BOOK OF ABSTRACTS

Joint Workshop DRS-7&14 projects:

"Aligning the resilience-related research efforts in the EU-DRS projects"

Brussels, September 13-14, 2017

Eds: A. Jovanović, E. Bellini
Published by: EU-VRi, Stuttgart, Germany, September 2017

Published by:

European Virtual Institute for Integrated Risk Management (EU-VRi), www.eu-vri.eu
Visiting address:
Lange str. 54,
70174 Stuttgart, Germany

September 2017, Stuttgart, Germany

Tel: +49 711 410041 29
Fax: +49 711 410041 24
info@eu-vri.eu

Acknowledgments

The Support of the European Commission provided for EU Projects DARWIN, RESILENS, SmartResilience, IMPROVER, RESOLUTE and SMR is gladly acknowledged here, as well as a direct support in providing the venue and facilities for the workshop.

Preface

Joint Workshop DRS-7&14 projects:

ALIGNING THE RESILIENCE-RELATED RESEARCH EFFORTS

IN THE EU DRS PROJECTS

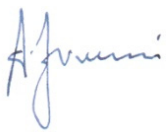
Brussels, Belgium, September 13-14, 2017

This Joint Workshop DRS-7&14 projects entitled "Aligning the resilience-related research efforts in the EU DRS projects'' takes place in conjunction with the Community of Users Meeting of September 12, 2017. The main issue tackled at the workshop is simple: new approaches to the resilience assessment and management methods, new guidelines and new tools are being developed in many current EU projects. Obviously, these development efforts should be consistent and aligned, but it is often not easy to achieve this goal in practice - this workshop should help in this sense.

The Workshop intends to go beyond simple presentations of project results. It will include intensive exchange of opinions, confronting the ideas, identifying clearly the pros and cons of different approaches and highlighting paths and opportunities for integration of results from different DRS projects. The Workshop involves over 150 practitioners, developers and decisions makers eager to find the best way to harmonize, integrate and enhance the project outcomes, and achieve tangible impact at the European level. International/global aspects of the successful resilience approaches are tackled, too, mainly thanks to the contributions of the OECD and the US participants. Training courses and an ''interaction space'', including project information exhibition booths and the room for perspectivity challenge board games, complete the scope of the workshop.

The workshop and the meetings, will be a unique opportunity to share experience in resilience and risk governance, communication, analysis and management, also by means of person-to-person talks, not only among the projects partners but also among all the interested stakeholders in Europe and worldwide.

Enjoy!



(A. Jovanovic, SmartResilience Project Coordinator, CEO EU-VRi)

(E. Bellini, Resolute Project Coordinator, Researcher, University of Florence)

Program Committee

- Emanuele Bellini
- Ivonne Herrera
- William Hynes
- Aleksandar Jovanović
- Stephane Jacobzone
- David Lange
- Paolo Nesi
- Jose Maria Sarriegi

Organization Committee

- Emanuele Bellini
- Aoife Doyle
- Ivonne Herrera
- Aleksandar Jovanović
- Roswitha Kokejl
- Jose Palma-Oliveira
- Katarzyna Tetlak

Table of Contents

Announcement

Joint Workshop DRS-7&14 in conjuction with the CoU - Community of Users (http://ereg.me/cou-sept-2017) meeting of Sept. 12, 2017:

Aligning the resilience-related research efforts in the EU-DRS projects

September 13-14, 2017

BAO Congress Centre
rue Félix Hap 11
1040 Brussels, Belgium

Following the initiatives coming from several DRS-projects and support expressed by the European Commission, this joint workshop is organized with the goal to ensure collaboration and alignment among the projects, especially in the areas related to methods, guidelines and tools developed in the projects. The challenges related to aligning experience, findings and lead to research in single project towards a "common approach" will be tackled during this workshop and the possibilities for joint practical actions examined.
The format of the joint workshop will include plenary sessions devoted to alignment of:

- Methods & Guidelines for resilience assessment
- Resilience Indicators
- Tools, operationalization, application
- International/global collaboration in the area of resilience involving international organizations (OECD, EU), ISO and partners from USA

as well as the

- Infobooths of single projects
- Posters & demonstrations
- Serious gaming (related to resilience)

The registration web-page will contain book of abstracts and presentations (after the workshop).

Program in a nutshell:

Start: September 13, 2017 11:30

Session 1:	Towards the aligned European Resilience Management Guidelines: How to achieve alignment and interoperability?
Session 2:	Resilience assessment and indicators: How to define them? How to monitor them? How to implement them?
Session 3:	Tools and methods for resilience operationalization
Session 4:	Application cases: Where the newly developed methods, guidelines & tools have been implemented / analyzed?
Session 5:	Importance of international/global cooperation in the area of resilience
	Final discussion

End: September 14, 2017 14:00

SHORT COURSE:
Indicator-based resilience assessment for critical infrastructures - the Smart Resilience methodology and tools
A. Jovanovic & K. Øien (SmartResilience), F. Petit (ANL)
September 14, 2017 14:00 - 16:30
Max no. of participants: 25 (registration closed)

Program Committee: E.Bellini (RESOLUTE), I. Herrera (DARWIN), W. Hynes (RESILENS), A. Jovanovic (SmartResilience), S. Jacobzone (OECD), D. Lange (IMPROVER), P. Nesi (RESOLUTE), J. M. Sarriegi Domínguez (SMR)

Organization Committee: E.Bellini, A. Doyle, I. Herrera, A. Jovanovic, R. Kokejl, J.M.Palma Oliveira, K. Tetlak

REGISTER HERE:

Register for the Webex - day 1

September 13, 2017

http://www.smartresilience2.eu-vri.eu/Events/default.aspx?EventID=11389

Register for the Webex - day 2

September 14, 2017

http://www.smartresilience2.eu-vri.eu/Events/default.aspx?EventID=11390

NOTE: Registration for personal attendence has been already closed, please use this links in order to register for online participation via Webex

Contact: K.Tetlak at:
WorkshopResilience2017@eu-vri.eu

www.h2020darwin.eu

www.improverproject.eu

RESILENS

www.resilens.eu

www.resolute-eu.org/

http://www.smartresilience.eu-vri.eu

SMR Smart Mature Resilience

www.smr-project.eu

The projects above have received support from the EU DRS project line - the support is gladly acknowledged

Partners from the EU-DRS projects are specifically invited and encouraged to participate,
all other interested Community of Users (CoU) members and external parties are cordially invited.
Please, register online (room limitations: 120 participants).
Contact organizers: Ms. K. Tetlak at WorkshopResilience2017@eu-vri.eu

Participation in the workshop and the course is free of charge, but registration is mandatory!

Program

Joint Workshop DRS-7&14 projects: ALIGNING THE RESILIENCE-RELATED RESEARCH EFFORTS IN THE EU DRS PROJECTS

Brussels, Belgium, September 13-14, 2017

Venue:
BAO Congress Centre
rue Félix Hap 11
1040 Brussels,
Belgium

http://www.bao.be/UK/PageEntreprises.php

Picture source:
https://lh3.googleusercontent.com/M1T5zlzNYWy9eDAm-K-DJl2msGWrfYGuF85GceefnQtyEHz0Op1vltykm62l_mvjW82OLCA=s150

The Resilience Workshop is an excellent opportunity among project partners from different DRS projects to communicate their results to the "outside world" and align further activities related to resilience. It is also an opportunity for interested professionals, not participating in above mentioned projects, to learn about them and theirs numerous results.

Conference Committee: E. Bellini (RESOLUTE), I. Herrera (DARWIN), W. Hynes (RESILENS), A. Jovanović (SmartResilience), S. Jacobzone (OECD), D. Lange (IMPROVER), P. Nesi (RESOLUTE), J. M. Sarriegi (SMR)

European Virtual Institute for Integrated Risk Management
Brussels 2017

The program of the workshop and its accompanying events comprises:

1. **September 11, 2017**

   EU-VRi/ETPIS Meeting

   General Assembly, Executive Board

2. **September 11, 2017**

ResiStand Workshop

ResiStand is a two -year Coordination and Support Action (CSA) that aims to identify new ways to improve the crisis management and disaster resilience capabilities of the European Union and individual Member States through standardisation. The project started in May 2016 and will continue until April 2018. During the workshop, validation of gaps and new potential standardization items by applying the Risk Assessment Framework (RAF) will be discussed.

3. **September 12, 2017**

Community of Users (CoU) Meeting

CoU objectives are: (1) Ensure that research programming takes into account practitioners' needs, thereby promoting research results that are relevant; (2) Identify the most promising tools (including those developed in FP7 and H2020 projects) that have the potential to be taken up by practitioners; (3) Support the competitiveness of EU industry by enhancing the market for research results; (4) Ensure that the expertise of practitioners is available to policy makers, thereby facilitating the policy-making process; and (5) Facilitate policy implementation.

4. **September 13, 2017**

DRS-7&14 Projects specific meetings

SmartResilience: Critical Infrastructure. Resilience Advisory Board Meeting, RESOLUTE Advisory Board Meeting

5. **September 13-14, 2017**

Main Workshop

With presence of representatives from European Commission, OECD, ANL and End-Users the Workshop aims to showing how the stakeholders can benefit from the projects results achieved so far.

Main topics to be covered at the workshop organized will be:

1) Towards the aligned European Resilience Management Guidelines: How to achieve alignment and interoperability?
2) Resilience assessment method and indicators: How to define them? How to monitor them? How to implement them?
3) Tools and methods for resilience operationalization
4) Application cases – where the newly developed methods, guidelines & tools have been implemented/ analyzed?
5) Importance of international/global cooperation in the area of resilience – How to enhance it in the future?

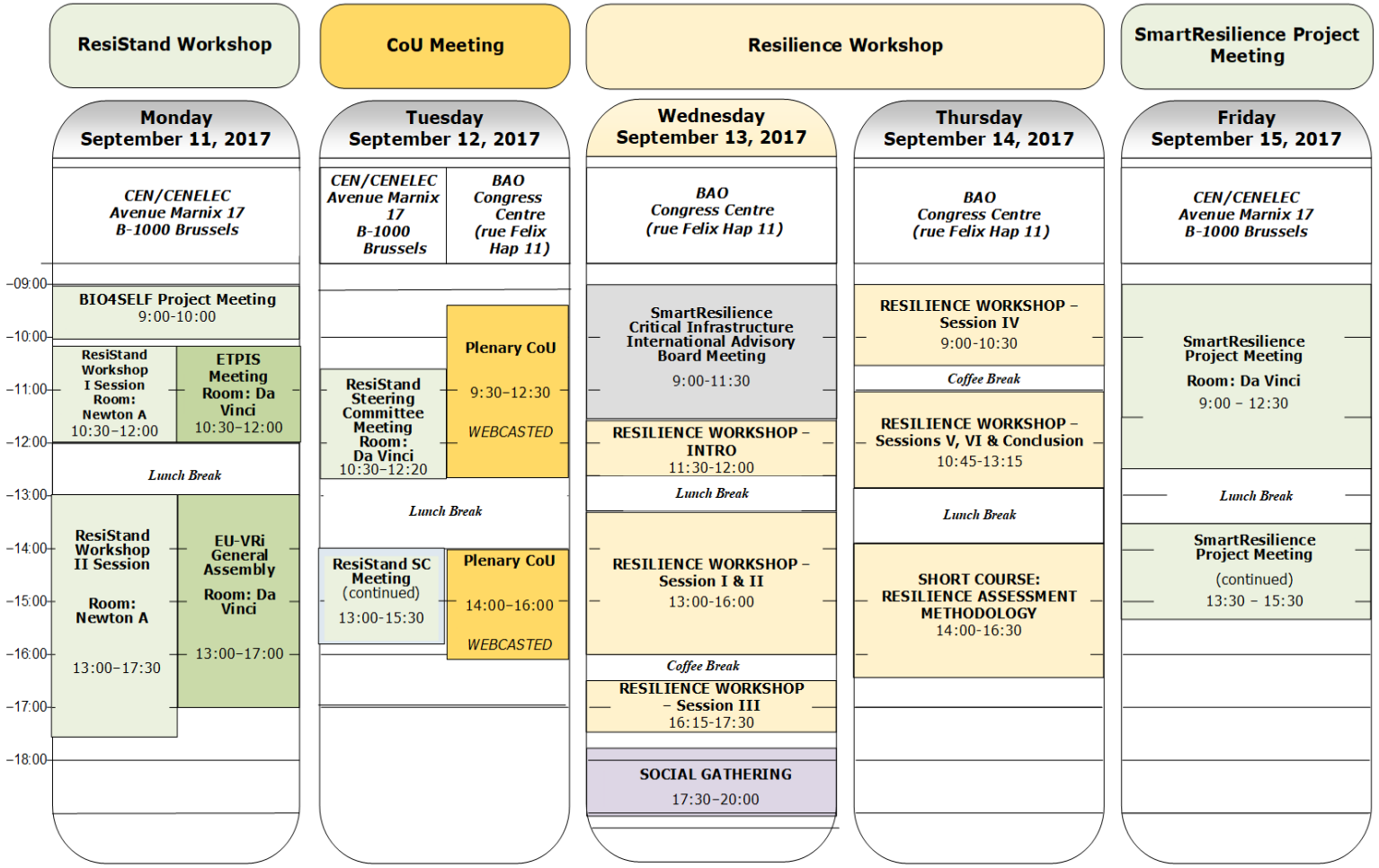
6. **September 15, 2017**

SmartResilience Project Meeting

Annual Project Partners Meeting, Steering Committee Meeting, Workpackage Leaders Meeting

For possible queries, please, feel free to contact us at WorkshopResilience2017@eu-vri.eu .

8th Event of Community of Users on Secure, Safe and Resilient Societies - Overview



Detailed Agenda

Joint Workshop DRS-7&14 projects: ALIGNING THE RESILIENCE-RELATED RESEARCH EFFORTS IN THE EU DRS PROJECTS

September 13-14, 2017
BAO Congress Centre, rue Félix Hap 11, 1040 Brussels, Belgium

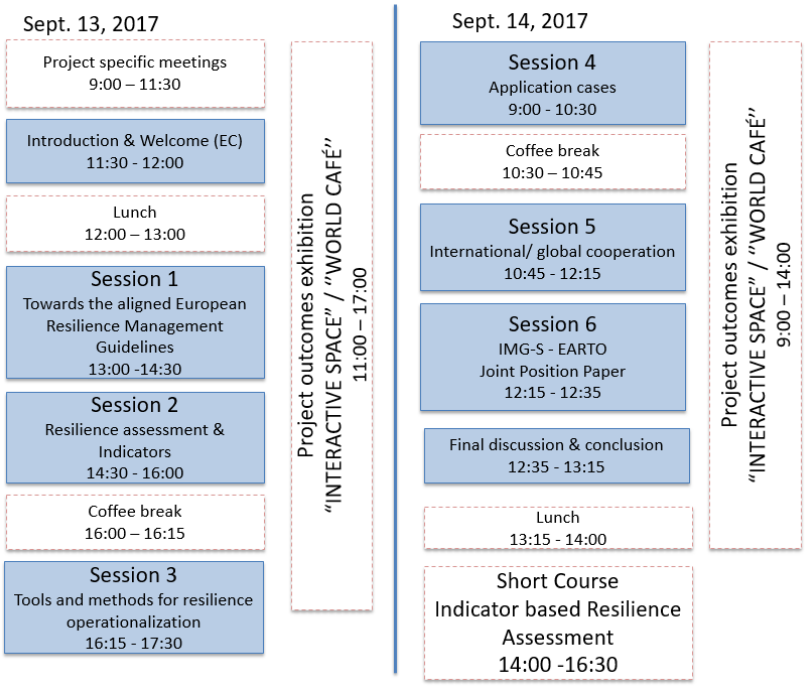
The workshop is funded by the European Commission Projects:
DARWIN, IMPROVER, RESILENS, RESOLUTE, SmartResilience, SMR
Other projects and institutions are welcome and will be invited specifically

Program Committee:

E. Bellini (RESOLUTE), I. Herrera (DARWIN), W. Hynes (RESILENS), A. Jovanović (SmartResilience), S. Jacobzone (OECD), D. Lange (IMPROVER), P. Nesi (RESOLUTE), J. M. Sarriegi (SMR)

Organization:

E. Bellini, A. Doyle, I. Herrera, A. Jovanović, R. Kokejl, J. M. Palma Oliveira, K. Tetlak
Contact: WorkshopResilience2017@eu-vri.eu



AGENDA

September 13, 2017

(09:00 -11:30)	**Project-specific meetings** ***(e.g. SmartResilience International Advisory Board Meeting, RESOLUTE Advisory Board Meeting; other projects may organize their meetings at the same time)***
11:00 - 12.00	**Registration for the workshop, coffee**
11:30 - 12:00	**Introduction & Welcome** This session will be dedicated to the introduction to the Resilience Research area within European Commission projects and the explanation of the targets: Overview of the DRS-7 & DRS-14 projects : 1) G. Lapeyre / P. Quevauviller: Searching for synergy and alignment (10 min) 2) A. Jovanovic: Goals and format of the joint workshop (10 min): 3) C. Fuggini: IMG-S - EARTO WG Security Research activities related to Resilience (10 min)
12:00 - 13:00	**Lunch**
13:00 - 14:30	**Session 1: Towards the aligned European Resilience Management Guidelines: How to achieve alignment and interoperability?** This interactive session will introduce the guidelines developed within the DRS7 projects and to identify with the practitioners the gaps, challenges and opportunities for their forthcoming integration in a view of their European-wide level adoption. Chairs of the session & discussion moderators: D. Lange, E. Bellini **Contributors:** 1) J. M. Sarriegi: European Resilience Management Guideline (SMR) (15 min) 2) S. Jacobzone: Achieving Resilience: sharing best practice, value and limit of guidelines (OECD)(15 min) 3) D. Lange: Integration of risk and resilience management (IMPROVER) (10 min) 4) W. Hynes: European Resilience Management Guidelines (ERMG) for the operators and owners of Critical Infrastructure (CI) (RESILENS) (10 min) 5) M. Branlat: Practical interventions to support critical infrastructures in enhancing their resilience (DARWIN) (10 min) 6) E. Gaitanidou: European Resilience Management Guidelines and their adaptation for UTS (RESOLUTE) (10 min) Panel discussion – Common set of the DRS - Guidelines?
14:30 - 16:00	**Session 2: Resilience assessment method and indicators: How to define them? How to monitor them? How to implement them?** A large number of indicators have been identified in different projects (over 600 so far just in SmartResilience). The session will tackle the ways of how to define, monitor and implement them. Chairs of the session & discussion moderators: J. M. Sarriegi, F. Petit **Contributors:** 1) R. Almeida: Assessing resilience based on the ISO/IEC 33000 standard series (IMPROVER) (10 min) 2) A. Jovanovic & L. Bodsberg: Which indicators can tell us if critical infrastructure is resilient? How do we know the ''quality of indicators?'' (SmartResilience) (15 min) 3) J. M. Sarriegi: Indicators for assessing the resilience-building process in cities (SMR) (10 min) 4) D. Verner, F. Petit: Assessing Resilience: from Facilities to Regions (ANL) (10 min) 5) E. Bellini: Exploiting SmartResilience indicators in RESOLUTE Resilience Assessment Framework (RESOLUTE) (10 min) Panel discussion – Common set of DRS - Indicators?
16.00 - 16:15	**Coffee break**

16:15 - 17:30	**Session 3: Tools & methods for resilience operationalization** This session will provide an information about tools, which have been used and created for the particular projects' needs. The ways of operationalization of the developed solutions will be discussed. Chairs of the session & discussion moderators: M. Branlat, I. Kozine **Contributors:** 1) G. Rafaeli: The RESILENS Toolkit – Decision Support for CI operators and owners (RESILENS) (15 min) 2) R. Almeida: A web tool for assessing resilience using any framework (IMPROVER) (10 min) 3) P. Nesi, A. Drosou: Evidence-driven Collaborative Resilience Assessment and Management Support System for Urban Transport System, A VA Platform for Personalized Crowd, Fleet & Resources Management (RESOLUTE) (15 min) 4) U. Barzelay: Why and how to use Interactive data visualization in resilience related projects? (SmartResilience) (10 min) 5) C. Grimes: Overview of the resilience tools developed and their intersections (SMR) (10 min) 6) I. Kozine: Capabilities-based approach to building and maintaining resilience (10 min) Panel discussion - Common set of DRS – tools?
17:30	The end of the first day

September 14, 2017

09:00 - 10:30	**Session 4: Application cases – are the newly developed methods, guidelines & tools implemented/analyzed?** This session will deal with the application cases and/or case studies being analyzed in different projects where the newly developed methods, guidelines & tools have been implemented. Chairs of the session & discussion moderators: Z. Szekely, K. Pala **Contributors:** 1) A. Corrigan: The RESILENS Pilot Demonstrations – Testing the Toolkit across three CI Sectors in Ireland, Portugal and Germany (RESILENS) (10 min) 2) E. Bellini: Florence pilot case (City of Florence) (RESOLUTE) (10 min) 3) Z. Szekely, I. Macsári: Case study DELTA and the significance of the SmartResilience project for the aviation security sector (SmartResilience) (15 min) 4) V. Latinos: Local Resilience Planning: A review of methodologies adopted for the SMR pilot implementation process (SMR) (10 min) 5) P. Berggren: DARWIN - Pilot application in Sweden involving among others health care, public sector and transport services (DARWIN) (10 min) Panel discussion – Are the uses really applying the results of the EU projects?
10:30 - 10:45	Coffee break
10:45 - 12:15	**Session 5: Importance of international/global cooperation in the area of resilience – How to enhance it in the future?** In importance of international/global cooperation in the area of resilience with participation of international institutions and organizations (OECD; ANL, DHS) the session will look at the issues related to the practical aspects of collaboration. Examples of the running agreements (e.g. between EU and OECD, EU-VRi and ANL) will be shown and the future opportunities for collaboration highlighted (e.g. The World Congress on Risks in 2019) Chairs of the session & discussion moderators: A. Jovanovic, S. Jacobzone **Contributors:** 1) W. McNamara: US DHS views on critical infrastructure resilience (15 min) 2) S. Jacobzone: Application of resilience concepts: the case of critical infrastructure (15 min) 3) I. Linkov: Resilience: State of Science and State of Applications in the USA (15 min) 4) F. Petit, D. Verner: Resilience Indicators and Interdependencies: Need to Promote a Global Approach (15 min) 5) C. Grimes: The role of local and regional networks and partnerships in resilience-building (SMR) (10 min) 6) J. Kieran: Enhancing International Collaboration through DARWIN's Community of Practitioners (DARWIN) (10 min) Panel discussion – Common global approach?

12:15 - 12:35	Session 6: Alignment of the Resilience Workshop findings/items with IMG-S - EARTO WG Security Research approach Joint Position Paper on Resilience in Security Research - discussion moderator: C. Fuggini
12:35 - 13:15	Wrap-up of the workshop: final discussion & conclusion
13:15 - 14:00	Lunch

Please note: Each session (incl. discussion) will be recorded.

14:00 - 16:30	SHORT COURSE: Indicator-based resilience assessment for critical infrastructures – the SmartResilience methodology and tools This extra session provides a short course on indicator-based resilience assessment method dedicated to the Critical Infrastructure operators, local authorities as well as end-users. ***Lectures:*** A. Jovanovic & K. Øien (SmartResilience), F. Petit (ANL)

Parallel events:
September 13 - 14, 2017

INTERACTIVE SPACE / ''WORLD CAFE'':
Project information exhibition booths and ''serious games'' (perspective-challenge board games)

The interaction space provides an opportunity to the critical infrastructure operators, service providers, researches, local authorities and end-users, to interact with the projects and see their current results in a more direct way.

September 13, Lunch break

Special presentations:

1) **O. Renn, Guest Key Lecture (video):** ''Resilience: A Re-insurance for Societies in Transition'' (30 min) - will be available also at: www.eu-vri.eu
2) **E. Dykstra**: TEDx-style presentation: "From Risk to Resilience...: we don't need more science but better stories!"

Abstracts

Welcome Session

G. Lapeyre[1], P. Quevauviller[1], A. Jovanovic[2], C. Fuggini[3]
[1]Project Officer, European Commission, Belgium, [2] EU-VRi, Germany, [3] Rina Consulting S.p.A., Italy

The welcome will address the general expectations of the European Commission towards the funded projects of the specific call DRS-7&14 Projects were answering to. It will also address the format of the workshop and provide instructions to participants. Also short introduction of IMG-S - EARTO WG Security Research activities related to Resilience will be presented here.

Session 1: Towards the aligned European Resilience Management Guidelines: How to achieve alignment and interoperability?

Chairs: D. Lange (SP Technical Research Institute of Sweden), E. Bellini (University of Florence)

1.1
European Resilience Management Guideline (SMR)

J. M- Sarriegi
TECNUN (University of Navarra), Spain

The main objective of the Resilience Management Guideline developed within the SMR project is to support the operationalisation of the resilience building process of European cities. This Guideline integrates five complementary tools that enhance significantly city resilience, defined as the ability "to resist, absorb, adapt to and recover from acute shocks and chronic stressed to keep critical services functioning, and to monitor and learn from on-going processes through city and cross-regional collaboration, to increase adaptive abilities and strengthen preparedness by anticipating and appropriately responding to future challenges". The five tools that integrates the Resilience Management Guideline are: 1) Resilience Maturity Model, 2) Risk Systemicity Questionnaire, 3) Portfolio of Resilience Building Policies, 4) System Dynamics Model and 5) Community Engagement and Communication tool.

1.2
Achieving Resilience: sharing best practice, value and limit of guidelines

S. Jacobzone
OECD, France

The OECD is engaging with countries to explore how they can achieve resilience at national, or regional level, through implementation of improved risk governance and management practices. The presentation will draw on a set of recent OECD studies, covering country cases on boosting resilience in countries such as Austria, Switzerland and France, to show how in practice countries are investing to create conditions for resilience in a tight public finance context. The presentation will highlight the role of soft law, and good practice guidelines in helping to mobilise countries towards strengthening their resilience management frameworks. It will discuss the role of comparative evidence, peer learning and comparative indicators in identifying areas for country progress, as well as helping to close gaps in implementation. The presentation will highlight the challenge for creating the scope for flexibility and adaptive capacity in institutional systems, which requires more systematic and holistic approaches to resilience.

1.3
Integration of risk and resilience management (IMPROVER)

D. Lange
RISE, Sweden

Within IMPROVER we have studied various methodologies for resilience analysis of CI. One conclusion of this work has been that while there are many methodologies for resilience analysis which could be applied to CI, the focus and objective of these varies. Further, the implementation or application of these methodologies to CI relies on the overall context in which a resilience analysis is being undertaken. While the different methodologies for analysing resilience are more or less well developed and can be used to guide the study of resilience to the goal of knowing the current level of resilience of the CI, their implementation to different CI and accounting for different hazards requires a far looser framework to be developed which describes the actual use of these methodologies within the context of the CI risk management process.

This presentation introduces the general framework for resilience assessment of CI being developed within IMPROVER. The proposal integrates the paradigm of resilience into the RA process according to ISO 31000. The presentation will introduce the framework applied on the *asset* (focus on individual CI assets) level. However the framework could also be applied on the *system* and the *national* or *regional* levels. It is applicable to individual CI assets accounting both for existing RA activities (at the CI operator level) and input from national or regional RA, while at the same time employing current, available tools and methodologies for resilience analysis.

1.4
European Resilience Management Guidelines (ERMG) for the operators and owners of Critical Infrastructure (CI) (RESILENS)

W. Hynes
Future Analytics Consulting Ltd (FAC), Ireland

Critical infrastructure (CI) provides essential functions and services that support European societal, economic and environmental systems. As both natural and man-made threats, disaster and crisis situations become more commonplace, the need to ensure the resilience of CI so that it is capable of withstanding, adapting and recovering from adverse events, is paramount. Moving resilience from a conceptual understanding to applied, operational measures that integrate best practice from the related realm of risk management and vulnerability assessment is the focus of the RESILENS project (Realising European ReSiliencE for CritIcaL INfraStructure). As part of this, the project is developing a user-friendly, citizen centric European Resilience Management Guideline (ERMG) to support the practical application of resilience to all CI sectors. This presentation provides an overview of the ERMG development process within RESILENS, including the wider context and rationale behind its establishment.

1.5

Practical interventions to support critical infrastructures in enhancing their resilience (DARWIN)

M. Branlat
SINTEF, Norway

Project DARWIN aims to build resilience management guidelines to support organisations in developing and enhancing their resilience in the face of crises. “Organizations”, for the project, are private or public companies, authorities or government agencies (either at international, national or local level), or community structures, all of which being potentially involved in crisis management activities. Such organisations typically already have a number of processes and tools in place to support their management of crises (e.g., preparation activities, contingency plans, procedures, learning activities). As a result, the guidelines do not aim to replace such process and tools, but rather to provide a critical view on the organizations’ crisis management activities. This perspective is grounded in research and practice on resilience management inspired by the fields of Resilience Engineering and Community Resilience.

DARWIN started with a vast review of literature, standards and operational documentation, as well as interviews of practitioners. This data collection lead to the identification and ranking of a large number of requirements. Those requirements included especially conceptual requirements that captured resilience management capabilities the guidelines aim at. The guidelines are constituted of three essential components:

- The building blocks are the Concept Cards (CC). CCs propose practical interventions in order to develop and enhance the resilience management capabilities captured in the conceptual requirements.
- The guidelines build on the Concept Cards by organising and relating them, because the resilience management capabilities they refer to are not independent. The CCs are organised in themes (higher level capabilities) and related to each other as well as to basic functions of crisis management. This organisation of the guidelines allows for multiple ways of accessing their content, and anticipates the variety of needs and interests of the intended users.
- A knowledge management platform, the DARWIN Wiki, facilitates the development, management and use of the guidelines. The platform offers opportunities to reconsider common views on the nature of guidelines, their necessary evolution and their multi-faceted, multi-purpose content.

The presentation will give an overview of the nature of the guidelines developed by the DARWIN project, highlighting aspects of the development process such as the involvement of end-users to build and revise content and incorporate operational perspectives. A specific guideline associated with resilience assessment will be presented to illustrate the content (examples of concept, interventions proposed, associated content) and briefly show elements of the DARWIN Wiki.

1.6
European Resilience Management Guidelines and their adaptation for UTS (RESOLUTE)

E. Gaitanidou
Centre for Research and Technology Hellas / Hellenic Institute of Transport, Greece

Within the framework of the Horizon 2020 project RESOLUTE, the necessity for the provision of a set of generic guidelines has been recognized which would facilitate decision makers and managers in organizing Critical Infrastructure (CI) in a resilient manner, while considering resilience as a useful management paradigm, within which adaptability capacities are considered paramount.

This led to the creation of the European Resilience Management Guidelines (ERMG), aiming to support in the process of self-evaluation multilevel gap analysis for resilience improvement in respect to the status of the considered CI. Thus, the ERMG development has adopted a system's perspective, applying the Functional Resonance Analysis Method (FRAM) to model a generic CI and to identify which are the desired functions and the related interdependencies that should be implemented in a CI to be resilient. Then for each function identified, recommendations are provided on how to dampen function performance variability to continue delivering the desired outcome under any unexpected condition/event. The objective is to sustain the adaptive capacity of the system in continuously changing operational conditions and the coherent pursuit of goals within their own timescales.

The generic ERMG have also been adapted for the needs of the Urban Transport System (UTS), aiming to serve as a roadmap for addressing some of the vulnerabilities UTS is facing (aging infrastructure, extreme weather conditions, terrorist attacks). As resilience does not only involve recovery, UTS resilience is an overall concept, defining a complex transportation system able to better withstand disruptions. The transportation system includes physical, technical, social, and institutional elements that are all critical to resilience.

Session 2: Resilience assessment method and indicators: How to define them? How to monitor them? How to implement them?

Chairs: J. M. Sarriegi (TECNUN), F. Petit (ANL)

2.1
Assessing resilience based on the ISO/IEC 33000 standard series (IMPROVER)

R. Almeida
INOV, Portugal

The purpose of the process assessment process is to determine the extent to which the organization's standard processes contribute to the achievement of its business goals and to help the organization focus on the need for continuous process improvement.

The purpose of the ISO/IEC 33000 Process Assessment Standard series is to provide a structured approach for the assessment of processes. The key elements of the process assessment process are Inputs, Activities, Roles and Responsibilities, and Outputs. In this presentation we will define and explain these key elements, giving a concrete example a Water Supply System located in Portugal.

2.2
Which indicators can tell us if critical infrastructure is resilient? How do we know the ''quality of indicators''? (SmartResilience)

A. Jovanovic[1], L. Bodsberg[2]
[1]EU-VRi, Germany, [2]SINTEF, Norway

Candidate indicators that may be used when assessing, predicting and monitoring resilience of smart critical infrastructures have been collected throughout the SmartResilience project and stored in a database. Some examples on indicators for selected critical infrastructures and relevant threats will be presented, focusing on the "issues" (factors, capacities, capabilities, etc.) that are most important for measuring resilience. Issues and corresponding indictors are collected for each of the five phases of the resilience cycle, from understanding risk to adapt and learn. The quality of indicators will be discussed as there are many relevant "quality" attributes and criteria/requirements for indicators. However, no single indicator will fulfil all the different requirements, and what is relevant for one user may not be the same for another user. When reviewing, and selecting indicators, the user should consider quality attributes that are most relevant for him/her.

2.3
Indicators for assessing the resilience-building process in cities (SMR)

J. M. Sarriegi,
TECNUN (University of Navarra), Spain

The Resilience Maturity Model developed within the SMR project comprises five maturity stages (Starting, Moderate, Advanced, Robust, and verTebrate) to guide cities through the optimal path of building resilience. Each maturity stage contains a description of the objectives of that maturity stage, the stakeholders that need to be engaged and a list of policies that should be developed to achieve the objectives defined in that maturity stage. Furthermore, the Resilience Maturity Model provides a set of indicators for monitoring and assessing the performance of the policies. The indicators are useful for cities to carry out a diagnosis of their current maturity stage across four dimensions (leadership & governance, preparedness, infrastructure & resources, cooperation).

2.4
Assessing Resilience: from Facilities to Regions

F. Petit, D. Verner
Risk and Infrastructure Science Center, Argonne National Laboratory, USA

There is a strong agreement among the research community that the concept of resilience must play a major role in assessing the extent to which various entities—critical infrastructure facilities, systems, communities, and regions—are prepared to deal with the full range of manmade and natural hazards they face. As resilience assessment methodologies continue to be developed and implemented, it is critical that a framework be developed to (i) utilize measurements of resilience at multiple levels to characterize an entity's resilience to potential hazards and (ii) integrate interdependencies among entities. Argonne National Laboratory, in partnership with the U.S. Department of Homeland Security, has developed a resilience measurement index that applies at facility level and proposes an assessment framework to tie together top-down and bottom-up approaches in order to produce a comprehensive "system of systems" understanding that can inform regional resiliency assessment. Through the application of these measures, an entity can better understand its current resilience posture, as well as implement a systematic approach to reduce vulnerabilities and consequences of potential hazards. The objective of this presentation is to (1) introduce the resilience measurement index, (2) explain the assessment framework, and (3) discuss elements to consider for assessing resilience from facility-level to regional-level.

2.5
Exploiting SmartResilience indicators in RESOLUTE Resilience Assessment Framework (RESOLUTE)

E. Bellini
University of Florence, Italy

Quantify resilience is a challenge that needs to be addressed in particular to support decision makers with evidences when they trying to optimally allocate scarce resources to cope with emergencies or should decide on investments to enhance system resilience. In RESOLUTE project, the evaluation framework under development aims at defining new indicators or selecting existing ones, that can be used to assess the impact of the RESOLUTE ERMG adoption and technology deployment on the UTS resilience enhancement.

In particular, since in RESOLUTE the UTS has been modelled as a number of functions and their interdependencies according to the FRAM approach, the selected KPIs should be relevant and suitable to show the performance variability of each function. The amount of variability damped by a function and the system as a whole through the adoption of RESOLUTE outcomes, is a quantitative metric that can reflect the resilience level of the system.

The KPI creation and selection process was organised in 2 sessions. The first one followed the following criteria:

a) pertinence with the UTS function under analysis (assessed with stakeholders);

b) actual measurability of the indicator (data/information availability, measurement costs, etc.) ,

c) sensitivity (capability to show a function performance variability).

Thus for most of the functions included in the UTS reference model of the RESOLUTE ERMG, one or more KPI have been associated.

The second session was about the KPI acceptability check. This was based on community agreement or standards adoption.

In particular, the acceptability based on standard adoption, has benefitted of the result of the Smart Resilience project. In fact a number of indicators identified in the first session has been replaced with others collected by the Smart Resilience project when they were considered semantically and substantially similar. Because of the Smart Resilience indicators database has been populated by end-users and stakeholders, their usage represents a solid background for the evaluation framework validaiton.

Session 3: Tools and methods for resilience operationalization

Chairs: M. Branlat (SINTEF), I. Kozine (Technical University of Denmark)

3.1
The RESILENS Toolkit – Decision Support for CI operators and owners (RESILENS)

G. Rafaeli
MTRS3 Solutions and Services LTD, Israel

This presentation will focus on the implementation of the resilience concept developed under the RESILENS project in the form of critical infrastructures resilience assessment and audit tools; and guidelines for critical infrastructures organisations on resilience management. Using visual tools, the presentation will illustrate the range of deliverables developed as part of the project, providing a clear picture of progress to date in finalizing the ERMG and the toolkit. As part of this, the presentation will also demonstrate progress towards the development of a RESILENS Decision Support Platform (RES-DSP), an interactive web based platform which will host the RESILENS toolkit and e-learning hub.

3.2
A web tool for assessing resilience using any framework (IMPROVER)

R. Almeida
INOV, Portugal

A resilience assessment tool was designed and is being developed for supporting the application of the methodology developed within the Improver project. The tool not only supports the methodology developed in Improver but also other frameworks such as or RMI.

