IMPROVED RISK EVALUATION AND IMPLEMENTATION OF RESILIENCE CONCEPTS TO CRITICAL INFRASTRUCTURE

D1.7 Report from associate partner workshops

Hannah Rosenqvist[1]

1. DBI

Deliverable Number:	D1.7
Date of delivery:	May 31, 2018
Month of delivery:	M36

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

Coordinator:	David Lange at RISE Research Institutes of Sweden

Table of Contents

1 Executive Summary

IMPROVER is a Horizon 2020 project focusing on how to improve European critical infrastructure resilience to crisis and disasters through the implementation of resilience concepts to real life examples of pan-European significance, including cross-border examples.

The associate partners in IMPROVER represent critical infrastructure operators and stakeholders, civil contingencies agencies and universities, throughout Europe. The associate partners have been critical for the IMPROVER project to achieve its objectives, by sharing their experiences and reviewing the project outcomes in three workshops covering different themes.

This report is a documentation of the three associate partner workshops that has been undertaken during the project. The report outlines the planning of the workshops as well as the minutes of the discussions that emerged during the workshops.

2 Acknowledgements

The authors would like to express our thanks to our associate partners and all of the workshop participants.

3 Aim and design

In order to achieve the projects overall objective of improving critical infrastructure resilience to crises and disasters, the project has addressed four underlying objectives. The objectives are as follows:

1. Improve our understanding of the application and interaction of different resilience concepts
2. Evaluate the baseline requirement of critical infrastructure in the event of a crisis
3. Development of a resilience management guideline including a methodology for implementation of resilience concepts to critical infrastructure
4. Pilot implementation of the proposed methodology in application to critical infrastructure of European significance

The associate partners have been critical for the IMPROVER project to achieve its objectives, by sharing their experiences and reviewing the project outcomes in workshops covering different themes. The associate partners in IMPROVER represent critical infrastructure operators and stakeholders, civil contingencies agencies and universities, throughout Europe. The organisations are broken down as follows: six infrastructure owners/operators, one civil contingencies agency, two rescue agencies and three universities.

There has been one associate partners' workshop every year over the duration of the project, resulting in three workshops in total. These workshops have contributed to the development of the IMPROVER Critical Infrastructure Resilience Framework (ICI-REF) as well complementary methodologies developed within the project and helped to ensure the operationalisation of the resilience concepts in real-life circumstances. The feedback from the associate partners provided central information for refining the work carried out within the project.

The workshops were all designed as one-day events and included presentations of the project, external key note speakers and group discussion sessions. All of the projects 12 associate partner organisations were invited to all workshops, as well as other stakeholders including infrastructure owners and operators, emergency response agencies, emergency management authorities and researchers.

To drive the group discussions, the IMPROVER consortium prepared a set of discussion questions relating to the workshop theme before each workshop. The questions were provided to the moderators of the discussion sessions.

The theme for the first workshop was existing methodologies for risk and resilience evaluation in critical infrastructure, as well as the definition of resilience. The second workshop focused on how critical infrastructure operators meet the requirements and expectations of the public, and how that can be improved in the context of a crisis. The theme for the third workshop was the usability of the methodologies and framework that has been developed within IMPROVER, as well as success criteria for the pilot implementations.

4 Workshop minutes

The following sections outline the main observations of the three associate partner workshops.

4.1 Associate partners workshop 1 – September 25th 2015, Copenhagen

The first workshop was held at DBI in Copenhagen, and the discussion topic for this workshop was the definition of resilience and resilience in critical infrastructure. There were in total a number of 35 participants at the workshop.

4.1.1 Opening presentations

IMPROVER project presentations

The workshop day started with a brief presentation of the IMPROVER project, by project coordinator David Lange (RISE). The shift in focus from protection of critical infrastructure to resilience of critical infrastructure was presented as a background to the project objectives. The living labs used in the project were also demonstrated. The objectives of the workshop were presented as:

- To engage with stakeholders and provide a forum for persons working in resilience to guide the projects technical direction from an early stage and to find out what opportunities they think that there are for developing the methods that are used to operationalize resilience
- To collect information on the topic of critical infrastructure resilience that cannot be retrieved from the existing literature on the topic including the opinions of people who work with resilience
- To help us to identify initiatives in the field of CI resilience and to begin to gather information from relevant projects inside of and outside of Europe

Project partner Marianthi Theocharidou (JRC) presented the state of the art on Critical Infrastructure Protection and Resilience in Europe. It was highlighted that critical infrastructure protection never can be guaranteed, and that resilience is a means to go beyond protection. Three steps to improve resilience of critical infrastructure were proposed as 1) understanding of critical infrastructure and their (inter)dependencies, 2) modelling, simulation and analysis, and 3) increase preparedness, protection and resilience.

External speaker presentation

Alec Hay (Director of the University of Toronto Centre for Resilience of Critical Infrastructure) held a presentation on infrastructure planning in a changing climate. The issues that we are facing today concern a changing world where consequences of loss are increasing due to the increasing complexity of infrastructure systems. The goal we should strive for is effective and efficient resiliency, and to get there we need to understand and plan for whole systems including all dependencies. Resilience planning is thus not equal to infrastructure hardening.

