and access routers), 2 switches, 2 load balancers, 2 firewalls and 1 server. Each of these components has information and attributes collected in the nodelist. An edgelist was also created describing the connections between the components. These two lists are then imported into CaESAR for the simulation.

Two different disruptive events are modeled: one corresponding to a knockout event (T1), e.g. malicious attack, and the other to a continuous

failure probability (T2), e.g. due to a bad weather condition. The knockout event, T1, is modeled by disabling 20% of the nodes at 10:30 am. For the continuous event, T2, it is assumed that each node has a probability of failure of 10% every 5 min between 10:10 and 10:30 am. This failure introduces a time component and can simulate a hurricane or storm that follows a certain path and moves over time. In each simulation, the attacked and failing nodes are picked at random and removed from the network, however future iterations could specifically define which nodes to remove thereby better modeling terror attacks where TV headends or nodes central in the network with many connections are attacked.

The recovery of a node begins as soon as it has failed. The time for recovery is estimated with the mean time to repair (MTTR), which is assigned randomly ranging from 30 minutes to 120 minutes for each node. Repaired nodes are rejoined with the remaining network.

Performance loss curves, see Figure 2 A, were computed for a set of three performance measures. These are the L1 connectivity, the technical functionality given by the percentage of working components and the voice service performance. The L1 connectivity corresponds to the size of the largest connected component (LCC) (size of largest sub grid connected to any single component) divided by the total size of the network. The voice service performance is calculated by investigating the number of nodes inside the LCC that are working and needed for voice service and dividing that number by the total number of nodes needed for voice service, including the nodes that fall outside of the LCC. Nodes that are not relevant for voice services, e.g. firewalls, therefore do not affect the associated performance measure. Representing the performance measure in this capacity allows for the services to be estimated without including any flow values, just graph theory estimations. It is assumed that the system is in a fully functioning state before any disruptive event is simulated.

For each threat, simulations were repeated 100 times leading to a variation of resulting performance curves, see Figure 2 A. The standard deviation of the mean response of the resulting distribution (grey band) is partially large and cannot be reduced by increasing the number of simulations. For the knockout event TI, the functionality (P2) is always reduced to 80% by design, while the impact on the L1 connectivity (P1) and Voice Service (P3) differ between the simulations due to the probabilistically chosen nodes. As expected, the continuous attack (T2) leads to more gradually falling performance curves compared to the instantaneous attack.

In order to allow a direct numeric quantification and comparison of results, Resilience Indicators (RIs) characterizing the CIs resilience curves are used in RESISTO. Three RIs are computed from the simulation results:

- RI_1: Maximum function performance loss expressed in percentage
- RI_2: Time between the event occurring and the complete performance recovery
- RI_4: Total performance loss from event to complete recovery (time integrated performance loss)

The estimated RIs are shown in Figure 2 B with a focus on their spread over the simulation results. In summary, T2 leads to worse effects on the infrastructure, represented by larger RI values. In addition, the predicted uncertainty is higher for T2 as larger fluctuations occur for the simulated performance curves. Mean RIs are presented in a matrix visualization in Figure 2 C. The matrix format will be used to store the simulation results in RESISTO (see section 4.3). Depending on the use and interpretation of the results, the maximal RI values should be used instead of the mean values.

4. RESISTO integration platform

The RESISTO platform integrates two mutually supporting control loops, the Short Term Control Loop and the Long Term one, both running on top of the Communication Infrastructure and its operational layer. A brief description of each one is given below.

4.1 *Short term control loop*

The **Short Term Control Loop** (STCL) is the runtime component of the platform. It is in charge of detecting physical and/or cyber events that might impact the operational life of the system and react promptly. It enhances situational awareness and provides operators with a Decision Support System cockpit able to implement the best reactions to an identified adverse event aiming at mitigating its effects and restoring standard operating conditions.