In this presentation, we will demonstrate the tool taking into account an example based on a Water Supply System located in Portugal

3.3

Evidence-driven Collaborative Resilience Assessment and Management Support System for Urban Transport System, A VA Platform for Personalized Crowd, Fleet & Resources Management (RESOLUTE)

P. Nesi[1], A. Drosou[2]

[1] University of Florence, Italy , [2] Centre for Reasearch & Technology Hellas / Information Technologies Institute, Greece

Evidence-driven Collaborative Resilience Assessment and Management Support System for Urban Transport System

Resilience of complex systems is about managing high variability and uncertainty in order to continuously pursue successful performance of a system. The aim is to deliver management guidance on human, technical and organizational resources, aiming to respond to different and possibly conflicting local operational needs ensuring successful operation. In the case of Urban Transport Systems (UTS), operations have developed a prominent safety and business critical nature, in view of which current practices have shown the evidence of important limitations in terms of resilience management and operationalization. To tackle this challenge three fundamental steps have been followed: (i) Sociotechnical System Analysis and Understanding in support of the identification of UTS critical aspects and functions using the Functional Resonance Analysis Method, (ii) (Big) Data Gathering, data analytics, semantic processing and mining for connecting multi-sources data flows to the models, (iii) development of a new generation of data driven Control Room and Decision Support Systems exploiting big data in an intelligent and fast way a human cannot do in reasonable time. A pilot of these concepts has been realized for the Florence (Italy) Urban Transport System and environment. The whole solution is accessible via its Control Room Dashboard with it CRAMSS (Collaborative Resilience Assessment and Management Support System). The CRAMSS is primarily a concept of a collaborative workspace in which different DSS operators can share their outputs of or information about their daily work among each other. This work has been supported by the RESOLUTE project (www.RESOLUTE-eu.org) and has been funded within the European Commission's H2020 Programme under contract number 653460.

A VA Platform for Personalized Crowd, Fleet & Resources Management

Physical disasters and the increased international terrorism cost the loss of many lives every year. Thus, in such cases, the immediate response of the responsible bodies and/or the immediate evacuation of the affected areas are of vital significance. Additionally, the accurate information of the population is crucial in order to avoid the confusion of the population and keep the resilience of a community

This presentation deals with a modular platform that processes and seamlessly fuses various information, such as traffic and weather data, emergency events and flood susceptibility map, providing decision support services and information. The platform can be serve the needs of both Urban Transport authorities and citizens, facilitating thus, an efficient management of the Urban Transport System (UTS) and real-time applicable countermeasures in critical situations (e.g. evacuation planning, etc.), as well as the accurate information of the population. The platform consists of three main components, the evacuation Decision Support System (eDSS), a web application for the Urban Transport authorities and an intuitive mobile app for the citizens that share the same back-end.

Contrary to the existing safety systems the proposed system dynamically co-processes the effect of the event over the urban transport network and the mobility profile (e.g. driver, pedestrian, age, impairments, etc.) of each individual related actor providing personalized and group-wised evacuation guidelines through the mobile app, as well as guidelines for the rescue team action planning.

Sample evacuation scenarios:

1. Citizen in Danger Evacuation

The ESSMA user sends a SOS message to the operator, requesting path to safe point. The CRAMSS operator receives the SOS message and set the safe point. Following that, requests for evacuation route from the eDSS. Once the evacuation plan is generated, the ESSMA user receives the route. During the evacuation the operator communicates through chat with the ESSMA user.

2. Groups of Citizens Evacuation

The CRAMSS operator uploads an image of an emergent event to the live updates and the ESSMA users are informed through the ESSMA about the event. The CRAMSS operator selects the areas to be evacuated in which the two groups of ESSMA users are located. Additionally, the CRAMSS operator marks two safe points & requests for evacuation plan from the eDSS. Upon receipt, the paths are sent to the ESSMA users that follow the guidelines to the safe points.

3. Collaborative Rescue Action

The citizen (ESSMA user) in danger presses the SOS Button in the ESSMA app. Their location appears to both the CRAMSS operator's and the voluntary helpers' screens. The CRAMSS operator starts a "Collaborative Action" by asking the availability of all potential helpers (rescuers). A voluntary helper (rescuer) responds their willingness to help and the available rescuer appears to the CRAMSS operator. The CRAMSS operator requests for rescue plan from the eDSS and send it to voluntary helper. In addition, a message appears to ESSMA user, informing that the helper is on the road. Finally, the helper reaches the citizen and the citizen declares that they are safe.

3.4
Why and how to use Interactive data visualization in resilience related projects? (SmartResilience)

U. Barzelay
IBM Research, Israel

A picture is worth a thousand words but a good visualization is worth more: Data visualization is the preferred way of user to access complex data and is considered as enabler for reasoning and decision making.

Raw data becomes useful when it is being visualized by mapping information to visual attributes such as size, color and shape. When mapping the raw data to visual elements, the data is obviously transformed and can be distorted and become misleading, but when the process is done carefully, the outcome of the visualizations can be used to provide insight that else would have been very difficult to come by and therefore it can assist the human expert to achieve his task.

By relying on human capabilities such as perception and domain knowledge, Interactive data visualization lets users to interactively explore the data and generate hypotheses while leveraging traditional methods from knowledge discovery data mining, artificial intelligence, statistics and mathematics.

In this talk we'll explore in high level WHY should one invest efforts in data visualization and WHAT are some of the resources that are available to us if we choose to incorporate data visualization to our project. In addition, we'll show a sample of a visualization that was crafted to explore raw data in the domain of resilience indicators as part of the SmartResilience project.

3.5
Overview of the resilience tools developed and their intersections (SMR)

C. Grimes
ICLEI – Local Governments for Sustainability, European Secretariat, Germany

The Smart Mature Resilience project held a European Workshop on Resilience in Cities and Communities in April 2017 for an audience of cities. As part of this workshop, the European-funded projects SMR, DARWIN, IMPROVER, RESILENS, RESOLUTE, RESCCUE and RESIN presented their tools to the cities assembled. In a parallel session, the tool developers compared their tools and relevant tools from related projects and their potential applications. Smart Resilience contributed their list of tools following this event. The outcome of this collaboration was collected in a table, which will be briefly presented in order to provide a context for the presentations during this session. The tools are categorised under the following headings: Definition, Strategy, Evaluation, Training, Implementation, Simulation and Others, and intersections between projects and categories are taken into consideration.

3.6
Capabilities-based approach to building and maintaining resilience

I. Kozine
Technical University of Denmark, Denmark

An approach to assessing critical infrastructure (CI) resilience will be presented. The approach was developed as part of EU project 'Resilience Capacities Assessment for Critical Infrastructures Disruptions' (READ) that was co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-Related Risks Programme, European Commission – Directorate-General Home Affairs. The approach is capabilities-based meaning that the key element of it, which is subjected to the analysis, is a resilience capability. A capability is defined as a combination of assets, resources and routines specifically arranged to accomplish a critical task and assure a key objective. The capabilities are grouped into clusters according to a resilience phase (preventive, absorptive, adaptive and restorative) where they are invoked; and according to a system type (technical, operational, social, and economic) which they belong to. Each capability is attributed a score reflecting its current capacity, which in turn is compared to a target resilience score. In this way, a resilience gap analysis is carried out that provides input to informed resource allocation and operation when planning to cope with CI disruptions. A software tool has been developed to apply the approach in a user-friendly environment. A test case exemplifying the use of it in the context of regional public-private collaboration for CI resilience in the Lombardy Region (Italy) will be provided.

Session 4 Application cases – where the newly developed methods, guidelines & tools have been implemented/ analyzed?

Chairs: Z. Szekely (BZN), K. Pala (AUTOMOTIVE STRATEGY EUROPE LTD)

4.1
The RESILENS Pilot Demonstrations – Testing the Toolkit across three CI Sectors in Ireland, Portugal and Germany (RESILENS)

A. Corrigan
Eastern & Midland Regional Assembly (EMRA); Ireland

The central outputs of the RESILENS project - The ERMG, the ReMMAT and the components of the RES-DSP - were tested and validated through stakeholder engagement, table-top exercises and three large scale pilots (transport CI, electricity CI and water CI) across three national contexts – in Ireland, Portugal and Germany. There were three primary aims with regards the pilot testing phases, as follows:

- To operationalise, evaluate and validate the draft ERMG & ReMMAT and to do this in as close to real-world conditions as possible.
- To transpose the principles and lessons learned from the Pilot Demonstration to the improvement of ERMG, ReMMAT and processes associated with their use.
- To enhance European critical infrastructure resilience management and coordination at varying spatial scales and at sectoral, societal and organisational levels

This presentation provides an overview of this process and demonstrates some of the key learning outcomes which have emerged from these testing exercises.

4.2
RESOLUTE: Florence pilot case study (City of Florence)

E. Bellini
University of Florence, Italy

The city of Florence is the most populous city in the region. It was declared an UNESCO World Heritage Site in 1982 due to its artistic heritage, being noted for its history, culture, Renaissance art and architecture and monument. So Florence is invested by broad touristic flow, with more than 12,000,000 visitors every year. Moreover its medieval structure characterized by narrow streets in the downtown, the increment of the extreme events like flash flooding or wind storm, the presence of several rivers, etc. increases the impact on the mobility of expected and unexpected critical events.

Within the RESOLUTE project, the Florence Municipality investigate four main scenarios for analysing the main city assets related to resilience of Urban Transport Systems:

1) The 200 years-probability Arno river flooding - This is the 200-years return probability event of Arno River flooding, with huge consequences on the City.

2) 30 years-probability Arno flooding- This is the 30-years return probability event of major and minor-rivers flooding. The main interested areas for this event are the Arno river (over Argingrosso zone), and Mugnone, Ema and Greve minor rivers.

3) Arno flood impact on tram line: This scenario is particularly significant with respect to tram line behaviour and usable assets during emergency (such as tram stop signage and audio messages on-board).

4) Water bomb in South Florence: This scenario is particularly significant with respect to specifically focused events (such as flash-floods/water bombs) and traffic re-routing.

Each of the above scenarios contains specific elements that are useful to design a suitable RESOLUTE pilot in Florence. In particular, a stronger cooperation within the municipality offices and among public and private Florentine organizations has been established. Official procedures as well as unofficial personal contacts have been created among different operators to speed up the communication, to share data or to coordinate the investment of different municipality departments towards solutions useful for enhancing city resilience (e.g. extension of public wifi in the city). Moreover, thanks to RESOLUTE, has been conducted a survey during a Civil protection exercise in the city that has increased the awareness of the authority about the level of preparation of the population. In fact only 20% of responders stated that they feel prepared to cope with an emergency; and 34% of the citizens claimed that they tend to follow their own heuristics instead of the official communications during the emergency. Only 6% of the responders indicated their willingness to adapt their behaviour according to the instructions provided by the authorities. Another interesting result of the questionnaire was related to the utility of the civil protection exercise in the area, as perceived by the citizens. 86% of the responders did not consider such exercise useful to increase their preparedness and safety. Such preliminary results reveal the existence of a critical issue at the community level towards the authorities devoted to deal with emergency situations. In turn, this status leads to apparent contradictions. In fact, citizens overestimate their own capabilities to cope with an emergency, leveraging personal experiences, while they admit the lack of preparedness. This result may suggest that citizens consider their low level of preparedness more reliable than the authority's capability to respond and manage the event. In this respect, the Municipality has decided to take into account the result of the questionnaire, and according to the RESOLUTE guidelines (that stress the fact that the people/citizens are an asset to be considered in resilience policy implementation), they decided to invest resources in programs to teach right behaviors during the emergency starting from the primary schools.

4.3
Case study DELTA and the significance of the SmartResilience project for the aviation security sector (SmartResilience)

Z. Szekely[1], I. Macsári[2]
[1]Bay Zoltan Nonprofit Ltd. For Applied Research, [2]Hungarian National Police, Hungary

The air transportation sector is the service provider of the world's leading transport modality in terms of people served. With 35.4 million flights and 3.5 billion passengers it earned 702 billion USD in 2016. Airports are the most important critical infrastructures of this sector. There are not mere airfields any more, Airport 2.0 generation merged airports with shopping, food, beverage and leisure facilities, Airport 3.0 generation focuses on automation, real-time stakeholder and passenger information as well as proactive operations based on the Internet of Things. These airports are the first representatives of "Smart Airports" and be the first Smart Critical Infrastructure in this sector. The next generation is expected in 10-15 years and will be Airport 4.0, the fully digital airport, smart, robotized, allowing seamless flow of passengers, pre-arrival security and border checks, biometric passenger identification, dynamic pricing, online duty free etc. But increased numbers and quality of digital services shall not result in increased vulnerability and decreased resilience. However, measuring resilience and selecting appropriate actions is different at a Smart Airport. Therefore, is the SmartResilience project dedicated to find new indicators to assess resilience of these new dimensions of service and operation. Hungary is participating in the project with providing a testbed with a set of scenarios, called DELTA and performed at Budapest Airport with 1000 participants.

4.4
Local Resilience Planning: A review of methodologies adopted for the SMR pilot implementation process (SMR)

V. P. Latinos
ICLEI Local Governments for Sustainability, European Secretariat, Germany

Municipalities play an integral part in building resilient communities and societies, which are not only prepared for short-term shocks, such as natural disasters, but also successful in mastering long-term stresses related to socio-economic challenges. The public sector often tends to rely on sectoral approaches and fails to involve relevant stakeholders in a broader co-creation process for resilience and sustainability. Cross-sector collaboration is the key for cities to overcome climatic and social challenges. It comprises both internal collaboration within a municipality and involvement of external stakeholders. The project aims at developing a European Resilience Management Guideline, including 5 tools: a maturity model for assessing a city's level of resilience, resilience policies to help a city to enhance resilience, a risk systemicity questionnaire supporting a self-assessment of vulnerabilities, a system dynamics model for simulating achievement towards resilience, and an information portal that promotes stakeholder/citizen engagement/communication. In order to co-create the tools having always the valuable input of city stakeholders, 5 pilot processes took place in the three tier-1 CITIES of Kristiansand, Donostia/ San Sebastian and Glasgow. The process was peer-reviewed by the four tier-2 CITIES Bristol, Vejle, Riga, and Rome. During this period, partners and representatives had the chance to explore and validate both tools in the security sectors that were already identified and to provide input to the developers for the finalization of the tools. In this presentation, we present key elements for cross-sector collaboration, which were extracted from the implementation process.

4.5
Pilot application in Sweden involving among others health care, public sector and transport services (DARWIN)

P. Berggren
KMC, Sweden

The DARWIN project aims to develop state of the art resilience guidelines and innovative training modules for crisis management. As a part of the resilience guidelines and training modules the DARWIN concept cards have been developed. In Linköping, the DARWIN project ran an exercise following a training in the operationalisation of the concept cards. The concept cards reflect different aspects of resilient behaviours and provide training directives. These concept cards have been developed in close cooperation with the DARWIN Community of Practitioners (DCoP).

The DARWIN pilot exercise in Linköping was a data collection opportunity where the concept cards could be tested during an exercise with personnel acting in their professional roles. The scenario involved an accident concerning a cruise liner with approximately 2000 passengers and a crew of 800 persons. A fire started on the ship while on Swedish waters, ca 100 km from Stockholm and 60 km from Norrköping. The exercise concerned the medical regional staff and governmental agencies, municipalities and other actors involved in crisis response (i.e., police, Maritime Search & Rescue, fire departments, ambulance services etc.). Main focus was the response of the medical regional staff manned with ca 8 persons, while the scenario in total required ca 40 persons to participate in the execution of the exercise (including research personnel for assessment and controlling scenario development. The scenario was run for ca 6 hrs. In addition to the evaluation of the assessment cards, several dependent measures were used, for example patient outcome, transportation times, use of procedures, coordination and information exchange between different actors, etc. Several technical platforms were used to control and monitor scenario development, i.e., Emergo Train System, Netscene, and F-Rex.

The preparation and planning of the DARWIN pilot in Linköping has been a major event, especially the adaptation of the concept cards towards national and regional requirements and demands. Another major effort has been the training of the involved personnel to be able to use the concept cards during the exercise. This training has been carried out over several occasions with a two-fold purpose: to train the personnel and to adapt the concept cards to contextual requirements. This has been an iterative and interactive process. As the participant have gained a better understanding of the concept cards they have been able to explain how national and regional demands affect the execution which in turn affect the use of the concept cards.

Session 5: Importance of international/global cooperation in the area of resilience – How to enhance it in the future?

Chairs: A. Jovanovic (EU-VRi), S. Jacobzone (OECD)

5.1
US DHS views on critical infrastructure resilience

W. R. McNamara
U.S. Department of Homeland Security, USA

The U.S. approach to advancing critical infrastructure security and resilience is based on voluntary partnerships between government and private industry. This approach recognizes that it is infrastructure owners who must take action and make investments that improve security and resilience. The U.S. government's primary role is then to coordinate action and provide critical infrastructure owners with resources that help them make the most informed risk management decisions. Many features of the modern infrastructure landscape, such as its increasing complexity and connectivity, present challenges to building resilience. The nature of infrastructure resilience itself, influenced as it is by dependent relationships among distinct systems, limits the ability of organizations to achieve desired levels of resilience on their own. Addressing these challenges to building infrastructure resilience requires a program that effectively combines partnership building and technical assistance at a regional level. To address this need, the U.S. Department of Homeland Security, which leads the national effort to secure and make resilient U.S. critical infrastructure, has developed the Regional Resiliency Assessment Program. This program conducts regional infrastructure assessment projects in collaboration with government and private industry partners with the goal of generating greater understanding and cooperative action to improve the resilience of the region's infrastructure

5.2
Application of resilience concepts: the case of critical infrastructure

S. Jacobzone
OECD, France

The OECD has identified the area of critical infrastructure as a priority for further investigating policy analysis that is geared to improve resilience and reduce the vulnerabilities associated with critical risks. The presentation will highlight the challenges in making critical infrastructure system resilient and the range of policy tools that are available to government, including incentives, regulation, financing and peer pressure. Developing partnerships with the private and infrastructure sector requires institutional leverage as well as appropriate institutional set ups. The presentation will highlight the role of critical infrastructure strategies, and corresponding implementation plans, and the need for risk vulnerability and interdependency assessment. It will discuss options for mitigating societal impacts, and the role of exercises ex ante, and post event reviews of lessons learned. As this is an area where further investment is needed, the presentation will open the way for future partnerships, the development of a set of case studies, across sectors or countries with a view to further identifying good practice.

I. Linkov
Carnegie Mellon University, US Army Engineer Research and Development Center

This presentation will review the history of risk assessment and management in the USA, discuss the emergence of resilience management, and the role of both constructs in addressing emerging risks. At the policy level, Resilience was a priority for Obama administration, especially in the context of climate change. Trump's administration is shifting the focus from climate change towards cyber and supply chain resilience, as it is reflected in recent Executive Orders. A major resilience impediment includes the lack of science of resilience, especially as it relates to assessing risks. Risk and Resilience are often used as synonymous even though they have a very different meaning, Risk-based approaches have been used to assess threats and mitigate consequences associated with their impact. Risk assessment requires quantifying the risk of failure for each component of a system and associated uncertainties, with the goal of identifying each component's contribution to the overall risk and ascertaining if one component poses substantially more risk than the others. These components become the basis of quantitative benchmarks for the system, and becomes the de facto standard for system improvements designed to buy down risk. In contrast to the definition of risk, resilience is focused on the ability to prepare and recover quickly from threats which may be known or unknown. Resilience is a property of the system itself and can be measured without identification and assessment of threats which act on or within a system. Managing for resilience requires ensuring a system's ability to plan and prepare for a threat, and then absorb, recover, and adapt. Coupled with a systems view that decomposes components across physical, information, cognitive, and social environments in which the system exists, is the basis of an approach to quantifying resilience with decision analytical tools and network science approaches.

I will present case studies of resilience assessment in the areas of infrastructure, transportation, cybersecurity, and organizational behaviour using tools of decision analysis and network science. In all the cases, rapid technological evolution, combined with the unprecedented nature and extent of emerging threats defy us to enumerate all potential hazards, much less estimate reliable probabilities of occurrence and the magnitude of consequences. A comprehensive approach to protecting the nation's critical infrastructure, economy, and well-being must be risk based—not risk exclusive—and must provide a way for decision makers to make their organizational systems resilient to a range of threats within specific cost and time restraints.

5.4
Resilience Indicators and Interdependencies: Need to Promote a Global Approach

F. Petit, D. Verner
Risk and Infrastructure Science Center, Argonne National Laboratory, USA

Policy and standard documents from the strategic level through the operational level require the consideration of interdependencies that can exist among infrastructure and how they affect business continuity, security, and resilience management. Furthermore assessing infrastructure protection and resilience requires consideration of many interconnected socioeconomic, ecological, climatic, and technical elements. These interconnections mean that disruption or failure of one asset can lead to cascading failures in others. Interdependencies among infrastructure systems lead to a level of complexity that masks many systemic risks. As a result, an impact to a single node or link—the proverbial "single point of failure" that is often hidden deep within these interconnected systems—can result in important economic and physical damage on a city-wide, regional, or even national or international scale. Therefore, assessing and managing resilience from facility to regional level require considering trans-jurisdictional and cross-borders consequences resulting from the management and operations of critical infrastructure facilities. This presentation specifically addresses (1) how resilience assessment tools and approaches developed for the United States have been adapted to be used in Canada and Europe, and (2) discuss the need to increase international collaboration to enhance the protection and resilience of critical infrastructure.

5.5
The role of local and regional networks and partnerships in resilience building (SMR)

C. Grimes
ICLEI – Local Governments for Sustainability, European Secretariat, Germany

Resilience-building cannot be comprehensively addressed without cross-sectoral, multi-level and international cooperation and collaboration. As resilience and risk involve and affect a broad range of systems and stakeholders across borders and scales, a holistic approach is crucial. For this reason, one of the objectives of the SMR project is to build a group of resilient cities that can support one another and other cities around the world. SMR aims to build cities' capacity to be able to function as robust resilience hubs in their regional and national networks and as resilient elements in the systems of which they are part. As part of SMR, three core project cities (Glasgow, Kristiansand, San Sebastian) have exchanged real examples, strategies, experiences and opinions regarding how resilience management works in their local contexts with a second group of cities (Bristol, Riga, Vejle and Rome), which will during the final year of the project, exchange this knowledge with a third and fourth group of cities.

This peer exchange and sharing of information is already happening in many partnerships and groupings between cities globally. One of these active city groupings is ICLEI – Local Governments for Sustainability. ICLEI forges strategic partnerships with international organizations, business, academia and financial institutions and designs ways for local and sub-national governments to team up with civil society, local businesses and all levels of government. Further notable local and regional partnerships include the 100 Resilient Cities campaign of the Rockefeller Foundation, of which three SMR cities are part, and the Resilient Cities Connect programme of the UNISDR.

5.6
Enhancing International Collaboration through DARWIN's Community of Practitioners (DARWIN)

J. Kieran
Carr Communications, Ireland

DARWIN aims to build resilience management guidelines that will support organisations in developing and enhancing their resilience in the context of crisis management. To improve international collaboration, cross-sector applicability, and the long-term relevance and uptake of the DARWIN project results, a Community of Crisis and Resilience Practitioners (DCoP) was established. This is a constantly growing, active community that brings together end-users in the fields of resilience, crisis management and emergency response, as well as healthcare and air traffic management. There are currently approximately 100 members from 14 countries across Europe, and beyond.

The DCoP is actively involved in an iterative development and evaluation process, ensuring that the resilience guidelines are relevant and user-friendly. Its members share knowledge, practices and experience with the DARWIN consortium to improve the project's developments. They have participated in surveys, interviews, workshops and innovation games providing suggestions to improve usability and facilitate future up-take of project results. Online collaboration within the DCoP was developed to overcome geographical and travel cost barriers, as well as constraints on practitioners' time. Through interactive meetings, webinars, and an online forum, DARWIN can reach a wider community to exchange knowledge and experience.

Session 6: Alignment of the Resilience Workshop findings/items with IMG-S - EARTO WG Security Research approach

Discussion moderator: C. Fuggini

The IMG-S – EARTO Joint Position Paper on Resilience in Security Research will be presented in this session. The document is published by the Integrated Mission Group for Security (IMG-S) and the Security Research Group (SRG) of the European Association of Research and Technology Organisations (EARTO) as a joint position paper on Resilience in Security Research, being in line with the objectives of the H2020 Secure Society Work Programme and other relevant actions and initiatives in the sector, taking into account the need to link security research to capacity planning and capability insertion for resilience. The paper provides the initial concepts and guidelines on Resilience, while a set of position papers addressing specific aspects (e.g., Resilience of Critical Infrastructure, Resilience of Soft Targets, Resilience of the Supply Chain, Resilience of Communities, etc.) will follow.

In this context, the overarching aims of the Position Paper are:

- To establish the resilience paradigm as an efficient aspect in the security culture and adapt the design of socio-technical systems in terms of protecting critical services and strengthen society's adaptation to new and emerging threats and hazards;
- To address the topic of Resilience in the context of the European Security Research, with a focus on how to potentially deliver harmonized policies and technologies, which can promote the take-up of best-practices and operational resilience procedures, aiming to cope with current and emerging risks;
- To define a common language that will facilitate and support common understanding, perception, and modelling of Resilience;
- To arrange and organize actual knowledge to develop and encourage a consensual view on the concept of Resilience and to investigate Resilience strategies and approaches, strengthening cooperation and collaboration among stakeholders and Communities, aiming to tackle emerging societal challenges on security in a common, agreed and harmonized way.

SHORT COURSE:
"Indicator-based resilience assessment for CIs - the SmartResilience methodology and tools"

K. Øien[1], A. Jovanovic[2], F. Petit[3]
[1]SINTEF, Norway, [2]EU-VRi, Germany, [3]ANL, USA

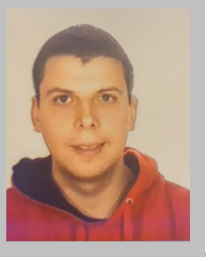
This course provides a lecture on indicator-based resilience assessment with focus on the developments in the SmartResilience project. The course describes step-by-step how to perform resilience assessments in a transparent and structured manner for one or more critical infrastructures within an area, e.g. a city. The most relevant threats, such as terrorist attacks and cyber-attacks, are assessed for each critical infrastructure focusing on the "issues" (factors, capacities, capabilities, etc.) that are most important to ensure resilience in each phase of the resilience cycle from understanding risk to adapt and learn. The issues are measured by resilience indicators, and any type or form of indicators are considered appropriate, meaning that it can be yes/no questions, numbers, percentages, portions, or some other type. Proposals for issues and indicators, i.e. "candidate" issues and indicators have been collected throughout the SmartResilience project and stored in a database. Suitable sets of indicators for selected critical infrastructures and relevant threats are generated as "dynamic checklists" from the database. This and other supporting tools will be explained in the course. One key reference method forming the basis for the SmartResilience methodology (in addition to the REWI method) is the method developed by ANL and extensively used in the US. The ANL method will be presented by one of its core developers.

Profiles of
Keynote Lecturers and Plenary Panelists

(in alphabetical order)

Mr. Rafael Almeida

www.tecnico.ulisboa.pt
rafael.saraiva.almeida@gmail.com



Rafael Almeida is currently enrolled in the Doctoral Program in Computer Science and Engineering at Instituto Superior Técnico, Lisbon. His main area of research is related with Enterprise Governance of IT (EGIT). He uses modeling techniques to model and to integrate different EGIT Frameworks such as COBIT and ITIL.

Previously, he worked in the largest Portuguese telecommunications company.

Rafael Almeida is author or co-author of 9 scientific papers, including: Almeida, R., Linares Pinto, P., and Mira da Silva, M. (2016). Using ArchiMate to Integrate COBIT 5 and COSO Metamodels. 13th European Mediterranean & Middle Eastern Conference on Information Systems (EMCIS 2016), Krakow, Poland.

Almeida, R., Linares Pinto, P., and Mira da Silva, M. (2016). Using ArchiMate to Assess COBIT 5 and ITIL Implementations. 25th International Conference on Information Systems Development (ISD 2016), Katowice, Poland.

Almeida, R., Linares Pinto, P., Lourinho, R., and Mira da Silva, M. (2017). Using Visual Models for Adopting IT Governance Practices. COBIT Focus, ISACA.

Lourinho, R., Almeida, R., Linares Pinto, P., and Mira da Silva, M. (2017). Mapping of Enterprise Governance of IT Practices Metamodels. 14th European Mediterranean & Middle Eastern Conference on Information Systems (EMCIS 2016), Coimbra, Portugal.

Percheiro, I., Almeida, R., Linares Pinto, P., and Mira da Silva, M. (2017). Towards Conceptual Meta-Modeling of ITIL and COBIT 5. 14th European Mediterranean & Middle Eastern Conference on Information Systems (EMCIS 2016), Coimbra, Portugal

Mr. Udi Barzelay

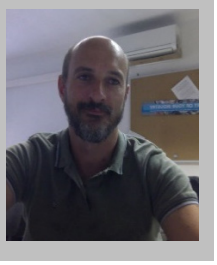
www.ibm.com
UDIB@il.ibm.com

Udi Barzelay is a research staff member in the IBM Research Lab, and a team leader in the multimedia analytics department where he develops cognitive analytics and solutions for the multimedia domain. He received his B.Sc. degree in Computer Science from the Technion – Israel institute of Technology and has been working at IBM since 2006.

Udi's experience focuses on software engineering and includes full software lifecycle, from idea inception, to system architecture, design and implementation, usually in a form of scalable cloud systems. Recently he is motivated with designing and implementing effective interaction for video data using IBM's Watson cognitive analytics services such as visual recognition, speech transcript, video scene detection, natural language understanding, and more, and then combing the analytics results together with interactive data visualization to help media companies and advertisers better target their video content.

Dr. Emanuele Bellini

www.disit.org
emanuele.bellini@unifi.it



Emanuele Bellini Ph.D. is senior research fellow and project manager at the University of Florence (Italy) - DISIT Lab (http://www.disit.org). He is the coordinator of H2020-DRS7-RESOLUTE project. He is an expert in risk and resilience of complex socio-eco-technical systems, human reliability, cognitive systems, decision support systems. He is collaborating in several risk and resilience working groups IETF, ESRA-TC-Risk Assessment and TC-Human Reliability and human Factor, CEN WS/88, etc.

Dr. Peter Berggren

www.regionostergotland.se/kmc
peter.berggren@liu.se

Peter Berggren has a PhD in Cognitive Science from Linköping University and a M.A. in Cognitive Science (Linköping University). He is employed as Research coordinator at the Centre for Teaching and Research in Disaster Medicine and Traumatology at the unit for the International Medical Program (KMC/IMP). Peter also holds a Senior Research Engineer position at the Department of Computer and Information Science, Linköping University (LiU/IDA). Previously Peter held the position as Senior Scientist at the Swedish Defence Research Agency (FOI).
His work has mainly concerned research projects within the human factors area. Main interests are team cognition, shared understanding, command and control, resilience, workload, performance assessment, situation awareness, decision making, crisis response and emergency management. Peter has co-editored a book on assessment of command and control.

Dr. Lars Bodsberg

www.sintef.no
Lars.Bodsberg@sintef.no

Lars Bodsberg, PhD is Senior Scientist at SINTEF Safety and Mobility. He was previous Research Director for SINTEF Safety Research. His main competence is within resilience engineering, process safety, risk indicators and risk control methods, risk and reliability analysis, and human and organizational factors. He has been Area Manager of Safety and Environment in 'Centre for Integrated Operations in the Petroleum Industry'. He is past president for ESRA Norway and SRA Europe

Dr. Matthieu Branlat

www.sintef.no
Matthieu.Branlat@sintef.no

Dr. **Matthieu Branlat** is Senior Scientist at SINTEF Digital (Trondheim, Norway), in the department of Systems Engineering, Safety and Security. He received a PhD in Cognitive Systems Engineering from the Ohio State University (USA) in 2011, and his background is in cognitive ergonomics and computer science. His thesis explored core functions, challenges and trade-offs associated with cyber security, through the investigation of decision making in cyber attack, cyber defense, and their interplay in the context of a day-long red vs. blue exercise. His research explores ways to contribute to the knowledge and improvement of socio-technical systems, particularly in high-risk environments. Themes of investigation include resilience engineering and system safety, decision-making, collaborative work, cross-cultural competences and the design of technology to support human operations. He has contributed to various publications in the fields of Resilience Engineering and High Reliability Organization. Recent and on-going projects are conducted in domains such as crisis response; air traffic management; military operations; intelligence analysis and cyber security; medical care and patient safety. He currently leads the development of resilience management guidelines (WP2) in DARWIN H2020 project. He also participates in SESAR 2020 projects PACAS (Participatory Architectural Change MAnagement in ATM Systems – system modelling activities) and PJ05 (validation of the Multiple Remote Tower concept against issues of network quality and cyber security).

Mrs. Andrea Corrigan

www.emra.ie
acorrigan@emra.ie

Andrea Corrigan has over 15 years of experience in environmental management, sustainable development, regulation and business support roles. She holds a BSc. in Environmental Science and MSc. in Environmental Protection. She has also completed post-graduate studies in Rural Development, Environmental Management and Client Business Development. In 2017, Andrea joined EMRA (Eastern and Midland Regional Assembly) to take up the post of RESILENS Project Officer. Her role to date has been concentrated on the successful completion of the Pilot Demonstrations (Work Package 4), in which EMRA was Lead Partner. EMRA is part of the regional tier of governance in Ireland, primarily focused on strategic planning, EU programming and funding, and coordination of certain local government activities. Based in Dublin, EMRA is one of three Regional Assemblies in the Republic of Ireland. EMRA's role as Lead Partner of Work Package 4 was to plan and manage the operationalisation, evaluation and validation of the RESILENS ERMG and Toolkit with our Critical Infrastructure (CI) partners. Andrea brings experience to the project from previous posts within public and private sectors, in Republic of Ireland and Northern Ireland. Prior to joining EMRA, she was employed by Enterprise Ireland, based in Local Enterprise Office Cavan and working with Cavan County Council. During that time, she contributed to various EU funded, cross-border, regional and international enterprise development projects. Her preceding role as Industrial Research and Development Associate on the INTERREG IVA CREST project (Centre for Renewable Energy and Sustainable Technologies) was aimed at providing R&D support to SMEs in the border region of Ireland. Formerly, Andrea was employed by Northern Ireland Environment Agency working in industrial pollution prevention and control, licensing, regulation and guidance. Earlier in

her career she worked with an SME on an EU LIFE funded waste to energy project, and also spent several years working in consultancy.

Dr. Anastasios Drosou

www.iti.gr
drosou@iti.gr

Dr **Anastasios Drosou** works as a postdoctoral Research Associate for the Information Technologies Institute of the Centre for Research & Technology Hellas, since January 2009. He received his Diploma in Electrical and Computer Engineering, from Aristotle University of Thessaloniki, and his MSc. In Communication Electronics from the Technische Universität München in 2004 in 2007, respectively. He also holds a PhD in Signal and Image pro-cessing from the Imperial College London since 2013. Up to day, he has participated in both the management and the Research & Development of several research projects, including both national (GSRT) and European funded ones (6th & 7th Framework Programme; H2020). His prior professional experience includes employments as Research Assistant for the both the Chair for Electronic Design Automation and the Chair for Nanotechnology in the Technische Universität München. Moreover, in the past he has worked for Infineon Technologies AG. Munich for more than a year in total, while earlier he has also served as Research Associate for both CERTH-ITI and the Art Diagnosis Centre “ORMYLIA”.

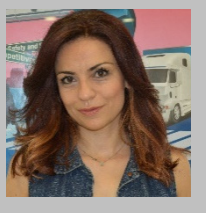
Dr. Clemente Fuggini

www.rinaconsulting.org
clemente.fuggini@rina.org

Clemente Fuggini is a PhD from University of Pavia. During its academic period, he was also lecturer in Risk (earthquakes, floods and wind), Vulnerability and Safety Analysis of buildings and infrastructures. He is currently responsible for R&D&I activities of Rina Consulting (formerly D’Appolonia) in the areas of infrastructures & the built environmental, security & space, as well as for the integration of R&I capabilities in these areas within RINA Group branch companies. In Rina Consulting he has been working on risk assessment, disaster resilience and crisis management, disaster risk reduction, critical infrastructures protection, probabilistic and vulnerability analysis, Global Information Systems (GIS), Decision Support System (DSS), in transport, security and space applications. At R&D level he has been involved in several EU projects in FP6 and FP7. He has been the coordinator of the FP7 Security project SPARTACUS, the Innovation Manager of the H2020 Security project EU-CIRCLE (Critical Infrastructure resilience to climate change), the Technical and Exploitation Manager of the H2020 Space project LOGIMATIC, the Business Innovation Manager of the H2020 project RAGTIME, etc. He is the chair of Technology Area 4 (TA4) “Resilience” of the Integrated Mission Group for Security (IMG-S). He is member of the European Virtual Risk Institute (EU-VRI), member of the EARTO Security Research Group, member of the Executive Board of the European Construction Technology Platform (ECTP). He is currently member of the Management Committee of the Transport Research Arena (TRA) conference (2018). He is author of more than 50 papers published in peer-review journals, book chapters and articles presented at international conferences. He is acting as reviewer for several international journals, such as Smart Structures and Systems (Techno Press) Computer-Aided Civil and Infrastructure Engineering (Wiley), Journal of Aerospace Engineering (ASCE), etc.

Mrs. Evangelia Gaitanidou

www.hit.certh.gr
lgait@certh.gr



Evangelia Gaitanidou has a Diploma in Civil Engineering from the Aristotle's University of Thessaloniki, Greece, where she also obtained her MSc on "Planning, Organization and Management of Transportation Systems" and is currently a PhD Candidate in Road Safety. She works in the Hellenic Institute of Transport since 2004, as a Researcher, head of the Vehicle Safety laboratory (2009-2012), the Clean Vehicles laboratory (2012-2014) and the Road Safety and Security laboratory (2014-present). She has so far participated in more than 20 EU funded projects in FP6 (IN-SAFETY, ASK-IT, AIDE, PReVENT, SUPREME, HUMABIO, RIPCORD-ISEREST, PEPPER, DRUID), FP7 (TeleFOT, ACCESS2ALL, 2DECIDE, BESTPOINT, FOTsis, VERITAS, REMOTE, SOLUTIONS) and in Horizon 2020 (SocialCar, RESOLUTE, AUTOPILOT) in most of which holding a significant role (assistant Coordinator/Technical Manager, Quality Manager, WP/Task leader). She has also had an active role in several National projects, such as "ERMIS" National Level Action (2011-2013) and KRHPIS (2013-2015), within the framework of the Operational Program "Competitiveness and Entrepreneurship" of the Ministry of Education and Lifelong learning, "Development of training curriculum and material for Road Safety Auditors training in Greece" as well as the "Development and operation of Electronic Driving Academy – eDrive Academy"of the Ministry of Infrastructure, Transport and Networks (2014-2015). She has about 30 publications in National and International peer reviewed Conferences and Journals, while, additionally, she is co-Editor of a book and co-author in 10 chapters in books. She has also acted as Assistant Editor in the European Transport Research Review (ETRR) Journal (2009 – 2013) in which she still acts as a reviewer. She is fluent in English and French and speaks good Italian. Her main fields of interest lie in the areas of: Road Safety, Automated Driving, Resilience, Clean Vehicles, Sustainable Transport, ITS, Transportation of E&D, Mobility for All, Advanced Driver Assistance Systems (ADAS), Cooperative systems, etc..