4.1.2 Discussion sessions

For the group work the participants were divided into 4 groups to discuss approximately 7 questions for an hour. Each facilitator was provided with a list of participants and a list of questions depending on the group numbers.

Q: Please provide a definition of resilience based on your own personal opinion and experiences.

Group 1 summary:

Resilience, in general, is often associated with resilience of people and used for example to characterize kids in relation to health issues, i.e. a resilient kid is not vulnerable (to diseases and injuries) and recovers quickly.

When this it comes to critical infrastructure, and specifically to the oil industry resilience means the ability to continue "business" after crisis times. This is ensured through business continuity planning and the term resilience is rarely used in everyday practice. However, the concept is there.

Resilience is not easy to define. The definition provided at the workshop presentation might be the most accurate as it is the recovering time that are prioritized.

Group 2 summary:

Resilience is the ability to recover after a negative event took place. It is the ability to keep functioning. Protection which is trying to avoid that things change and the ability to keep functioning after things have changed are both part of resilience.

Resilience is about how to withstand and how to recover. It is the capacity of a system to function at minimum level.

Group 3 summary:

Resilience is a strategy wherein you can use protection tools like redundancy. Protection is a tool for resilience. But you need to make the strategy for what you want to protect. Protection is more individual than resilience. When people talk about protection they talk about protecting an asset as opposed to a function. Resilience is protecting capabilities. That is why equity of access is such an important part of it.

Hazards cannot be separated. Treating an ice storm as a single hazard is a massive mistake, there are multiple hazards connected to it. You have to put it into context and use an all hazard approach. You also have to take into account how the population reacts. It changes the parameters of the problem.

Resilience is having a capability. There are two types of resilience; Community resilience which is far too complex to understand and Operational resilience which enables community resilience. If a community is resilient it will survive an event. However, for a community to be resilient it needs to be enabled by the surroundings. That is why community resilience is so difficult.

Group 4 summary:

Resilience is the capacity and ability to quickly bounce back and recover from shocks. The definition will change scale and level of detail depending on the specific context. It is the capacity to adopt and recover.

Resilience is the property of the system – not only the ability to recover under shock as all systems will be able to react – it is more interesting to recover and attain a more sustainable place. Resilience is a very flexible system; able to prepare for shocks and react to it as well as adaptability taking the system to a new sustainable level.

Resilience is more of a process i.e. you fall and you pick yourself up again – you recover from shock. Effectively we have done this for years. What is new is the societal push towards more interconnected infrastructure – now we are designing systems that can possibly fail.

Q: How would you define critical infrastructure resilience?

Group 1 summary:

Critical infrastructure is essential for the functioning of society. In order for the resilience of the infrastructure to be determined it must be broken down into smaller pieces to create a better overview and give the ability to supply where it is needed. However the community in your own sector is not enough, you have to communicate and look at other sectors as well.

Group 2 summary:

What is the scale of the infrastructure? There are many scales to analyze the infrastructure and it depends on the event. They must look to the basic needs of the population like water and food supplies.

Communication is a critical infrastructure because it can help to overcome disorganization of the system. Missing communication lines are not a problem in itself for the people, but for the organization. However the organization is essential for the community's recovery. It is resilience of a system. It is hard to make an entire system resilient so it is important to find the critical nodes.

Group 3 summary:

Resilience is about very accurate dependency modeling. It is a tool for strategy. Resilience is a strategy development tool. However it is important to look outside a single organization as the surroundings are equally important. Resilience encourages you to point at different pieces of infrastructure and question their importance in order to keep functionality during an event.

Critical infrastructure is any system that offers key functions to the citizens. The key is to offer services which are vital for the survival of the community. It is maintaining key societal functions. It has serious influence on your life and your nation. The list of objects that can be defined as critical infrastructure is very long.

Group 4 summary:

Resilience is a part of the critical infrastructure. The infrastructure is also a social structure. It is about the objective you are trying to achieve.

You have nodes that you need to make resilient. The critical infrastructure of these nodes and how they are connected makes a whole grid. This grid of nodes could be an organization or a power company etc. However there are key nodes in every system – they just need to be defined.

Q: What service is provided by your facility or asset to the society? Would you classify your facility or asset as critical infrastructure?

Group 1 summary:

Port of Oslo provides infrastructure for service providers from different sectors including oil and glass industry and transportation of various types of goods. The Port is inevitably a critical infrastructure since many important societal functions depend on its services e.g. 40% of Norway's oil supply and all fuel to Oslo Airport are handled in the Port.

Q: How should we measure resilience? What examples of indicators are you aware of?

Group 1 summary:

To measure resilience, we need to be able to measure performance. However, in different sectors, different indicators exist (e.g. amount of oil transported, amount of traffic, and amount of water supplied). Even within one sector several functions might exist with various indicators of each functional performance. Therefore the indicators of resilience will be different in different across

different sectors and functions. A major challenge is how to compare them and/or combine them. A possible solution is to assign weights, importance factors etc. to each indicator.