The STCL:

- monitors the communication CI to collect and/or detect anomalies and by correlating the physical and cyber domain events issues early warnings on security attacks or events adversely impacting the provided services;
- evaluates through the Risk/Impact Predictor module the event impact with respect to

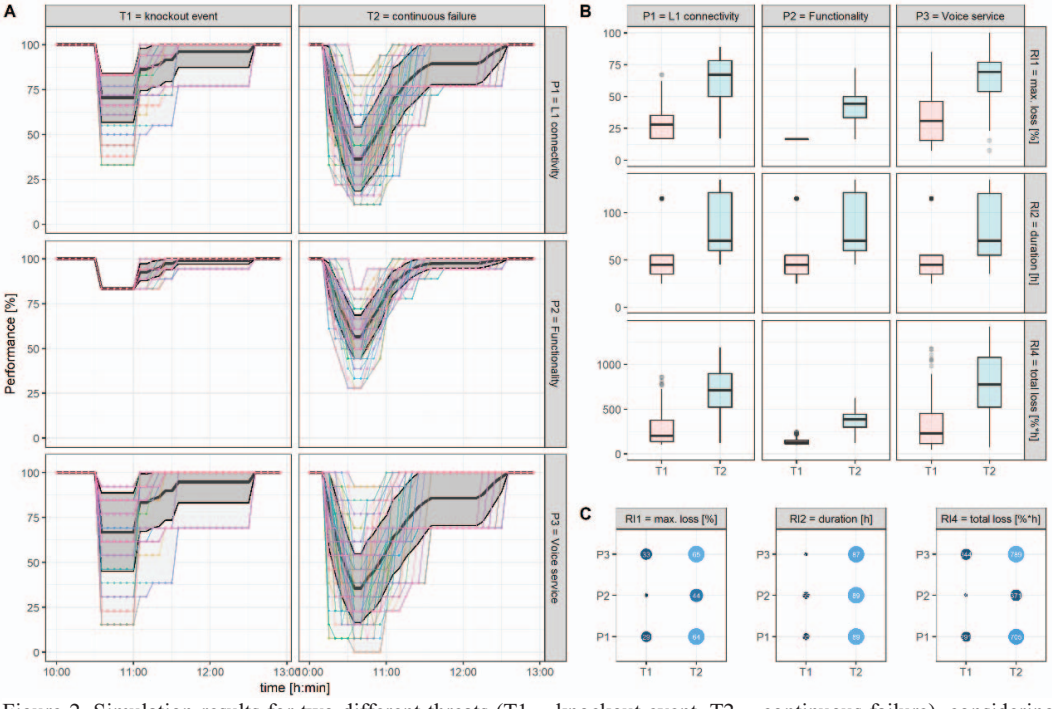

Figure 2. Simulation results for two different threats (T1 = knockout event, T2 = continuous failure), considering three performance measures (P1, P2, P3) as described in the main text. For each threat type, 100 time-resolved performance curves were simulated (colored lines) and the mean performance curve with one standard deviation (black line with dark-grey band) computed (A). The light-grey area represents the maximal performance coverage of all simulations. Three types of resilience indicators (RI1, RI2, RI4) were computed from the performance curves and their median (black horizontal lines) with 25 and 75 percentiles (colored boxes), maximal range (vertical lines) and outliers (grey dots) calculated per threat and performance function (B). Resilience indicator matrices for the three indicators based on the mean values obtained from the 100 simulations (C).

service degradation and cascading effects to interlinked CIs;

- supports decision making with a qualitative and quantitative What-If analysis tool to evaluate the best telecom CI reconfiguration;
- drives reaction and mitigation through action workflows (directives to intervention teams, physical protection devices activation) and orchestrates network reconfiguration and protection function activation by means of a 5G oriented Orchestration Controller.

The STCL can collect adverse event detections coming from existing sensors, Physical Security Information Management (PSIM) systems and Security Operation Centers (SOCs) as well as by innovative detectors offered by RESISTO based on state-of the-art technologies (i.e. Machine Learning, anti-UAV sensors, EM Spectrum Analysis). The latter are also partly covered and supported by the LTCL simulative capability and its tabular assessment approach. Both can be used to support the optimum selection of the short, medium and long term improvement measures.

4.2 *Long term control loop*

The **Long Term Control Loop** (LTCL) is an offline activity, aiming to assess CI vulnerabilities and cyber and physical security threats. The LTCL is based on the Risk and Resilience assessment and management process described in section 3. Consequently, this loop defines assets configuration and interventions to improve CI risk control (low susceptibility and vulnerability, low initial damage, high robustness) and resilience (short down time, fast recovery / resourcefulness, complete or better bounce back).