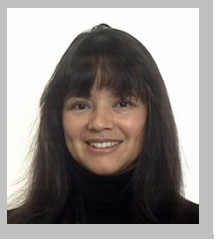
Mrs. Clara Grimes

www.iclei-europe.org
clara.grimes@iclei.org

Clara Grimes joined ICLEI in August 2015 as an Officer in the Communications and Member Relations team. Clara and her team manage and guide the organisation's relationships with its members and communicate concepts on sustainability to a variety of audiences including cities, partners, policymakers, researchers, media and citizens. Clara is responsible for dissemination and communication of ICLEI Europe's work in the fields of resilience, climate change adaptation and nature-based solutions, serving as a focal point for ICLEI Europe's policy work in these areas, collecting lessons learned from living labs and research and synergizing and articulating these into accessible information and tools to support the transition to more sustainable urban environments. As part of this work, Clara is involved in the organization and production of conferences, including the Informed Cities Conference, and media work at ICLEI's membership events including ICLEI Europe's Membership Assembly and the European Conference on Sustainable Cities and Towns. Clara is also an online content expert and led the redesign of the CIVITAS.eu website, applying the experienced she gained through her work for Google and Web Reservations International. Clara completed a traineeship with the Council of Europe, and worked in the administration and grant management of European research projects at University College Dublin. She is also a literary translator and has professional experience as a self-employed copywriter, online content editor, translator and event promoter and has toured internationally as a session musician

Dr. Ivonne Herrera

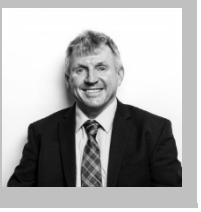
www.sintef.no
Ivonne.a.herrera@sintef.no



Dr. **Ivonne Herrera** is a Senior Scientist at SINTEF and Associate Professor at the Norwegian University of Science and Technology (NTNU). She has degrees in Electrical Engineering, a Master in Aeronautical Maintenance and Production and a PhD in Safety Management and Resilience Engineering. Dr. Herrera is the Project Coordinator of Horizon 2020 Project DARWIN – Expect the unexpected and know how to respond. She has more than 20 years of experience in the industry and research on avionics engineering, maintenance, safety management, risk analysis and resilience engineering for aviation and petroleum industries. Since 2003, she has been invited as an independent expert acting as an evaluator or reviewer of aeronautics research activities for FP6, FP7 and H2020 by the European Commission. In 2010 and 2013, she was member of the expert Panel for the Interim Evaluations of Clean Sky Joint Undertaking. In 2016, she was a member of the expert Panel conducting the interim evaluation of Horizon 2020 Societal Challenge "Smart, Green and Integrated Transport". Her teaching includes courses addressing societal safety, risk governance, safety management and resilience. Ivonne co-chairs the Scientific Committee of Clean Sky Joint Undertaking, chairs a newly established European Safety and Reliability (ESRA) Technical Committee on Resilience Engineering and has been member of the executive committee of the Resilience Engineering Association. She has been invited as a reviewer for different journal such as Reliability Engineering and System Safety, Safety Science, International Journal of Applied Aviation Studies, Information and Software Technology and Theoretical Issues in Ergonomics Science.>

Dr. William Hynes

www.futureanalytics.ie
william.hynes@futureanalytics.ie

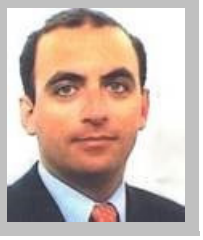


Dr. **William Hynes** (BSc MRUP MSc PhD MRICS MSCSI MRTPI MIPI MCILT) is a Chartered Town Planner, a Chartered Surveyor, urban economist, and a founder and director of Future Analytics Consulting. William has been one of Ireland's most successful private sector researchers within the Seventh Framework Programme (Secure Societies strand), and has key experience in both Project Coordination and Work Package/Task leadership and delivery. In addition, William has extensive experience providing expert advice to public and private sector clients in the following areas: strategic spatial planning including at national, regional, county and local levels, demography, housing and economic analysis and forecasting that is fully integrated with spatial planning, health planning, retail impact assessment and infrastructure planning (roads, rail, services, etc.), and is currently providing social and socio-economic expertise across a range of economic development and regeneration projects.

William, who is a member of the Central Statistics Office (CSO) Expert Group on national and regional population projections, is a former chairperson of the Royal Town Planning Institute (RTPI) Irish Branch Southern Section. William is also a visiting lecturer at University College Dublin and Dublin Institute of Technology lecturing in the areas of land use and transportation planning, strategic spatial planning, infrastructure planning, demographic analysis, research methods and GIS. He is also currently holds the position of Adjunct Professor at University College Cork.

Dr. Stephane Jacobzone

www.oecd.org
stephane.jacobzone@oecd.org



Stephane Jacobzone takes a leading role in coordinating public governance activities at the OECD, including through the High Level Risk Forum (HLRF). The HLRF led the development of ground-breaking OECD Principles on the Governance of Critical Risks, building on a set of thematic activities as well as peer reviews. These thematic activities include Strategic Crisis Management, Risk Communication, Disaster prevention, indicators for disaster losses, management of critical infrastructure, National Risk Assessment and disaster related contingent liabilities. S. Jacobzone has worked in several OECD areas, including regulatory and risk management, the governance of regulatory oversight, public governance, as well as health and ageing related issues. M. Jacobzone has conducted multidisciplinary country reviews of regulatory reform in a dozen of countries and reviews and studies of risk management policies in Mexico, France, Morocco, Austria, Switzerland etc...He also co-ordinated the OECD 2015 Public Governance Ministerial Meeting held in Helsinki. He started his career at the French Treasury. Mr. Jacobzone is a former alumni of the Ecole Polytechnique and ENSAE (French National Academy for Statistics and Economics), France. He taught at the French Institut d'Etudes Politiques, Ecole Nationale d'Administration, ENSAE, the French national school for statistics and economics, Brazil National School of Public Administration and has had affiliations with the US National Bureau of Economic Research. He is the author of many books and peer reviewed articles.

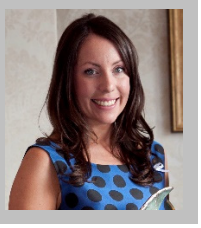
Prof. Dr. Aleksandar Jovanovic

www.eu-vri.eu
jovanovic@eu-vri.eu

Aleksandar Jovanovic is the director of the Steinbeis Advanced Risk Technologies group in Stuttgart, Germany providing consultancy in the areas of risk assessment and management for industry and public sector. As from 2006 he is also the CEO of European Virtual Institute for Integrated Risk Management (EU-VRi) and the EU Project Director at ZIRUS (Center for Interdisciplinary Risk and Innovation Studies, University of Stuttgart), teaching the courses in the area of CSR (Corporate Social Responsibility) and Risk. He has acted as Seconded National Expert (Germany) with the EU in Brussels, Belgium, Directorate-General Research – Industrial Technologies and Materials. His previous teaching assignments were in France (Ecole Polytechnique), Japan (University of Tokyo), USA (La Jolla) and other countries. A. Jovanovic has over 50 large international/multinational projects in the area innovation management, new technologies, business risk management, structured project management, advanced data analysis and data mining, and related areas. Main clients in the projects have been from the EU, national governments (Norway, Belgium, Japan…), industry, utilities, insurances companies, R&D and academia. Main topics covered by the projects have dealt with risk management in industry including HSSE (Health, Safety, Security, Environment), RCM (Reliability Centered Maintenance), RBI (Risk-Based Inspection), KPIs (Key Performance Indicators) and RCFA (Root Cause Failure analysis), and many applied in industry and/or used as the basis for further standardization. A. Jovanovic is author of five books and over 200 publications.

Mrs. Judith Kieran

www.carrcommunications.ie
judith.kieran@carrcommunications.ie



Judith Kieran is an Account Director at Carr Communications (Dublin, Ireland), in its European Projects Team. Her background is in public relations and communications and she joined the Irish SME's PR department in early 2008. Judith provides consultancy services to a range of clients in the public, private, and not-for-profit sectors. Working closely with their senior management teams, she manages communication strategies from initial development through to implementation. Judith's proven track record in strategic communications, media relations, event management and crisis management includes a number of award-winning national events and information campaigns. She has been involved in dissemination and exploitation for FP7 and H2020 research projects since 2010 – across themes such as Transport, Factories of the Future, and Space. Working with partners from industry and academia, she designs and delivers communications and dissemination strategies. In the DARWIN H2020 project, Judith supports the activities in Work Package 6, Outreach: Dissemination & Exploitation. She also participates in H2020 projects Factory2Fit (Empowering and participatory adaptation of factory automation to fit for workers), PASSME (Personalised Airport Systems for Seamless Mobility and Experience), and SCENT (Smart Toolbox for Engaging Citizens into a People-Centric Observation Web). Judith holds a BA (Hons.) in Media Arts from Dublin Institute of Technology, a Diploma in Digital Marketing and Social Media from the European Institute of Communications, and a Diploma in Event Management from the Fitzwilliam Institute. She is a full member of the Public Relations Institute of Ireland (MPRII).

Dr. Igor Kozine

www.man.dtu.dk
igko@dtu.dk

Igor Kozine studied at the Moscow Institute of Physics and Engineering (Technical University) and received his M.S. and Ph.D. in Systems Sciences from the same university. Since then he worked at the Obninsk Institute of Nuclear Power Engineering, Russia, as associate professor and senior scientist. For two years worked at Risø National Laboratory, Denmark, as a guest scientist, and for one year studied as a Fulbright Scholar at the State University of New York at Binghamton. At present he works at the Technical University of Denmark (DTU) as a senior researcher. His research is concerned with reliability, risk and uncertainty analysis as well as simulation of human performance. Over the last few years, his risk research has been extended to resilience assessment and management of critical infrastructure. He has been a co-developer of a resilience assessment framework within the EU co-funded project READ. He teaches two master courses on related topics at DTU.

Dr. David Lange

www.ri.se
david.lange@ri.se

Dr. David Lange is a senior research scientist at RISE Transport and Safety / Fire Research in Sweden. Originally from Edinburgh, he has a Masters in Structural Engineering with Architecture and a PhD in Structural Fire Engineering, both from the University of Edinburgh. Prior to joining RISE, David worked at the University of Edinburgh as a researcher in fire safety engineering, as well as a teaching fellow in civil and environmental engineering. While working as a research associate he was subcontracted part time to Rushbrook consulting Engineers, where he acted as principle fire engineer gaining experience in risk engineering for the insurance industry evaluating highly protected risk sites; as well as working in the fire engineering industry in the UK, with clients including architects and local authorities.

His research interests are in performance based design and risk assessment; evaluation of cascading effects; resilience of critical infrastructure as well as structural and fire engineering. He is currently the coordinator of the IMPROVER DRS 7 project, and is participating in two other European projects as well as various nationally funded projects

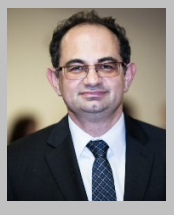
Mr. Vasileios P. Latinos

www.iclei-europe.org
vasileios.latinos@iclei.org

Vasileios Latinos joined ICLEI Local Governments for Sustainability in February 2016, as Project Officer for Sustainable Resources, Climate Adaptation and Resilience at the European Secretariat in Freiburg. He is responsible for implementing projects and services in the topical areas of natural resource management, climate change adaptation and urban resilience, as well as supporting the strategic and programmatic development of ICLEI Europe in this field. He has 8 years experience in consulting and research in Germany and Greece. Vasileios worked previously as an expert for 100 Resilient Cities, pioneered by the Rockefeller Foundation, as associate lecturer for the Technical University of Berlin, as a field researcher and research assistant for EU funded projects like the EU FP7 funded, ''Welfare, Wealth and Work for Europe'' and the IMA-Stadt ''TransUrbanLife'' project and as a consultant for the start-up company Stadt Consulting. Vasileios has always been very engaged in the research about climate change policies and urban resilience and how global, environmental policies, concepts and strategies can be transferred and applied locally, in cities and municipalities; therefore, ICLEI has been a very insightful and important career driver for him.

Dr. Igor Linkov

www.cmu.edu
ilinkov@yahoo.com



Dr. **Igor Linkov** is the Risk and Decision Science Focus Area Lead with the US Army Engineer Research and Development Center, Adjunct Professor with Carnegie Mellon University and Consulting Scientist with Factor Social. Dr. Linkov has managed multiple risk and resilience assessments and management projects in many application domains, including transportation, supply chain, homeland security and defense, cybersecurity, and critical infrastructure. He was part of several Interagency Committees and Working Groups tasked with developing resilience metrics and resilience management approaches, including the US Army Corps of Engineers Resilience Roadmap. Dr. Linkov has organized more than twenty national and international conferences and continuing education workshops, including workshops on Risk and Resilience in Berlin (2014), Aspen (2015) and Azores (2016) and 2015 World Congress on Risk in Singapore and is Chairing Program Committee for 2019 World Congress on Risk in South Africa. He has published widely on environmental policy, environmental modeling, and risk analysis, including sixteen books and over 300 peer-reviewed papers and book chapters. He is author and editor of 3 books focused on resilience published by Springer and International Risk Governance Council. He has served on many review and advisory panels for DOD, DHS, FDA, EPA, NSF, EU and other US and international agencies. Dr. Linkov is Society for Risk Analysis Fellow and recipient of 2005 Chauncey Starr Award for exceptional contribution to Risk Analysis as well as 2014 Outstanding Practitioner Award. He is Elected Fellow with the American Association for the Advancement of Science (AAAS). Dr. Linkov has a B.S. and M.Sc. in Physics and Mathematics (Polytechnic Institute) and a Ph.D. in Environmental, Occupational and Radiation Health (University of Pittsburgh). He completed his postdoctoral training in Risk Assessment at Harvard University.

	Mr. István Macsári www.police.hu macsari@rri.police.hu	-declined-

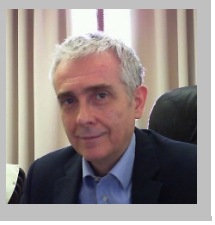
Pol. Lt. Col. **Macsári István** (male) is the head of the Aviation Security Department of the Aiport Police Directorate. External expert of the Civil Aviation Authority and partner as national aviation security auditor, including air cargo. He has 23 of years policing experience, out of 15 years operational (9 years as crime investigator, 1 years as duty officer commanding patrols at the airport, 5 years as head of aviation security department) experience and 8 years in close cooperation with the Civil Aviation Authority as national auditor. His expertise includes law enforcement, aviation security policy, management, and international relations, speaking French (C1), English (B2), and Hungarian (mother tongue). Aviation security expert and instructor/trainer for security personnel, security screeners (aiport and cargo) and also for security managers and managers/agents of internal/external aviation security quality control activities. He is the secretary of the Aiport Security Committee in Budapest, leader of the WG, and expert of the Aviation Security Commission at national level. Former member of the Explosive Detection Dog WG (EU COM) and initiative of the AIRPOL organisation. As EU COM qualified national audior, he is also European Commission aviation security inspector (airports), takes part of EU inspections regurarly at european airports.

	Mr. William R. McNamara www.dhs.gov William.mcnamara@hq.dhs.gov	-declined-

William R. McNamara is a Security and Resilience Analyst at the Department of Homeland Security's Office of Infrastructure Protection. Mr. McNamara joined the U.S. Department of Homeland Security in 2009, and currently serves as the Coordinator for the Office of Infrastructure Protection's Regional Resiliency Assessment Program (RRAP). He previously led the Protective Security Coordination Division's Front Office support team, guiding the Division's overarching policy and strategic initiatives, and managing its strategic communications efforts and international engagements. Mr. McNamara holds a Master of Science and Technology Intelligence degree from the National Intelligence University, a Master of Forensic Sciences degree from the George Washington University in Washington, DC and a Bachelor of Science degree from Virginia Commonwealth University in Richmond, Virginia.

Dr. Paolo Nesi

http://www.disit.org
paolo.nesi@unifi.it



Paolo Nesi is Full Prof. at the University of Florence (Italy) and chief of DISIT Lab (Http://www.disit.org), a research lab focused on big data, artificial intelligence, and natural language processing. He has been coordinator of several research and innovation projects of the European Commission, and of local Gov., and international conferences. He is chairing the smart city Http://www.km4city.org action adopted by a number of projects.

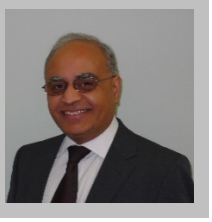
Dr. Knut Øien

www.sintef.no
knut.oien@sintef.no

Knut Øien, PhD is Senior Scientist at SINTEF Safety and Mobility. He was previous Research Manager for SINTEF Safety Research and Adjunct Professor at NTNU, Trondheim. His main competence is within risk indicators and risk control methods, risk and reliability analysis, human reliability analysis, organizational factors, expert judgment, emergency preparedness analysis, root cause analysis, accident Investigation and maintenance management. He has been project manager for developing the REWI method, which is a method for establishing safety indicators based on resilience thinking. He has been involved in EU projects since FP4, and he was a key project team member in the FP7 iNTeg-Risk project

Mr. Kishor Pala

kpala@easn.eu



Kishor Pala is an International Transformation Consultant & Senior Strategy Manager with over 20 years' experience and a sustained record of success in the International Collaboration arena. Extensive background in EU funding, bids and contract delivery, leading strategy development and driving effective implementation. A pragmatic leader and highly respected team player who creates robust strategies to translate vision into a Win/Win reality. Strong analytical, problem solving and decision-making skills with a passion for making a difference, together with an extensive network of contacts across Europe and UK.

Dr. Frederic Petit

www.anl.gov
fpetit@anl.gov

Frederic Petit is a Research Scientist specializing in critical infrastructure interdependencies and resilience at Argonne National Laboratory. With a background in earth sciences and civil engineering, Dr. Petit has focused on risk management and business continuity since 2002. Dr. Petit leads the development of methodologies for the assessment of preparedness, mitigation, response, recovery, and overall resilience capabilities of facilities, communities, and regions. He also lends his expertise to work on risk, vulnerability and threat analysis of critical infrastructure. Dr. Petit received his PhD from the École Polytechnique de Montreal in Civil Engineering, focusing on vulnerability analysis techniques for critical infrastructure cyber dependencies. Dr. Petit is member of various program committees for conferences, such as the Symposium on Risk Management and Cyber-Informatics (RMCI) and the National Symposium on Resilient Critical Infrastructure. He serves as Regional Director for North America of the International Association of Critical Infrastructure Protection Professionals (IACIPP) and is member of the International Advisory Board for the SmartResilience Project.

Mr. Gilad Rafaeli

giladr@mtrs.coml

Gilad Rafaeli has acquired more than 20 years of expertise and experience in the field of security in general, and in transport security in particular, with specific emphasis placed on railways and public transport systems. Mr. Rafaeli specialises in multiple aspects of security operation, on the one hand, and in security training, on the other hand. His expertise covers the performance of comprehensive risk assessments; and the development of risk management policies, CONOPS (Concepts of Operations), security and emergency plans, emergency procedures (EOPs) and recovery & business continuity plans; in defining resilience building measures and in operations planning. In the area of security training, Mr. Rafaeli specialises in the development of training programmes for diverse populations, including security managers, based on a variety of methods, including classroom (frontal) training, table top and field exercises, and CBT (computer based training) for initial and recurrent/refresher training.

Dr. Jose Mari Sarriegi

www.tecnun.es/en
jmsarriegi@tecnun.es

Prof. Dr. **Jose Mari Sarriegi**, Industrial Engineer (1994, PhD 1999) is a professor of Information Systems, Project Management and Modelling and Simulation at TECNUN. His research interests include resilience, security management, knowledge management and complex systems modelling. He has led several European research projects in all these topics. Currently, he is the coordinator of the Smart Resilience Project (H2020) and he has also coordinated the SEMPOC (CIPS) and ELITE (FP7) European projects. He has published in journals such as Technological Forecasting and Social Change, International Journal of Critical Infrastructure Protection, Business strategy and the Environment, IEEE Software, International Journal of Computer Integrated Manufacturing and IEEE Internet Computing. He has also presented dozens of papers in international conferences

Dr. Zoltán Szekely

www.bayzoltan.hu
dr.szekely.zoltan@gmail.com

-declined-

Zoltán Szekely dr. jur. (Mr.) is currently working as university assistant lecturer, he is also qualified as a lawyer, having undertaken the Bar Exam. He has 14 of years policing experience, both operationally (2 years as patrol, 9 years as commanding officer for patrols at the airport, 1 year as lawyer) and in the provision of training with the Police College, Faculty of Border Management (2 years). His expertise includes law, law enforcement, IT, management, and international relations, ISO 9001, speaking English (C1), German (B2), Romanian (B1) and Hungarian (mother tongue). Székely Zoltán is the leader of the research team at BZN.

Mr. Duane Verner

www.anl.gov
dverner@anl.gov

Duane Verner is the Resilience Analysis Group Leader within the Global Security Sciences Division at Argonne National Laboratory. He oversees staffing and technical assignments, including critical infrastructure vulnerability assessments, modelling, and dependency analyses. He has provided methodology development and project implementation support to the U.S. Department of Homeland Security Regional Resiliency Assessment Program since its inception in 2009.

Duane is vice-chair of the National Academies Transportation Research Board's (TRB) Committee on Critical Transportation Infrastructure Protection and a member of the TRB Military Transportation Committee. He regularly contributes to the international resilience research community through publications and trans-Atlantic collaboration. Prior to his position with Argonne, he was a project manager for a private sector engineering firm in New York City, working in the transportation, homeland security, and defence sectors.

Preliminary List of Participants

(as on September 4, 2017, the updated list will be distributed to the participants at the registration)

No.	Last Name	First Name	Company	Country
1	Abad	Jaime	BRGM	France
2	Adekola	Josephine	University of Glasgow	United Kingdom
3	Akgungor	Caglar	AKUT Search and Rescue Association	Turkey
4	Al Khattab	Adel	yahoo co	Ma'an
5	Alberto	Paulo	EDP Distribuição - Energia, S.A.	Portugal
6	Almeida	Rafael	INOV	Portugal
7	Annesi	Nora	Sant'Anna School of Advanced Studies	Italy
8	Antunes	Dalila	Factor Social	Portugal
9	Arnesen	Tor	Eastern Norway Research Institute	Norway
10	Barzelay	Udi	IBM Research Lab Haifa	Israel
11	Battistini	Alessandro	University of Florence - Earth Science Department	Italy
12	Bellini	Emanuele	University of Florence	Italy
13	Berbenni-Rehm	Caterina	ENCIRCLE	Luxembourg
14	Bergerhausen	Ulrich	Federal Highway Research Institute (BASt)	Germany
15	Berggren	Peter	Katastrofmedicinskt centrum (KMC)	Sweden
16	Bezrukov	Dmitrij	NIS Petroleum Industry of Serbia	Serbia
17	Blazevic	Dragana	NIS Petroleum Industry of Serbia	Serbia
18	Bodsberg	Lars	SINTEF Technology and Society	Norway
19	Bonnamour	Marie Christine	Public Safety Communications Europe	Belgium
20	Bouklis	Panagiotis	European Dynamics SA	Greece
21	Branlat	Matthieu	SINTEF	Norway
22	Brennan	Justin	Irish Water	Ireland
23	Buldrini	Marco	NIER Ingegneria S.p.A.	Italy
24	Büttgen	Klaus-Dieter	German Federal Agency for Technical Relief - Headquarters	Germany
25	Caillard	Bastien	European Virtual Institute for Integrated Risk Management	Germany
26	Casciati	Fabio	University of Pavia	Italy
27	Castulik	Pavel	Agriconsulting S.A.	Belgium
28	Chalupa	Jiri	MOI - DF FRS	Czech Republic

No.	Last Name	First Name	Company	Country
29	CHARLAFTIS	ANGELOS	ePAPHOS ADVISORS TEAMWORK	Belgium
30	Choudhary	Amrita	European Virtual Institute for Integrated Risk Management	Germany
31	Clarke	Jonathan	University of Warwick	United Kingdom
32	Corrigan	Andrea		Ireland
33	Cozzani	Valerio	University of Bologna	Italy
34	Crabbe	Stephen	Crabbe Consulting Ltd	Germany
35	Davis	Dennis	CTIF	United Kingdom
36	De Vigili	Stefano	CIVIL PROTECTION DEPARTMENT - AUTONOMOUS PROVINCE OF TRENTO	Italy
37	Deloukas	Alexandros	ATTIKO METRO	Greece
38	Desmond	Gerard	Cork City Council	Ireland
39	Di Giovanni	Daniele	University of Rome Tor Vergata	Italy
40	Diagourtas	Dimitris	Satways Ltd	Greece
41	Diego	César	MINISTERIO DEL INTERIOR	Spain
42	Dominique	SERAFIN	CEA	France
43	Doyle	Aoife	Future Analytics Consulting Ltd.	Ireland
44	Drosou	Anastasis	RESOLUTE	United Kingdom
45	Dubaguntla	Raja Sekhar	OVGU	Germany
46	Dusserre	Gilles	armines	France
47	Dykstra	Eelco	Daily Impact Emergency Management (DIEM)	Netherlands
48	Eftychidis	Georgios	KEMEA	Greece
49	Eriksson	Henrik	Linköping University	Sweden
50	Faravelli	Lucia	University of Pavia	Italy
51	Ferreira	Pedro	Instituto Superior Técnico - CENTEC	Portugal
52	Finger	Jörg	Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, EMI	Germany
53	Florescu	Elisabeta	European Commission DG Joint Research Centre	Belgium
54	Fontanalw	Ignasi	OptiCits	Spain
55	Fuggini	Clemente	Rina Consulting S.p.A. - Formerly D'Appolonia S.p.A.	Italy
56	Gaitanidou	Lila	CERTH/HIT	Greece
57	Galvagni	Alessandro	Civil Protectione Department - Autonomous Province of Trento	Italy
58	Gehrke	Josef	European Virtual Institute for Integrated Risk Management	Germany

No.	Last Name	First Name	Company	Country
59	Gerbec	Marko	Jozef Stefan Institute	Slovenia
60	Giannopoulos	Georgios	European Commission	Italy
61	Gimenez	Raquel	Universidad de Navarra, Tecnun	Spain
62	Goodchild	Clive	BAE Systems	United Kingdom
63	Grimes	Clara	ICLEI - Local Governments for Sustainability European Secretariat	Germany
64	Grøtan	Tor Olav	SINTEF, Technology and Society	Norway
65	Guay	Fanny	Danish Institute of Fire and Security Technology	Denmark
66	Havarneanu	Grigore	International Union of Railways (UIC)	France
67	Haverhals	Merel	NEN	Netherlands
68	Hynes	William	Future Analytics Consulting	Ireland
69	Jacobzone	Stephane	Organisation for Economic Co-operation and Development	France
70	Jaskowiak	Joanna	Council of the EU	Belgium
71	Johansson	Per-Erik	FOI	Sweden
72	Jovanovic	Aleksandar [EU-VRi]	European Virtual Institute for Integrated Risk Management	Germany
73	Kaiafas	Georgios	REA B4	Belgium
74	Karakostas	Anastasios	Centre of Research and Technology Hellas (CERTH)	Greece
75	Kelly	Dominic	CBRNE Ltd	United Kingdom
76	Kessie	Bryan	Skills for Justice	United Kingdom
77	Kieran	Judith	Carr Communication	Ireland
78	Kintzios	Spyridon	Hellenic Ministry of Defence	Greece
79	Knape	Thomas	Applied Intelligence Analytics	Ireland
80	Kozine	Igor	Technical University of Denmark	Denmark
81	Kröger	Wolfgang	Swiss Federal Institute of Technology Zurich	Switzerland
82	Kyrieri	AIKATERINI-MARINA	EUROPEAN COMMISSION	Belgium
83	Lang	Mary-Ellen	City of Edinburgh Council	United Kingdom
84	Lange	David	SP Technical Research Institute of Sweden-Fire Research	Sweden
85	Lapeyre	Guillaume	European Commission- REA - Research Executive Agency Unit B.4 – Safeguarding Secure Society	Belgium
86	Larrañeta	J. Javier	Fundacion Tecnalia Research & Innovation	Spain

No.	Last Name	First Name	Company	Country
87	Latinos	Vasileios	ICLEI - Local Governments for Sustainability European Secretariat	
88	Liedtke	Christopher	German Institute for Standardization (DIN e. V.)	Germany
89	Linkov	Igor	Carnegie Mellon University	United States
90	Löscher	Michael	ARTTIC	Germany
91	Macsári	István	Hungarian National Police	Hungary
92	Mandelli	Giacomo	European Virtual Institute for Integrated Risk Management	Germany
93	Marterer	Robin	Padeborn University	Germany
94	Matschke Ekholm	Hanna		Sweden
95	McNamara	William R.	DHS Office of Infrastructure Protection	United States
96	McNeill	Anja	MPV Meß- und Prüftechnik Vogt GmbH	Germany
97	MEBARKI	Ahmed	MEBARKI Ahmed	France
98	Mendoza	Lucile	HUMANIST VCE	France
99	Milenov	Kristian	ASDE-ECOREGIONS	Bulgaria
100	Misak	Marek	Commission of the Bishops' Conferences of the EU (COMECE)	Belgium
101	Mkrtchyan	Lusine	ETH Zurich	Switzerland
102	Morelli	Stefano	University of Firenze (Italy)	Italy
103	Muhasilovic	Medzid	University of applied Sciences	Germany
104	Nesi	Paolo	Università degli Studi di Firenze	Italy
105	Neubauer	Georg	Austrian Institute of Technology	Austria
106	Nikolic	Mirjana	NIS Petroleum Industry of Serbia	Serbia
107	O'Brien	John	Nestlé Research	Switzerland
108	Øien	Knut	SINTEF Technology and Society	Norway
109	OLARU	Paul	SETEC	Germany
110	Olivero	Sergio	SiTI	Italy
111	Pala	Kishor	Automotive Strategy Europe Ltd	United Kingdom
112	Pallis	Geroge	Factor Social	Portugal
113	Palma-Oliveira	José Manuel	University of Lisbon	Portugal
114	Papadopoulos	Vasileios	Hellenic Air Force	Greece
115	Pedrini	Gabriele	Autonomous province of Trento	Italy
116	Pestana	Maria	EDP	Portugal
117	Petersen	Laura	EMSC	France

No.	Last Name	First Name	Company	Country
118	Petit	Frederic	Argonne National Laboratory, Global Security Sciences Division	United States
119	Piper	Marc	EUK Consulting	Belgium
120	Pizzi	Roberto	Presidenza del Consiglio dei Ministri - Dipartimento della Protezione Civile	Italy
121	Potenza	Pierluigi	risorseperroma	Italy
122	Pyrko	Igor	University of Strathclyde	United Kingdom
123	Quevauviller	Philippe	European Commission, Directorate-General XII - Science, Research and Development	Belgium
124	Radisch	Jack	Organisation for Economic Co-operation and Development	France
125	Rafaeli	Gilad	MTRS3 Solutions and Services Ltd.	Israel
126	Rautjärvi	Juha	Societal Security Solutions Ltd.	Finland
127	Remenyte-Prescott	Rasa	University of Nottingham	United Kingdom
128	Reuge	Elodie	European Organisation for Security (EOS)	Belgium
129	RIGAUD	Eric	MINES ParisTech	France
130	Robb	Malcolm	BAE Systems Maritime - Naval Ships	United Kingdom
131	Rolandi	Claudio	University of Applied Sciences and Arts Southern Switzerland, Department of Innovative Technologies	Switzerland
132	Rosenqvist	Hannah	DBI	Denmark
133	Roure	Francoise	French Ministry of Economy and Finance	France
134	Sakurai	Mihoko	University of Agder	Norway
135	Sanchez	Almudena	GMV	Spain
136	Sanne	Johan M.	IVL Svenska Miljöinstitutet	Sweden
137	Sarriegi	Jose Mari	TECNUN	Spain
138	Sauerland	Torben	University of Paderborn	Germany
139	Sdongos	Evangelos	Institute of Communication & Computer Systems	Greece
140	Searle	Rachel	Skills for Justice	United Kingdom
141	Seker	Danny	ISERD	Israel
142	Serreault	Brigitte	Université de Nice-Sophia Antipolis	France
143	Sfetsos	Thanasis	ncsr demokritos	Greece
144	Shaw	Eddie	Carr Communications	Ireland
145	Stepanyan	Magda	risk-society	Netherlands
146	Stojadinovic	Bozidar	ETH Zurich	Switzerland

No.	Last Name	First Name	Company	Country
147	Székely	Zoltán	Bay Zoltan Nonprofit Ltd. for Applied Research	Hungary
148	Tapia	Mariela	University of Bremen	Germany
149	Tetlak	Katarzyna	Steinbeis Advanced Risk Technologies	Germany
150	Theocharidou	Marianthi	European Commission Joint Research Centre	Italy
151	Thier	Pablo	University of Bremen, Department of Resilient Energy Systems	Germany
152	Thums	Christian	Frontex European Border and Coast Guard Agency	Poland
153	Tofani	Alberto	ENEA	Italy
154	Toret	Jean-Baptiste	Irish Water	Ireland
155	Vamvakeridou-Lyroudia	Lydia	University of Exeter/Centre for Water Systems	United Kingdom
156	Van Harte	Malcom	Eskom	South Africa
157	Vannuccini	Gianluca	RESOLUTE	Italy
158	Velat	Nora	Czech Technical University, Dept. of Security Technologies and Engeneering	Czech Republic
159	Ventikos	Nikolaos	National Technical University of Athens	Greece
160	Verner	Duane R.	Argonne National Laboratory, Global Security Sciences Division	United States
161	Vollmer	Maike	Fraunhofer Gesellschaft zur Förderung der Angewandten Forschung e.V.	Germany
162	Wittmer	Dominic	European Commission, Joint Research Centre Sustainable Resources Directorate – Land Resources Unit	Italy
163	Wright	Juliane	Social Research Centre - Central Scientific Institute of TU Dortmund University	Germany

Project Papers

DARWIN

Dr. Ivonne Herrera, Project Coordinator

SINTEF, Trondheim, Norway

Corresponding author:
Ivonne Herrera
SINTEF
Department of Software Engineering, Safety and Security
Postboks 4760 Torgarden
NO-7465, Trondheim
Norway
Phone: +47 90680634
Ivonne.a.herrera@sintef.no

Main authors:
Ivonne Herrera, Matthieu Branlat and Christina Hanssen (SINTEF)
Contributions to this article are collected from DARWIN deliverables managed by:
Rogier Woltjer (FOI), Per Schachtebeck (TUBS), Luca Save (DBL), Peter Berggren (KMC), Eddie Shawn (CARR)

Abstract

The DARWIN project addresses the improvement of responses to expected and unexpected crises affecting critical infrastructures and social structures. It covers the management of both man-made events (e.g. cyber-attacks) and natural events (e.g. earthquakes). The main objective is the development of European resilience management guidelines. These will improve the ability of stakeholders to anticipate, monitor, respond, adapt, learn and evolve, to operate efficiently in the face of crises.

To avoid that the guidelines become "dust collectors" on a shelf, they will be made available in different formats for easy usage and maintenance. To enable dynamic, user-friendly guidelines the project will adapt innovative tools (e.g. serious gaming for training purposes), test and validate the guidelines, and establish knowledge about how organizations can implement the guidelines to improve resilience.

A multidisciplinary approach is applied, involving experts in the field of resilience, crisis and risk management and service providers in the Air Traffic Management and health care domains. To ensure transnational, cross-sector applicability, long-term relevance and uptake of project results, a new EU-Wide DARWIN Community of Crisis and Resilience Practitioners (DCoP) has been established, including stakeholders and end-users from various domains and critical infrastructures as well as resilience experts. The DCoP members are involved in an iterative development and validation process to provide feedback on the guidelines.

The target beneficiaries of DARWIN are crisis management actors and stakeholders responsible for public safety, such as critical infrastructures and service providers, as well as community groups.

1 Introduction

The DARWIN project develops state of the art resilience guidelines and innovative training modules for crisis management. The guidelines, which will evolve to accommodate the changing nature of crises, are developed for those with the responsibility of protecting population or critical services from policy to practice. The guidelines build on interrelated resilience capabilities and key areas, such as:

- Capability to anticipate threats, opportunities and cascade effects.
    - Mapping and addressing possible interdependencies
- Capability to monitor performance in a flexible way
    - Explore how multiple actors and stakeholders operate in rapidly changing environments
- Capability to respond and adapt (readiness to responds to the expected and the unexpected)
    - Investigate successful strategies for resilient responses
- Capability to learn and evolve
    - Enable cross-domain learning on complex events

Key areas: bringing innovation into DARWIN through living and user-centred guidelines; creative and integrative collaboration, evidence through pilot exercises, continuous evaluation and serious gaming.

Readers from industry and researchers can use this document to get an overview of project work and expected results.

Project partners:

Stifftelsen SINTEF (SINTEF, Coordinator, Norway)

Technische Universität Braunschweig (TUBS, Germany)
Carr Communications (CARR, Ireland)
Deep Blue Srl (DBL, Italy)
ENAV S.p.A (ENAV, Italy)
InstitutoSuperiore de Sanità (ISS, Italy)
Totalförsvarets forskningsinstitut (FOI, Sweden)
Katastrofmedicinskt Centrum (KMC, Sweden)
Ben-Gurion University of the Negev (BGU, Israel)

Project web-site:

www.h2020darwin.eu

2 Background

Crises and disasters in recent years have made it abundantly obvious that a more resilient and adaptive approach to preparing for and dealing with such events is badly needed. The Eyjafjallajökull (2010, total losses: approx. 1 billion euros) highlighted the importance of better emergency management at European level, the need for better tools for forecasting and anticipation, and the need for collective, coordinated action by different organisations. The Deepwater Horizon disaster (2010, 11 fatalities and environmental damage from almost 5 million barrels of oil) highlighted the need to improve organisational and individual awareness, and the need to develop resilient safety management strategies that can adapt to anticipated and unanticipated changes. A study of Fukushima Daiichi in 2011 reported that Resilience Engineering provides a critical proactive approach that is essential for improving safety in nuclear facilities. The study particularly highlights the need for the ability to manage unforeseen events. These examples are reminders of the urgent need for tools to reveal, assess and manage resilience in everyday operations and during a crisis.

Resilience management addresses the enhancement of the abilities of an organisation to sustain adaptability and continue operations as required when facing expected and unexpected events. It includes “everyday operation” as this information is essential to ensure that the organisation functions. This information includes how multiple activities work together to produce successful outcomes for different kinds of systems and organisations at different levels. It combines technical structures and social systems and interplay of different kind of systems and organisations at different levels.