Q: What scales do you use for measuring resilience?

Group 1 summary:

It is outermost important to define the functions first that the critical infrastructure provides. This could be done e.g. as a catalogue of services (IT sector), which then could be used to define key performance indicators.

Q: Is there a scope for collaboration between sectors using the indicators and measures which have been discussed? What obstacles are there for this or how can this be enabled?

Group 1 summary:

The system needs to be broken down to individual components as each component might have different hazards, safety targets, design lifetimes etc. Vulnerability assessment is often carried out by looking at different scenarios, which might consider foreseen technological interdependencies and cascading effects; however, they are limited to the scope of the analysis including e.g. system definition and hazard identification. Assessment of the actual resilience of critical infrastructure seems more complex as it should include time aspects (recovery), organisational issues (allocation and prioritisation of available resources), unforeseen and non-technological interdependencies and cascading effects (e.g. availability of operating personnel affected by failure of interconnected system).

Q: What dimensions are there for measuring resilience i.e. temporal, financial?

Group 1 summary:

Consequences of critical infrastructure are often expressed in financial loss. However, measuring the temporal dimension is quite rare. To do knowledge of the group it is only used in earthquake engineering, mainly in the US. For buildings and structures different damage states and recovery times are defined to classify performance for different hazard levels.

Classifications exist in other sectors as well, but often based on individual contracts e.g. supplying a hospital with energy has more strict requirements than a regular building.

Q: Should resilience be measured qualitatively or quantitatively? What are the pros and cons of these two approaches?

Group 1 summary:

Resilience should be measured both qualitatively and quantitatively depending on the purpose of the assessment and nature of the system. Even semi-quantitative methods could be useful in certain situations.

Perhaps it is good to start with a qualitative assessment, providing a detailed understanding of the underlying principles, which can be further developed in a quantitative evaluation with a complexity adapted to the nature of the problem and the information available.

Thus an obvious advantage of a qualitative assessment is that more detailed information could be obtained. However, it needs more data, which can be 1) unreliable and 2) time consuming to process. Thus a “too advanced” quantitative analysis could be misleading, build up unjustified confidence and waste unnecessary resources.

Group 4 summary:

Both qualitative and quantitative methods are useful but it should be in balanced. The qualitative dimension is important however a comparison between resilience is problematic. Therefore, both methods are necessary to use.

Q: Please give details about any obstacles for operationalizing resilience.

Group 1 summary:

An obvious obstacle is the cost implementation. That is a main reason why we need to have a better understanding of operationalizing resilience, so the costs could be reduced.

For advanced methods the practical application might be difficult due to lack of information, level of data and complexity of the systems.

When operationalizing resilience we should take into consideration the political environment and public perception as these can make the process smoother or create obstacles.

Group 2 summary:

Bureaucracy is important for keeping track of things however it can also be a major obstacle when it comes to changing things. Knowledge, organizations and money can all be obstacles. It is too much bureaucracy and a lack of resources, knowledge and organization that creates the biggest problems.

Q: Does the facility/organization you work in have a strategy for implementing resilience concepts to critical infrastructure? If yes, please provide a short overview of this strategy or a reference to a document detailing this strategy. Are you aware of any shortcomings with this strategy (if yes, please elaborate)?

Group 2 summary:

There is awareness at high level, but it is still in early stages and not at the required level. One thing is resilience in the organization in itself. Common sense is related to the perception on risk. So risks that are not high on that perception are not dealt with at all. There are no terrorist attacks in Portugal until now – so it is not on anyone's priority. They will have an emergency plan for an accidental explosion but not a terrorist attack.

Q: What opportunities are there for improvement?

Group 2 summary:

There are different stages. The high level is national and the specific level is local. There are different scales at the companies and in the communities and there is plenty of room for improvements. You can look top-down or bottom-up – every change will help. Both perspectives are important and they each depend on the city.

Q: In training and exercises how have these been tested / how can these be tested?

Group 3 summary:

The only way to test resilience is to fail – to turn of the system. Then you are failing something in a controlled manor. The most important result is how fast you recover. The test is the recovering time. However resilience can only be tested at a certain level because the test gives false negatives and false positives. Nonetheless, you cannot measure resilience you can only measuring the effects of resilience.

Q: Who currently owns the risk? Who should own the risk? Who has responsibility for implementation of resilience? Who should be responsible?

Group 4 summary:

The risk is very context specific where scale is important. There is a long list of stakeholders and the responsibility is therefore distributed to a lot of people.

Q: What opportunities and obstacles are there for standardization in the field?

Group 4 summary:

Looking at resilience based on standardization would be a massive mistake – standardization is when we look at something and classify a standard for it. The environment in which we live can by definition not be standardized. And then you are unable to respond to an unclassified event. Thinking of resilience from a basis of standardization might be a problem as you cannot expect the same level of resilience everywhere.

Q: Aside from on a European level, is there a legal basis for operationalizing resilience in your country? Who has overall responsibility for ensuring this is adhered to (is it the owners/operators of the infrastructure or is it the municipalities)?