While the STCL provides tools for direct reaction against attacks in real-time, the LTCL should be conducted on a periodic basis or in case of specific events, e.g. after changes in the setup of the infrastructure or discovery of new threats or previously undetected vulnerabilities. It can be used to evaluate new measures or actions that operators are debating implementing, and can give an idea of the potential outcome. However, also longer lasting response and recovery

activities start with fast initial counter-actions. Hence, in particular the last two items of section 4.1 should supported by pre-calculated advice on best response vectors and be provided in what-if look up tables. This especially holds true for effective damage containments by switching off connections to restrict the overall loss of connections to small areas.

4.3 *Interactions between long term and short term control loops*

The interaction between the LTCL and STCL can be seen in Figure 3. This figure describes the RESISTO platform, focusing on the Resilience Indicators (RIs) of section 3.3. In reality, the platform is more complicated, the STCL includes more features than just real time measurement of RIs, see section 4.1. Some abstract relations between the two control loops include:

- The risk and resilience assessment and improvement process often identifies the need for fast mitigation of damages, requiring a near real time detection capability.
- Tracking the observed damage and response histories can be used to better simulate the multitude of potential events, e.g. in terms of distributions of event types, event intensities, response actions taken, stabilization, response and recover times and levels.

During the last steps of a LTCL cycle (see Figure 1, steps 6 to 9),

- the telecom CI's "As-Is"-resilience is characterized (quantified) for the most critical couples of performance functions and threatening events (as identified in step 5);
- critical couples of performance function and events showing resilience indicators not in line with the system level requirements (as defined in step 1 and 2) are identified;
- interventions are selected to improve resilience for most critical functions / events couples; the RIs are estimated for the new "To-Be"-resilience configuration (step 8);
- interventions are implemented (step 9).

At the end of each LTCL cycle estimated RIs for specific couples (function; event) are stored in a matrix format in the Knowledge Base (KB), see Figure 3. During the operation system life, STCL operators could face real events for which RIs were previously estimated. In those cases, actual RIs are measured and values stored in the KB. Thus, a feedback loop is introduced with the comparison between the estimated and measured RIs. This comparison allows for a validation of the simulation results and is taken into account in the next LTCL cycle to improve the resilience simulation model if needed. This process triggers a continuous resilience improvement for the CI.

5. Summary and conclusions

The paper shows how to combine and complement a flexible performance-based risk and resilience assessment process as a long-term activity for communication CIs. This is supported by tables and dependency matrices, with a risk and resilience input-output simulation process for coupled grids, advancing past approaches (Cimellaro 2016), since attack vectors and response options are simulated allowing determining of the average overall resilience curves.

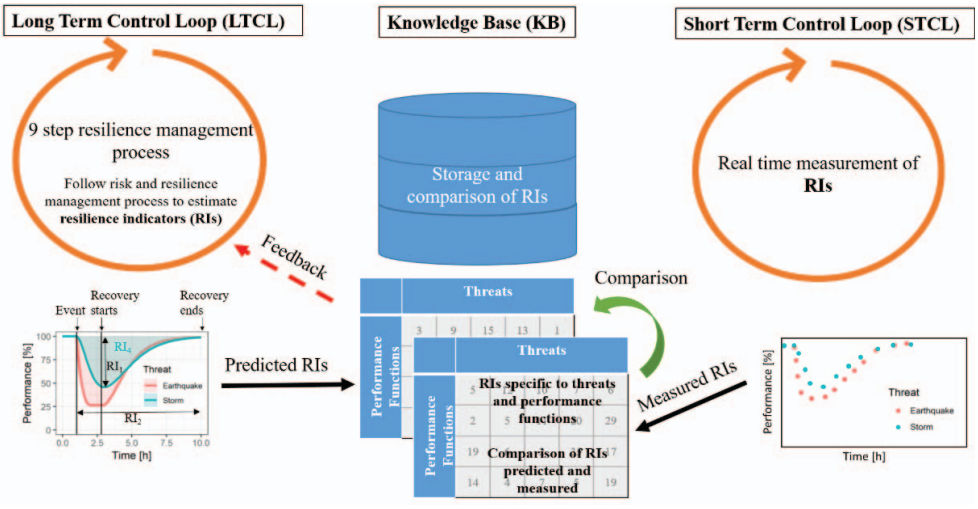

Figure 3. The RESISTO platform, with a focus on the resilience indicators, includes two control loops, a long term and short term, with the Knowledge Base linking them.