2.1 Project objectives

The main objective of the DARWIN project and core results is the development of European resilience management guidelines for crisis management. However, infrastructure operators and resilience practitioners need something much more dynamic relative to updates and applicable in practical settings than a set of documents filed neatly on a shelf somewhere. Thus, the sub-objectives of DARWIN are as follows:

- To make resilience guidelines available in a format that makes it easy for a particular critical infrastructure operator to apply them in practice, by: Surveying and cataloguing resilience concepts, approaches, practices, tactics and needs and adapting them to the needs of a domain or specific organisation;
- To enable use of resilience guidelines in non-crisis situations, for the purposes of: Basic learning and practical training, (based different techniques including “serious gaming”).
- To facilitate evolution of resilience management guidelines in terms of: simple ways to make updates and propagate these to the wider community of infrastructure operators, with straightforward processes and technical infrastructure for approving changes and managing revisions and variants;
- To establish a forum - the DARWIN Community of Resilience and Crisis Practitioners (DCoP) - with a lifetime that will extend beyond the end of the project, that will: Bring together infrastructure operators, policy makers and other relevant stakeholders and allow them to exchange views and experiences in a dynamic, interactive and fluent way;

To build on “lessons learned” in the area of resilience by: identifying criteria that provide indicators of what works well and what does not and applying these criteria in defining and evolving resilience guidelines.

To carry out two pilots that apply project results in two key areas - Health care and Air Traffic Management (ATM) – and use the experience gained to improve project results and demonstrate their practical benefits in these domains, as well as add value to established risk management practices and guidelines.

To establish activities that will lead to project results being adapted to, and later adopted by, practitioners in domains other than the two used in the pilots. (Work done within the scope of the project will initiate the process and provide the basis; full adoption will happen after the project, as part of “Impact”).

2.2 Description of action

The work is divided into 6 work packages (WP) are grouped into research and development (R&D), outreach and uptake:

- WP1 Survey of resilience approaches and synthesis of requirements analyse, consolidate and evaluate most promising resilience approaches and practices for crisis management.
- WP2 Development of evolving resilience management guidelines consisting of a catalogue of concepts, practices and guide for application. These concepts will support the resilience abilities to anticipate, monitor, respond and adapt and learn and evolve to expected and unexpected disturbances. Special attention is given to complement to existing risk management. WP2 works with the adaptation of these guidelines to two domains health care and air traffic management
- WP3 Enabling tools for resilience management guidelines provide means for easy access and evolution of the guidelines. It includes tools and training for pilot implementations
- WP4 Pilots: Demonstration and evaluation offer feedback to the establishment and development of the guidelines at an early stage prior to operationalization and after pilots' applications
- WP5 Outreach: Creating a Community of Crisis and Resilience Practitioners (DCoP) is responsible for exchange of experiences, lead evolution of guidelines and providing feedback to the project
- WP6 Uptake: Dissemination and exploitation will create material and organise events that raise awareness and share DARWIN knowledge targeted to specific market.

3 Current project results

All DARWIN deliverables are public available at www.h2020darwin.eu/deliverables. The following information provide examples of DARWIN results. It is extracted from DARWIN publications.

3.1 DARWIN Community of resilience and crisis practitioners

To ensure transnational, cross-sector applicability, long-term relevance and uptake of the DARWIN project results, different stakeholders and end-users from critical infrastructures and resilience experts are actively involved in their development and evaluation.

Figure 1: DARWIN Community of Practitioners – Workshop 2017 - variety of different disciplines and countries, and from a diversity of levels and responsibilities, e.g. from USA, Israel, Italy, Sweden, Germany, Norway, Kosovo, Ireland, France, Denmark, and Spain

Various activities have been performed involving end-users and experts to ensure relevance and us ability of DARWIN results. Type of interactions include:

Interview and surveys

All interviews and surveys are first tested with end-users within the consortium. Then, members of DCoP practitioners and experts have contributed to interviews to identify resilience and brittleness aspects from significant crises and everyday practices. Members have also participated into surveys designed to select the most appropriate resilience, concepts, approaches and practices for their incorporation in the guidelines. Surveys have also performed to support stakeholder analysis to identify type of stakeholders and their needs.

Workshops

DARWIN workshops have been successful in gathering high qualified people representing different critical infrastructures from policy to practice from different countries. The DCoPs have contributed to the creation, assessment and improvement of DARWIN work. The participants remarked the potential to learn both vertical and horizontal, vertical within one domain and one country, horizontally across countries and domains. Results from workshops are available on the DARWIN website.

Webinars

DARWIN webinars have been designed to present specific topics and gather feedback in a virtual environment. Resilience concepts and guidelines have been presented to people outside the project team.

Further work: The challenge is to keep momentum. Virtual collaboration, participation in pilot exercises and 3rd DCoP workshop are foreseen. DCoP members are invited to face-to-face as well as virtual interactions.

3.2 Resilience concepts

A systematic literature survey (SLR) was conducted on concepts and approaches to resilience from a range of disciplines, identifying associated indications of maturity of operationalization or implementation into practice (for example, through guidelines and tools.

A total amount of 440 articles are identified as relevant for further synthesis and analysis. In addition, 91 relevant articles from the DARWIN Description of Action (DoA) were revisited. Common topics in the form of concepts, theories and practices emerged from the literature. Example of topics are

Resilience definitions: delineated actions that must be implemented to achieve resilience. Classification of definitions based on actions address adaptability, bounce back, sustain adaptability, absorption and prevention

The generic characteristic of the resilience concept's premise of complexity is inherent to all papers. In this topic key issues include presence of disturbances, potential of cascading effects, applicability to non-crisis situations and that the dynamics of the situation and resilience responses are inseparable

The literature shows that the resilience domain put emphasis on the phases before and during the event when addressing needs and issues, and on both planning and responding when discussing solutions and practices.

An interview study of relevant stakeholders (members of the DCoPs and others) involved in crisis management was conducted to identify practices and needs. The interviews highlight the practices that indicate a degree of resilience, flexibility and adaptability to the circumstances in practice. Important elements to consider in crisis management include cultural awareness with respect to individuals and organizations, a structure with possibility to be reinforced when needed, competence and authority to act and improvise when plans no do not cover the ongoing situation. An interesting issue is that the reliance on procedures in some organisations is stronger than in others. The degree of adaptation to procedures also varies among organisations, as well as the support that is expressed that the procedures provide, which may also vary for different phases of crisis management. Working groups that at national and regional levels develop guidelines and procedures and adapt or implement them at regional or local levels seem to be a common way of organizing guideline development. Resilience management should thus address everyday work, complexity, dynamics of the events and the need to be flexible and stay flexible and not trapped into getting more procedures. Learning practices in place are generally based on events that previously have been managed. Training exercises and drills are performed regularly for most organisations.

Status: Completed and documented in DARWIN Consolidation of resilience concepts and practices for crisis management Deliverable D1.1. The target audience for the catalogue presented in this deliverable is both industry and researchers. Readers from industry and researchers can use this document as a body of knowledge

with potential relevance to their context of operations or as baseline for further work in the area of resilience and crises management. There is to the authors' knowledge no previous similar systematic literature review in the area of resilience and crises management with the same scope and level of detail and rigorousness. The work delineates the landscape of research within resilience and crisis management.

3.3 The DARWIN resilience management guidelines (DRMG)

Nature of the guidelines

The guidelines offer a critical overview of an organization's activities from the standpoint of resilience management, with the aim to effectively assist it in the creation, assessment or improvement of its own processes and documents. In other words, DARWIN is not developing guidelines for crisis management per se, but rather guidelines at a meta level: the context is that of organizations that already have a number of processes and tools in place to support their management of crises (e.g., preparation activities, contingency plans, procedures, learning activities). As such, the DARWIN guidelines can be complementary to existing guidelines or procedures in an organization, but they do not replace them. The guidelines are directed towards critical infrastructure managers, crisis and emergency response managers, service providers, first responders and policy makers. They provide these actors of crisis management with a perspective on these processes and with tools grounded in research and practice in resilience management.

The requirements identified and ranked by practitioners from the DCoP included especially conceptual requirements that captured resilience management capabilities the guidelines aim at. The guidelines are constituted of three essential components:

The building blocks are the Concept Cards (CC). CCs propose practical interventions in order to develop and enhance the resilience management capabilities captured in the conceptual requirements.

The guidelines build on the Concept Cards by organising and relating them, because the resilience management capabilities they refer to are not independent. The CCs are organised in themes (higher level capabilities) and related to each other as well as to basic functions of crisis management. This organisation of the guidelines allows for multiple ways of accessing their content, and anticipates the variety of needs and interests of the intended users.

A knowledge management platform, the DARWIN Wiki, facilitates the development, management and use of the guidelines. The platform offers opportunities to reconsider common views on the nature of guidelines, their necessary evolution and their multi-faceted, multi-purpose content.

Development and involvement of end-users

The guidelines' development process is a 4-step process established to be collaborative and iterative, and to include operational input early and as often as possible. The process changed and solidified during the course of the task as a result of the evolving understanding of what type and content of guidelines would be useful to develop and of how to produce such guidelines while fulfilling the various objectives of the project.

The guidelines need to be relevant to actual operations in order to be useful. For this purpose, operational experts representative of potential end-users are involved throughout the project. First, three end-user organizations are part of the project consortium: ENAV, the Italian Air Navigation Service Provider; ISS, the Italian National Health Institute; and KMC, a Swedish center for Disaster Medicine and Traumatology. In addition, members of the DCoP or additional experts from the fields of crisis and resilience management are solicited regularly, for instance: in the modified Delphi process that led to the selection of concepts, approaches and practices to be incorporated in the resilience management guidelines and judgment of their relative importance; in planned pilot studies to support the evaluation of the guidelines.

Current guidelines content

The DARWIN Resilience Management Guidelines, in their current form, provide guidance on the following themes and associated resilience management capabilities:

Supporting coordination and synchronisation of distributed operations: Ensure that the actors involved in resilience management have a clear understanding of their responsibilities and the responsibilities of other involved actors; promoting common ground in cross-organizational collaboration in crisis management; and establish networks for promoting inter-organizational collaboration.

Managing adaptive capacity: Adapt to both expected and unexpected events (all-hazard approach), and adapt relative to procedures.

Assessing resilience: Identifying sources and manifestations of brittleness and resilience, for organisations as well as communities.

Developing and revising procedures and checklists: Systematic management of policies involving policy makers and operational personnel for dealing with emergencies and disruptions.

Involving the public in Resilience Management: Communication strategies for crisis management organisations – interacting with the public not yet affected or involved.

Further work: Initial version and prototype of the guidelines produced. After finalizing the first set of guidelines, their scope will be broadened to address more themes and resilience management capabilities. The iterative development process will aim to further involve end-users (e.g., from the DCoP) in the development of the guidelines, as well as include end-users from the public and business domains.

3.4 Innovative tools

Innovative tools include simulations, serious games to support evaluation and training. This section describes a main innovative tool developed within the DARWIN project.

DARWIN Wiki

An objective of the project is to allow for flexible use of the guidelines, which corresponds to two different needs: (1) supporting the development and management of the evolving nature of the guidelines, requiring regular revisions of the content; (2) Generating a variety of means to access the guidelines, to account for the variety of envisioned users and uses. These needs correspond to Knowledge Management (KM) issues associated with the storage, versioning, variants, representation, and delivery of content. It quickly appeared that creation of content in typical office documents would constitute a strong limitation to effectively and efficiently update the guidelines as their structure evolve and scope increase, as well as to propose a variety of formats and means to access information. To better fulfil the project KM needs, a wiki-type platform, more specifically based on Semantic MediaWiki, was developed. The DARWIN Wiki provides a standardized way to create content collaboratively, facilitates the management of updates and offers flexible means for delivery of information. The core idea is to separate development of and access to guidelines through structuring the content of the guidelines, content that can then be used in various ways, for instance: reusing content in different formats for different purposes; sorting or aggregating information automatically; creating links between elements.

The main envisioned end-users, e.g., policy makers in a critical infrastructure administration, can consult the guidelines online. Content is organized in four main sections: “Implementation”, “Understanding the context”, “Relevant Material” and “Navigate in the DRMG”. Content related to internal management and review, used for development, is not displayed to end-users. The main information of interest is the “Implementation” section, i.e., the description of the set of interventions proposed for a particular capability. This content, organized by

phases of crisis management (across phases, before, during, after), is potentially complemented with "triggering questions", which aim at pointing users to the relevant issues via a set of questions users can reflect on and try to answer.

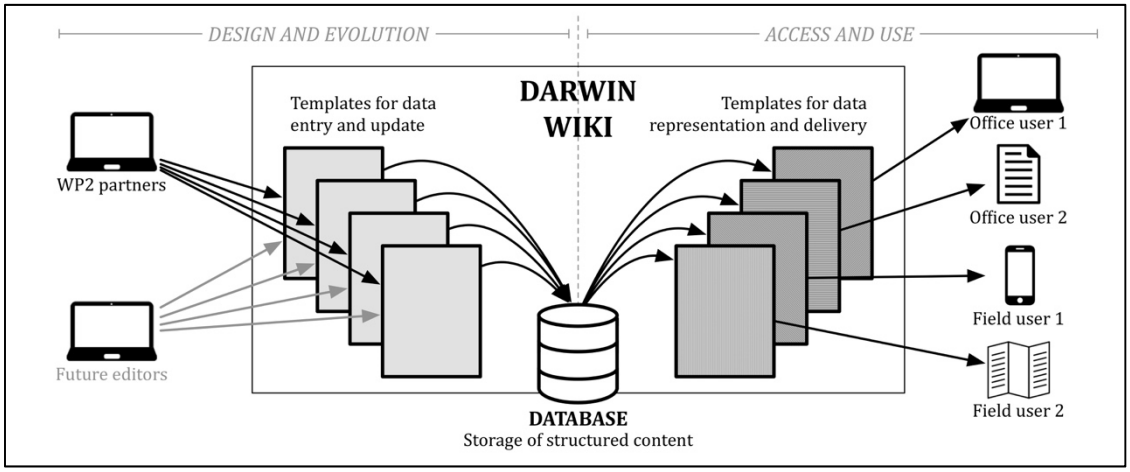


Figure 2: DARWIN WiKi application support for develop and use of the guidelines

For users who would like to better understand the context of the interventions proposed, or refer to original documents describing a method recommended in the CC (sections "Understanding the context" and "Relevant material" respectively), content is available on demand: clicking on the corresponding section title reveals or hide the text. This content access principle is used in other parts of the wiki in order to make the core content more compact and readable (clickable sections or elements are represented by the use of italic text format). Finally, the "Navigate in the DRMG" section groups in a table the various links that the user can follow to access related DRMG content, e.g., other CCs associated with the same resilience ability, or parent theme. Following the example of existing guidelines (e.g., WHO, 2008), a "DRMG Field Guide" was created to propose a minimal format to access guidelines outside of the office, i.e. in the field. The Field Guide is not thought of as a complete view of the guidelines, but rather as a quick reference material to remind of and guide people in the field to the right issues, as is the case with a checklist. The assumption for the envisioned use is that access to the guide is possible, whether in real-time online or as a saved document (depending on the constraints). The Field Guide proposed is simply an aggregation of the title, purpose and "triggering questions" for all the existing concept cards, organized by themes.

Further work: Involve end users on providing feedback on WiKi application in terms of format and content to facilitate exploitation of the guidelines. This collaboration is foreseen through the DARWIN website, workshop and webinars.

3.5 Evaluation and pilot studies

The evaluation process is based on three main pillars: (1) an initial evaluation involving representatives of the end users internal to the DARWIN Consortium, with experience in HC and ATM domains; (2) the collection of feedback from members of the DCoP, including experts of crisis management from a wide variety of domains (not limited to the HC and ATM); (3) the application of the guidelines in a set of 'pilot exercises' with the active participation of practitioners with experience in the HC and ATM sectors, as well as of experts from different domains which are impacted by the cascading effects of the crisis types identified in the pilot exercises.

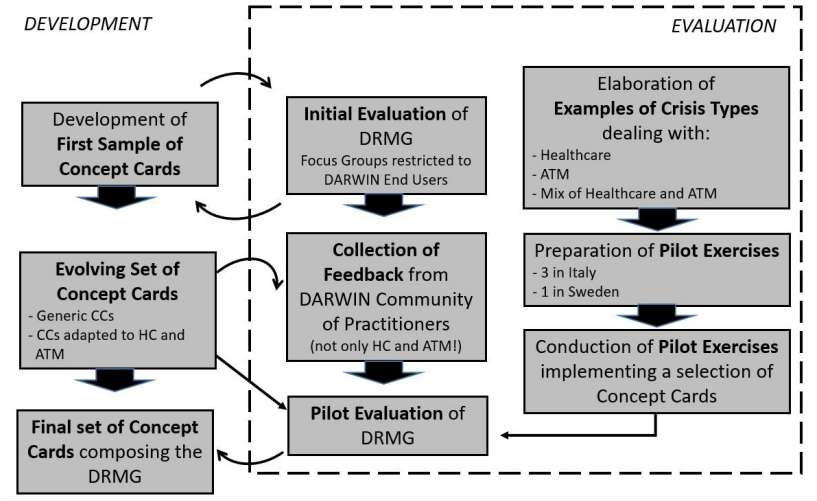


Figure 3: Evaluation of the DARWIN resilience management guidelines

- The initial evaluation has been performed already. It essentially consisted in two focus group meetings in which a first sample of three Concept Cards was analyzed in collaboration with experts from the three end-user organizations in DARWIN. The participants of the focus groups reflected on the potential use of the sample concepts cards in their own crisis management activities, providing feedback on their applicability and insights on the opportunities and showstoppers for their implementations in different contexts. Overall, they also helped to better understand the characteristics of the Concept Card format that are more important to develop.
- The collection of feedback from outside the project mainly occurred during a DCoP workshops organized in 2016 and 2017, which was attended by DCoP (approximately 25 people outside the project each time), belonging to 19 organizations, from 9 different countries. This allowed comparing the experiences of crisis management practices from countries different from Italy and Sweden and from sectors different from the HC and ATM (e.g., water and wastewater networks, civil protection organizations, fire, NGOs and rescue organizations).
- Finally, the core part of the evaluation will occur during the pilot exercises organized in the second part of 2017 in Italy and Sweden. The pilot exercises consist of different evaluation sessions taking as reference a set of crisis type scenarios identified and designed with the collaboration of the DARWIN end-user representatives. Each scenario will be used to investigate the impact of applying the guidelines in real crisis scenarios. Particular attention will be given to crises affecting a mix of the two main domains addressed in DARWIN, but the cascading effects on other domains will also be investigated, with adequate participation of experts from these domains (e.g., fire brigade, civil protection and regional emergency agencies).

The theoretical approach guiding the evaluation of concept cards is mainly informed by the I-CMO framework (Pawson and Tilley, 1997). This framework is appropriate for formative evaluation of social policies and change programs, and emphasizes the investigation of the conditions (Context) and impact (Mechanisms, Outcome) to understand the fitness for purpose of the Interventions proposed. This evaluation framework is therefore quite relevant to investigate operational issues associated with the implementation of the guidelines developed

Current and further work: Initial evaluation has been implemented and documented (Darwin deliverable D4.2). Pilots evaluation are currently ongoing in Sweden and Italy, DCoP members are invited to participate in the evaluation.

4 Scientific and societal contributions

In the areas of resilience engineering and community resilience, the project is essential in terms of addressing the gap between resilience theory and its practical application, by creating and producing:

- **Community of Resilience and Crisis Practitioners (DCoP)** is an open association including crisis and resilience practitioners which facilitates interactive communication concerning topics related to resilience. Members of the DCoP are from different CIs and are important contributors to and users of resilience management guidelines. Membership is voluntary. Activities include face-to-face workshop, webinars, surveys, interviews performed at different stages of the project. DCoP portal is part of DARWIN webpage.

- *Potential users:* CI managers and operators, crisis and emergency response managers, policy makers, practitioners, researchers, professionals (individuals and organizations).
- *Benefit for the users:* Share experience on resilience and crisis management across CIs. Contribute to resilience innovations and lead evolution of resilience research and practice
    - **Catalogue of resilience concepts and requirements for resilience management guidelines.** Worldwide catalogue of relevant resilience concepts, approaches and evaluation methods including users' experiences and existing practices and tactics.
      Potential users: Service providers - critical infrastructures; Policy makers and EU, researchers.
      Benefit for the users: Discovery and overview of concepts and strategies when dealing with real-life crisis situations to inform and educate practitioners.
    - **Practitioner and academic requirements for resilience management guidelines.**
      Overview of requirements derived from extensive literature and consensus among representatives from the Community of Practitioners (DCoP).
- *Potential users:* Policy makers, civil protection units, service providers of critical infrastructure, first responders, public and media
- *Benefit for the users:* Insights of current requirements for elaboration of guidelines from the end-users' perspectives.
    - **Generic resilience management guidelines.** The guidelines are developed around Concept Cards representing interventions to develop and enhanced specific resilience management capabilities. To facilitate storage, easy access and interactive development, the guidelines are organised in a knowledge platform DARWIN Wiki prototype.
- *Potential users:* Policy makers, decision makers and managers at different levels in a private or public organisation (national, international or local level. Those with responsibility for the functioning of a critical infrastructure and associated services.
- *Benefit for the users:* Harmonize resilience concepts across critical infrastructures. Enable organizations to enhance their resilience capabilities and practices supporting response when facing expected and unexpected events.
    - **Resilience Guidelines adapted to specific domains.** Generic resilience guidelines for critical infrastructures adapted to health care and ATM. Concrete examples of adaptation of the guidelines to make implementation easier.
- *Potential users:* Air Traffic Management and Health Care stakeholders with responsibility for the functioning of a critical infrastructure and associated services.
- *Benefit for the users:* Harmonize resilience concepts across critical infrastructures. Discovery and facilitate adaptation of the generic guidelines to specific needs and context.
    - **Tools for simulation, serious games and training.** Tools for simulation and serious gaming enable deployment of the guidelines. Simulation is used to support pilot exercises. Serious gaming, in the form of mini games, can be used by organisations to train their resilience concepts. Training modules on resilience management guidelines to be used by DARWIN users.
- *Potential users:* Ai CI managers and operators, crisis and emergency response managers, policy makers, practitioners, researchers, professionals (individuals and organizations).

- *Benefit for the users:* Improve understanding on resilience management concepts and associated interventions so they can start adapting DARWIN results in their CIs.
  - **Pilot demonstration.** Pilots' implementation and evaluation reports and videos documenting results for the application of the guidelines in different countries, and within two domains; ATM and health care.
- *Potential users:* CI managers and operators, crisis and emergency response managers, policy makers, practitioners, researchers, professionals (individuals and organizations).
- *Benefit for the users:* Assurance, concrete evidence and experiences of how organisations with the DRMG are better prepared to cope with expected and unexpected events.

5 Conclusions

DARWIN innovations are based on good interaction between academia and users. We create an arena where end users can provide their critical views and share experience contributing to the enhancement and operationalization of resilience concepts. DARWIN DCoPs have become co-creators of project results. The guidelines aim ease to recognise the complexity between different actors and interactions in the system with result of more efficient responses at different levels in the organisations.

So far, we have received positive feedback and appreciation on concept cards and wiki type applications. The prototype wiki application, foreseen virtual and face to face interactions with end users will enable the project to produce relevant and exploitable results.

Further work includes guidelines updates, development and experiment of serious games for training purposes and evaluation during pilot exercises. Virtual and face-to-face interactions with end users including the DARWIN Community of Practitioners.

Acknowledgements

The research leading to the results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653289. Opinions expressed in this publication reflect only the authors' view and that the Agency is not responsible for any use that may be made of the information it contains.

6 References

Detailed references available on DARWIN deliverables available at: www.h2020darwin.eu

[1] DARWIN D1.1 Consolidated resilience concepts and practices for crisis management
[2] DARWIN D1.2 Evaluation and Selection of Resilience Concepts and Approaches
[3] DARWIN D1.3 Practitioner and Academic Requirements for Resilience Management Guidelines
[4] DARWIN D2.1 Generic Resilience Management Guidelines
[5] DARWIN D3.1 Diverse representation and evolution of resilience guidelines support V1
[6] DARWIN D3.2 Diverse representation and evolution of resilience guidelines support Final
[7] DARWIN D4.1 Evaluation Plan
[8] DARWIN D4.2 Initial Evaluation of the Guidelines
[9] DARWIN D5.1 DARWIN Community of Risk and Resilience Practitioners (DCoP) – (previously CoCRP) Terms of Reference
[10] DARWIN D5.2 Resilience concepts users and academia interactive workshop (WS1)
DARWIN D5.3 Resilience concepts users and academia interactive workshop (WS2)
[11] DARWIN D6.1 Dissemination, Exploitation and External Collaboration Strategy
[12] DARWIN D6.2 Presentation of the Project

IMPROVER

David Lange, Project Coordinator

RISE Research Institutes of Sweden, Borås, Sweden

Corresponding author:
Dr David Lange
RISE Transport and Safety / Fire Research
Box 857, Borås, 501 15
Sweden
Phone: +46 (0) 10 516 5861
david.lange@ri.se

Abstract

IMPROVER (Improved risk evaluation and application of resilience concepts to critical infrastructure) is a three year Horizon 2020 project which was funded under the Horizon 2020 Secure Societies work program and aims to improve European critical infrastructure resilience to crises and disasters through the implementation of combinations of societal, organisational and technological resilience concepts to real life examples of pan European significance, including cross-border examples.

1 Introduction

Large scale crises are affecting critical infrastructures with a growing frequency. This is a result of both basic exposure and dependencies between infrastructures. Because of prohibitive costs, the paradigm of protection against extreme events is expanding and now also encompasses the paradigm of resilience. In addition to strengthening and securing systems; system design objectives are now being set, and response planning is being carried out, to facilitate a fast recovery of infrastructure following a large scale incident.

The IMPROVER project aims to develop a framework and associated methodologies to allow the resilience management of critical infrastructure to be operationalized alongside the existing risk management practices of the infrastructure operators. The project comprises three phases: an international survey to identify methods for implementing resilience concepts to critical infrastructure; an evaluation of these methods; and the further development of promising methods for application to European critical infrastructure. At the time of writing, the project is in its final stage, with the initial testing and iteration of the projects frameworks, prior to the planned pilot implementations, under way.

1.1 Project partners

The project consortium is comprised of 10 partners who collectively have the wide range of expertise required to complete the projects objectives. The project is coordinated by RISE, Research institutes of Sweden. The consortium includes 9 additional beneficiaries from throughout Europe including: DBI – the Danish Institute of Fire and Security Technology in Denmark, INERIS and the Euro-Mediterranean Seismological Centre in France, University College London and the University of Sheffield in the UK, RISE Fire Research and the Arctic University in Tromsø in Norway, INOV in Portugal, and the JRC's Institute for the Protection and the Security of the Citizen in Italy.

1.2 Project web-site and other media

The project website is available at www.improverproject.eu. The project also maintains an active social media presence, through twitter @improverproject; Research Gate and LinkedIn.

2 Background

According to the definition of the European Union [1], Critical Infrastructure (CI) is an asset, system or part thereof located in Member States (MS) which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions. These functions depend on networks of highly connected infrastructures forming complex systems of various sectors.

According to the Organization for Economic Cooperation and Development (OECD) [2], the benefit of interconnection of infrastructures is to allow for an easier and faster exchange of services of various forms. Although this is a natural consequence of technological development, the downside is that it increases the speed and scope for cascading failures or effects to occur in the event of crises [3], e.g. financial collapse, epidemics, or natural hazards that may affect whole networks of interdependent infrastructure. The World Economic Forum (WEF) also highlights that technology is changing physical infrastructure: "greater interdependence among different infrastructure networks is increasing the scope for systemic failures – whether from cyberattacks, software glitches, natural disasters or other causes – to cascade across networks and affect society in unanticipated ways" [4].

In 2010, the European Commission prepared guidelines for national Risk Assessment (RA) [5], based on which the MS prepare their assessments. These RA could be used in order to draw conclusions about the most important disaster risks that the societies in MS currently face [6]. One of the most addressed hazards of the national RA is the loss of CI.

Because CI is essential for the maintenance of vital societal functions, and CI disruption or destruction could have a significant impact in one or more than one MS, the European Commission adopted a proposal for a Directive on the identification and designation of European CI (initially focused on the energy and transport sectors) with the intention to improve their protection [1]. The Directive is implemented by the European Programme for CI Protection (EPCIP) [7], which recommends an all-hazards and sector-based risk management approach due to specificities of each sector.

Such a risk-based approach, however, has not been formalised and there is no single means of RA or risk evaluation which is commonly implemented across national borders or between sectors, unlike what is now becoming a European practice in the related field of Civil Protection.

The year 2012 marked the evaluation of EPCIP [8] as specified in the Directive, with conclusions and issues to be taken up in the future published in 2013 [9]. The 2013 conclusions take up especially two issues, namely increasing CI resilience and dealing with interdependencies. While there are some widely shared definitions on the latter concept, the concept and operationalization of CI resilience is much more obscure and contested. The revised EP-CIP also identified the limits of the sectorial approach and encouraged a systems approach to be followed, covering the issue of interdependencies between CI [9].

The National Risk Assessments (NRA) usually cover threat scenarios of national impact (they can affect the whole country or specific regions); whereas CI operators implement their risk treatment plans based on their own RA, which may also account for the same threats as in NRAs. Enriching NRAs with data from the CI operators is only partially done and usually at a regional level, as the complexity of modelling the effect to multiple CI increases when we consider threat scenarios of a national scale.

Recent years have seen a shift in focus – in both policy and technological analysis as well as on the political level – from protection to resilience of CI [9, 10].

2.1 Project objectives

The overall objective of IMPROVER is to improve European critical infrastructure resilience to crises and disasters through the implementation of combinations of societal, organizational and technological resilience concepts to real life examples of pan-European significance, including cross-border examples. This implementation will be enabled through the development of a methodology based on risk management techniques and informed by a review of the positive impact of different resilience concepts on critical infrastructures.

2.2 Description of the action

IMPROVER focuses on critical infrastructures comprising four living labs which are made up of the projects partners and associate partners. Working within and across these living labs, the partners in IMPROVER break down and study resilience concepts in order to better understand them and to evaluate and adapt potential methodologies for their implementation in critical infrastructure.

The interaction between different resilience concepts has been studied, as well as the impact of individual resilience concepts on critical infrastructure. The proposed framework arising from IMPROVER identifies opportunities for quantifying the overall reduction of risk to infrastructure resulting from the implementation of combinations of resilience concepts; as well as the potential for streamlining of the overall resilience strategy by identifying resilience concepts with overlapping effects.

By studying the impact of the complete or partial loss of critical services on society through improved population engagement we have also evaluated the impact of loss of critical infrastructure on society and propose to use this as a base line acceptance criterion for a resilience assessment methodology.

Operationalization of the methodology will be demonstrated via a pilot implementation to two of the living labs within the project. According to the description of work, the project is split into three stages: Stage 1 is a review

of existing methodologies; stage 2 is the assessment of existing methodologies (stage 2a) and the development of an improved methodology which is compatible with the EU risk assessment guidelines (stage 2b); and stage 3 is a pilot implementation of the improved methodology. As of the time of writing, we are at the end of stage 2b and working on stage 3.

3 Current project results

3.1 Work completed to date

The project consortium have reviewed the current approaches for defining, evaluating and implementing resilience concepts in critical infrastructure [11]. One of the outcomes from the literature review and the other project work which has been ongoing is a lexicon of definitions of terms related to critical infrastructure resilience [12]. Terms from this lexicon have already been included in the CIPedia platform.

The project relies on '4 living labs' for testing the methodologies and tools which we are developing and studying. One important task early on was the definition of relevant hazard scenarios to study within the project [13]. For this process we relied on a process of structured elicitation of expert judgement, which is a formalized process to determine a rational consensus among subject-matter experts on the uncertainties associated with problems where sufficient empirical or historical data is not available to characterize uncertainties statistically.

The first *Associate partner* workshop, intended to gather the projects associate partners together to present and discuss the projects results in plenary, was held at DBI's facility in Copenhagen in October 2015. The second workshop was held as an associated event with the CRITIS conference in Paris in October of 2016. The third is planned for the 21st of September in London.

The *operators* workshops are held annually in collaboration with the ERNCIP operators workshops. This allows an interaction between the IMPROVER partners and the ERNCIP thematic groups. The first workshop was held in April of 2016 at the JRC's Ispra site. The discussions with the ERNCIP operators and the thematic groups in one open forum were very fruitful [14]. The second operators workshop was also held at Ispra, in May 2017 and was equally successful [15]. The third is tentatively planned to be held in Lisbon in March 2018.

The project has also reported on the expectations of CI operators which the public has in times of crisis. It is based on a review of literature, semi structured surveys with CI operators within the living labs, and a public survey. Questions were focused on minimum acceptable level of service for food and essential goods, water, and transportation and expectations of help and information provided by CI operators [16].

The project consortium have developed the Critical Infrastructure Resilience Index (CIRI), for analysing the resilience of infrastructure based on indicators grouped under the phases in the crisis management cycle and mapped to the phases of the resilience triangle (resistance, absorption and recovery) [17]. We have also studied methodologies for measuring technological and organisational resilience independently [18, 19]; as well as developed guidelines for CI operator communication with the public in times of crises [20], an activity that can help to manage expectations from the public during the recovery phase of a crisis.

3.2 Progress beyond the state of the art

There is no consensus within scientific community about resilience or its correlates. Different authors argue for different definitions of resilience, which indicates how contested and ambiguous the concept is. While analysing the evolution of the concept, three facets of resilience were found in the literature, namely engineering resilience, ecological resilience, and social-ecological resilience.

While conducting our literature review, we found several tools and models for evaluating and measuring resilience. Within IMPROVER we also presented the Critical Infrastructure Resilience Index (CIRI), and demonstrated how the related methodology works with a few illustrations to different infrastructures. The methodology is applicable to all types of infrastructure, including a possibility to tailor it to the specific needs of

different sectors, facilities and hazard scenarios. The user of the methodology is supposed to be the critical infrastructure operator in terms of self-auditing. The innovative potential is that with CIRI one is able to transfer the quantitative and qualitative evaluations of individual sector-specific resilience indicators into uniform metrics, based on process maturity levels.

Including CIRI, all of the methodologies for resilience analysis require to account better for the requirements of a resilience assessment tool for CI operators. This is being addressed in work package 5 of the project, which is developing a resilience management framework including resilience analysis and resilience evaluation methodologies.

The proposal integrates the paradigm of resilience into the risk assessment process according to ISO 31000. The framework is nested and consists of three levels, namely (a) asset (focus on individual CI assets), (b) system (focus on dependencies between CI assets) and (c) national (focus on societal aspects). It is applicable to individual CI assets accounting both for existing risk assessment activities (at the operator level) and input from national risk assessments, while at the same time employing current, available resilience analysis tools. The framework can also be applied on a system level, accounting for the results of risk and resilience assessment of individual assets, but also accounting for interdependencies and their effect on performance on interconnected CI.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653390.

4 References

[1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union, 23 December 2008.

[2] OECD, 2011. Future Global Shocks, Improving Risk Governance. OECD Reviews of Risk Management Policies. ISBN 978-94-09520-5. 139 p

[3] Lee, B., Preston, F. & Green, G., 2012. Preparing for High-Impact, Low probability events, Lessons from Eyjafjallajökull. A Chatam House Report, 47 p.

[4] World Economic Forum, The Global Risks Report 2017 12th Edition, 2017.

[5] SEC (2010) 1626 Final commission staff working paper Risk Assessment and Mapping Guidelines for Disaster Management.

[6] De Groeve, T., 2013. Overview of Disaster Risks that the EU faces. Publications Office of the European Union, JRC Scientific and Policy Reports. EUR 25822 EN.

[7] COM(2006) 786 final, Communication from the Commission on a European Programme for Critical Infrastructure Protection.

[8] SWD(2012) 190 final, Commission Staff Working Document on The Review Of The European Programme for Critical Infrastructure Protection (EPCIP) Brussels, 22.6.2012.

[9] SWD(2013) 318 final, Commission Staff Working Document a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, Brussels, 28.8.2013.

[10] Pursiainen, C. and Gattinesi, P., 2014. Towards Testing Critical Infrastructure Resilience; Joint Research Centre Institute for the Protection and Security of the Citizen; ISBN 978-92-79-36632-1; doi:10.2788/41633.

[11] L. Melkunaite; M. Alheib; G. Baker; G. Cadete; E. Carreira; K. Eriksson; C. Gaspar; P. Gattinesi; F. Guay; D. Honfi; I. Ioannou; J. Kinscher; D. Lange; L. Petersen; P.J. Reilly; B. Rød; R. Salmon; R. Stevenson; M. Theocharidou; A. Utkin; IMPROVER Deliverable 1.1 International Survey; 2016; available from www.improverproject.eu

[12] M. Theocharidou; L. Melkunaite; K. Eriksson; D. Winberg; D. Honfi; D. Lange; F. Guay; L. Lin; IMPROVER Deliverable 1.3 Final Lexicon of definitions related to Critical Infrastructure Resilience; 2016; available from www.improverproject.eu

[13] I. Ioannou; W. Aspinall; C. Bouffier; E. Carreira; D. Honfi; D. Lange; L. Melkunaite; N. Reitan; T. Rossetto; K. Storesund; R. Teixeira; IMPROVER Deliverable 2.1 Methodology for identifying hazard scenarios to assess the resilience of critical infrastructure; 2016; available from www.improverproject.eu

[14] M. Theocharidou; D. Lange; IMPROVER Deliverable 1.4 Report of operator workshop 1; 2016; available from www.improverproject.eu

[15] M. Theocharidou; IMPROVER Deliverable 1.5 Report of operator workshop 2; 2017; (Pending)

[16] L. Petersen; L. Fallou; P. Reilly; E. Serafinelli; E. Carreira, A. Utkin; IMPROVER Deliverable 4.1 Social resilience criteria for critical infrastructures during crises; available from www.improverproject.eu

[17] C. Pursiainen; B. Rød; M. Alheib; G. Baker; C. Bouffier; S. Bram; G. Cadete; E. Carreira; P. Gattinesi; F. Guay; D. Honfi; K. Eriksson; D. Lange; E. Lundin; A. Malm; L. Melkunaite; M. Merad; M. Miradasilva; L. Petersen; J. Rodrigues; R. Salmon; M. Theocharidou; A. Willot; IMPROVER Deliverable 2.2 Report of criteria for evaluating resilience; 2016; available from www.improverproject.eu

[18] D. Honfi (editor); D. Lange; A. Malm; P. Mindykowski; M. Alheib; C.Bouffier; L. Cauvin; A. Willot; I. Ioannou; B. Rød; IMPROVER Deliverable 3.2 Technological resilience concepts applied to critical infrastructure; 2017; available from www.improverproject.eu

[19] E. Serafinelli; P. Reilly.; R. Stevenson; L. Petersen.; L. Fallou.; E. Carreira.; IMPROVER Deliverable 4.2A communication strategy to build critical infrastructure resilience; available from www.improverproject.eu

[20] S. Bram; H. Degerman; L. Melkunaite; T. Urth; E. Carreira; IMPROVER Deliverable 4.Organisational resilience concepts applied to critical infrastructure; available from www.improverproject.eu

RESILENS

Dr. William Hynes*

Future Analytics Consulting Ltd., Dublin, Ireland

Corresponding author:
Dr. William Hynes
Future Analytics Consulting Ltd. (FAC)
23 Fitzwilliam Square
Dublin 2
Ireland
Phone: +353 (0) 1 639 4836
william.hynes@futureanalytics.ie

(*with inputs from the entire RESILENS consortium)

Abstract

RESILENS (Realising European ReSiliencE for CritIcaL INfraStructure), is a three year, EU H2020 funded project with 12 consortium partners across Europe, including CI providers, owners, operators, and municipal and regional authorities. Over the course of the project, RESILENS will develop a European Resilience Management Guideline (ERMG) to support the practical application of resilience to all CI sectors. Accompanying the ERMG will be a Resilience Management Matrix and Audit Toolkit (ReMMAT) which will enable CI systems (encompassing assets and organisations) to quantitatively and qualitatively index their level of resilience. The proposed toolkit will also allow for the quantitative analysis of the resilience of the CI systems at different spatial scales (urban, regional, national and trans-boundary), which can then be iteratively used to direct users to aspects of their systems where resources could be concentrated in order to further improve their resilience levels. The ERMG and resilience management methods have been tested and validated through stakeholder engagement, table-top exercises and three large scale pilots (transport CI, electricity CI and water CI) in Germany (BASt), Ireland (Irish Water) and Portugal (EDPD and CML). The ERMG and accompanying resilience methods will be hosted on an interactive web based platform, the RESILENS Decision Support Platform (RES-DSP). The RES-DSP will also host an e-learning hub that will provide further guidance and training on CI resilience. Overall, RESILENS will aim to further advance the state of the art in CI resilience management and intends to increase and optimise the uptake of resilience measures by CI stakeholders.