Group 4 summary:

The laws are very context specific. There are a lot of laws concerning business continuity etc. but they do not apply to resilience.

Q: Do you consider the company you are working in to be resilient to man-made and natural disasters?

Group 4 summary:

All participants had a varied degree of resilient workspaces; however it was determined that even though you have strategies and long term plans – resilience wise you are still dependent on other parties.

Q: **Has your organization participated in any activities focused on researching or operationalizing concepts of resilience on a national or regional scale? Could you please give details?**

Group 4 summary:

The group had a lot of different experiences working with IMPROVER, EU projects, port of Brisbane, fire brigades, H2020, FP7 Harmonize, FP7 CI project INDICATE as well as other industrial and civil projects.

4.2 Associate partners workshop 2 – October 13th 2016, Paris

The second workshop took place at UIC in Paris, and the topic for the workshop was how critical infrastructure can meet public expectations in response to crisis. There were in total a number of 39 participants at the workshop.

4.2.1 Opening presentations

IMPROVER project presentations

Project coordinator David Lange (RISE) opened the workshop by introducing the project and the progress from the last workshop. The drivers for resilience of critical infrastructure are the growing complexity of infrastructure systems, the increased frequency and magnitude of disasters and a paradigm shift from protection to resilience. The constraints to achieve resilience are that risk assessments are not harmonized across countries or sectors and that there currently is no legislation on a European level requiring the consideration of critical infrastructure resilience.

Project partner Laura Petersen (EMSC, Paris) presented her work regarding expected performance of infrastructure in times of crisis. The main findings were that the public seems to be willing to tolerate a reduction in service during disasters for a limited amount of time, and that the expectations varies depending on age, education level and previous disaster experience. Information from the infrastructure operator to the public leads to more realistic expectations.

Project partner Nina Kristine Reitan (RISE Fire Research, Trondheim) spoke about resilience methodologies in practice. A number of existing resilience evaluation approaches were presented, as well as the Critical Infrastructure Resilience Index (CIRI) developed within IMPROVER, as examples for the participants to consider when answering the question of what they would require in terms of a resilience evaluation methodology.

External speaker presentations

Dimitris Diamantidis (OTH Regensburg) shared his knowledge of risk and reliability assessment in major infrastructure projects. Some examples of historical structural failures of infrastructure were demonstrated and the common ways to prevent structural collapses (risk assessment and reliability analysis) were presented. There is a need for better metrics to combine human, economic and environmental risk criteria, and resilience can be a way of doing that. There is also a need for standardization, communication and consultation to manage risks through resilience criteria.

Rui Teixeira (Municipality of Barreiro, Portugal) represented one of the living labs in IMPROVER; Barreiro water supply system for human consumption. Details of Barreiro municipality and their water supply system architecture were presented, as well as their management procedures. The expectations they had on the IMPROVER project were:

- To be guided in drawing up plans for internal and external communication so that we can involve and engage not only all the services of our organization but also other stakeholders, such as the population;
- To guide us in managing the expectations of all our stakeholders in crisis or disaster situations;
- To validate the project outputs through a pilot demonstration in Barreiro, for a future integration of the “resilient component” in our Water Safety Plan;
- To get an European Directive from the guidelines resulting from the project and moreover, that this directive can be later reproduced in Portuguese Legislation so that the resilience of the systems will become a legal imperative;
- To act as an “umbrella” for the Water Safety Plan or yet to be a complement not only for risk assessment and crisis or disaster situations management but also at the level of governance.

4.2.2 Discussion sessions

For the group work the participants were divided into 4 groups to discuss approximately 2-5 questions for 1, 5 hour. Each facilitator was provided with a list of participants and a list of questions depending on the group numbers.

Group 1 summary - Hazard scenario identification

Q1: What methods do you use for scenario identification when doing risk assessment?

There are different approaches to identifying scenarios depending on the operator. In addition to the risk assessment of scenarios given by the authorities, critical infrastructure operators also define their own scenarios internally in their organisation. Context related regulations can also affect the methods being used.

In Denmark, the major electricity provider assess risk scenarios given from authorities every 3rd year. In addition to these scenarios, they define their own scenarios.

In the case of the port of Oslo the administration reports to the municipality, who distributes a general plan for risk assessment in the municipality with a list of scenarios, and the port adds their own scenarios to the list. This has not been working sufficiently, and the municipality is now working on a new acceptance criteria. All enterprises in port have their own regulations and plans.

In France the framework for identifying risks and risk analysis is regulated by French authorities, but not the methodologies. Methodologies are agreed upon between risk experts and industrial sites, and methodologies are chosen specific for each site.

Q2: Do you assess risks of every possible hazard to your infrastructure?

Assessing risk for possible hazards are carried out to a different degree by operators, from evaluating all relevant risks to evaluating risks which have a high probability or potentially large consequences. These risks involve both man-made and natural risks. In some cases the evaluation of these risks along with hazard maps are defined by experts and municipality. If the site belongs to risk areas, the operator has to study these risks. Now new regulation takes terrorism into account, this poses an administrative challenge due to the number of reports and their confidentiality.