It was shown how for two threat and response type regimes respectively three different performance functions along with three resilience measures can be determined and evaluated based on averaged simulative performance curves, which allow to compare in detail the resilience in both cases.

It was indicated how long-term tabular and simulative CI assessment (the RESISTO LTCL) aligns with, mutually supports and empowers short term monitoring and counter-activities selection and implementation (the RESISTO STCL) for better overall risk control monitoring and resilience assessment, in a holistic approach.

Further work will take advantage of this rich framework, for more comprehensive and operationally validated quantification of the approach. A next step in the RESISTO project will be the implementation of models to simulate cyber-attacks; the transfer of the approach to the future 5G infrastructures poses a major challenge due to the new level of complexity and virtualization that needs to be modeled.

Acknowledgement

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

References

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

Cimellaro, Gian Paolo. 2016. *Urban Resilience for Emergency Response and Recovery.* Switzerland: Springer International Publishing. doi:10.1007/978-3-319-30656-8.

Faist, K., und M. Fehling-Kaschek. 2019. „Risk and resilience management process for cyber-physical threats of telecom CI." *RESISTO project | Deliverable.* Aug. Zugriff am 29. April 2020. http://www.resistoproject.eu/resources/.

Fehling-Kaschek, Mirjam, Katja Faist, Natalie Miller, Jörg Finger, Ivo Häring, Marco Carli, Federica Battisti, et al. 2019. „A Systematic Tabular Approach for Risk and Resilience Assessment and Improvement in the Telecommunication Industry." *Proceedings of the 29th European Safety and Reliability Conference.* Hannover, Germany. 1312-1319.

GSMA. 2019. *Mobile Telecommunications Security Threat Landscape.* https://www.gsma.com/security/wp-content/uploads/2019/03/GSMA-Security-Threat-Landscape-31.1.19.pdf.

Häring, Ivo, Giovanni Sansavini, Emanuele Bellini, Tatyana Kovalenko, Maksim Kitsak, Georg Vogelbacher, Katharina Ross, Ulrich Bergerhausen, Kash Barker, und Igor Linkov. 2017. „Towards a Generic Resilience Management, Quantification and Development Process: General Definitions, Requirements, Methods, Techniques and Measures, and Case Studies." In *NATO Science for Peace and Security Series C Environmnetal Security*, von Igor Linkov und José M. Palma-Oliveira, 21-80. Dordrecht: Springer Netherlands.

Hiermaier, Stefan, Sandra Hasenstein, und Katja Faist. 2017. „Resilience Engineering - How to Handle the Unexpected." *7th Resilience Engineering International Symposium.* Belgium.

ISO 31000. 2018. *2018-02: Risk management - Guidelines.* https://www.iso.org/standard/65694.html.

Khosroshahy, Mascood, Dongyu Qui, und Mustafa Ali. 2013. „Botnets in 4G cellular networks: Platforms to launch DDoS attacks against the air interface." *2013 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT).* Montreal, QC, Canada: IEEE. 30-35.

Marojevic, Vuk, Raghunandan Rao, Sean Ha, und Jeffrey Reed. 2017. „Performance Analysis of a Mission-Critical Portable LTE System in Targeted RF Interference." *IEEE VTC*, September.

RESISTO. 2020. *Resilience enhancement and risk control platform for communication infrastructure operators. EC Grant agreement ID: 786409.* https://cordis.europa.eu/project/id/786409.

Rose, Scott, Oliver Borchert, Stu Mitchell, und Sean Connelly. 2019. *Zero Trust Architecture.* NIST Special Publication 800-207, U.S. Department of Commerce, National Institute of Standards and Technology .

Shaik, Altaf, Shinjo Park, Ravishankar Borgaonkar, und Jean-Pierre Seifert. 2018. „On the Impact of Rogue Base Stations in 4G/LTE Self Organizing Networks." *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks.* Stockholm, Sweden: Association for Computing Machinery. 75-86.

SnowBall. 2017. *Lower the impact of aggravating factors in crisis situations thanks to adaptative foresight and decision-supprting tools. EC Grant agreement ID: 606742.*

Teppo, Patrik, und Karl Norrman. 2019. „Security in 5G RAN and core deployments." *Ericsson.* 29. November. Zugriff am 7. January 2020. https://www.ericsson.com/en/reports-and-papers/white-papers/security-in-5g-ran-and-core-deployments.