1 Introduction

In an era that has seen a multitude of high impact disasters and crisis events ranging from natural events such as earthquakes and floods to man-made acts of terrorism and cyber attacks, there is a greater need than ever before to assess the resilience of modern societies to withstand and recover from unexpected adverse events. Against this backdrop, concepts of resilience offering all encompassing, integrated approaches to planning for, responding to and recovering from all manner of man-made and natural disasters have gained increasing attention within recent discourse on disaster and crisis reduction and management.

In particular, the frequency and severity of impacts of disasters and crises events has channeled increasing attention to vulnerable physical assets – including towards Critical Infrastructure (CI). CI provides essential functions and services that support societal, economic and environmental systems at national and European scales. As disasters and crises, both natural and man-made, become more commonplace, the need to ensure the resilience of CI so that it is capable of withstanding, adapting and recovering from disruptive events, is paramount. Moving resilience from a conceptual understanding to applied, operational measures that integrate best practice from vulnerability assessment and risk management is the focus of the RESILENS project.

RESILENS (Realising European ReSiliencE for CritIcaL INfraStructure), is a three year, H2020 funded project with 12 consortium partners across Europe, including CI providers, owners, operators, and municipal and regional authorities (A full list of consortium partners is included in the 'Acknowledgements' section of this article). It is coordinated by Future Analytics Consulting (FAC), a spatial planning, economics and research consultancy based in Dublin, Ireland. The project has an ambitious but achievable and practically applied research agenda that will result in significant advancements in the resilience of CI. The primary aim of the RESILENS project is to develop a user-friendly, citizen centric European Resilience Management Guideline (ERMG) which is founded in the principles of risk management and vulnerability reduction and which will, through its uptake and interactive qualities, lead to clear, coherent and effective crises and disaster resilience management for Critical Infrastructure, and in turn will contribute to more resilient and secure economic and societal systems. This article outlines progress towards achieving this central goal.

2 Background

The last two decades have been remarkable for the volume of high impact crises disasters and global incidents which have highlighted the vulnerability, complexity and interdependency of contemporary infrastructure. In turn these events have been catalytic in advancing the political prioritisation of enhanced security and risk management strategies. As a result, they have fostered greater interest in the concept of resilience, which its proponents contend offers an all-encompassing, integrated approach to planning for, responding to and recovering from all manner of disruptive events, as well as a new way to engage with future uncertainty and the wider issue of complexity (Coaffee et al, 2008; UNISDR, 2012; Zolli and Healey, 2013; Chandler, 2014).

While the interest in resilience has been shaped by recent disaster events and their social consequences, so too has the focus on CI sprung from service disruptions, accidents and in particular, cascading failures. Indeed, an integrated and holistic approach to resilience is especially important due to the increasing system complexities and interdependencies associated with current CI systems, where the cascading effects of a system breakdown on other interconnected systems is of significant concern (Rinaldi et al, 2001). Interdependencies, which lead to cascade failures, can be classified as having a spatial dependency, due to location, or functional dependency as a result of functional reliance's (such as electricity for ICT control networks) (ibid). A vivid example of cascade failure in CI,is provided by the events following the attack on the World Trade Centre in New York :

> *"The WTC disaster provides a graphic illustration of the interdependencies of critical infrastructure systems. The building collapses triggered water-main breaks that flood rail tunnels, a commuter station, and the vault containing all of the cables for one of the largest telecommunication nodes in the world."* (O'Rourke, 2007: 25)

Given the vital importance of CI to a functional society, its protection is progressively being enshrined in a range of national and transnational policies and institutions. Increasingly it is the concept of resilience which is shaping the way in which we perceive the challenges that CI faces as well as providing a potential framework by which to respond. However, whilst resilience is something which is seen as positive and a position to be attained, it is a term which remains highly contested and with varied interpretations understood both in theory and, more particularly, in practice. These disparate readings and understandings of resilience are increasingly translated into a variety of different approaches to resilience enhancement, which vary according to the study areas or settings in which they are adopted. Moreover, it is critical to note that to date the majority of work on resilience has been predominantly theoretical and insufficiently grounded in everyday practice (Coaffee and Clarke, 2015). It is this gap in the state-of-the-art which the RESILENS project seeks to fill and advance.

2.1 Resilience Management for C.I

As part of the RESILENS project, one of the early tasks involved a current state of the art (SOTA) assessment with regards how resilience management is currently practiced in CI within each of the project partner nations. Using the knowledge and experience of the project consortium, these findings were ultimately made available for the USA, European Union, Germany, Ireland, United Kingdom, Portugal, Canada, Australia and Israel. To supplement this, infrastructure providers from Germany, Ireland and Portugal provided their practitioners' view on the current implementation and application of resilience aspects in their responsibility. The findings are summarised below.

One general headline finding of this review is that currently there is no uniform implementation standard for CI resilience in the considered countries nor is there a consistent definition for resilience. In all countries, there are policies and/or guidelines for CI protection, partially only for individual infrastructures. These approaches generally relate to the identification and the assessment of hazards and risks. For example, in Germany all legal requirements and other policies focus on hazard analyses, risk analyses or risk managements, whilst in Ireland the approach currently applied for infrastructure management has mainly been focused on the identification and assessment of risks and hazards, highlighting the impacts/consequences of those hazards.

In most countries, the approaches nevertheless go beyond this basic approach and consider further aspects of resilience. This mainly comprises responding to disruptive events. In Germany for example there is a risk management cycle, consisting of prevention, implementation and exercises, response as well as analysis and evaluation. Likewise, in Ireland the approaches go beyond pure risk management by putting forward schemes guiding the preparation and execution of emergency responses in the event of a hazard. However, this review also demonstrated how resilience management approaches utilise different stages and cycles in different countries, focusing most often upon the earliest stages. However, in almost all countries there are risk-related approaches. To find a solution to combine risk-related approaches with the resilience management developed in the RESILENS project is thus a central issue.

It was thus proposed that RESILENS adopts a necessarily broad interpretation of resilience that will allow us to operationalise it within the working practices of CI, in all its forms and scales which encompasses key resilience principles, but is sufficiently flexible enough to be useful across the full range of CIs, as follows:

> *'Resilience is the ability of a system or systems to survive and thrive in the face of a complex, uncertain and ever-changing future. It is a way of thinking about both short term cycles and long term trends: minimizing disruptions in the face of shocks and stresses, recovering rapidly when they do occur, and adapting steadily to become better able to thrive as conditions continue to change. Within the context of CI, the resilience process offers a cyclical, proactive and holistic extension of risk management practices.'*

In defining CI resilience specifically, the project has developed the following conceptualisaton:

'Critical Infrastructure Resilience is 'a transformative, cyclical process, that builds capacities in technical, social and organisational resources for critical system function, so as to mitigate the impacts of disruptive events and long-term incremental changes, thus guaranteeing the continued provision of its basic functions. CIR is based upon new forms of risk management, adaptability and the assessment of potential trade-offs between parts of a system'.

Fundamental to the RESILENS approach is the view that current attempts to enhance the resilience of CI are 'transitional' and represent an extending of traditional risk management orthodoxies. This reflects a wider journey from the traditional, techno-rational approach with prescriptive, rigid methodologies to a more transformative understanding of CIR that benefits longer-term viewpoints and complex system dynamics. These would focus more on adaptability, flexibility and holistic thinking which seek to move beyond defence and protection and embrace resilience. This approach recognises the importance of risk management processes to the CI sector. However, we must also be aware how the complexities of large, integrated CI systems, the scope of their interdependencies and the uncertainty of future events, predicates the use of resilience approaches and newer forms of resilience management praxis.

The RESILENS project identified a range of knowledge, assessment and operational barriers, which currently restrict the extent to which CI operations can transition from a modus operandi focused on protection to one which embodies the principles of resilience. For example, there are knowledge barriers including:

- Lack of a clear practical definition of resilience;
- Gaps in information sharing between agencies;
- Non-use of common platforms and lexicon;

Resilience assessment barriers are also evident and include:

- Difficulty in evaluating impact;
- Problems around exposure and concerns about sharing of sensitive information with other organisations;
- Financial benefits have not been made concrete.
- Not integrated in current widely adopted assessment tools and methods.

Together, these barriers combined with shortcomings in institutional infrastructure have also served to create a range of operational barriers to the operationalisation of CI resilience practice:

- Financial restrictions and reasons (no legal requirement);
- Difficulty in having system redundancies (sub-optimisation);
- A lack of political drive and guidelines;
- Disinterest of managers (especially since resilience is perceived as a passing buzz word);
- Lack of technical knowhow and human resources to facilitate resilience.
- Resistant to changing organisational culture.

Foremost amongst these barriers were organisational capacities and resources; primarily financial. As such, many CI stakeholders associated resilience with additional redundancy and thus increased costs. Given the difficulties of evaluating the impact of resilience measures and 'management indifference', it was not an organisational priority. This problem was often compounded by the absence of methodologies, guidelines and political drive/legislation. While an integrated conception of CI resilience, including an understanding of cross-sector impacts, was identified as key to the enhancement of CIR, this was often limited by business sensitivities around information sharing. At a holistic level, a resistant culture and a lack of 'buy-in' by stakeholders was seen as a critical barrier to resilience practice.

Overall, there are a range of 'barriers' that highlight 'gaps' in the current drive towards advancing CIR. Increasing resilience is ultimately about change and unpacking the implications of this on the CI sector is central to RESILENS: how can our desired outcomes be operationalised? How can we measure and monitor the success of this change? And, what are the implications of this for society and economy?

In the below sections we set out our vision/goals as a set of outcomes that has emerged from both our existing understanding of attempts to enhance the resilience of CI as well as the noted gaps in practice expertise.

3 Scientific contributions

The primary aim of the RESILENS project is to develop a user-friendly, citizen centric European Resilience Management Guideline (ERMG) which is founded on the principles of risk management and vulnerability reduction and which will, through its uptake and interactive qualities, lead to clear, coherent and effective crises and disaster resilience management for Critical Infrastructure, and in turn will contribute to more resilient and secure economic and societal systems. The ERMG builds on existing good practice in risk based management of critical infrastructure protection (CIP) to develop a more process-orientated, resilience understanding of CI resilience (CIR) and CI resilience management (CIRM).

Two fundamental requirements for the development of the ERMG within RESILENS have been defined as follows:

- To develop an ERMG which will operationalise crisis and disaster resilience concepts that are specifically tailored to CI, and within which risk management approaches are inherently embedded, and;
- To prove its applicability for all types of CI, and to validate its effectiveness in successfully addressing human and social dynamics which are critical to resilience, through pilot implementation.

The ERMG provides CI organisations with tools for managing the resilience of their CIs. It provides the ability to deal with the range of central issues associated with CI resilience management in a generic and straightforward manner. This ability is expressed in the following:

- Presentation of the CI resilience management methodology as a cycle and the provision of a common language for CI resilience management.
- An explanation of resilience including the reasons and considerations behind CI resilience management.
- Guidelines on how to assimilate resilience management in their organisations.

The ERMG has four parts:

Part A: Foreword – an introduction covering the objectives and explaining what the ERMG provides.

Part B: What is resilience and resilience management; Why is it necessary – the implications.

Part C: How to implement it in your organisation – associated issues & guidelines

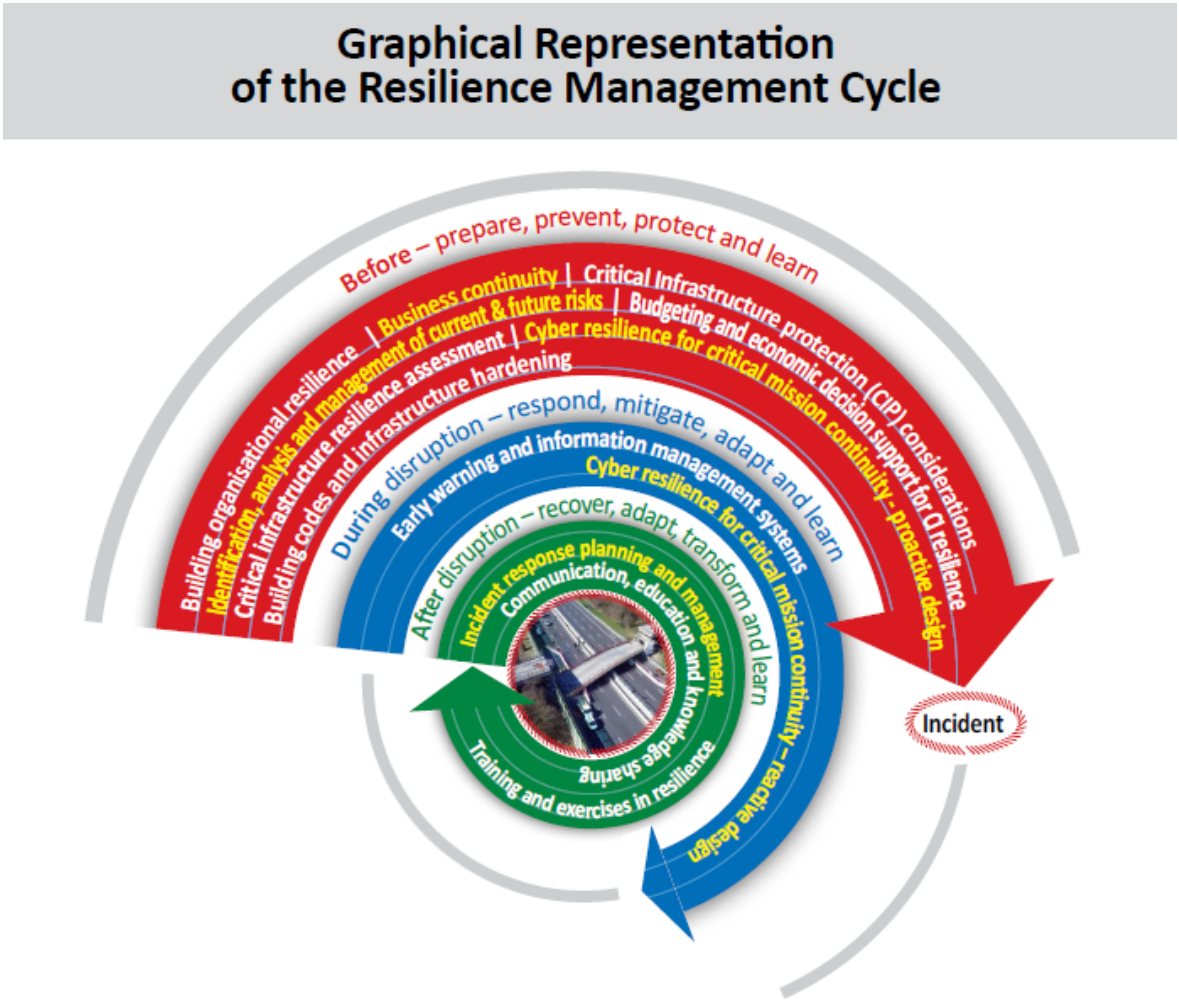
Part D: Annexes – acronyms, definitions, supporting information and project overview.

Thus, the ERMG provides a step-by-step guide for organisations to enhance the resilience of individual and interconnected critical infrastructure systems. This process builds upon existing good practice in risk management, augmented through organisational and change management requirements. This new approach seeks to move from the more technical and risk based understandings of critical infrastructure protection (CIP) to a more process-orientated, resilience understanding of critical infrastructure resilience (CIR). It seeks to assist stakeholders to transition into adopting resilience into their everyday working practices. This is translated through the steps and stages approach to critical infrastructure resilience management (CIRM), which establishes a systematic yet flexible process that promotes greater foresight, organisational learning and collaboration, with the inclusion of social, organisational and behavioural factors.

Unique to RESILENS, this process is both ‘multi scalar’ and ‘multi sector’ in its scope; allowing a holistic approach to resilience to be considered and improved at a range of scales from the local to the national, and as a means to tackle the implicit interdependencies, and includes the more traditional utilities of power, water and transport, with the increasing range of ‘social infrastructures’ such as health provision and social care. Further, the ERMG seeks to assist both the operators and owners of CI, organisations that work alongside them, such as emergency services, as well as providing guidance to those who have a key interest in the CIs approach, such as regulators,

local government and resilience forums. The ERMG may also assist operators and owners of other infrastructure that may not be legally identified as CI.

To build this diverse and holistic approach to resilience, there is a need to establish shared understandings and concepts of resilience. To do this, the ERMG provides a comprehensive guide to measuring and understanding resilience within the CI sector, through a series of structured sections that address the key concerns and considerations through an ongoing and iterative process. For example, a graphical representation of the draft resilience management cycle included within the ERMG is included below.



Key to the ERMG approach is the connection to the RESILENS toolkit and the e-Learning hub. The primary purpose of the ERMG is to establish a shared understanding and outline the process of managing resilience within the CI sector, but it also directs users to sources of more detailed information: the ReMMAT toolkit provides a means to measure and audit resilience in a bespoke manner, whilst the e-Learning hub functions as an education resource for organisational learning. In doing so, the ERMG presents resilience management as a process which extends the risk practices of organisations to incorporate the much wider appreciation of resilience.

3.1 ReMMAT

As outlined above, accompanying the ERMG will be a Resilience Management Matrix and Audit Toolkit (ReMMAT). The web based ReMMAT is a combination tool of complementary methods, encompassing a suite of

functionalities and is designed to operate in logical progression as a "single functioning unit" to achieve the overall goal of providing a resilience assessment function, resulting in the scoring of the resilience level of the CI system evaluated. In addition to this, the resilience evaluation function of the toolkit also provides an indication of the most relevant stages of the resilience cycle that the CI operators can focus on, as a means to further improving their resilience levels. The ReMMAT also contains an audit tool aimed at providing guidance to the CI operators on the interpretation of their obtained resilience scores, how to use the scores, and to support the incorporation of organisational, societal and political considerations for developing implementable resilience enhancement strategies. In addition, a GIS visualisation of the resilience of investigated CI assets or systems is provided in the ReMMAT toolkit which is linked to the resilience scores, and supports the CI operator/owners understanding of the spatial resilience status of the different investigated assets in their CI system.

3.2 RES-DSP

The ERMG and accompanying resilience methods will be hosted on an interactive web based platform, the RESILENS Decision Support Platform (RES-DSP). The RES-DSP will also host an e-learning hub that will provide further guidance and training on CI resilience. It is important to note that the Resilience Management tools will form part of the ERMG (within the methods sections), but will also be available as stand-alone applications on the RES-DSP.

A number of technical objectives will support the development and application of the RES-DSP, as follows:

- Operationalisation of the ERMG and Resilience Management tools components of the RES-DSP to prove its applicability, through pilot demonstrations which will allow multiple simulated testing events and will address the entire life-cycle of a crisis/disaster involving a man-made threat or natural disaster.
- Develop an integrated multi-agency CONcept of OPerationS framework (CONOPS) focusing on the roles of the various stakeholders, their interactions, critical dependencies, use of resources and knowledge requirements. This will include the roles and activities of emergency responders, utilities providers, infrastructure managers and public administration as well as examining the role of the citizen in terms of achieving and maintaining resilience.
- Through the ERMG, provide a solid foundation on which future regulatory standards for application across all CI sectors may be formulated.

3.3 Pilot Demonstrations

The ERMG, the ReMMAT and the components of the RES-DSP were tested and validated through stakeholder engagement, table-top exercises and three large scale pilots (transport CI, electricity CI and water CI) across three national contexts – in Germany, Portugal and Ireland.

These Pilot Demonstrations aimed to operationalise and validate the draft ERMG and management tools across a number of CI and public settings, in conditions which were as close to real world conditions as possible. This was achieved through a series of real world, or simulated real world, pilot actions, to demonstrate the applicability of the ERMG and ReMMAT in relation to different forms of threats/risks and within the context of varying types of CI and spatial scales. The demonstrations were hosted in operational environments in collaboration with the CI provider partners. They involved multiple participating actors, including municipalities, regional or national authorities and wider society, and they featured a mix of actual and simulated data. They were designed to be as close to real world scenarios as practicable, in order to represent an accurate evaluation exercise, and to ensure that the resulting final ERMG and ReMMAT are fit for purpose and lead to delivery of best practice.

Following these demonstrations, a large number of recommendations were recorded in relation to improving the ERMG in terms of language, simplicity, clarity, formatting, presentation, graphics, consistency etc. Numerous recommendations were also made in relation to concepts, topics and content. The pilot demonstrations also

generated much practical feedback regarding ReMMAT functionality, efficiency and added value. The CI partners considered how they would envisage their organisation using the tools and potential benefits that could be gained from their use e.g. by adding functionality which facilitates inputs and comparison of resilience scores across different departments allowing an organisation to identify where improvement in resilience awareness, practice or resources might be needed.

The demonstrations also provided a wider set of lessons around conducting such testing exercises. A key thread running through all of the pilot demonstrations was the benefit and importance of bringing different organisations and stakeholders to work together, face to face, to address resilience and interdependencies. Benefits included, for example, establishing lines of communication, developing contacts and relationships, understanding each others functions, services and limitations, and laying the groundwork for a collaborative approach to preparing for and responding to incidents/crises.

Our overall conclusions in relation to these exercises are that (a) the Pilot Demonstrations were effective in testing the value of the ERMG and (b) results demonstrate that the ERMG will provide significant value to the enhancement of European Resilience Management. Indeed, within the Irish context, partners indicated that the process of going through the ERMG was "very thought provoking" and a valuable way to reflect on their "existing processes in place for dealing with all of the resilience management concepts presented". It also provided clarified awareness and insight into the different departments and the roles played by them in such activities. Similar feedback was recorded in the Portuguese context, with partners reporting that the demonstrations also promoted greater awareness of and reflection around the different roles played different actors within the organization. In Germany, significant positive feedback was recorded regarding the principles and actions of the tools and guidance. For example, it was reported that RESILENS outputs will be beneficial to provide a good holistic/collective overview of the overall resilience of the whole organisation and its processes, whereas previously the participant organisations would only have considered resilience at asset level.

4 Conclusions

As part of its overarching objectives, RESILENS aims to further advance the state of the art in CI resilience management and intends to increase and optimise the uptake of resilience measures by CI stakeholders. Key to the RESILENS understanding of CIR is that resilience is a property of a system and that CIs need to be considered as a system within a wider system of systems; often defined at a spatial level. By contrast, initial stakeholder engagement within the project found that often CI providers' primary focus is on internal priorities. Stakeholders also appeared to confirm the limitations of traditional risk management approaches, with the acknowledgment that understanding of cross-sectoral or cascading impacts were currently beyond existing measures, and hence the need for new and updated solutions. Indeed, as a whole, the stakeholder engagement exercises conducted over the past number of years – including within the pilot demonstrations - have yielded much evidence of the burgeoning need for more holistic and developed resilience approaches, benchmarks and associated tools of the kind being developed in RESILENS.

For more information on the RESILENS project please visit www.resilens.eu

Acknowledgements

This research was supported by the work carried out as part of the EU RESILENS project "Realising European Resilience for Critical Infrastructure", Grant no 653260. I am thankful to my RESILENS consortium colleagues who provided expertise and input which greatly assisted the development of this article. A list of the full RESILENS consortium is provided below.

- Federal Highway Research Institute (BASt), Germany
- Camara Municipal de Lisboa (CML), Portugal
- Eastern and Midland Regional Assembly (EMRA), Ireland
- EDP Distribuição (EDPD), Portugal

- Factor Social, Portugal
- Fraunhofer, Germany
- Future Analytics Consulting (FAC), Ireland
- Irish Water, Ireland
- MTRS, Israel
- Skills for Justice, UK
- Trinity College Dublin, Ireland
- University of Warwick, UK

5 References

[1] Chandler, D. (2014) Beyond neoliberalism: resilience, the new art of governing complexity. Resilience, 2 (1), p.47–63.

[2] Coaffee, J., Murakami Wood, D. & Rogers, P. (2008) The Everyday Resilience of the City: How Cities Respond to Terrorism and Disaster. Palgrave/Macmillan, London.

[3] O'Rourke, T.D (2007) Critical Infrastructure, Interdependencies, and Resilience, The Bridge – Linking Engineering and Society, 37(1), pp. 22-30.

[4] Rinaldi, M., Peerenboom, J.P. and Kelly, T.K., (2001) Critical Infrastructure Interdependencies, IEEE Control System Magazine, 12.

[5] UNISDR (2012) How to Make Cities More Resilient - A Handbook for Mayors and Local Government Leaders.United Nations International Strategy for Disaster Reduction, Geneva.

[6] Zolli, A. & Healy, A. (2013) Resilience: Why Things Bounce Back. Headline, London

RESOLUTE

Dr. Emanuele Bellini, Project Coordinator

University of Florence, Italy

Corresponding author:
Emanuele Bellini
University of Florence
DISIT Lab
Piazza di San Marco, 4,
50121 Firenze FI
Italy
emanuele.bellini@unifi.it

Abstract

The RESOLUTE project works on identifying solution to make city critical infrastructures such as the transport system, energy, etc., more resilient; that means capable to react and recover to unexpected natural and manmade disasters through sustaining their continuous adaptation to changing conditions. The project has produced guidelines and tools for supporting city operators to be more prepared, to better react and to recover efficiently from those critical situations that seem to more frequently occurring because of the increasing complexity and interdependency of the socio-technical systems. The solutions are under trial in Florence and will be also used in Athens, and consist of a number of instruments (such as European Resilience Management Guidelines, control room and decision support solution) for the city operators, but also for the citizens to be prepared and promptly informed to reduce their personal risk and discomfort. The technologies adopted are derived from the big data science and the artificial intelligence. RESOLUTE has provided a 3 tier platform composed by :

- Semantic aware Big Data platform for aggregating data in a city coming from different sources
- Collaborative Resilience Assessment and Management Support System (CRAMSS)
- Dashboard for displaying resilience-relevant data to the different stakeholders (the Mayor, the Control Room, the Fire Brigade, the public utilities, etc),
- a game-based app to teach citizens suggested behaviours in case of emergency

1 Introduction

Increasing resilience to critical events is a topic of highest political concern in the EU. Regarding the case of transport systems, operations have developed a prominent safety and business critical nature, in view of which current practices have shown evidence of important limitations in terms of resilience management. Enhancing resilience in transport systems is considered imperative for two main reasons: such systems provide critical support to every socio-economic activity and are currently themselves one of the most important economic sectors and secondly, the paths that convey people, goods and information, are the same through which risks are propagated.

The RESOLUTE EC-funded project, based on the vision of achieving sustained adaptability of UTS (Urban Transportation System) to enhance resilience, is tackling these challenges. The final goal of RESOLUTE is to adapt and adopt the identified methods for the operationalization of the European Resilience Management Guidelines and for their evaluation when addressing UTS as a Critical Infrastructure. The resilience is considered an emergent property of a complex system and it is about managing high variability and uncertainty in order to continuously pursue successful performance of a system. Understanding the sources of operational variability, the mechanisms through which it may potentially propagate and the impact on the system performance, are at the core of RESOLUTE approach. The resources and system capacities needed to manage and cope with operational variability are the main drivers of the analysis.

The issue at hand is to deliver management guidance on such human, technical and organisational elements, aiming to respond to different and possibly conflicting local operational needs, whilst achieving fundamental system level synchronisation and coordination that, as best possible, ensures successful operation. This requires three fundamental methodological stages:

- system analysis and understanding in support of the identification of relevant aspects and critical functions through the application of tools like FRAM, RAG and Network analysis/science techniques that also permit to infer, model, simulate and predict possible events propagation, preventing/mitigating cascading behaviour in the complex socio-technical system;
- (Big) Data (i.e. from the smart city) gathering, semantic processing and mining to connect data flows to the models. Such a data driven analysis provides the means to assess the levels of criticality of interdependencies at evidence and quantitative level and seeks to enhance the capabilities of UTS to take right decision at strategic, tactical and operational level, with the aim of maintaining operations under continuously changing conditions;
- a Collaborative Resilience Assessment and Management Support System able to adopt an highly synergic approach towards the definition of a resilience model for the next-generation of collaborative emergency services and decision making process. Within this framework, it can be stated that the pursuit of RESOLUTE objectives faces the challenge of relating dynamic and emergent system features, to a wide diversity of human, technical and organisational elements that at each time and place, generate equally diversified operational needs.

The RESOLUTE project is a 3-year funded project

Project partners

University of Florence (coord.)

End users

- City of Florence
- ATTIKO Metro

Industry

- Thales Italia
- Swarco Mizar

Academia & Research org.

- CERTH
- Consorzio Milano Ricerche
- Universidade Lusófona

Stakeholder Network

- Humanist

Project website:

www.resolute-eu.org

2 Background

European UTS. The project recognises foremost the on-going profound transformation of urban environments in view of ecological, human and overall safety and security needs, as well as the growing importance of mobility within every human activity. Sustainability is rapidly becoming an imperative need across all economic and social domains. Among many things, this requires overall heightened operational efficiency, mainly by optimising the allocation and utilisation of available resources (organisational technical and human), whilst striving to continuously minimise any source of waste, namely incidents, accidents and other operational failures. Within this context, RESOLUTE considers resilience as a system ability to continuously adjust to ever-changing operational environments to damp system variability. According to this the RESOLUTE project objectives are:

- • Development of European Resilience Management Guidelines (ERMG) able to support decision makers in applying those improvements capable to dampen daily system variability.
- • Operationalize and validate the ERMG by implementing the RESOLUTE Collaborative Resilience Assessment and Management Support System (CRAMSS) for Urban Transport System (UTS) addressing Roads and Rails Infrastructures.
- • Enhancing resilience through improved support to human decision making processes, particularly through increased focus on the training of final users (first responders, civil protections, infrastructure managers) and population on ERMG and RESOLUTE system

3 Scientific Contribution

The main RESOLUTE project contribution can be summarised in the following outcomes:

a) The European Resilience Management Guidelines for CI and their UTS adaptation; and
b) The ERMG operationalization that includes the development of a 3 tiers platform:
   - Semantic aware Big Data platform (backend)
   - Collaborative Resilience Assessment and Management Support System (CRAMSS)
   - Dashboard
   - Game base training app

European Resilience Management Guidelines

The aim of the ERMG is to support decision makers of different critical infrastructures in a self-evaluated multilevel gap analysis for resilience improvement. To this end the ERMG development has adopted a system perspective applying the Functional Resonance Analysis Method (FRAM) to model a generic CI of reference and to identify which are the desired functions and the related interdependencies that should be implemented in a CI to be

resilient. The activity has defined 25 functions and for each one has been provided a number of recommendations on how to dampen its performance variability to continue to deliver the desired outcome under unexpected changed condition. The objective is to sustain adaptive capacity of the system to continuously changing conditions and the continue and coherent pursuit of the goal within their own timescales. The ERMG has been designed taking into account that they will be used by multiple experts.

RESOLUTE ERMG Operationalization

The ERMG operationalization includes the implementation of those technologies needed to support system adaptive capacity. In this respect, a 3-tier evidence driven platform composed by a) Semantic aware big data layer, b) CRAMSS, c) Dashboard, has been implemented.

1st platform tier - Semantic aware Big Data Layer (SBDL)

There are four types of data being collected and managed by the SBDL and used by the CRAMSS: urban data, UTS data, human behaviour data and social network data. There are four types of data being collected and used by the upper tiers:

- Static and real time Urban data: include municipality open data, such as: structure of the city, seismic risk maps, hydrological risk maps, services, statistics, time series of major disasters, descriptors of structures such as schools, hospitals, streets, IoT sensors are river level, city emergency rooms status, weather conditions, position of Wi-Fi AP, locations of people aggregation facilities (such as: gym, schools, mall, social house, theatres, stadium, hospital).
- UTS Big Data such as: description of the public transportation, busses timelines, taxi, parking areas and availability, metro status and position, cycle paths, restricted traffic zone, street direction and capabilities, traffic flow information, origin destination matrices for cars, traffic flow movements, etc.
- Human behaviour data may be either individual or group-based and include activity related and behavioural personal or collective profiles addressing psychological, habitual and cognitive aspects. These profiles may be extracted based on different kinds of sensors: Wi-Fi network, Bluetooth servers, traffic flow sensors as spires, TV-cameras, mobile cells from telecom operators, mobile Apps, etc., by using data mining, data analytics techniques, processing huge amount of data related to the single movements in the city.
- Social networks data: a social network crawler is used to manage and analyse all real-time data streaming generated by citizens on social media. The crawler is language independent utilizing multilingual thesaurus. Text processing and knowledge mining techniques are used to discover hidden information.

These heterogeneous datasets are accommodated in a scalable and interoperable Knowledge Base based on specific resilience oriented ontology. Furthermore, the Data Analytics Semantic Computing component included in the layer computes several elaboration to generate new knowledge (such as: extraction of typical human trajectories in the city, computation of the origin destination matrices at different time slots and week day, compute predictions about eventual city dysfunctions, compute sentiment analysis with respect to major city services) to enrich the Knowledge Base.

2nd platform tier - Collaborative Resilience Assessment and Management Support System (CRAMSS)

The CRAMSS is primarily a concept of a collaborative workspace in which operators (e.g. Infrastructure managers, first responders, civil protection, etc.) can share their outputs of or information about their work among each other. At theoretical level, the CRAMSS is a frame to gather and display output information from separate institutions/entities that usually act as silos in daily activities. Thus CRAMSS connects several existing or new systems in the city as the EvacuationDSS, Urban Traffic Manager, and ResilienceDS) and components (Network Analysis tool)

The main purpose of the CRAMSS is to support reference actors at the UTS, such as infrastructure managers, with their decision making under both, standard operating conditions and emergency conditions.

Evacuation DSS (eDSS) + Emergency Support Smart Mobile App (ESSMA).

The eDSS is the responsible module for providing evacuation planning to the evacuation responsible (eDSS operator) in critical situations, facilitating them to take critical decisions. In order to provide optimal evacuation plans, considering the number of the involved ones and the critical situation, the eDSS co-processes and fuses all the available information from all the existing sources. Thus, the eDSS considers information retrieved from the SBDL, the rest CRAMSS's components, the eDSS's front-end, as well as data retrieved from the ESSMAs. Except from the evacuation plans the eDSS is also responsible for identifying possible individuals or groups of individuals as rescuers or to-be-rescued, assigning the appropriate task to each and providing the corresponding guidance. Connected to the eDSS there is the **Emergency Support Smart Mobile App (ESSMA)**. The ESSMA is meant to be used by professionals, such as rescue teams, and civilians. It turns its users into sensors and active agents of the resilient urban transport system. Thereby, it turns these actors into resources to be managed by the operator of the eDSS. It follows two main purposes: one is to track user movement and behaviour and thus provide the eDSS with data on a level of detail that could not be achieved otherwise. The other is to provide each user with individualized information, aiming to support self-rescue or to divert passenger flow in the UTS in case of a disruption, or to provide guidance to other citizens in need of help.

UTM DSS

The UTM DSS is one of the components of the CRAMSS which, through the implementation of strategic traffic management, enables cooperative operations control by means of definition and automatic identification of control strategies for both daily-life and emergency situations. It covers the following ITS applications (in terms of monitoring, and decision-support system when identifying pre-set network situations):

- Urban traffic control
- VMS control
- Parking management
- Streetlight control

Resilience DS

The Resilience Decision Support, **ResilienceDS** is a collaborative web based tool developed to support FRAM modelling. The tool includes some extensions of the FRAM notation to better describe the complexity of the system under investigation. Moreover a first attempt to compute a FRAM model through the connection to the data available in the SBDL is on-going. Such tool allows modeling of a sociotechnical system and the generation of formal models for continuously assessing the CI resilience.

Network Analysis component

This component analyse the public transport network (e.g. bus lines) vulnerability using network science technologies. The scope is to identify the most critical nodes using static as well as real time information about the status of the service. Such a information can support operator in gaining a better understanding on potential cascade effects that may be triggered if critical events happens close to such nodes for instance.

3rd platform tier - Dashboard

The Dashboard helps increase the resilience of UTS by providing features that help (possibly) locally dispersed actors make best use of the given resources, resulting in optimal efficiency and efficacy. To achieve this, the Dashboard serves mainly as a distributor of information; the operators can retrieve information from it that is entered in an automated manner. The Dashboard supports operators in their sense-making cognitive process when they manage alerts and emergencies. The dashboard provides a number of user-friendly widget to represent simple as well as complex (e.g. georeferenced) information. It can be customized according to the operator information needs.

The Game Based Training App (GBTA) is a smartphone-based application, which allows the user to learn how to behave in certain critical in situations. In the RESOLUTE project, the GBTA was filled with learning contents that refer to flooding scenarios. However, the development consists in a framework that can easily be used to host any other learning content as well. From a user's perspective, the game-based training app is meant to be a fun activity and to prepare the user for serious situations in real life. The users is motivated to complete all scenarios with success and thus test or improve their knowledge about what to do. The game transforms the critical elements derived by the FRAM analysis in decision points in which the player tests his/her knowledge and mastery of critical situations.