There is a change in the way of considering hazards, being more directed towards business continuity now than before.

Q3: Do you use experts in risk assessments?

Experts are used in the risk assessment to different extent. Some only use internal experts whilst others only use external experts. In the case of Oslo port it would not be accepted to do internal risk assessments for activities that are important for the port activity, therefore they buy risk assessment services from companies i.e. experts.

Danish electricity provider uses internal experts conduct the assessment, nevertheless they also gather data from other experts, i.e. meteorological agencies.

Q4: Are you happy with current procedures?

There are side effects of using scenarios which would perhaps require external assessment. These side effects are not assessed today. Too little is included about cascading effects e.g. who, i.e. which organization, will be responsible for actions in a cascade of events? One organization states that they are mostly satisfied with how it is done today, stating that some procedures are good and some are not.

Topic 2

Q1: Do you know the public expectations, and do you measure them?

None of the group members identify or measure public expectations. One group member stated that they know about e.g. potential disruption to services, but not about the public expectations related to these services.

Q2: Do you use social media

Operators use social media to different degrees. Some only uses their web site to give information and others use Twitter and SMS services to communicate with the public, authorities and journalists. Here one operator collaborates with another company that provides telephone numbers etc. whereby they send SMSs to areas where people live. Information spreads quickly this way, and it makes the public prepared for an expected power outage, or informs about estimated time to recovery if there is an outage. This works well because information increases people's acceptance and the operators avoid that everyone calls you.

Q3: Do you have a company strategy for social media

Times are changing and people have expressed the need for two-way communication in crisis, cf. all the Facebook groups that are created in crisis. The operators are at different stages when it comes to a social media strategy. Where some have a clear strategy others have SMS services that are currently being updated to a regular company strategy.

Group 2 summary - Public expectations

Q1: Are operators aware of which levels of reduced service the public is willing to tolerate in the face of a disaster (and for how long)? If so, how do they measure them/take them into account?

Operators need to understand the needs of the public. Operators are aware that there are minimum levels of tolerance in relation to reduced services of disruptions but there is a need for criteria and guidelines. At the moment there is no knowledge and no measurements in regards to public expectations. Therefore, it is difficult to respond efficiently to meet public expectations. There is also the challenge that people, during their daily life, have different expectations compared to emergency situations; as soon as the operator informs the public about a "crisis" (mentioning the word "crisis") public expectations suddenly change.

Q2: Do you think that minimum acceptable service levels are a good lens with which to examine resilience?

There is a general view that minimum service levels are a good thing. Countries should always work to provide minimum levels. It is further believed that people need to be prepared when they are not going to have minimum acceptable services levels; because it is strongly believed that communication calms the public. The question remains of who should determine these minimum levels. Should it be defined by politicians or the public? Minimum acceptable service levels need to be defined by politicians together with the public. One way could be to develop guidelines upon the events that happened in countries with crisis.

In countries where there are not many accidents there is not much attention on emergency and crisis events. In countries like America, they are prepared compared to Copenhagen, where fewer accidents make the basis for measuring emergency events and tolerance levels less evident.

Professor at the University Of Regensburg, Germany expressed that minimum acceptable services levels should be thought of in relation of the variable of 'time': interactional time and normalization time during which the 20% of services should still be served.

In Denmark the fire services are partially regulated and are working on developing the appropriate regulation. The service that they deliver depends on the training that the firemen have. The representative of the Danish Fire Brigade also adds that the public should 'ask the right questions' in order to allow them to provide a good service. They also need to speak a language understandable by the public. Furthermore, if someone calls in 'sick' during crisis they have 4 substitutes in place. In Portugal on the other hand they do not have enough personnel to substitute the employees who call 'sick'.

Referring to a fire in Madeira the tourists were going towards the fire meanwhile local people were helping them asking them to go toward the sea and wait. The strong communication barrier and lack of communication produced panic. To improve action in the event of emergency meetings are held every second year, where politicians and community representatives decide how to work during disasters.

Q3: What types of information should operators share with the public during a disaster? How should operators communicate with the public during a disaster (traditional media, social media)?

There is the necessity to define the type of communication to employ on social media as well as face-to-face communication e.g. mediators on the spot. At the moment operators use different types of information media such as radio, Facebook, Twitter and SMS to communicate with the public. The general attitude is that information should be shared although not all operators the whole truth all the time.

One operator within fire services states that although they use social media, there is a need to know more in relation of the type of communication within different media, maintaining consistency between promises and reality. They do not use SMS because they are too expensive. They measure their communication impact in relation to people's reaction online. The communication strategy is formed by: informing and dictating (i.e. what to do, what not to do). Then, after 5-20 minutes they follow up with additional information in relation to people responses. In the case of an emergency they employ interpreters to communicate and inform in Danish and English after 5 hours.

The water suppliers in Portugal have a smart app now. They send mediators to look after fragile people e.g. the elderly. In that way they talk about potential solutions face-to-face. They say almost everything during big disasters to contain the panic.

Q4: Would a communication guide on how to use social media to communicate directly with the public during a disaster be useful for operators? What would you expect from such a guide?