4 Conclusions

The fundamental idea of RESOLUTE is that the system will constitute the mean for enabling an efficient cooperation between citizens themselves and between citizens and public authorities (public administrations, civil protection, fire brigade, police, etc.), Critical Infrastructure managers, volunteers, etc.. RESOLUTE adopts a highly synergic approach towards the definition of a resilience model for the next-generation of collaborative emergency services and decision making process. According to its scope, RESOLUTE will offer to final users:

- • Reducing cost and time for implementing resilience guidelines
- • Drastically reduce the risks for citizens
- • Reduce the time for taking right decision
- • Make the resilience assessment and management process easier and effective
- • Move to a paperless mode of work
- • Reduce administrative burdens
- • Efficiency in resource allocation during the emergency
- • Establish coordination with all stakeholders involved in UTS resilience management
- • Make emergency services more user-friendly
- • Ensure widespread accessibility of emergency services
- • Increase communication with citizens and authority
- • It will also constitute a way not only for the co-creation of new resilience oriented services, but also for the redesign and enhance of existing one

Acknowledgment

This work has been supported by the RESOLUTE project (www.RESOLUTEeu.org) and has been funded within the European Commission's H2020 Programme under contract number 653460. This paper expresses the opinions of the authors and not necessarily those of the European Commission. The European Commission is not liable for any use that may be made of the information contained in this paper. A part of the work described in this paper (namely the Km4City model and tools) has been also supported by Sii-Mobility SCN MIUR project on smart city mobility and transport in Italy.

SmartResilience

Aleksandar Jovanović

European Virtual Institute for Integrated Risk Management, Stuttgart, Germany

Corresponding author:
Aleksandar Jovanović
EU-VRi
European Virtual Institute for Integrated Risk Management
Lange str. 54, 70174 Stuttgart
Germany
Phone: +49 711 410041 29
jovanovic@risk-technologies.com

Abstract

Modern critical infrastructures are becoming increasingly smarter (e.g. the smart cities). Making the infrastructures smarter usually means making them smarter in the normal operation and use: more adaptive, more intelligent etc. But will these smart critical infrastructures (SCIs) behave smartly and be smartly resilient also when exposed to extreme threats, such as extreme weather disasters or terrorist attacks? If making existing infrastructure smarter is achieved by making it more complex, would it also make it more vulnerable? Would this affect resilience of an SCI as its ability to anticipate, prepare for, adapt and withstand, respond to, and recover? What are the resilience indicators (RIs) which one has to look at?

These are the main questions tackled by SmartResilience project.

The project envisages answering the above question in the following steps

1. By identifying existing indicators suitable for assessing resilience of SCIs
2. By identifying new smart resilience indicators including those from Big Data
3. By developing, a new advanced resilience assessment methodology based on smart RIs and the resilience indicators cube, including the resilience matrix
4. By developing the interactive SCI Dashboard tool
5. By applying the methodology/tools in 8 case studies, integrated under one virtual, smart-city-like, European case study.

This approach will allow benchmarking the best-practice solutions and identifying the early warnings, improving resilience of SCIs against new threats and cascading and ripple effects. The benefits/savings to be achieved by the project will be assessed by the reinsurance company participant. The consortium involves seven leading end-users/industries in the area, seven leading research organizations, supported by academia and lead by a dedicated European organization. From the external world, leading resilience experts are included in the Critical Infrastructure Resilience Advisory Board.

SmartResilience is a 3-year project which started in May 2016. The project's holistic approach considers an integrated view on resilience assessment, addressing a broad variety of issues including human factors, security, geo-politics, sociology, economy, etc., and increased vulnerability due to changing threats. This holistic approach:

- Is focused and driven by the case studies tackling a variety of critical infrastructures
- Implements integrative resilience assessment before an event/crisis and after as well as all three resilience types: Structural, Integrative, Transformative/ Adaptive
- Considers "Smart Resilience indicators" built upon:
    - Indicators accepted in the related areas, e.g. proposed by OECD, GRI, API and other organizations
    - New indicators proposed by experts in the project
    - New indicators delivered out of Big and Open Data

Combines all the above in a new, coherent Smart Resilience methodology and tools to be facilitate the resilience of infrastructures (to identify and define the indicators and determine their values).

Project partners:

European Virtual Institute for Integrated Risk Management (Coordinator)

End users: Industry and public bodies:

- IBM Israel Science & Technology Ltd.
- Swiss Reinsurance Company Ltd
- City of London Corporation (to be replaced with City of Edinburgh)
- Stadtwerke Heidelberg GmbH
- Cork City Council
- Hungarian National Police
- Petroleum Industry of Serbia

Service to industry & research organization:

- Technical Research Centre of Finland Ltd.
- Stiftelsen SINTEF
- Swedish Environmental Research Institute
- Steinbeis Advanced Risk Technologies GmbH
- Fraunhofer Gesellschaft e.V.
- European Dynamics SA
- Applied Intelligence Analytics
- Bay Zoltan Nonprofit Ltd. for Applied Research

Academia:

- Medical University of Vienna
- Heidelberg University of Applied Sciences
- University of Wuppertal
- University of Stuttgart

Project web-site:

http://www.smartresilience.eu-vri.eu/

1 Introduction

The overall resilience of modern societies is largely determined by and dependent on resilience of their critical infrastructures such as energy grids, transportation systems, governmental bodies and water supply. This is clearly recognized by the European Union in its policies and research agenda, such as the DRS (Disaster-Resilience) actions and projects safeguarding and securing society, including adapting to climate change [12]. In this context, the issue of "measuring resilience" has an important place and it is tackled primarily by means of indicators, within the DRS-14 line of calls [12] emphasizing the need for "… a better understanding of critical infrastructure (and)… for defining measures to achieve a better resilience against threats in an integrated manner including natural and human threats/events (e.g. due to human errors or terrorist/criminal attacks)…". The overall goal of the current research agenda is, hence, to improve current approaches by providing an innovative "holistic" methodology for assessing resilience of critical infrastructure. The methodology proposed here is based on resilience indicators. The EU does not provide a clear definition or framework for tackling the concept of resilience – single projects and activities currently follow a number of often quite different paths. Thus, one main goal of the recent research agenda is to establish common frameworks, approaches, definitions and guidelines.

Resilience concepts have been developed by the Federal Agency of Emergency Management (FEMA), which is a part of the United States Department of Homeland Security (USDHS) [13], by the OECD [27] and the United Nations Office for Disaster Risk Reduction (UNISDR) [45]. New research, initiated by the EU Horizon 2020 projects like RESILENS [37], RESOLUTE [38], DARWIN [7] and SmartResilience also addresses the issue of developing resilience approaches [40]. The need for guidelines and frameworks for resilience is particularly important in the areas of IT security and related critical infrastructures, which may be considered as "smart infrastructures". While the information technology provides more and more possibilities to make critical infrastructures "smarter", it also creates more risks and vulnerabilities [44]. The EU research project SmartResilience makes an attempt of combining a common framework for resilience with the need to adapt this framework to new technology related risks and opportunities.

The basic idea is that modern critical infrastructures are becoming increasingly "smarter" (e.g. "smart cities"), providing an increasing amount of data and thereby, the possibility to measure resilience by using indicators derived big and open data. Following this idea and the objectives of the project, SmartResilience defines resilience of an infrastructure as "*Resilience of an infrastructure is the ability to anticipate possible adverse scenarios/events (including the new/emerging ones) representing threats and leading to possible disruptions in operation/functionality of the infrastructure, prepare for them, withstand/absorb their impacts, recover from disruptions caused by them and adapt to the changing conditions*" [20].

Making an infrastructure "smarter" usually means making it smarter in normal operations and use. Further, these "smarter" systems may be characterized by the following features [22]

1. Integrative and interconnected
2. Intelligent by the use of ICT, web technology and smart computing
3. Smart governance oriented, inclusive of end-users
4. Sustainable/progressive/future-oriented
5. Efficient and maximize service

However, it has to be checked if such a smart critical infrastructure (SCI) will behave equally "smartly" and be "smartly resilient" also when exposed to extreme threats, such as extreme weather disasters or, e.g., terrorist attacks. Similarly, the question is, if making existing infrastructure "smarter" is achieved by making it more complex, would it also make it more vulnerable? Would this affect resilience of an SCI in its ability to anticipate, prepare for, adapt and withstand, respond to, and recover? These questions are of increasing interest for the research community. Thus, the SmartResilience project is developing a new, advanced, resilience assessment methodology, which takes the vulnerability of SCIs into account in a holistic manner. This methodology is based on the identification of existing and new, smart indicators of resilience [40].

The approach proposed here assumes that an event challenging the resilience of modern infrastructure will potentially be an emerging risk [21]. Emerging risk is understood as a risk not necessarily well known and spreading increasingly in its infrastructural context over time, leading to cascading and ripple effects. Figure 15 visualizes an example for such an emerging risk, a man-caused release of toxic aromatic liquids. Policy priorities in such a situation can, and often will, evolve over time. Thus, emerging risks, especially if combined with Smart Critical Infrastructures (SCIs), represent a challenge for both infrastructure owners and the policy-makers.

Further, with the indicator-based approach, one of the pressing challenges to find trends and patterns in the large and high-dimensional datasets can be captured by means of intuitive indicators of high practical use. Many infrastructures lend themselves exceptionally well to be analyzed from a complex network perspective [2]. Many real-world networks (such as communication networks, metabolic networks, or social networks) have a surprising high degree of robustness with respect to random errors or perturbation. However, this robustness comes at the high price of extreme vulnerability to targeted attacks. Network science methods have resulted in actionable information on network vulnerabilities in response to disruptive events in the context of transportation [15], power [41], and communications [9]. An additional challenge in the design of resilient infrastructures is that multiple interdependencies between mutually dependent networks induce an additional component of fragility [9], see also Figure 15.

The challenges for applying the approach are, obviously, greater when dealing with more complex infrastructures, and, generally, the “smart infrastructures” are more complex than the conventional infrastructures.

2 Basic idea of the approach

As mentioned in the introduction, in order to keep pace with new emerging risks and Smart Critical Infrastructures, it is crucial to develop new methodologies and tools; hence, it uses the UV model. Further, when it comes to resilience of critical infrastructures, the "UV"-model (or –curve) is more suitable, because "tipping points" are not of main interest, whereas the response phase is highly relevant. Since the response necessarily takes some time, a flat bottom curve is more representative, than a "V"-curve [22]. Moreover, the "UV"-model (or –curve) is more of a conceptual model. In reality, it will hardly be a smooth curve. It is more likely to fluctuate, making it difficult to model. Moreover, if there are interdependencies and cascading effects, several curves are needed to represent resilience graphically.

In addition, new smart resilience indicators can potentially be built upon [39]:

- Indicators not specifically envisaged as resilience indicators, possibly already accepted and applied in related areas, such as risk, safety, business continuity, sustainability, e.g. those proposed by OECD, GRI, API, HSE, IAEA and other organizations;
- New resilience specific indicators proposed by experts (the “conventional way” of creating and using indicators), including those proposed in standards;
- New resilience indicators derivable out of Big Data and Open Data.

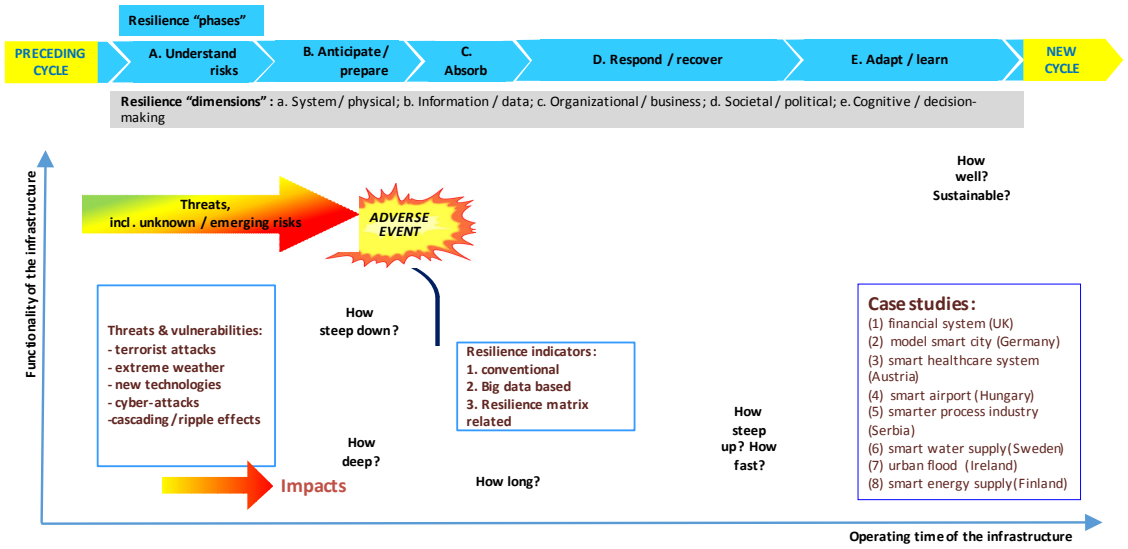


Figure 4: Resilience UV curve in SmartResilience project

The indicators can be, e.g., "supervised" or "unsupervised", lagging or leading, basic or more sophisticated, more or less dynamic. In principle, unconventional indicators can be considered to be "smarter" and, thus, are more appropriate in order to measure "smart resilience indicators". Each of the above sources might provide useful indicators for single phases of the resilience cycle (Figure 4).

Phase A, *understand risks*, is applicable prior to an adverse event. It emphasizes the emerging risks (ERs) and includes their early identification and monitoring; e.g. what could the "adverse event" be? This is followed by phase B, *anticipate/prepare*, also applicable before the occurrence of an adverse event. It includes planning and proactive adaptation strategies, possibly also "smartness in preparation" [20]. Phase C, *absorb/withstand*, comes into action during the initial phase of the event and shall include the vulnerability analysis and the possible cascading/ripple effects; e.g. "how steep" is the absorption curve, and "how deep" down will it go? Phase D, *respond/ recover*, is related to getting the adverse event under control as soon as possible, influencing the "how long" will it last, question. Further, it includes the post event recovery; e.g. "how steep up" is the recovery curve for normalization of the functionality? It is followed by phase E, *adapt/learn*, which encompass all kinds of improvements made on the infrastructure and its environment; e.g. affecting "how well" the infrastructure is adapted after the event, and whether it is more resilient and "sustainable". The activities in this phase also lead to preparation for the future events and hence, this resilience curve also exhibits a reoccurring cycle [20].

These five phases along with five resilience dimensions form the 5×5 SmartResilience resilience matrix (RM) as shown in Table 1. The dimensions help in categorizing the indicators. Dimension a, *system/physical*, includes technological aspects of the given infrastructure, as well as the physical/technical networks being part of a given infrastructure, and interconnectedness with other infrastructures and systems. Dimension b, *information/data*, is also related to the technical systems but is dealing with information and data, specifically. Further, dimension c, *organizational/business*, covers business-related aspects, financial and HR aspects as well as different types of respective organizational networks. Dimension d, *societal/political*, encompass broader societal and social context, also stakeholders not directly involved in the operation and/or use of the infrastructure (e.g. social networks). Lastly, dimension e, *cognitive/decision-making*, accounts for perception aspects (e.g. perceptions of threats and vulnerabilities) [20].

Table 1: Resilience Matrix: Resilience indicators in different phases of the resilience cycle and resilience dimensions [20]

Phases →→→ vs. Dimensions ↓↓↓	A. Understand risks	B. Anticipate / prepare	C. Absorb / withstand	D. Respond / recover	E. Adapt / learn
a. System / physical					
b. Information / data		5×5			
c. Organizational / business					
d. Societal / political					
e. Cognitive / decision-making					

Depending on a given situation (infrastructure, scenario) all the sources may yield, often a large number of, indicators for all the phases of the resilience cycle. However, for practical purposes too many indicators may become a burden, especially in the case when the resilience of different infrastructures should be compared. In practice, the indicators cannot be considered neither independent, nor standardized. Ideally, in such a case, one would prefer dealing with one resilience indicator only. One indicator might be good for comparison, but it can hardly represent the complexity of practical situations (e.g. complex scenarios, unknown responses, uncertainties). The methodology being proposed in the SmartResilience project [21], [40], shown in Figure 6 and explained in Section 4, tries to combine the advantages of "one resilience indicator" (convenient for use, but not transparent) with the advantages of many indicators (transparent, but cumbersome).

For collecting the indicators and applying the approach, the theoretical framework for variable selection, weighting, and aggregation must be defined [6]. Once when the set of indicators is considered/accepted as representative, the dynamic/"smart" resilience assessment "check-lists" can be created and used for the assessment of the respective SCI (e.g. water, energy, smart city) as described in Section 7.

3 Scenarios: Threats and infrastructures

The project covers 8 scenarios with a mix of infrastructures and related threats in order to assess the resilience of the smart critical infrastructures (SCIs), and in addition one hypothetical case to simulate a case showing cascading effects. The cases are ordered as per the phonetics [35] from ALPHA to INDIA as shown in Table 2.

Case 1 (ALPHA) of smart finances in the city of London emphasize to consider any disruptions to business continuity, whether it is a terrorist attack, cyber-attack or a natural threat such as a hurricane [4].

Case 2 (BRAVO), i.e. Heidelberg in Germany, considers terrorist attack and cyber-attack as major threats to their infrastructure [4], whereas natural threats such as urban floods are considered partly applicable.

Case 3 (CHARLIE) of smart health care system infrastructure (in Austria) considers cyber-attack leading to massive breach of privacy as the prime threat to their CI. Increasingly, terrorist attacks are also considered important. Further, different scenarios are considered important such as disasters and man-made crises that may lead to challenges in normal mode of operations or events leading to exceeding the capacity of emergency departments and failures in other critical infrastructures such as power supply for hospitals [4].

Case 4 (DELTA), i.e. smart transportation system of an airport in Hungary, considers terrorist attacks as most important threat. Besides this, property crimes endangering or disrupting operations, malevolent use of airport systems or airplane, attacks or incidents from outside the airport (UAV fly-in, firing lasers at approaching airplanes), accidents and disruptions caused by human negligence as well as strikes, are considered as specific threats. Natural disasters are second in importance for this case [4]. Case 5 (ECHO), i.e. smart industrial system case in Serbia, identifies terrorist attack, cyber-attack and extreme weather conditions as most important threats and these could possibly lead to interruptions in the critical supply chains.

Table 2: Critical infrastructures and threat scenarios

Infrastructure (CI) / Scenarios	Terrorist attack	Cyber attack	Natural threats	CI-specific events
Case 1 (ALPHA): Smart finances (UK)	✓	✓	✓	Disruptions leading to business continuity e.g. cyber risks, climate risks
Case 2 (BRAVO): Smart cities (Germany)	✓	✓	(✓)	Social unrest, urban floods
Case 3 (CHARLIE): Smart health care (Austria)	✓	✓	(✓)	Massive breach of privacy, disruption in power supply, scenarios of disasters and man-made crises, interconnected events
Case 4 (DELTA): Smart transportation (airports, Hungary)	✓	✓	(✓)	Disruption of airport services
Case 5 (ECHO): Smart industrial/production plants (Serbia)	(✓)	✓	(✓)	Industrial accidents
Case 6 (FOXTROT): Smart water supply (Sweden)		✓	✓	Climate change leading to water shortage, heavy rainfall leading to heavy water contamination
Case 7 (GOLF): Smart city (Ireland)			✓	Flash floods in urban areas leading to disruption of several CIs
Case 8 (HOTEL): Smart energy supply systems (Finland)		✓	✓	Interruption of coal supply & district heating
Case 9 (INDIA): Integrated Virtual case Study (Combined scenarios in all SCIs)	✓	✓	✓	Cascading effects
Applicability: ✓- yes, (✓) - partly				

Case 6 (FOXTROT), i.e. smart water supply in Sweden, evaluated climate change related events as crucial to the drinking water supply leading to either shortage or a heavy rainfall leading to contamination [4]. Also, cyber-attack is consider important in relation to security/ICT/human error.

Case 7 (GOLF), i.e. city of Cork, has been vulnerable to extreme weather and flooding events in urban areas leading to disruption of several CIs [4]. Case 8 (HOTEL) of smart energy supply system in Finland recognizes cyber-attack and extreme weather conditions as major threats. Also, interruption in critical supply chain such as coal supply and district heating are of considerable importance [4]. Case 9 (INDIA) is a hypothetical integrated case as shown in Figure 15, considering multiple infrastructures and multiple threats leading to cascading and ripple effects. Overall, a recent survey with the project case studies indicate (see Figure 3) that natural (NAT) hazards, malicious attacks including terrorist attacks, cyber-attacks are of main relevance for the case studies in the project [47].

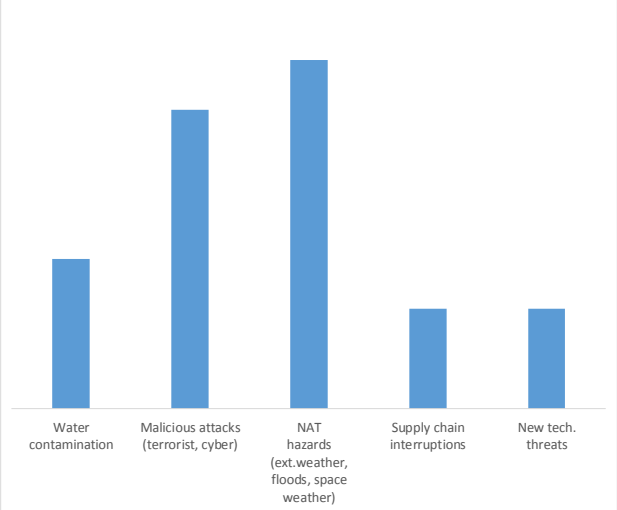


Figure 5: Number of case studies identifying different threats

4 Assessment methodology

4.1 Reference approaches

The methodology developed in the SmartResilience project [40] is based on several previous methods, notably the ANL/Argonne method [14], the Leading Indicators of Organizational Health (LIOH) method [10]], [11], [33], and the Resilience-based Early Warning Indicator (REWI) method [30], [29], [31], [32].

The ANL/Argonne method for assessing a resilience index (RI) is structured in five levels, providing indicators on the lowest level. A similar hierarchy is used in the SmartResilience project for assessing resilience levels, entering the indicators on level 6. The structure is somewhat similar in the two approaches, and many of the resilience attributes are the same; however, the level at which the various resilience attributes are found, differs between these two methods.

The LIOH method focused on developing indicators for a set of seven themes important for the "health" of a nuclear power plant, some of which have their roots from the research on high reliability organizations (HRO) [46]. They also formed part of the basis for factors considered important in resilience engineering. The LIOH method uses three distinct terms for the levels in their structure of the method. These are *themes*, *issues* and *indicators*. The issues are in principle divided in general issues and specific issues (for nuclear power plants); however, in some of the applications it was regarded as sufficient to use only one common level for the issues.

This idea was brought further to the REWI method, using three levels to identify early warning indicators for resilience, i.e. starting with resilience attributes, followed by issues important for these resilience attributes, and finally develop indicators to measure the issues. In REWI, the level of resilience attributes is not termed themes

as in LIOH, but rather *contributing success factors* (CSFs). Thus, the structure consists of *CSFs*, *issues* and *indicators*. The CSFs are determined based on identification of factors contributing to successful operations including recovery of potential incidents, prior to causing any accident with consequences; thus the term contributing success factors [43]. They are structured in two levels, of which the lowest level consists of eight factors, or resilience attributes. The CSFs are partly, but not entirely sequential.

4.2 Basic idea and assumptions

In SmartResilience, the resilience attributes are based on the definition of resilience used in the project [40], described in the introduction. From the definition, the five phases of the resilience cycle, presented Table 1, are obtained.

For each of these phases, the issues that are important for them are identified, and indicators to measure those issues are developed. Thus, the three lowest levels in the SmartResilience structure are *phases*, *issues* and *indicators*. In addition, the issues (and corresponding indicators) are structured according to five dimensions [20], also presented in Table 1. These phases and dimensions forms the Resilience Matrix, as illustrated in Table 1 and Figure 6. Variations of such resilience matrices exists in the literature (e.g. Linkov et al. [25], IMPROVER project [18] and READ project [36].

One difference with the 5×5 matrix in SmartResilience, compared to some other matrices proposed (4×4, 7×3, etc.) is that the dimensions are only used for structuring the issues and indicators, and to support the identification of issues. It is the phases which are important and it is not necessary to fill every cell in the matrix with issues and indicators. The cells themselves have no part in the calculations of the resilience levels.

4.3 Levels of assessment

In addition to the three lower levels of the structure, i.e. phases, issues and indicators, the overall structure consists of three more levels. Starting from the top, is the area level, e.g. a city or smart city, for which the degree of "smartness" will differ, but the assessment methodology applies for all cases. The second level consists of the critical infrastructures (CIs), and the third level deals with the threats. The overall structure of the SmartResilience methodology is illustrated in Figure 6.

Since the users performing resilience assessments of their area/city, critical infrastructures and/or specific threats are not assumed to be resilience or risk experts, the SmartResilience methodology is deliberately kept as simple, transparent and easily understandable as possible. Thus, there is reluctance to add additional levels or crosscutting topics, which will increase the complexity of the model. All models are simplifications of reality, and it will always be a balance between having a model that is simple and transparent on one hand, and being sufficiently realistic on the other hand.

Three specific features are treated within the six level structure. These features are related to how to deal with the Information & Communication Technology (ICT) infrastructure as an overarching infrastructure, how to deal with cascading effects, interdependencies and interactions, and finally, how to deal with the potential vulnerability and opportunities of smart features being increasingly introduced in critical infrastructures.

The ICT infrastructure may affect several of the other critical infrastructures, and this need to be explicitly considered as a potential issue when issues are defined in the resilience matrix for the ICT infrastructure. This is indicated in Figure 6 adding an asterisk, i.e. ICT*. Cascading effects are treated as a specific type of threat, also shown in Figure 6. Other types of interdependencies or interactions may also be treated as specific threats, and added as indicated by "others/specify" in Figure 6. Smart features ("smartness") of critical infrastructures are included explicitly as smartness vulnerability and smartness opportunity on issue level. These are default issues (candidate issues), for which the relevance should be considered for all phases in all types of assessments.

Another specific issue, which could be treated on issue level, is related to one of the distinctions between resilience assessment and risk assessment, which is the focus on the unexpected, and how well a city/area or

critical infrastructure, is prepared for the unexpected. This can be explicitly focused by e.g. measuring the number of incidents/accidents not included in the response plans, and the degree of learning from incidents/accidents experience by others, which may occur in your own case, but not being included in the response plans. This could be included as issues in the adapt/learn resilience phase.

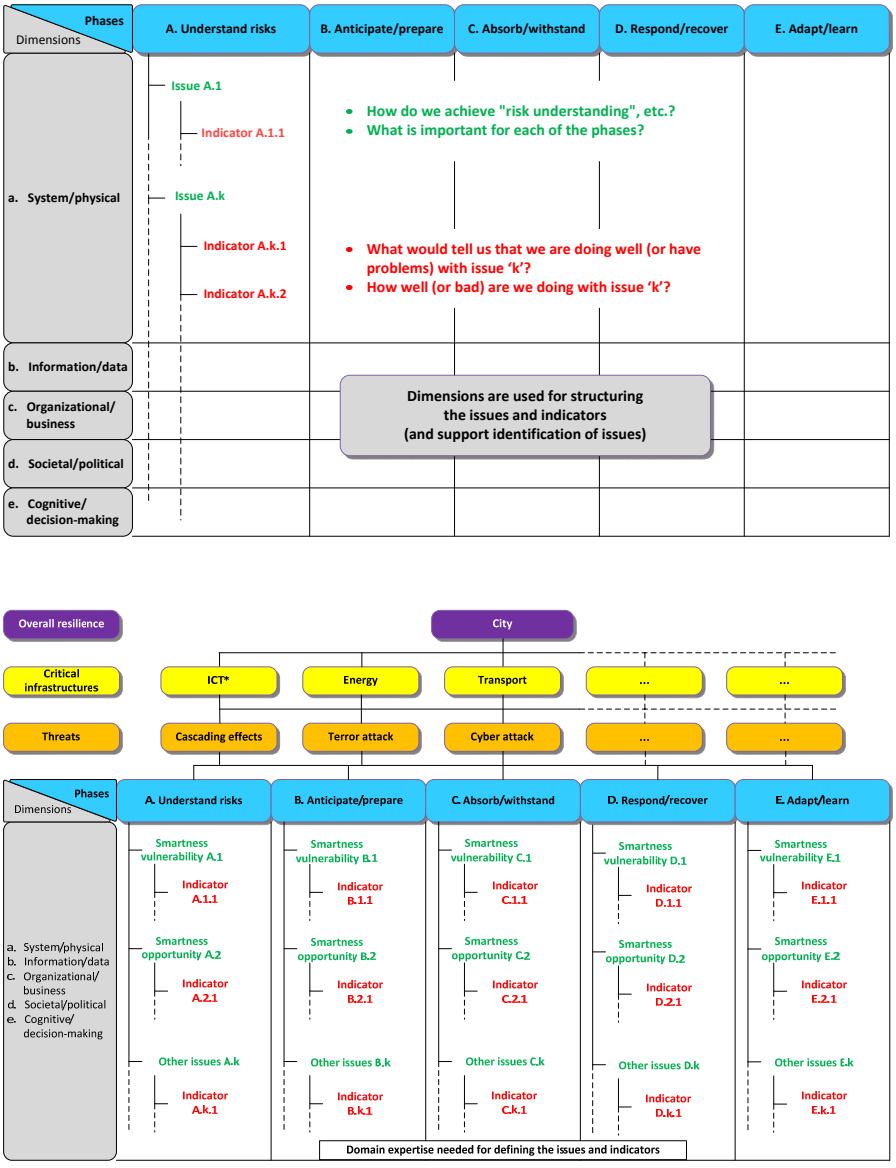


Figure 6: Basic outline of the methodology

Two important general features of the methodology are its flexibility, and its demand for domain expertise in "configuring" the resilience model for a specific area/city or critical infrastructure. A fixed list of critical infrastructures for cities in Europe does not exist, and it must be up to each city or area using the methodology to decide which infrastructures that are critical for them. Similarly, no fixed list of threats exists, neither on area level nor for the single critical infrastructures. Thus, it will be up to the users to define which threats they consider relevant. This is shown in Figure 6 with "others/specify" both for critical infrastructures and threats.

Domain experts are needed in order to define the important issues, and how to measure these issues, i.e. identifying the indicators. They are in a way "configuring" the resilience model, which largely is a one-time effort prior to using the model for calculating the resilience levels, although some adjustments, tuning, and reconsiderations are expected. Thus, in the implementation phase, it is important with close collaboration between the users, the method developers, and the IT developers (of calculation and presentation tools).

4.4 Resilience index

The assessment of resilience can be performed at different levels, e.g. for an entire city or some other area, for one or more critical infrastructures, and for one or more threats. It may also be an assessment of a particular threat within an area, affecting certain critical infrastructures, e.g. flooding in a city affecting water supply, energy and transport. The term "scenario" is used here, for a specific selection of critical infrastructures and threats for a given area/city, i.e. the selected area, critical infrastructures and threats.

Table 3: Methods steps [48]

Step	Method step description	Level in model
Define the scenario		
Step 1	Select the area, e.g. a smart city	Level 1
Step 2	Select the relevant smart critical infrastructures (SCIs) for the area	Level 2
Step 3	Select relevant threats for each smart critical infrastructure	Level 3
Define the analysis framework		
Step 4	Consider each phase (in the resilience matrix) for each threat	Level 4
Step 5	Define the issues within each phase (alternatively structured according to the dimensions)	Level 5
Step 6	Search for the appropriate indicators for each issue	Level 6
Perform the analysis ("calculate")		
Step 7	Determine the range of values (best and worst values) for each indicator	6
Step 8	Assign values to the indicators (and optionally weights – on all levels)	1-6
Step 9	Perform the calculations (i.e. calculate scores and resilience levels)	1-6
Use the results and make decisions		
Step 10	Compare/make trends, benchmark, "stress-test", etc.	1-6

Steps 1-6 are selections and considerations related to the six levels of the methodology as explained previously, whereas steps 7-10 are related to the calculations and the use of the results.

Any type/form of indicators are considered appropriate in the SmartResilience methodology, meaning that they can be yes/no questions, numbers, percentages, portions, or some other type. Their real values, of whatever type, are collected and transformed to a *score* (or rating) on a scale from 1 (worst) to 5 (best). This requires the determination of best and the worst values for each indicator, i.e. Step 7. The score is obtained by interpolation between the best and worst values.

At every level, there is a possibility to give *weights*; however, it is recommended to be restrictive with the use of different weights as this will lead to less transparent calculations and results. Thus, equal weights are the default values at all levels. When performing the resilience assessment, the indicators' real values are entered into the calculation (Step 8), and the issue scores are obtained as average weighted scores of the indicator scores. Thus, also issues (level 5) are measured using scores on a scale from 1 to 5, similar as the indicators (level 6). It is also possible to let a specific indicator overrule the effect of the other indicators, i.e. having "knock out indicators" where, in the case of a low value, the effect is not "averaged away" through an average weighted score of all the

indicators. On the next higher level (level 4 – phases), the scores are transformed to a scale from 0 to 10, providing *resilience levels*. This scale is kept from phases and upwards, i.e. for threats (level 3), critical infrastructures (level 2) and areas (level 1).

The reasoning behind the selected scales is that a scale from 1 to 5 for indicators (and issues) are sufficiently broad, especially if there are needs to perform expert judgments to provide scores for the indicators (or directly for the issues) in case of lack of data [28]. A main goal of the SmartResilience project has been to develop a method for assessing level of resilience using a scale approach of resilience level, which was included in the call text for the project [39]. This has similarities to the use of safety integrity levels (SIL) for safety instrumented systems [17], only using integer values from 0 to 5. However, in SmartResilience the resilience levels are increased to a scale from 0 to 10, which is considered to provide sufficient differentiation, and at the same time not give the illusion that the assessment is more accurate than it can really be. The calculation is performed in a database and the assessment for the given case/scenario is saved (Step 9). Only the selections made at each level are shown, since the "complete" structure for the most complex case may consist of thousands of nodes. The method steps are described in Table 3, starting from the top of the model, i.e. at Level 1:

The results of the resilience assessment, which in the case of a full scope assessment for a smart city covers all the relevant critical infrastructures, all relevant threats for each critical infrastructure, all five phases of the resilience cycle, all relevant issues for each phase and all indicators for measuring the issues, can be used in various ways (Step 10). One is to compare with previous assessment, i.e. providing a trend showing how the level of resilience is progressing. Since the calculation is performed on all levels, it is also possible to "drill down" and identify the reason for an increase or decrease in resilience compared to the previous assessment. Another use is to compare with other cities, areas or critical infrastructures, i.e. to benchmark against others, which provides the opportunity to learn from others. The resilience of a city/area or a critical infrastructure can also be assessed by imposing a set of threats (including defined challenges such as interactions and cascading effects), i.e. stress-testing the resilience ability of the city/area/critical infrastructure, and compare the results with predefined criteria. This is further described in Section 7.

4.5 Use cases

Selected use cases have been employed during the development of the structure of the model, the mathematical equations and the overall calculations. The development and testing of the equations and calculations have been performed independently using the SmartResilience database, in a progressive manner starting from simple and transparent examples, such as case dealing with one threat and one infrastructure to cases dealing with multiple threats, multiple smart critical infrastructure and ripple effects.

The three use cases have been selected from the eight case studies in the SmartResilience project. The three use cases are:

1. Refinery in the city of Pančevo in Serbia, representing production/supply as a critical infrastructure

2. Heidelberg Bahnstadt in Germany, representing a smart city/area

3. Budapest Airport in Hungary, representing a critical transport infrastructure

Use cases #2 and #3 have only been used to develop the structure, not for any calculations, whereas use case #1 has been used for development of the equations and calculations. The use cases (sample application cases) are further described in Section 6.

5 Implementation of the methodology

5.1 Data collection

The data collection is performed in phases and are refined through an iterative process. It consists of relevant issues and corresponding indicators that are used in each case (as specified in Section 3) to measure the resilience of the respective infrastructure.

So far, over 1300 candidate issues and indicators have been collected in the SmartResilience database for assessment of resilience of CIs. The prime proportion of these are conventional indicators and only a small proportion represent the big data indicators. This collection of indicators will be further refined after domain experts select the issues and indicators relevant for the applicable scenario in their case studies and a final dynamic checklists of issues and indicators will be devised. Then, these indicators are structured according to the methodology [20] into phases of the resilience cycle as explained in Section 4. The data for each of the indicators will then be collected in the database for the resilience assessment of the SCI.

5.2 Tools – visualization

Considering that the number of indicators to assess the resilience and the data related to each of these indicators especially big data can be overwhelming to analyze and create problems in understanding the impact of any disruptive event and the corresponding cascading effects on the critical infrastructure. Hence, it is crucial to use data visualization to ease the process. In order to do so, D3 (Data-Driven Documents) a JavaScript library is used. It brings data to life through its interactive visualization tools [8] and will support the indicator based methodology to measure resilience of SCI and inform decision making. The levels in the resilience assessment will be visualized based on the interactive tree map structure shown in Figure 7.

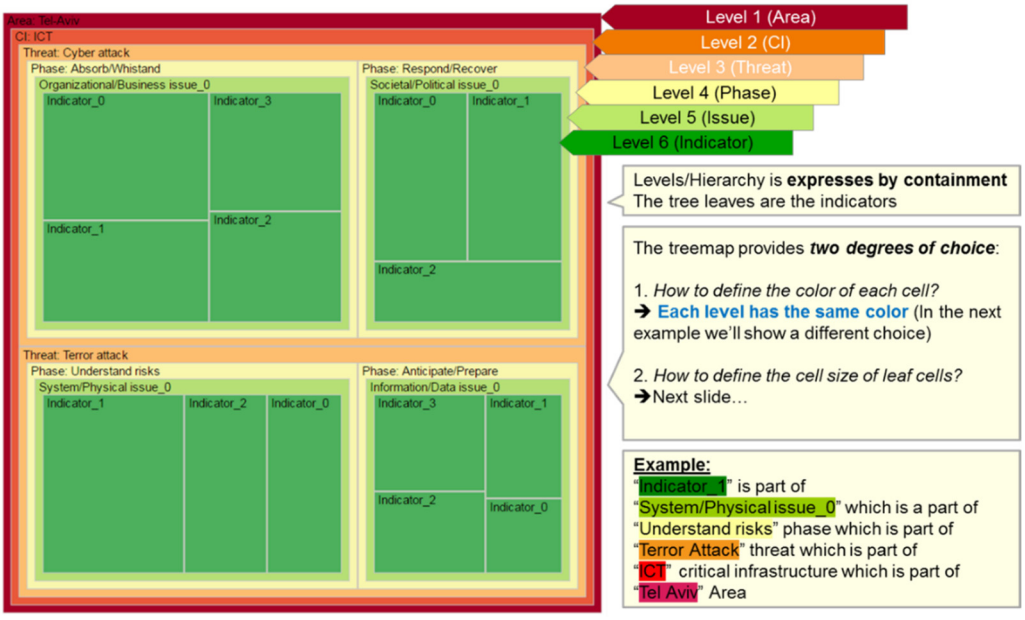


Figure 7: Interactive tree map structure visualization of the resilience of infrastructure [49]

6 Sample application cases

6.1 A smart city

One of the use cases introduced in Section 4, use case #2, is Bahnstadt in Heidelberg, Germany. It constitutes an example/representation of a smart city, or smart community/neighborhood, i.e. a defined area within the city of Heidelberg. Bahnstadt in Heidelberg is one of Germany's largest urban development projects. It is designed to be Heidelberg's first smart neighborhood. Bahnstadt is located in the southwestern part of Heidelberg's city center,

6.2 Smart production (refinery)

Use case #1, introduced in Section 4, is a refinery in an industrial zone of the city of Pančevo in Serbia, representing (smart) production/supply as a critical infrastructure.

City of Pančevo with its Southern Industrial Zone is chosen to represent a case study for the resilience of critical infrastructures as a representative of industry sector, with many recognized threats in the neighborhood, in a smart city. In order to perceive and understand the influence of industry in the sense of resilience it is necessary to cover the impact of each individual risk factor in this industrial zone as well as the impact of this zone on other systems of smart city [4]. City of Pančevo has the so called Southern Industrial Zone located at the southeast edge of town, right next to the residential area of the city, approximately 4 km from the city center. In addition to the compound of the HIP-Petrohemija a.d. Pančevo, this zone includes the HIP Azotara Pančevo a.d. and NIS Oil Refinery Pančevo. The area is connected to road, rail and river circulation by means of the port on the Danube River. In this industrial zone, there is a production of petroleum products, basic chemical products, poly-ethylenes, mineral fertilizers, calcium ammonium nitrate, carbamide and NPK fertilizers [4].

In general, the industrial zone is an area covering one type of critical infrastructure (although multiple plants), is exposed to multiple threats, and needs to be resilient in all phases through multiple issues measured by multiple indicators. In the simplified use case referred to in Section 4, only one single plant and one threat are included; however all phases are covered, but only for the calculations. The threat selected is cyber-attack, although this is not explicitly highlighted by the stakeholders [4]; thus, this use case is fictitious. The main emphasis of this use case was the development of the calculations. The scenario is illustrated in Figure 8, with some examples of issues and indicators. Only the phase respond/ recover is shown.

6.3 Smart transportation

Use case #3, introduced in Section 4, is the Budapest Airport in Hungary, representing a smart transportation critical infrastructure. The Budapest Liszt Ferenc International Airport is the largest international airport in Hungary and is built at the easternmost limits of the Hungarian capital city, Budapest. The total land area of the

facility is 15,050,000 square meters, 25% larger than London Heathrow International Airport [3]. The facility has both commercial (passenger, cargo) and general aviation traffic, but is also occasionally serving military airplanes (e.g. KC-130s [24] airplanes in the Balkan wars). In 2015, the commercial aviation served 10,298,963 passengers, 92,214 airplanes and 91,421 tons of cargo with coordinated work of approximately 12,000 people [1] [4].

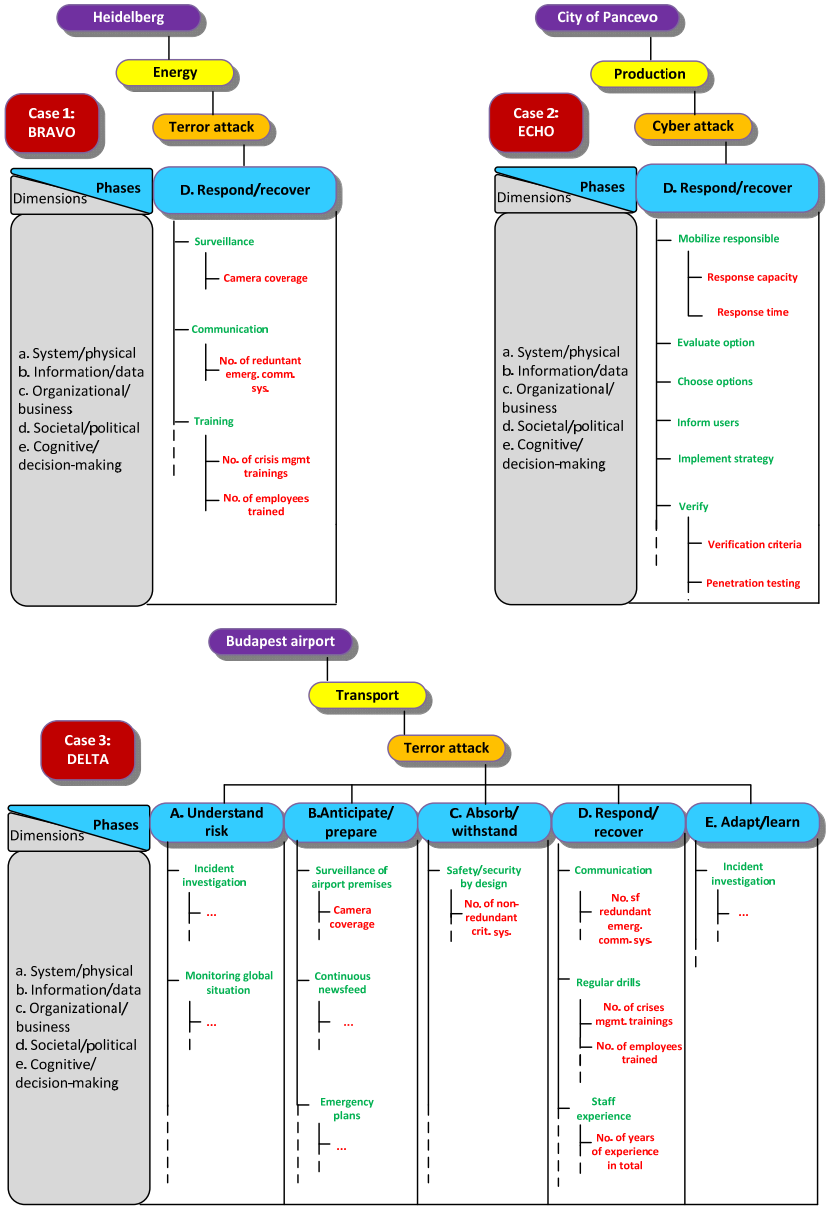


Figure 8: Examples of different scenarios for the use cases BRAVO, ECHO & DELTA

Currently, BLFNR is the second most protected critical infrastructure in Hungary. The level of security is provided by a well-coordinated cooperation of authorities (including first responders) and private companies, with the airport operator company in the first place. With 52 flight companies, 8 authorities, 3 ground handling companies, 27 shops and so on, there are more than one hundred of actors, all obliged to take its part in protection of the airport as a critical infrastructure [4]. In general, an airport is a specific type of critical transportation infrastructure, exposed to multiple threats requiring resilience in all phases through multiple issues measured by multiple indicators. In the simplified use case referred to in Section 3, only one threat is considered; however all phases, and multiple issues and indicators are included. Terrorism is considered one of the main threats, and are selected in this use case. Issues identified as important are e.g. drills, staff experience,

communication, and incident investigation [4]. This is illustrated in Figure 8, including examples of potential indicators to measure the issues. All phases are covered, but it is not distinguished between the different dimensions.

The sample application cases are illustrated using only specific limited scenarios. The threats are selected from those considered as important by the sample application cases themselves [20] and the same is true for the issues (except for use case #1, where the issues were identified in a separate workshop by the method developers). When the method is tested in the case studies in the SmartResilience project, including the three use cases, it is important that domain experts identify all relevant issues and indicators for all phases, all relevant threats, and all relevant critical infrastructures. This will provide a full scope testing of the calculation of the resilience level on all relevant levels.

As an alternative to define issues first and then indicators, it is possible to start with existing indicators in use and ask what issue they actually measure, and then consider if these issues are of sufficient importance to be included in the overall resilience model. Further, the database of collected (resilience) indicators in the SmartResilience project can be reviewed in order to (i) determine if some of these are relevant as supplementary indicators for measuring the already identified important issues, or (ii) determine whether some of the indicators are relevant measures of new issues.

7 Resilience level vs. resilience curve – expressed in terms of indicators

The tacit assumption has been that the "functionality" is something that the analysist or the owner of the infrastructure or the assessor of its resilience will be able to define, possibly explicitly and simply. The case studies in the SmartResilience project have, however, already shown in [47] that this is not a trivial task. No matter how intuitively one might say that the critical functionality of an airport is to "keep the air traffic going" or that the critical functionality of a refinery is "to produce the gasoline", a more detailed consideration shows that the things are not necessarily that simple: the air traffic, e.g. in terms of passengers boarding's or cargo, should at the same time be safe, possibly satisfying the environmental norms, etc. Not satisfying the latter could also be a loss of critical functionality and that was the reason to explore this issue more in detail.

The considerations are of particular importance when looking to assess the resilience in terms of "loss of critical functionality" (Figure 9), i.e. by assuming that, for a given threat/scenario, the resilience of the infrastructure will be inversely proportional to the loss of critical functionality. In other words, the less of the critical functionality that is lost, the more resilient the infrastructure is. In order to quantify this, e.g. by calculating the integral under the curve, one has to be sure

1. what is the curve representing exactly and
2. how to calculate the main points at the curve (e.g. those delimiting the resilience cycle phases).

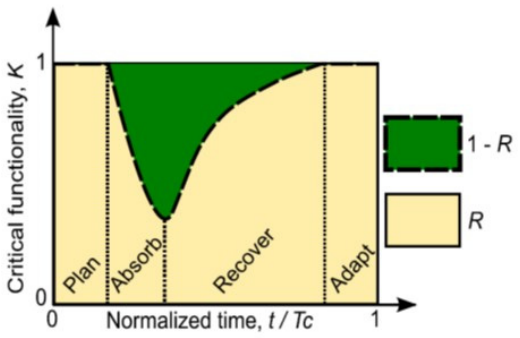


Figure 9: Example of "calculating" resilience (as integral)

The method proposed here, pertinently to the overall methodology in SmartResilience, proposes by do it by means of

- Functionality elements (FE) are “single functionalities” that contribute to the overall functionality of the CI (correspond to the issues in the main SmartResilience method for defining the resilience level) and
- Functionality indicators (FI) provide the values in order to measure the elements (in this particular case the “the indicators of functionality” or “the indicators of functionality level”).

These two form the lower two levels in the functionality assessment methodology.

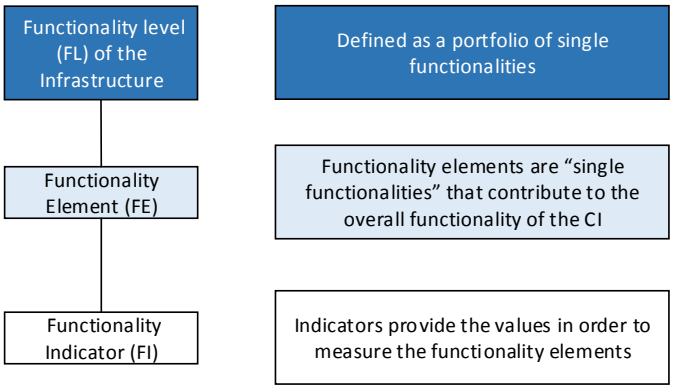


Figure 10: Structure to define the functionality of the infrastructure

NOTE: This portfolio of functionality elements and functionality indicators Figure 10 shall normally NOT change over the resilience cycle. I.e. once defined to be representative, it will be used until the end of the cycle. It is important here to distinguish between the **functionality level and critical functionality of an SCI.** The critical functionality is defined by the minimum level or threshold level for each of the phase in resilience cycle needed by the CI to be operational. The structure of assessment is based on five levels (Figure 11) comprising of

Level 1. Functionality Level of the City
Level 2. Functionality Level (FL) of the Infrastructure corresponding to the SCIs in the project.
Level 3. Threat relevant for each of the SCI
Level 4. Functionality elements (FE)
Level 5. Functionality Indicators (FI)

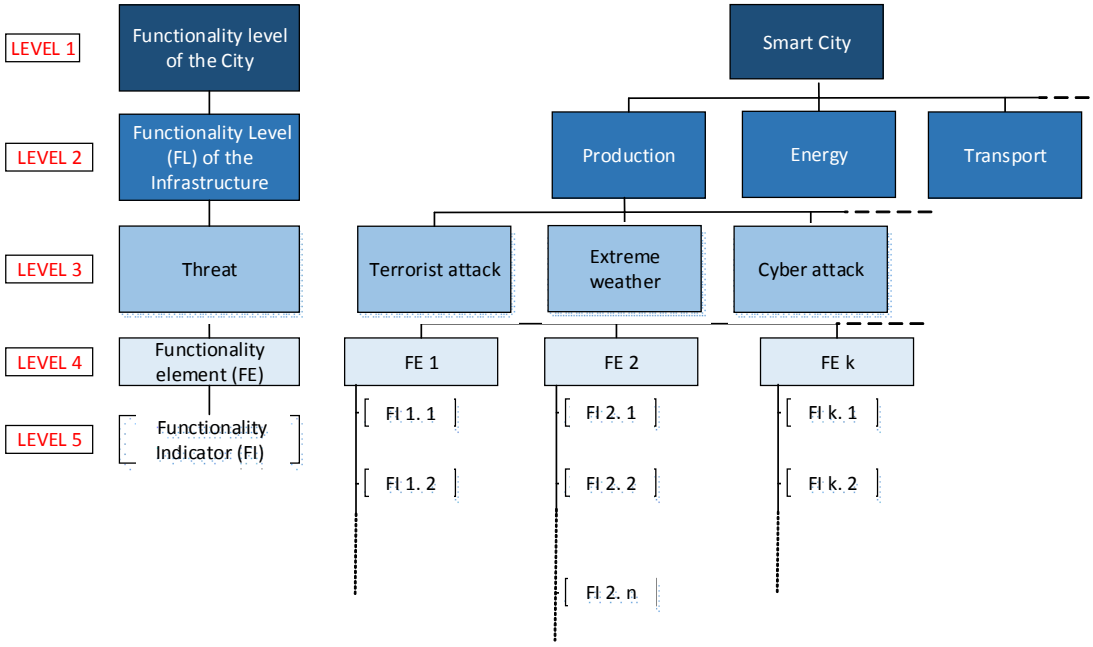


Figure 11: Structure for assessment of the functionality level of the SCI

This structure forms the basis for deriving the functionality level of the SCI. The method for defining functionality of the SCI has the following main steps:

Defining the scenario:

Step 1. Select the CIs to be assessed in the Smart City

Step 2. Identify the relevant threat to create a scenario

Defining the functionality of the Infrastructure:

Step 3. Define the functionality of each CI as a portfolio of the functionality elements (FE) (Figure 12), which may include some core single functionalities such as production and/or some supporting elements such as safety and/or environmental performance or similar. Consider the relevant threats while defining these elements.

Step 4. Define the "functionality elements" which are logically group the functionality indicators (FI) (similarly to the "issues" in the resilience level assessment) e.g. tons of oil produced, number of passengers processed, amount of electricity produced, etc.

Performing the analysis (calculate):

Step 5. Define the maximum value for each FI

Step 6. Assign real/current values to the FI (and optionally weights for FI and FE levels)
NOTE: The values of indicators can be assigned by an expert, derived from the monitoring systems or from the big data analysis.

Step 7. Perform calculations (i.e. calculate scores and FLI) at t_0
NOTE: Determine this FL as the „100% FP level" of the infrastructure (the nominal level) at time t_0 ; this should be the reference functionality level for the whole resilience cycle, allowing to answer the questions such as "how steep", "how deep" etc. and assess the final outcome after the resilience cycle (e.g. in the stress-test)

Step 8. Calculate the FL of the infrastructure (similar to Step 5-Step 7) for times t_1, t_2, t_3, t_4 and t_5, or any other time of the resilience cycle
NOTE: The system operates at this functionality level until a disruptive event occurs. This disruptive event is followed by a series of events in time (for e.g. see Figure 13). The FL of the infrastructure is calculated at following times:

- t_0: time before the event
- t_1: time at which the event occurs
- t_2: time at which the infrastructure lost its full functionality or part of its functionality
- t_3: time at which the infrastructure starts to recover
- t_4: time at which the infrastructure reaches the initial functionality level
- t_5: time at which the infrastructure increases its functionality through learning and adapting (if so)

Step 9. Plot the resilience curve, based on the FLI versus the SCENARIO time (Figure 13).

Step 10. Aggregate the functionality of all the selected infrastructures to the city level

Note: The critical functionality of the system can be calculated by following the above Step 1-Step 7. The only difference is that the user needs to assign minimum or threshold value for each of the corresponding functionality indicators.

8 Conclusions: Comparison, benchmarking and stress testing of resilience in different CIs

The examples presented in Chapter 6 integrate smoothly into a "smart city" integrative example (see Figure 15). In other words, the "smart city example" is the integration platform for different critical infrastructures including

the examples considered in Chapter 6. The approach presented in this contribution is a snapshot of the development efforts in the SmartResilience project. The approach is at this point in time still under development and it is expected to be extended in the direction of its applicability for other features (models/tools) within the project ([22] [23] [40]):

- the “resilience cube”
- the “dynamic checklists” and
- the resilience indicators based on and derived from the “big data”

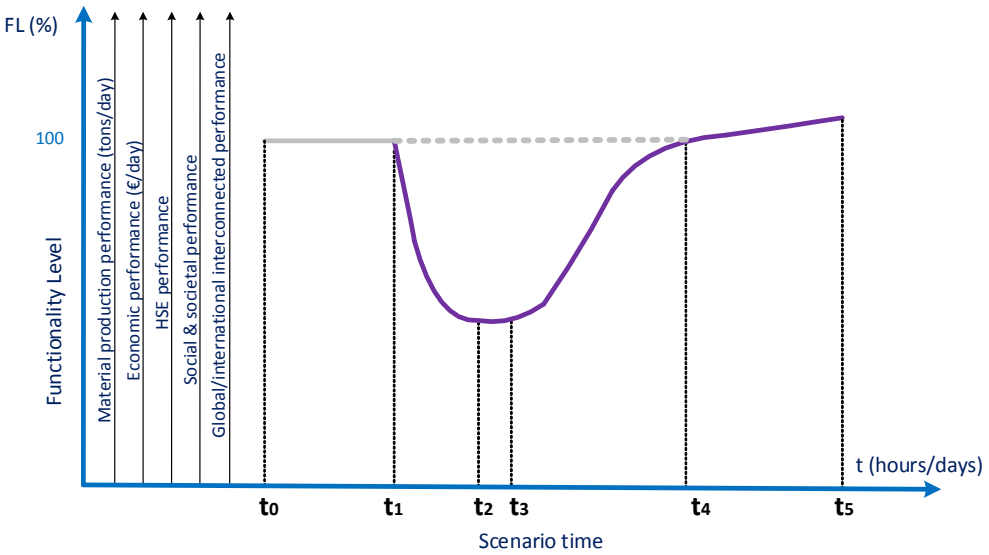


Figure 12: Step 3- “Defining” functionality as a portfolio of single functionality elements

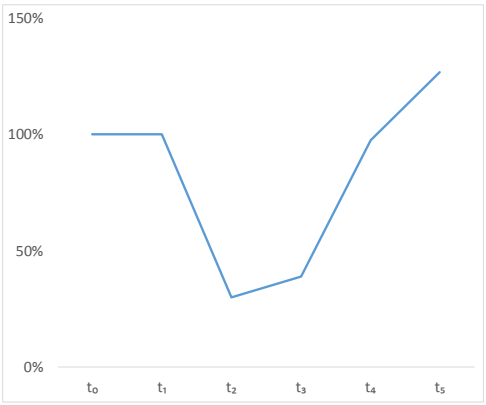
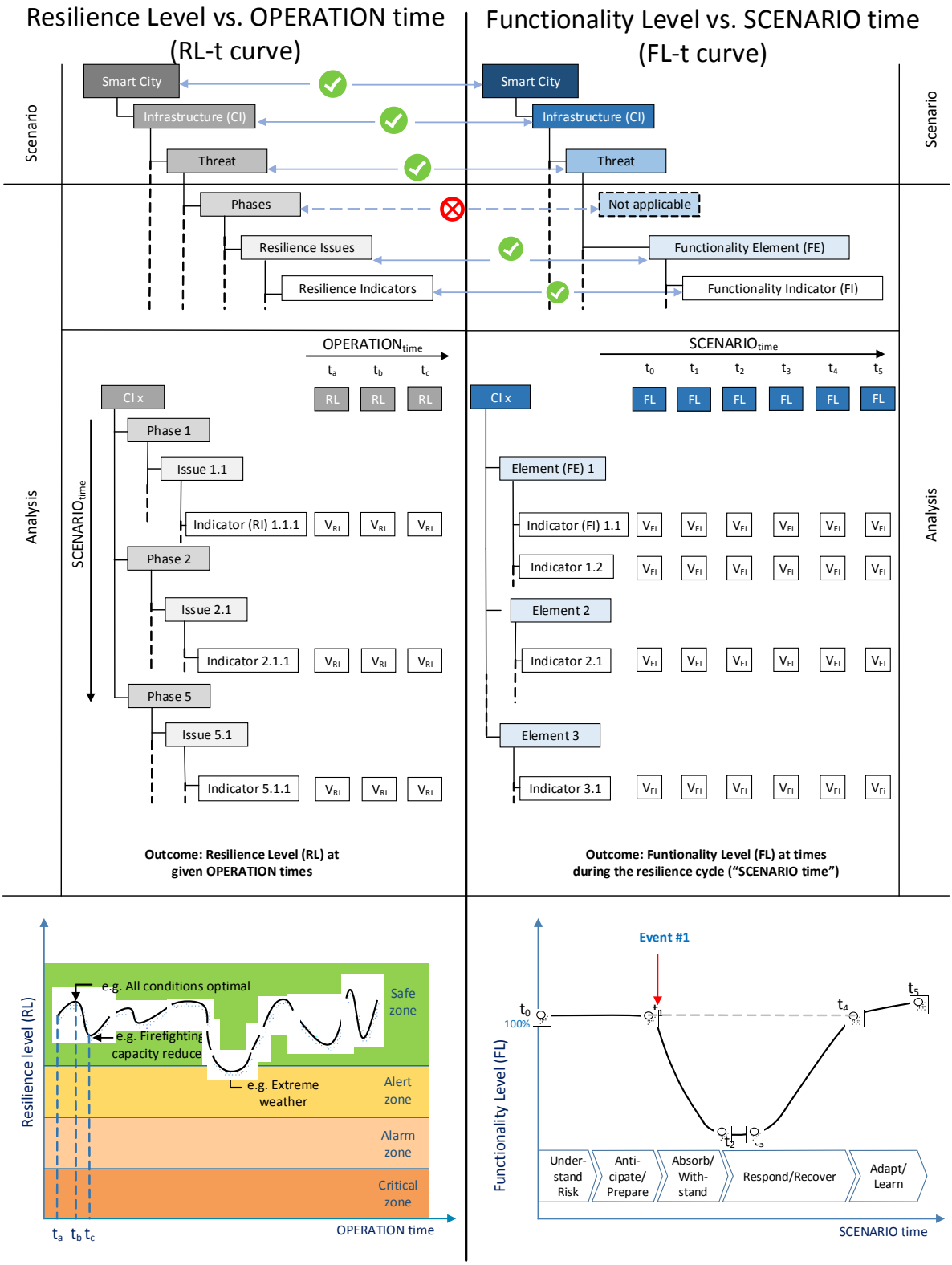


Figure 13: Functionality level of the infrastructure vs SCENARIO time curve

Comparing this approach to some of those applied elsewhere ([6] [13] [25] [26] [27]), one can see that its orientation onto critical infrastructures and use of indicators, make it probably more adapted for the quantitative resilience assessment. This improved qualitative assessment was one of the main goals of the resilience model development in the SmartResilience project.

Once when developed and implemented in terms of the IT tools, it will enable improved assessment, comparison, benchmarking and stress-testing of resilience in different critical infrastructures, in particular the “smart” infrastructures. Basic idea of this type of use of the approach is shown in Figure 16, showing that, for instance, the comparison of resilience in different phases in the resilience cycle can be done in a very intuitive and transparent way. The stress-test of resilience for all infrastructure is, on the other hand will be based on the

assessment of the functionality of the infrastructure. This methodology will be applied to the case studies in due course. Particular challenges to be addressed are those related to the cascading/ripple effect in multi-infrastructure systems (e.g. Figure 15) and consistent consideration of time in the analysis.



CI: Critical Infrastructures; FLI: Functionality Level of the Infrastructure; FE: Functionality Element; FI: Functionality Indicator; RI: Resilience Indicator; RL: Resilience Level; t: time; V: Value

Figure 14: Resilience level and functionality level assessment of the CI

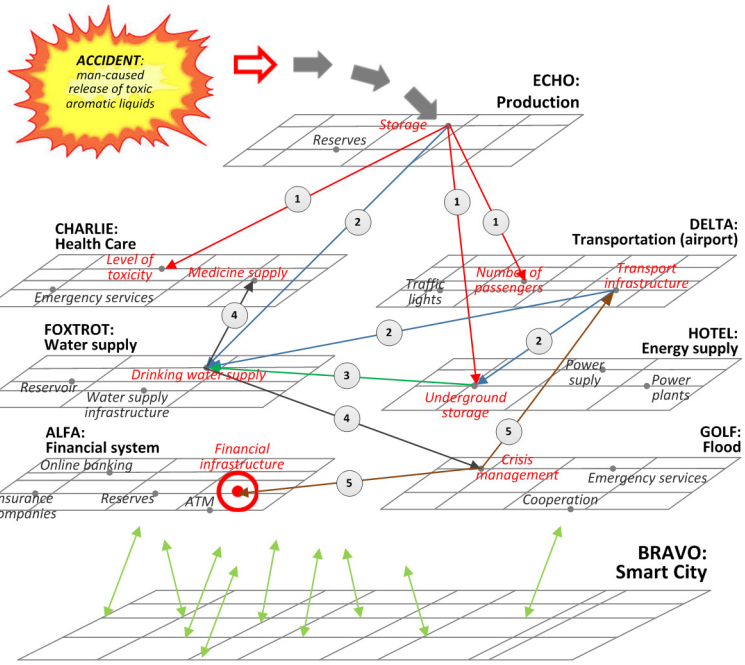


Figure 15: Interaction between the SCIs in a hypothetical case taking place in a "Smart City" (The SmartResilience "integrative" hypothetical case [39] [40])

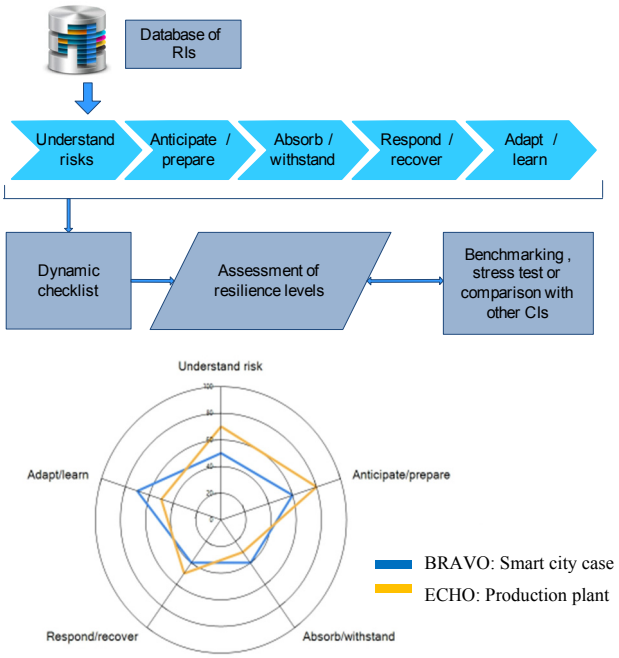


Figure 16: Application of the approach for benchmarking, stress test and comparison of resilience of different CIs

Acknowledgements

The contribution is based on the Grant Agreement No. 700621 supporting the work on the SmartResilience project provided by the Research Executive Agency (REA) ('the Agency'), under the power delegated by the European Commission ('the Commission'). This support is gladly acknowledged here, as well as the collaboration of all the partners and their representatives (persons) involved. Special thanks go to Mr. M. Jelic of EU-VRi for the IT support.

9 References

[1] Airports Council International Europe (2016). Airport Traffic Report (December Q4 and Full Year 2015), ACI, Brussels.

[2] Albert R., H. Jeong, A. L. Barabási (2000). Error and attack tolerance of complex networks, Nature 406, 378-382

[3] Allet, T. (2004). Budapest 'New' EU Airport, Airports International, 37(4) 37-39.

[4] Buhr, K., Karlsson, A., Sanne, J.M., Albrecht, N., Santamaría, N.A., Antonsen, S., ... Warkentin, S. (2016). SmartResilience D1.3: End users' challenges, needs and requirements for assessing resilience, EU project SmartResilience, Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany.

[5] Bundesministerium des Innern (2009). Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), Bundesministerium des Innern, Berlin.

[6] Cutter, S. L., C. G. Burton, Ch. Emrich (2010). Disaster Resilience Indicators for Benchmarking Baseline Conditions, Journal of Homeland Security and Emergency Management: Vol. 7: Iss. 1, Article 51.

[7] DARWIN project (2016). Expecting the unexpected and know how to respond. Retrieved from http://www.h2020darwin.eu/

[8] Data-Driven Documents (2016) Introduction. Retrieved from https://d3js.org/

[9] Doyle J. C., et al (2005). The "robust yet fragile" nature of the internet, Proceedings of the National Academy of Sciences USA 102, 14497-14502

[10] EPRI (2000). Guidelines for Trial Use of Leading Indicators of Human Performance: The Human Performance Assistance Package. EPRI (U.S. Electric Power Research Institute), Palo Alto, CA, 10000647.

[11] EPRI (2001). Final report on Leading Indicators of Human Performance. EPRI, Palo Alto, CA, and the U.S. Department of Energy, Washington, DC, 1003033.

[12] European Commission (2013). Call H2020-DRS-2014-2015: Disaster Resilience: Safeguarding and securing society, including adapting to climate change, Retrieved from https://ec.europa.eu/research/participants/portal/ desktop/en/opportunities/h2020/calls/h2020-drs-2014-2015.html#c,topics=call Identifier/t/H2020-DRS-2014-2015/1/1/1/default-group&callStatus/t/Forth coming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&call Status/t/Closed/1/1/0/default-group&+identifier/desc

[13] FEMA (2014). FEMA Strategic Plan 2014–2018. Washington, DC

[14] Fisher, R.E., Bassett, G.W., Buehring, W.A., Collins, M.J., Dickinson, D.C., Eaton, L.K., ... Peerenboom, J.P. (2010). Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-10-9, Argonne, IL, USA http://www.ipd.anl.gov/anlpubs/2010/09/67823.pdf

[15] Guimerá R, Mossa S, Turtschi A, Amaral L. (2005). The worldwide air transportation network: anomalous centrality, community structure, and cities' global roles, Proceedings of the National Academy of Sciences USA 102, 7794-7799.

[16] Heidelberg-Bahnstadt (2016). Portrait of Bahnstadt, http://heidelberg-bahnstadt.de/en/portrait-bahnstadt, accessed on Oct. 10, 2016.

[17] IEC 61508 (2010). Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. Part 1-7. Geneva: International Electrotechnical Commission

[18] IMPROVER (2016). IMPROVER - Improved risk evaluation and implementation of resilience concepts to Critical Infrastructure. Deliverable 2.2: Report of criteria for evaluating resilience. Retrieved from www.improverproject.eu/2016/06/23/deliverable-2-2-report-of-criteria-for-evaluating-resilience/.

[19] Jovanovic, A., Auerkari P. (2016), EU project SmartResilience: The concept and its application on critical energy infrastructure in Finland, Baltica X- International conference on life management and maintenance for power plants, Vol. 1, Helsinki, June 07-09, 2016

[20] Jovanovic, A., Klimek, P., Choudhary, A., Schmid, N., Linkov, I., Øien, K., ... Lieberz, D. (2016). SmartResilience D1.2: Analysis of existing assessment resilience approaches, indicators and data sources: Usability and limitations of existing indicators for assessing, predicting and monitoring critical infrastructure resilience, EU project SmartResilience, Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany.

[21] Jovanovic, A., P. Klimek (2015). Risk & Resilience: Emerging risks and resilience – how to find right indicators. Risk and Resilience in the face of Global Change, Aspen Global Change Institute, Aspen, Col., Nov. 30 - Dec. 5, 2015

[22] Jovanovic. A., Choudhary. A., Jovanovic. M., Szekely. Z. (2016) SmartResilience D2.1 draft report: Understanding "smart" technologies and their roles in ensuring resilience of infrastructure, EU project SmartResilience, Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany.

[23] Jovanovic. A., Schmid. N., Klimek. P., Choudhary. A. (2016). Use of indicators for assessing resilience of Smart Critical Infrastructures, IRGC Resource guide on resilience. Lausanne: EPFL International Risk Governance Center. v29-07-2016

[24] KC 130 https://en.wikipedia.org/wiki/Lockheed_Martin_KC-130

[25] Linkov, I. et al. (2014). Changing the Resilience Paradigm. Nature Climate Change 4(6), 407-409. Retrieved from (http://www.nature.com/doifinder/ 10.1038/nclimate2227).

[26] Linkov, I. et al. (2014). Changing the resilience paradigm. Nature climate change, Vol. 4, June 2014

[27] OECD (2014). Guidelines for resilience systems analysis, OECD Publishing

[28] Øien, K. (2001). A framework for the establishment of organizational risk indicators. Reliability Engineering and System Safety, 74, 147–167.

[29] Øien, K. (2010). Remote operation in environmentally sensitive areas; development of early warning indicators. 2nd iNTeg-Risk Conference, Stuttgart, Germany, 15-16 June 2010.

[30] Øien, K. (2013). Remote operation in environmentally sensitive areas: development of early warning indicators, Journal of Risk Research, 16(3-4), 323-336.

[31] Øien, K., & Nielsen, L. (2012). Proactive Resilience Based Indicators: The Case of the Deepwater Horizon Accident. SPE / APPEA International Conference on Health, Safety and Environment in Oil & Gas Exploration and Production, Perth, Australia, 11-13 September 2012.

[32] Øien, K., Massaiu, S., & Tinmannsvik, R.K. (2012). Guideline for implementing the REWI method; Resilience based Early Warning Indicators. SINTEF report A22026, Trondheim, Norway.

[33] Øien, K., Massaiu, S., Tinmannsvik, R.K., & Størseth, F. (2010). Development of early warning indicators based on Resilience Engineering. International Conference on Probabilistic Safety Assessment and Management (PSAM10), Seattle, USA, 7-11 June 2010.

[34] Øien, K., Utne I.B., & Herrera I.A. (2011). Building Safety Indicators. Part 1 – Theoretical foundation. Safety Science 49(2), 148-161.

[35] Radiotelephony phonetic alphabet (2016), International Civil Aviation Organization, Retrieved from http://www.icao.int/Pages/AlphabetRadio telephony.aspx

[36] READ (2016). READ - Resilience Capacities Assessment for Critical Infrastructures Disruption: www.read-project.eu/

[37] Resilens project (2016). Realising European Resilience for Critical Infrastructure. Retrieved from http://resilens.eu/

[38] Resolute project (2016). RESilience management guidelines and Operationalization appLied to Urban Transport Environment. Retrieved from http://www.resolute-eu.org

[39] SmartResilience (2015). Smart Resilience Indicators for Smart Critical Infrastructures – Project proposal Call: H2020-DRS-2015, DRS-14-2015. Coordinator: EU-VRi, www.smartresilience.eu-vri.eu.

[40] SmartResilience (2016). Smart Resilience Indicators for Smart Critical Infrastructures – The European Union's Horizon 2020 Research and Innovation Programme, Grant Agreement No 700621 (2016-2019). Coordinator: EU-VRi, www.smartresilience.eu-vri.eu.

[41] Solé R, M. Rosas-Casals, B. Corominas-Murtra, S. Valverde (2008). Robustness of the European power grids under intentional attack. Phys Rev E 77, 026102.

[42] Stadtwerke Heidelberg (2016). Profile, Retrieved from https://www.swhd.de/de/SWH/Unternehmen/Profil/Die-Stadtwerke-Heidelberg_163643.html, accessed on Oct. 10, 2016.

[43] Størseth, F., Tinmannsvik, R.K., & Øien, K. (2009). Building safety by resilient organization – a case specific approach. The European Safety and Reliability Conference (ESREL '09), Prague, Czech Republic, 7-10 September 2009.

[44] The future of smart cities: Cyber-physical infrastructure risks (2015). US Department of Homeland Security, Office of Cyber and Infrastructure Analysis

[45] UNISDR (2015). The Sendai Framework for Disaster Risk Reduction 2015-2030, United Nations Office for Disaster Risk Reduction

[46] Wreathall. J. (2006). Properties of resilient organizations: an initial view. In: Resilience Engineering: Concepts and Precepts. Ashgate, Aldershot.

[47] SmartResilience (2017). Deliverable D 5.1: Report on the results of the interactive workshop http://www.smartresilience.eu-vri.eu/sites/default/files/publications/SmartResD5.1.pdf

[48] SmartResilience (2017). Deliverable D 3.2: Assessing resilience of SCIs based on indicators http://www.smartresilience.eu-vri.eu/sites/default/files/publications/SmartResD3.2.pdf

[49] Barzeley. U (2017). T3.5 Interactive Visualization as support to indicator-based decision making. EU project SmartResilience, Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany

SMART MATURE RESILIENCE (SMR)

Jose Maria Sarriegi

TECNUN University of Navarra, San Sebastian, Spain

Corresponding author:
Clara Grimes
ICLEI
ICLEI European Secretariat
Leopoldring 3, 79098, Freiburg
Germany
Phone: +49-761/368920
Fax: +49-761/3689219
<clara.grimes@iclei.org>

Abstract

The Smart Mature Resilience (SMR) project responds to the need for enhanced resilience in European cities. Researchers work with cities to co-create five tools (Resilience Maturity Model, Risks Sistemicity Questionnaire, Resilience Information and Communication Portal, System Dynamics Model, and Policy Tool) to assess and develop cities' resilience. With the support of city network ICLEI, the tools are piloted in a group of three core cities (Glasgow, San Sebastian and Kristiansand) and reviewed and evaluated by researchers and Tier 2 cities (Rome, Bristol, Vejle and Riga) in an improvement cycle. A third group of cities will now be trained in the use of the finalized tools, and during the final year the tools will be disseminated to further cities and project results exploited through standardization processes initiated by German standardization body DIN.