The communication during crisis needs to be coordinated, facilitated, and needs to go beyond linguistic barriers; hence there is a need for an internationalization of the communication guide.

There are mixed views on whether it is necessity to take into account tourists and different languages. One example that speaks for diversification is a fire in Madeira last summer (2015) where nobody informed tourists of what was happening and where to go. There were simply no policies in place in these types of emergency events. The use of new technologies might help, such as a tip device that sends notifications to people's phone.

At the moment the process of communicating and uploading information can be time consuming. Therefore there is a large potential for making information on social media easier.

Group 3 summary – Public communication practices

Q1: How do/should operators communicate with the public during a disaster using traditional and social media?

During national or local disasters a reliable source is important to get information to the public. Due to the risk of webpages crashing they should not be used alone. The Twitter app is reliable as it uses little bandwidth. Using several channels helps disseminate the information more broadly.

An app for disaster information can be used, but it should be more than just a disaster app. The app should also contain a useful information in times when there is no disaster to keep it useful at all times.

An example is that in Japan every smartphone sold has an app that authorities can use for emergency messages. Some cultures would accept this but others would not, as it would be seen as if "Big Brother" sees everything you do.

There is also a question as to the difference between what an operator and authorities should disseminate during crisis.

Another observation is that on-site operations/rescue work and information to the public is not always coordinated nationwide, but work better on regional and local level.

At the moment some operators use websites and social media to communicate with the public while others do not have specific means to communicate with the public in case of crisis. At present there is no plan on how to solve this issue. In some cases Twitter is used together with the national warning system.

Q2: What factors have influenced your use of social media for communicating with the public during a disaster? And what kinds of information do/should operators share with the public during a disaster?

The public has a need to share information but there is not always a practical way to solve this.

In Denmark the disaster message is the same nationwide. There is no adaptation after culture, region etc. as it is perceived that there is no need for this. At e.g. a terrorist attack the public needed and demanded updated info. In this situation the police gave new updates every 30 minutes even if there were no new issues to report.

Group 4 summary - Resilience methodology

Q1: What are your requirements for moving from risk assessment to a broader resilience assessment?

- **Type of tool (survey, software)**
- **Resources (cost, competence requirement, user-friendliness of tool)**
- **Etc.**

To make the move from risk assessment to resilience it is important to identify who is responsible for making this happen i.e. who is responsible for ensuring resilience (top accountable entity).
The mechanisms of risk assessment and resilience assessment are perhaps similar, but a change in the mindset of management is needed. Currently the main focus is to avoid scenarios and the recovery aspects are usually missing.

The view is that it can be very expensive to be "resilient", without being visible. There needs to be something to justify the efforts and motivate operators to move from risk assessment to resilience. This could be with a push from authorities and legislation in order to facilitate this transition. This also

means that authorities should be informed about resilience aspects to be able to formulate requirements/approve assessments and methods. (Authorities sometimes want to know how much CI operators can provide vs. CI operators want the authorities to guide them.)

In terms of tools they need to be easy-to-use with simple interfaces e.g. spreadsheets, list of actions in case of crisis, and a way to note where something is not good enough. The presented methodologies are really scientific, theoretical and not practical for operators.

Furthermore the assessment needs to be repeatable, objective and transparent. Security of the tools is also important. Perhaps authorities should provide the assessment tools.

There are pros and cons for both internal- and external audit. Perhaps it is good to get assistance from a public and/or competent organization to the audition of an infrastructure and give precise and realistic measures for improved resilience of the infrastructure.

Resilience aspects need to be broken down in "chunks" so the operators can understand the underlying mechanisms and how it can be improved.

Q2: Do you prefer to evaluate risk/resilience as absolute or relative measures? "Relative" may imply evaluation of resilience relative to other similar facilities, or monitoring change over time within your own facility.

Absolute evaluation is difficult!

It is important that the evaluation should facilitate improvement of resilience. Tools for this might already be available, but need to be combined: e.g. business continuity management + historical data + risk assessment.

It is important to note the difference between business continuity and service continuity.

4.3 Associate partners workshop 3 – September 21st 2017, London

The third workshop was help at UCL in London and the topic for the workshop was usability and success criteria for the IMPROVER resilience management framework (ICI-REF). There were in total a number of 35 participants at the workshop.

4.3.1 Opening presentations

IMPROVER project presentations

Project coordinator David Lange (RISE) opened the workshop by presenting the current status of the project and the living labs. The main focus of the project was at this moment to link resilience assessment with risk assessment. A communication strategy has been developed within the project, and a resilience treatment plan is in progress. Resilience is not really anything new in terms of how critical infrastructure operators work.

Project partner Rafael Almeida (INOV, Lisbon) presented the current status of the ongoing pilot implementation in Barreiro water supply system. The scenario that has been studied is an earthquake and the effect on a critical pipeline in the water supply system. The pilot implementation includes user expectations and an assessment using the Critical Infrastructure Resilience Index (CIRI) developed within the project. There were some ambiguity and lack of understanding with regards to the CIRI indicators.

External speaker presentations

Chris Sweetapple (University of Exeter) presented his work within the Safe & SuRe Water Management project. The Safe & SuRe project considers reliability, resilience and sustainability to manage different kinds of extreme events. Sustainability addresses the long term, meaning that whether or not a given design is sustainable will depend on future conditions. It is therefore important to ensure that interventions to increase resilience are not detrimental to sustainability. Thereafter, the sustainability of the intervention can be evaluated. The key messages from this presentation is that resilience must be well defined, and resilience should address extremes that risk management cannot cover.

Rasmus Dahlberg (Assistant Professor at Royal Danish Defense College) shared his experiences from working with crisis management, risk and resilience in the arctic. The main challenge for emergency management in the arctic is that all infrastructures are critical, and they are isolated. Three means to enhance resilience and crisis management in the arctic was proposed: 1) synchronization, meaning to have a common operational picture, 2) speed, with regards to response and decision-making, and 3) scalability of infrastructure, to cope with uncertainty and unpredictability.

4.3.2 Discussion sessions

For the first discussion group session the participants were divided into 3 groups to discuss 5-7 questions for 50 minutes. The participants were then mixed into 3 new groups for the second session to discuss 3 questions for 50 additional minutes.

Session 1: The resilience management framework structure

Q: Based on today's presentation of the framework, do you find the structure comprehensible or does it need more explanation?

Group 1 summary:

Yes, the structure seems to be comprehensible.

Group 2 summary:

The group seemed to be a bit uneasy when asked if they understood the framework. As the discussion unraveled the group seemed to have understood the over-all concept but questioned the underlying meaning and how the methodologies were linked to the framework, the difference between framework and methodology was unclear.

The framework makes sense because it considers different aspects. The fact that risk assessment and resilience are separated is also interesting. However, there is some confusion about what is behind the blocks and the different parts of the framework. One participant was also a bit skeptical when it comes to resilience measure framework, as he is not sure what we are measuring and if the measurement is helpful. The wording between, frameworks, methodology, dimensions, it is a bit confusing.

The resilience assessment is added as an extension to the already existing risk assessment guidelines, and that the operator does not need to something completely new. Risk assessment is more about prevention, while resilience assessment deals with the crisis itself and the recovery phase.

The technical resilience triangle is difficult to understand for someone who's not an engineer or has worked with it before. It should to be better described, perhaps presented in a different way.

Group 3 summary:

The conceptual model (the framework process diagram) is more confusing than clarifying. It is not clear what the inputs and outputs look like. The model needs more structuring. There needs to be more explanation, but that doesn't mean it's not useful. It needs some time to get familiar with.

The terminology is confusing. Everything is called framework, both the overall methodology and the different kinds of analysis and it is difficult to understand how the pieces fit together. It is also not clear what our definition of resilience is and how that presents itself within the framework.

There is a contradiction about simplification and understanding. The more we speak in general terms, the more difficult it is for the users to understand. Need to take it "back to the basics" in order to make it useful, have concrete descriptions. When it's about a large and complex system it is very hard to use and understand.

Q: Does it appear to be a practical and useful framework for assessing your CI's resilience?

Group 1 summary:

The framework is useful and comprehensive, but needs to be improved to be applicable for daily use. There is a need for more useful/specific indicators as there are too many indicators which we are unable to answer right now. It is important to see how their partners are responding to indicators.

Currently, the road maintenance company in Hungary does not have a particular risk analysis in place and only use prevention plans. We have more of a reactive response in terms of maintenance (short and long term), accidents and road construction/works. Accordingly, this is a new system for them. The system that they have in place involves a group of people (e.g. police stations) working in the road areas which firstly receive an alarm when there is a problem who then call responsible persons. Social media is also used for sending out updates.

Group 2 summary:

The argument behind the framework is that the operator should move from risk assessment to resilience assessment. In order to do this, IMPROVER should make it simple for the operator. How things are framed and presented is very important, it should be user-friendly for the operator, and the consortium could be inspired of the work of other similar projects.

At the moment, the framework is in a conceptual stage and should soon move into the implementation phase, where it should be easy for operators to use. It should be better framed and presented, for example in a clear web application, hand-books etc., and communication is important. Right now there seems to be a gap between concept and implementation.

There is also a need for clarification of the different analysis methods, and which methodology to choose for each domain. There should be an explanation of why there are different methodologies. The need for different methodologies comes from the fact that it then becomes possible for an operator to get different perspective on resilience depending on the methodology chosen. Are you doing a resilience framework or a resilience inventory?

Group 3 summary:

The operators would need more information and knowledge to be able to say if the framework could be useful, it also depends on how the framework is supposed to be implemented; as a self-assessment or an external audit.

It is a big advantage that the resilience assessment uses the same starting point as the risk analysis. This makes it much more appealing. One participant suggests that we should enhance this aspect when presenting the framework because for him it is an important thing. It is however not very

clear what it is that you are gaining by applying this resilience assessment on top of an already existing risk management practice. It is not clear what the framework ACTUALLY contains and what the connection between risk management and resilience assessment mean in practice. Need to make it more explicit if we are talking about quantitative or qualitative risk and how the outputs from those fit in with the resilience analysis.