1 Introduction

European cities face an increasing frequency and intensity of hazards and disasters, which are exacerbated by climate change and social dynamics, such as demographic change and an ageing population. As Europe's cities continue to grow, there is an urgent need for far-reaching and holistic approaches to enhance cities' resilience towards potentially critical effects of hazards.

The topic call defines resilience as "the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions". The SMR project has developed a slightly updated definition of city resilience, which is "the ability of a CITY or region to resist, absorb, adapt to and recover from acute shocks and chronic stresses to keep critical services functioning, and to monitor and learn from on-going processes through city and cross-regional collaboration, to increase adaptive abilities and strengthen preparedness by anticipating and appropriately responding to future challenges".

2 Background

The units of analysis of the Smart Mature Resilience project are entities that we refer to as CITIES (upper case). CITIES are analysed from the perspective of service to their citizens and their metropolitan area, with the Critical Infrastructures (CIs) located in or operationally involved in the area, and their functional roles as part of Europe's multi-level governance.

About SMR and its context:

- The SMR project develops tools to assess and build cities' resilience.
- The SMR project results advise the decision-making process towards enhanced resilience.
- Cities need to become more resilient.
- Resilience relies on adaptable critical infrastructures, dynamic social interactions and the capacity to withstand and accommodate to the effects of climate change.
- A holistic approach can enhance resilience in Europe.

3 Scientific contributions

3.1 The SMR tools

The five tools developed within the SMR project are: 1) Resilience Maturity Model, 2) Risk Systemicity Questionnaire, 3) Resilience Information and Communication Portal, 4) System Dynamics Model and 5) Policy tool.

3.1.1 The SMR Maturity Model

The SMR Maturity Model is a strategic tool that provides a roadmap about how the resilience process may be through the policies defined in each stage. The SMR Maturity Model enables, from a strategic level, the identification of areas that need to be improved in each city and reflect these in policymaking and planning.

The SMR Maturity Model helps enhancing the communication among stakeholders since it facilitates a continuous process of discussion and participation of the city stakeholders, which increases their awareness, engagement and commitment on the resilience building process. This tool also helps increasing common understanding of resilience understanding resilience as a multidimensional objective.

The SMR Maturity Model defines five maturity stages: Starting, Moderate, Advanced, Robust, and verTebrate. Each of these maturity stages includes a description of the objectives of each stage, the actors/stakeholders involved in each maturity stage, in addition to a list of policies that should be developed in order to achieve the objectives defined in each maturity stage. The implementation of these policies will allow cities to move forward from one stage onto the next.

These policies have been classified considering four resilience dimensions: Leadership & Governance, Preparedness, Infrastructure & Resources and Cooperation. Using these dimensions, an analysis of the city resilience level can be done independently for each dimension as cities can be at different maturity stages depending on each policy dimension. Additionally, a set of indicators are proposed to monitor the level of implementation of the policies.

The tool can be applied to develop a diagnosis of the current maturity level of the city based on the four resilience dimensions. Cities could be aware in this way about the level of their capabilities, thereby positioning themselves within one of the maturity stage (S-Starting, M-Moderate, A-Advance, R-Robust and V-VerTebrate) for each dimension described in the model. This process can be repeated periodically to evaluate the city progress in the resilience building process.

The tool is already available in its online version whereby users can filter the extensive information in the form to find policies that apply to them. The tool is available at http://smr-project.eu/tools/MM/. The next stage will be the integration with the Resilience Policies tool, which will allow cities to find case study examples of policies that have been implemented by other cities, and that they can take as replication examples.

The SMR Maturity Model:

- helps cities identify their level of resilience maturity
- helps cities to identify suitable policies to implement to develop resilience
- provides a point of reference for self-assessing effectiveness of resilience development
- is useable as part of strategic planning
- helps cities prioritise resilience policy implementation on the basis of diagnosis and assessment

3.1.2 Risk Systemicity Questionnaire

The Risk Systemicity Questionnaire is an Excel based tool where users are asked to consider the relative likelihood of a broad range of risks in their cities. These risks are spread across nine topics and are considered as networks of interrelated risks:

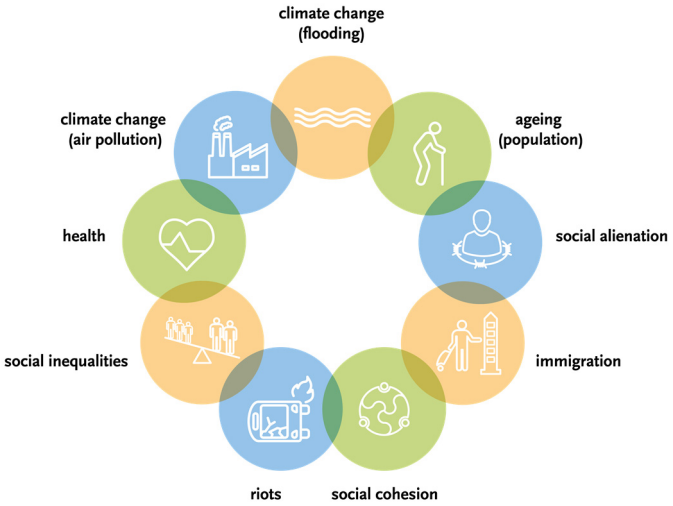


Figure 17: Risk topics within the Risk Sistemicity Questionnaire.

These networks of risks are presented as risk scenarios, some of which result in vicious cycles. Users progress through the tool by completing questions, which ask them to consider whether defined risks scenarios are likely or not to occur in their cities.

Based on the responses to the questions contained in each of the topics of the RSQ, participants are provided with a relative risk score (an estimated risk level for the city) and an awareness score (the level of knowledge the city has about the possible risk scenarios). In addition to this, users can access suggested portfolios of mitigating actions that may be used to address those risk scenarios that are of most threat to the city.

Not only does completing the Risk Systemicity Questionnaire help cities to assess their exposure to risk, but it also indicates their level of awareness of risk and where cities should prioritise their efforts. The purpose of the questionnaire is for it to be used by groups of users with diverse areas of expertise so that it can prompt valuable discussions where different stakeholders' experiences can be brought together to determine a city's priorities to enable them to anticipate and appropriately respond to future challenges.

The Risk Systemicity Questionnaire:

- Helps to appreciate different types of risks as mutually interacting, rather than viewing risks as being independent to one another
- Helps to appreciate the combined effects of risks, including vicious feedback loops and non-obvious ramifications
- Compares risk level and risk preparedness with respect to different areas of risk
- Is a tool to facilitate a focused discussion and reflection to share knowledge of risk amongst a variety of stakeholders including different municipal departments
- Can involve multistakeholder groups, including citizens and politicians
- Offers suggestions for portfolios of mitigating actions aimed at mitigating the ramifications of risks interactions
- Complements the existing resilience tools and methods in cities
- Updates and compliments the existing EU guidelines with respect to Risk Assessment and Disaster Management
- Allows cities to monitor and compare their progress through periodic re-assessment
- Does not require expert knowledge or research.

3.1.3 Resilience Information and Communication Portal

The Resilience Information and Communication Portal serves as a toolbox that can complement and enhance the platforms and software that cities already have in place. It allows cities to display data internally or publicly that is already available to the city as it applies to resilience, vulnerability and crisis situations. The portal allows for different levels of users to allow for city managers, critical infrastructure providers, citizens or other stakeholders to be able to contribute information as applies to a given city context. The portal offers added value not available otherwise to cities (as they self-reported), as the cities have multiple (and in Glasgow's case, dozens) of platforms in place in their municipalities for internal communication, but the wealth of information available to them is not integrated, streamlined or fully utilized.

Furthermore, the tool includes a number of levels of users, which accounts for the complexity of the network of stakeholders and target groups that are to be considered in building resilience. Lastly, the toolbox format facilitates the practical reality in cities, which is that replacing existing communication systems is impractical and would cause unwarranted disruption. Therefore, providing the platform as a toolbox allows cities to select the elements not already available to them without undoing or disrupting facilities and channels that already function effectively.

The portal particularly serves two purposes: 1) to support communication within the city, between the city and its stakeholders, and between the city and its citizens. In addition, the integration of social networking services is

supported and 2) to enable knowledge sharing as a long-term communication activity. Similarly, to short-term communication support, the city, its stakeholder, and citizens are included.

The Resilience Information and Communication Portal:

- aims at building a collaborative environment in order to facilitate awareness and engagement among key partners in resilience building
- enables cities to improve their own IT systems
- is provided as a toolbox which shows desired functionality for implementing the design principles summarized next
- allows different levels of permissions and users
- can complement and enhance the platforms and software that cities already have in place.

3.1.4 Systems Dynamics Model

The aim of the System Dynamics model is to explain the structure that develops the behavior that the cities should achieve during the Resilience Building process. The model will allow the cities to understand the precedence relationship of the policies included in the Maturity Model and it will provide a learning environment to better understand how the Maturity Model works, and how the Maturity Model should be implemented.

The System Dynamics Model should accompany use of the Maturity Model to help to link the Maturity Model's abstract concepts to a decision-making and budgeting mindset. First of all, the users need to calibrate the model determining the values of the most important parameters of the model: the implementation cost of the policies, the implementation time of the policies and the depletion time of the policies. Once the model has been particularized for each city, the decision making process starts, where the user needs to plan which policies will be implemented yearly. At this stage, they have identified which policies they need to identify, and are ready to find some examples using the Resilience Policy tool. the Model runs simulations of the effects of implementing certain policies over a realistic timeframe (yearly to a total of 40 years). When users implement the policies in the appropriate, wise and effective order, they achieve effective results and their resilience level increases eventually until reaching 100% in each of the resilience dimensions.

The System Dynamics Model:

- is an interactive online learning game
- can be used as part of strategic planning
- helps to build knowledge to support staff in budgeting the resources needed for the resilience building process and also analysing budgetary deviations during the development of resilience.
- supports deep understanding of reasons for budgetary decisions for resilience strategising and the logic behind prioritising policies
- supports deep understanding on the impact of the temporal order in which the policies should be implemented
- supports understanding of the Resilience Maturity Model

3.1.5 Policy Tool

The Resilience Policies tool is an extension of the online version of the SMR Maturity Model. It combines custom ways to view policies contained in the SMR Maturity Model with detailed information and examples from; case studies detailing policy implementation in SMR cities, references of sources to case studies from other cities around the world, and links to risk mitigation actions that support the policies (and are included in the Risk Systemicity Questionanire). The tool provides a comprehensive reference centre for high-level strategic managers in cities as well as municipal workers tasked with implementing the policies that have been planned.

The Policy tool

- comprises illustrative real case studies of policy implementation in cities

- includes references to other sources that provide details of case studies of policy implementation in cities
- provides a practical point of reference for cities considering the implementation of related policies
- provides illustrative detail for the policies in the SMR Maturity Model and the System Dynamics Model
- can be navigated conveniently via a dedicated webpage

4 Conclusions

The SMR project partner DIN (German Institute for Standardization) is supporting the dissemination of the SMR tools by constituting joint European standards. For the development of the so-called CEN Workshop Agreements (CWA), DIN promoted the SMR tools at the 'European Workshop for Resilience in Cities and Communities' on the 4th of April in Berlin to project external city representatives, researchers and consultants. The basis for the envisaged three CWAs will consist of SMR tools, but cooperation with project externals in the development of the standards will be of public good. That is why DIN invited project external experts from other Horizon2020 projects to elaborate to the documents and by doing so DIN furthermore disseminated the SMR tools.

The following three CWAs are envisaged to be developed out of the SMR project:

- City Resilience Development – Maturity Model
- City Resilience Development – Operational Guidance
- City Resilience Development –Information Portal

The kick-off meeting of the latter one took place in June 2017 in Brussels. The kick-off meetings for the other two envisaged CWAs is planned for November 2017 and DIN is going to invite the participants of the European Workshop to join the development of these standards. In November 2017 DIN will publish a report (D6.4) on the envisaged CWAs.

1 Executive Summary

This document is published by the Integrated Mission Group for Security (IMG-S) and the Security Research Group (SRG) of the European Association of Research and Technology Organisations (EARTO) as a joint position paper on Resilience in Security Research, being in line with the objectives of the H2020 Secure Society Work Programme and other relevant actions and initiatives in the sector, taking into account the need to link security research to capacity planning and capability insertion for resilience.

The paper should be considered as an introductory and non-exhaustive document in the topic of resilience, providing basic concepts such as framing challenges, setting priorities, providing recommendations, etc. The aim is to help the readers to identify areas and/or sectors that deserve particular attention and to initiate a thorough investigation of the Resilience potential, within the overarching topic of Disaster and Risk management in the context of Security Research & Innovation initiatives. To this end, following this first document that provides initial fundamental concepts and guidelines on Resilience, a set of position papers addressing specific aspects (e.g., Resilience of Critical Infrastructure, Resilience of Soft Targets, Resilience of the Supply Chain, Resilience of Communities, etc.) will follow. Moreover, this document is intended to pave the ground for discussions among stakeholders involved in resilience-relevant topics and to provide a mechanism for engaging them in future and more detailed technical contributions. In this context, the overarching aims of this paper are:

- To establish the resilience paradigm as an efficient aspect in the security culture and adapt the design of socio-technical systems in terms of protecting critical services and strengthen society's adaptation to new and emerging threats and hazards;
- To address the topic of Resilience in the context of the European Security Research, with a focus on how to potentially deliver harmonized policies and technologies, which can promote the take-up of best-practices and operational resilience procedures, aiming to cope with current and emerging risks;
- To define a common language that will facilitate and support common understanding, perception, and modelling of Resilience;
- To arrange and organize actual knowledge to develop and encourage a consensual view on the concept of Resilience and to investigate Resilience strategies and approaches, strengthening cooperation and collaboration among stakeholders and Communities, aiming to tackle emerging societal challenges on security in a common, agreed and harmonized way.

To make this happen a paradigm shift is required, which will define the context and the rationale for reconsidering the actual security thought-pattern concerning disaster, risk and crisis management. In this frame, it is of upmost importance that all potential sources and causes of societal, technical, economic and environmental disruptions (e.g., physical, cyber and hybrid threats, CBRNE, natural and man-made disasters including terrorism, etc.) will be considered and revised [1].

2 Background Information

Among others, the following background information have been considered when preparing this position paper:

- The Global Strategy for the European Union's Foreign and Security Policy [2], presented by Federica Mogherini, High Representative of the Union for Foreign Affairs and Security Policy in 2016;
- the overall policy goals of the Europe 2020 Strategy [3], the European Union (EU) growth strategy for the next ten years supporting the European ambition to become a smart, sustainable and inclusive economy with associated societal and economic benefits in terms of safety, security, quality of life, well-being, productivity, employment and social peace;
- the EU Security Industrial Policy [4], promoting innovation and competitiveness in the security industry sector, with one of the highest growth and employment potential in Europe;

- the European Security Strategy – A secure Europe in a Better World (ESS) [5], adopted by the European Commission in 2013, that establishes for the first time principles and sets clear objectives for advancing the EU's security interests based on EU core values;
- the principles and guidelines set out in the EU Internal Security Strategy [6] (ISS) for dealing with security threats, namely organised crime and cross border illegal activities, through an integrated strategy;
- the European Defence Action Plan [7], which proposes a European Defence Fund and other actions to support member states' more efficient spending in joint defence capabilities, strengthen European citizens' security and foster a competitive and innovative industrial base;
- the Community of Users (CoU) [8] on Safe, Secure and Resilient Societies initiative of DG-HOME.

3 The challenge

Within the European Research agenda, the thematic area of security is a well-established field of research since the 7th Framework Programme, which was initiated in 2007. Since then, a myriad of research projects have focused on investigating topics and developing solutions to prepare for risks, to prevent disasters, to manage a crisis' response efforts and to recover from them as quickly as possible. More recently, specifically with the introduction of Horizon2020, the security research agenda has evidently been broadened towards a more holistic disaster management approach that aims at linking the various perspectives and actions before, during and after an adverse event. The term this development is prominently linked to is related to the concept of resilience. Today, reference to resilience can be found in almost all research programs while the concept attracts the interest of social scientists, technology developers, risk managers, engineers, operational and academic researchers, etc. However, a clear challenge that is often observed is that the term "resilience" and the perception of it isn't defined in a clear and transparent way. Some argue that resilience is part of disaster risk management, whereas others link most of the resilience perspectives to crisis management activities, hence to post-disaster situations, etc. Additional confusion results from the fact that in many cases, resilience is seen as a built-in feature of systems and societies that can be planted to engineered infrastructures by retrofitting technology or by design. Others rather refer to it as a strategic concept or a masterplan element that can be applied in order to reach comprehensive security for socio-technical systems.

In this fragmented, highly differentiated and dynamic context, this paper can be seen, in a first step, as a starting effort and contribution towards a common understanding of the term and the concept of Resilience and, in a second step, as a document to set the ground for identifying research needs and priorities to integrate the resilience culture within the European Security Research Programs.

4 The concept of Resilience within the entire cycle of disaster management

Resilience has emerged in the last decade as a concept for better understanding the performance of infrastructures, especially their behaviour during and after the occurrence of disturbances, e.g. natural hazards or technical failures. Recently, resilience has grown as a proactive approach to enhance the ability of infrastructures to prevent damage before disturbance events, mitigate losses during the events and improve the recovery capability after the events, beyond the concept of pure prevention and hardening (Woods, 2015)[9]. The concept of resilience is still evolving and has been developing in various fields (Hosseini, Barker, & Ramirez-Marquez, 2016)[10]. Like any new area or field, the interest gained for resilient systems has created a vast array of relative definitions, processes, tools and metrics that have clouded the concept of resilience. A first definition described resilience as "a measure of the persistence of systems and of their ability to absorb change and disturbance, and still maintain the same relationships between populations or state variables" (Holling, 1973)[11]. Several domain-specific resilience definitions have been proposed thereafter (among the others: Ouyang, Dueñas-Osorio, & Min, 2012[12]; Adger, 2000[13]). The resilience and policy committees of the National Academy of Sciences (NAS) defined resilience as the ability of a system "to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events" (Cutter et al.[14], 2012,

Cutter et al., 2013[15]). A modern and simple definition of resilience is provided by Nan, Sansavini, & Kröger (2016)[16], stating that is "the ability of a system to resist the effects of disruptive forces and to reduce performance deviations". Ultimately resilience is not just about bouncing back from adversity but is more broadly concerned with adaptive capacity and how we better understand and address uncertainty (Gibson and Tarrant, 2010)[17].

From an operational viewpoint, *resilience can be defined as the ability of the system to withstand an unexpected harmful change or a disruptive event by reducing the initial negative impacts (absorptive capability), by adapting itself to them (adaptive capability) and by recovering from them (restorative capability)*. Enhancing any of these features will enhance system resilience. It is important to understand and quantify these abilities hat contribute to the characterization of system resilience (Fiksel, 2003)[18]. In addition and to be more specific, the following definitions of resilience seems to take the operational perspective into account: *"Resilience determines the persistence of relationships within a system and is a measure of the ability of these systems to absorb changes of state variables, driving variables, and parameters, and still persist" (Holling, 1973)*; *"Resilience is the ability of a system to resist the effects of disruptive forces and to reduce performance deviations" (Nan, Sansavini, & Kröger, 2016).* This leads to the consideration that the various aspects or phases of resilience can be depicted as a cyclical model, as presented below.

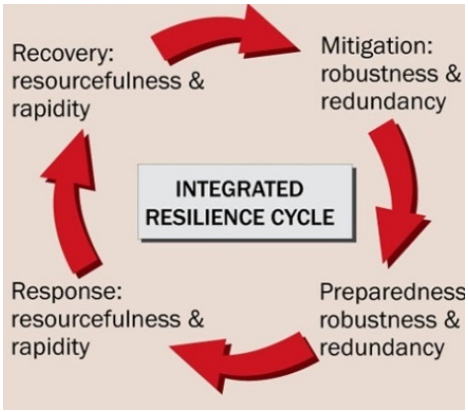


Figure 18: The Resilience Cycle (Charlie Edwards [19])

Anyway, before making any further assumption or attempting to quantify and model relative procedures to "measure" the resilience it is of primarily importance to create and reach a consensus on the concept of resilience in a very wide way. To this end, one can come up with the following widely-accepted definitions:

- Resilience is the capability of a system, organization (infrastructure, factory, business, city, region, etc.) when facing catastrophic incidents, emergency events or crises episodes to successfully overcome them, minimise their negative effects and recover to "normal" operational levels as soon as possible (i.e., the everyday way of living and performance of the community gets disturbed in lesser extent and during less time);

- Resilience is the capability of the infrastructure itself (including the managing/operating people at all levels) to maintain its operability under all circumstances and to minimize potential damages (i.e., assure business continuity).

In addition, how resilience is linked with the Disaster Risk Management approach is a further aspect to be considered and worth of clarification. Indeed, conceptually, risk analysis quantifies the probability that the system will reach the lowest point of the critical functionality profile. Risk management helps the system prepare and plan for adverse events, whereas resilience management goes further by integrating the temporal capacity of a system to absorb and recover from adverse events, and adapt accordingly [20]. Thus, resilience, on the basis of the definitions aforementioned, is not a substitute for principled system design or risk management[21] but is

rather a complementary attribute that uses strategies of adaptation and mitigation to improve traditional risk management. Indeed, given a certain event, the customization of Resilience within the Disaster Risk Management Cycle is depicted below, where the proper elements of resilience are integrated into or added to the phases (prevention, preparedness, response and recovery) of the Disaster Risk Management Cycle.

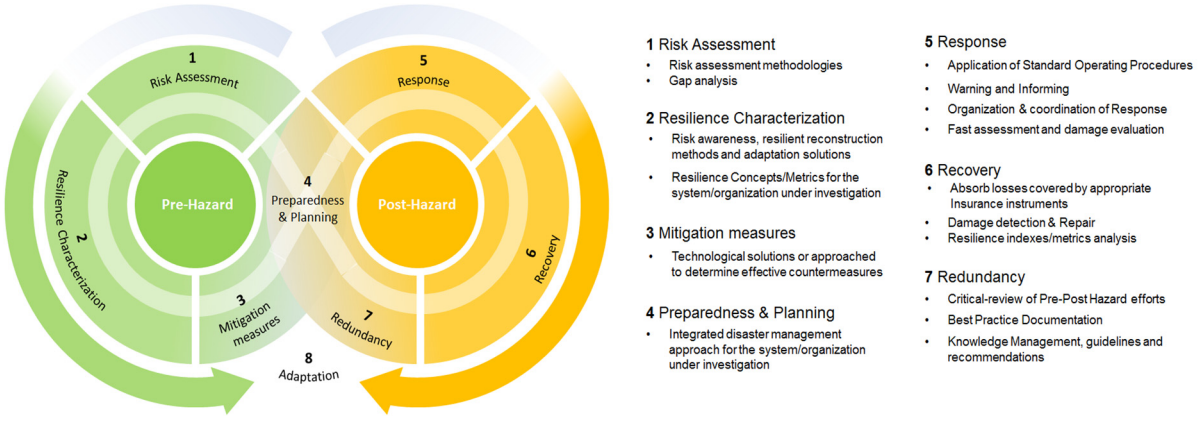


Figure 19: Holistic Approach in Disaster Management – Resilience as "linking" concept

In this sense, looking at the previous picture, Resilience can be seen as the link or capability to link pre-hazards and post-hazards activities/phases moving from 1) risk assessment to 2) resilience characterisation, to 3) mapping and screening of countermeasures and mitigation actions, to 4) preparedness and planning, enabling a more effective 5) response, leading to a 6) an efficient and timely recovery, that takes into accounts 7) redundancy actions up to adaptation 8), being represented by the outer arrows.

5 Resilience perception and strategies

Given the definition of Resilience provided above and the relation identified between the Resilience cycle and the lifecycle of disaster management, it can be said that resilience can be perceived as focusing on the fluctuation of the system performance which is harassed by an unexpected disturbance (also called resilience curve) (See below).

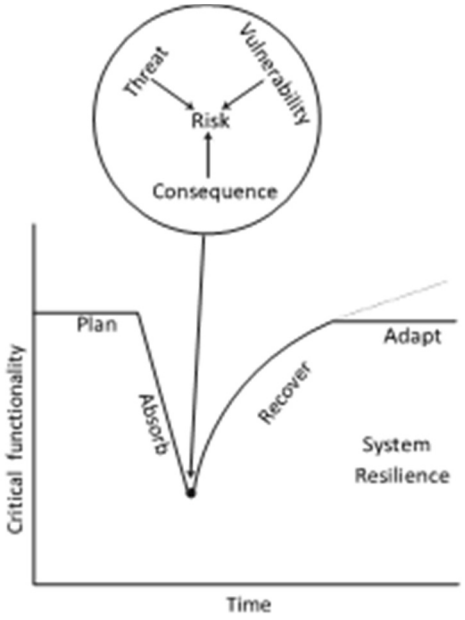


Figure 20: Risk and resilience management relationship (Linkov et al, 2014)

Over there, the transient area of performance defines the system response and the respective level of resilience. The smaller the area, the better is the resilience of the system.

The four schematic representations of changes in critical functionality over time, shown in the figure below, depict the interplay of risk and resilience in a system's performance during an adverse event. The size of the initial perturbation reflects the total risk to the system while the shape of the recovery curve is controlled by the system's resilience. The area under the curve is indicative of the overall system functionality. Systems that face high risks with high resilience perform better than those facing similar risks but with low resilience. Systems with low risk and low resilience may perform the same as, or possibly worse than, systems with high risk and high resilience.

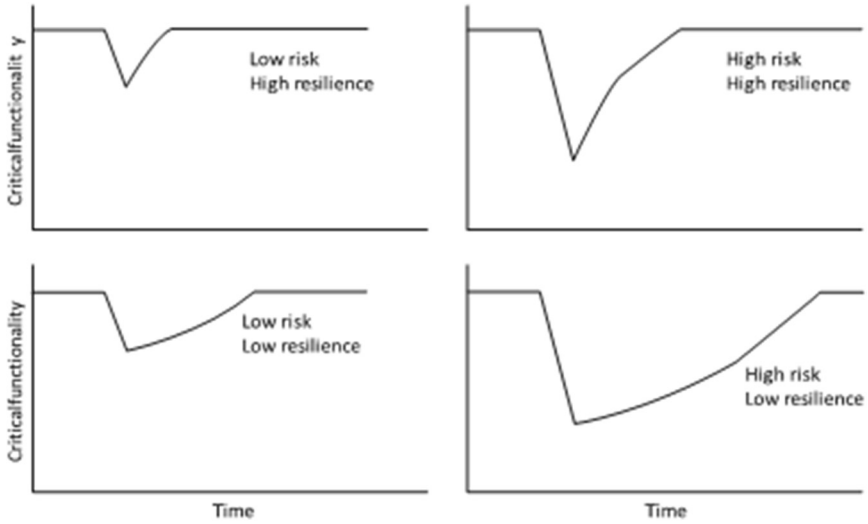


Figure 21: Interplay of risk and resilience levels (Linkov et al, 2014)

When the concept and context of resilient is perceived, a number of strategies have to be considered in order to strengthen the system's response and enhance its resilience. There are several strategies and improvements

that might be considered for this purpose. In particular, in what regards systems, infrastructures, etc. such resilience strategies can be:

- Planning ahead during the design phase, aiming to ensure robust or stochastic optimization against uncertain future scenarios.
- Self-healing, adaptation and control, i.e. graceful degradation: the system cannot be design with respect to every uncertain scenario, therefore a resilient design should consider how to prevent the disturbance from spreading across the whole system, creating systemic contagion and system-wide collapse. In this respect, cascading failures analysis, and engineering network systems to be robust against outbreak of outages and propagations of cascading failures across their elements are key strategies. Control engineering can provide strategies to create robust feedback loops capable of enabling infrastructures to absorb shocks and avoid instabilities. Designing structures and topologies which prevent failure propagation, and devising flexible topologies by switching elements which allow graceful degradation of system performances after disruptions are also valuable resilience-enhancing techniques.
- Recovering quickly from the minimum performance level: robust or stochastic optimization of the recovery and restoration process in the face of uncertainties in the repair process or in the disruption scenarios.
- Effective system restoration: through the combination of restoration strategies, e.g. repairing the failed elements and building new elements, the infrastructure can achieve a higher performance with respect to the pre-disruption conditions.
- Exploiting interdependencies among infrastructures: interdependencies and couplings in systems operations can foster the propagations of failure across coupled system; on the other hands, interdependencies might also provide additional flexibility in disrupted conditions and additional resources that can facilitate achieving stable conditions of the coupled system.[22]

6 Setting a common ground for understanding and prioritizing

It is well assessed that Resilience depends on many factors such as technological (i.e., platforms and tools for monitoring and surveillance), human (i.e., capability of intervention by first responders and exploitation of social networks and citizens as a source of information) and acceptance by end-users (willingness and awareness of the necessity to consider the added value provided by the state of art and novel technological and scientific products for the improvement of operative capabilities in infrastructure and urban areas management, during ordinary and extraordinary conditions). Presently, the approach to improving resilience is going to change deeply, not only for the revolutionary evolution of technologies (i.e., technologies directly related to resilience and driven by resilience needs), but also because the approaches to the full risk cycles and multi-hazards risks understanding is changing. Therefore, new perspectives are arising in resilience, despite the fact that the already operative services still underexploit these new capabilities, which have been recently developed. Despite the fact that is being an established feature of sustainable technological, ecological and sociological systems [23], planned resilience still requires metrics that are both adequate to measure individual system qualities and generalizable to inform resource allocation and operations. To date, the failure to understand resilience in the context of complex system has precluded the creation of an actionable metrics framework to inform resilience decisions [24].

On this basis, the following issues among others need to be preliminary drafted, being relevant in setting priorities towards a common improvement of Resilience in Security Research:

- To enable a resilient-informed risk assessment to tackle new and emerging threats. In this sense the existence of a comprehensive risk management framework across the whole life-cycle of the disaster management loop is mandatory, in combination with a multi-hazards approach.
- To build a rigorous resilience framework to organize a comprehensive list of different notions of resilience; to associate the elements of such list to different contexts, to define smart adaptable

7 Concluding remarks

Resilience is the ability of a system to withstand an unexpected harmful change or a disruptive event by reducing the initial negative impacts (absorptive capability), by adapting itself to them (adaptive capability) and by recovering from them (restorative capability).

In line with the aim of this document, the following conclusions can be drafted as a synthesis of priorities based on the information provided here above:

- To promote the concept of resilience within community's organization and strengthen the sharing of information and data to build resilient socio-technical systems;
- To integrate the potential of resilience within the Disaster Risk Management Cycle and security plans to maintain the continuity of essential services against actual and emerging threats and ensure system's bounce-back;
- To advance in the fundamental understanding and practical application of resilience towards the development of resilience process quantification, as well as comparison of resilience approaches in multiple social, environmental and engineering contexts in order to come up with generalizable principles.

On this basis, among the others, the following high-level capabilities can be identified as highly recommended in the context of Resilience in Security Research:

- Connection: to establish, in line with policy goals, a common understanding of resilience capacity to address uncertainty shifting thus from robust to sustainable sociotechnical systems, built on resilient approaches.
- Communication: to organize open-discussions among security stakeholders and spread the word on resilience capacity to address and counterbalance actual and emerging risks so that people can understand (raising awareness) and participate (end-users and citizens' involvement here is mandatory).
- Modeling and Quantification: to figure out ways to model, assess and quantify resilience aspects, by means of proper and agreed methodologies.

Therefore, the way forward for relevant Security Research R&D can be shaped around the following recommendations:

- Recommendation 1: Investigate policies and elaborate research frameworks that may contribute to strengthening the design and development of socio-technical solutions enhancing resilience and systems sustainability. This can be achieved by raising awareness on resilience, supporting and strengthening discussion among decision and policy makers, on the basis of groups of interests and group of experts, supporting the work of the CoU on Disaster Risk Management which aims to provide a common understanding of the matter and a contribution to a consolidation of priorities (short term).
- Recommendation 2: Be ready to tackle emerging risks, based on adaptative capacities developed within a relevant resilience framework, by creating a common understanding on the new and incoming risks and assessing the benefit in making systems resilient towards them. Bringing together all stakeholders, end-users and suppliers, will set the way to plan for an EU framework for resilience and later on for market uptake of innovative solutions, based on such framework and, aiming to tackle such risks (short to medium term).
- Recommendation 3: Elaborate ways to model and quantify Resilience, encouraging to build the future generation of practices and afterwards standards in resilience metrics. This could be supported by working on methodological approach and paradigm shifts in cooperation with, among others, research initiatives in US, Japan, and Australia (medium to long term).

Note to the reader:

The "Joint Position Paper on Resilience in Security Research" has been elaborated by:

The Integrated Mission Group for Security (IMG-S)

IMG-S is a wide multi-disciplinary European professional network bringing together experts from Industry, SMEs, Research and Technology Organisations (RTOs), Academia and End-users. It has more than 200 members from more than one hundred organizations representing 24 European countries. IMG-S aims to support the European Commission and its Member States to build world-class European technological capabilities. By defining research priorities for the security domain at all levels, from fundamental research to mission capabilities and system integration, IMG-S contributes to ensure that short, mid- term and long-term security needs are addressed (*http://imgs-eu.org*).

European Association of Research and Technology Organisations (EARTO)

EARTO is the European Association of Research and Technology Organisations (RTOs) founded in 1999. It promotes RTOs and represents their interest in Europe. EARTO groups over 350 RTOs with a combined staff of 150.000, top-level R&D infrastructures and facilities and more than 1000 000 partners from public and private sector annually. The EARTO Security Research Group (SRG) is a working group comprised of 14 RTO's experts from member organisations, assisting EARTO in formulating security research policy positions and elaborating technically complex issues in topics of security (*www.earto.eu*).

IMG-S Contact:	EARTO Contact:
Clemente Fuggini, R&D&I Responsible in the areas of Transport & Infrastructures; Security & Space, D'Appolonia S.p.A. IMG-S TA4 Chair *clemente.fuggini@dappolonia.it* +39 3440179979 *www.imgs-eu.org*	Georgios Eftychidis, Research Associate, Project Manager DRM & CIP Group, Center for Security Studies - KEMEA EARTO Working Group Security Research Member *g.eftychidis@kemea-research.gr* +30 2107710805 (ext.339) www.earto.eu

This paper has been edited by Clemente Fuggini, D'Appolonia (clemente.fuggini@dappolonia.it), IMGS-TA4 Chair, and by Georgios Eftychidis, KEMEA (g.eftychidis@kemea-research.gr), EARTO SRG Member.

Contributors and reviewers are listed below (in alphabetic order)

Juan Arraiza Irujo, jarraiza@vicomtech.org, Vicomtech, EARTO SRG Member
Andrzej Bialas, andrzej.bialas@ibemag.pl, Institute of Innovative Technologies EMAG, IMG-S TA4 Member
Matthaios Bimpas, mbibas@esd.ece.ntua.gr, NTUA, IMG-S TA4 Member
Miklos Biro, Miklos.Biro@scch.at, UAR/SCCH, EARTO SRG Member
Géraud Canet, geraud.canet@cea.fr, CEA, EARTO SRG Chair
Vincenzo Cuomo, vincenzo.cuomo@imaa.cnr.it, CNR IMAA, IMG-S TA4 Member
Luis Emaldi Atucha, luis.emaldi@tecnalia.com, TECNALIA, IMG-S TA4 and EARTO SRG Member
Jakub Główka, jglowka@piap.pl, PIAP, IMG-S TA4 Member
Clive Goodchild, clive.goodchild@baesystems.com, BAE Systems, IMG-S TA4 Co-Chair
Sorin Iacob, sorin.iacob@nl.thalesgroup.com, Thales, IMG-S TA4 Member
Anna-Mari Heikkilä, Anna-Mari.Heikkila@vtt.fi, VTT, EARTO SRG Member
Daniel Hiller, Daniel.Hiller@emi.fraunhofer.de, Fraunhofer EMI, IMG-S TA4 Member
Marcin Kowalski, marcin.kowalski@wat.edu.pl, WAT, IMG-S TA4 Member
Artur Krukowski, krukowa@intracom-telecom.com, Intracom Telecom, IMG-S TA4 Co-Chair
Isabelle Linde-Frech, isabelle.linde-frech@int.fraunhofer.de, Fraunhofer INT, EARTO SRG Member
Marco Manso, marco.manso@imgs-eu.org, Rinicom ltd., IMG-S Chair
Francesco Soldovieri, soldovieri.f@irea.cnr.it, CNR IREA, IMG-S TA4 Member

8 References

[1] http://www.preventionweb.net/files/43291_sendaiframeworkfordrren.pdf

[2] https://europa.eu/globalstrategy/sites/globalstrategy/files/regions/files/eugs_review_web.pdf

[3] https://ec.europa.eu/info/strategy/european-semester/framework/europe-2020-strategy_en

[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF

[5] https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF

[7] http://ec.europa.eu/DocsRoom/documents/20372

[8] https://www.securityresearch-cou.eu/

[9] https://www.researchgate.net/publication/276139783_Four_concepts_for_resilience_and_the_implications_for_the_future_of_resilience_engineering

[10] https://www.irgc.org/wp-content/uploads/2016/04/Barker-Ramirez-Marquez-Infrastructure-Network-Resilience.pdf

[11] http://www.zoology.ubc.ca/bdg/pdfs_bdg/2013/Holling%201973.pdf

[12] https://www.researchgate.net/publication/261615193_A_three-stage_resilience_analysis_framework_for_urban_infrastructure_systems

[13] http://journals.sagepub.com/doi/abs/10.1191/030913200701540465

[14] http://www.tandfonline.com/doi/abs/10.1080/00139157.2013.768076

[15] http://www.environmentmagazine.org/Archives/Back%20Issues/2013/March-April%202013/index.html

[16] https://www.irgc.org/wp-content/uploads/2016/04/Sansavini-Engineering-Resilience-in-Critical-Infrastructures.pdf

[17] https://ajem.infoservices.com.au/downloads/AJEM-25-02

[18] http://www.eco-nomics.com/images/Designing_Resilient_Sustainable_Systems.pdf

[19] https://www.demos.co.uk/files/Resilient_Nation_-_web-1.pdf

[20] https://www.researchgate.net/publication/263808670_Changing_the_resilience_paradigm

[21] https://www.researchgate.net/publication/230831578_Integrating_Risk_and_Resilience_Approaches_to_Catastrophe_Management_in_Engineering_Systems

[22] https://www.irgc.org/wp-content/uploads/2016/04/Linkov-Trump-Fox-Lent-Resilience-Approaches-to-Risk-Analysis-and-Governance-1.pdf

[23] http://www.eco-nomics.com/images/Designing_Resilient_Sustainable_Systems.pdf

[24] https://www.irgc.org/wp-content/uploads/2016/04/Seager-et-al.-A-Multidimensional-Review-of-Resilience.pdf