When it comes to implementation it is not clear *how* the framework is to be implemented and how to gain a common understanding. You would need a clear methodology and to see examples to understand it properly.

Q: Does it seem appropriate to divide resilience management into the three domains (technological, organizational and societal) instead of performing a general assessment combining all domains?

Group 1 summary:

From Barreiro, they think that the societal dimension needs to be separated from the technological dimension.

The railway system is typically analyzed in terms of a technical system. They do not have a resilience model. Managers do not know about the human factor and the technical factor usually dominates. Based on a personal opinion, three subcomponents are relevant and should remain as is. Toolbox should be flexible for the end user, so it is important to have the different dimensions available. It should be possible to refine or expand the system which can be tailored for different needs. The most important consequence which is looked at after an incident is shut down time. They try to resume the traffic as soon as possible, which has a higher value than human lives. Railway operations are a business and they cannot afford having the traffic down for extended periods of time (all operators share this point of view).

Group 2 summary:

There was a bit of disagreement about how resilience should be perceived, on one side, resilience can be seen with the engineering mind, or on the other side, with an ecological or more holistic approach. For some, it made sense to divide resilience into different domains, and that we need to answer the question: “Resilience of what?”

For others, resilience is a holistic approach and therefore dividing resilience into different domains is difficult and an outdated approach. The engineering approach doesn't rise above robustness, redundancy. If you want to use the power of resilience, you need to use a holistic approach which is more complex.

Though the holistic approach was also accepted in the discussion, it was also clear that it would not be possible to apply in the context of the project.

Group 3 summary:

It is helpful that you can choose the domain that you are interested in (technological, organizational, or societal), since all domains might not be relevant to all scenarios.

Q: Does it seem practically possible to incorporate the framework into your CI’s work, with regards to existing procedures and risk management processes?

Group 1 summary:

It could be useful but is currently not being used in the road maintenance company. They do not know how they could maintain it. They are prepared for hazards/incidents but they do not assess it in great detail.

For the water distributor, they update the water risk assessment annually and when incidents occur.

Q: Are the resilience indicators understandable and well phrased?

Group 1 summary:

Some indicators are clearer than others, but it is subjective for some end users. It could be useful to include a nomenclature of indicators. Brief definition or explanation of each indicator could avoid any type of confusion. Intervals with numbers are a good way. The card is the best way to do it.

Group 2 summary:

The indicators are suggested in the framework and can be chosen if they are relevant, otherwise they can be left out. There is a need to have sector defined indicators, but because the project should include all types of infrastructures, they are at a high general level. The question remaining is who would then be responsible to define these indicators, as it can't be the operators themselves, if they are the same ones to then also evaluate/assess them.

How do we collaborate and communicate in order to collect relevant indicators? One suggestion could be sector-specific agreement through meetings and workshops to point out the relevant indicators. Maybe ERNCIP could organize something. There might be a possibility to create EU-standard.

It is difficult to understand how to respond to just a word, as the indicators now are, instead they should be phased in concrete questions, well defined.

Group 3 summary:

Many indicators are too general. Need to be more precisely defined as they are impossible to assess as they are phrased right now.

Q: Which resilience indicators are more relevant to your CI?

Group 3 summary:

The connection to stakeholders is important.

Q: Are the resilience indicators sufficiently specific to be assessed at your CI?

Group 1 summary:

Many indicators cannot be answered, as there is no "data" available. Some indicators are difficult to describe according to the presented numerical scale. Societal indicators are difficult to include in the current card format.

It depends on the circumstances at hand. If there is not an accident they do not highly value data. If someone needs to build a bridge they need to know how many cars travel on the bridge. Database could probably be made available in this project.

Group 2 summary:

The framework is clear in terms of structure, but concerning the indicators there are several issues. Clear definitions are needed and more detailed descriptions on how to weigh and measure indicators.

Further, the high-level indicators are too vague and should be more detailed, and at this stage there is a need to move from concept to implementation.

Group 3 summary:

There are pros and cons with indicators that are not well described. If an indicator is too general you don't get that push to try to find what you normally don't see but on the other hand, if it is too detailed, you might loose a lot of information that only you as an operator would know about. The indicators should be understandable but also leave room for site specific information.

Session 2: Pilot implementation and critical evaluation of the framework's fit-for-purpose

Q: Are the success criteria relevant? Should we add or exclude some? Are some more important than others?

Group 1 summary:

One participant believes that we have too many different criteria. You need to be more careful to what you want to achieve and demonstrate. Create clear and simple yes/no questions/statements instead. These statements should not be too long. What does success look like in terms of time and consumption? For example, "Ability to use existing routines" – what is the statement of success in that?

Self-assessment could be reformulated. As an organisation, are you able to apply the framework to your organisation? Where is the help if you need it? Adoption is potentially more than the system just being secured. Explain the security of the system. Also describe it related to time and simplicity to adopt. Business continuity should be included. Consider other standards than ISO 31000. Appropriateness – are we aligned with standards?

"6. Effective and coherent crisis and disaster resilience management" – should be further clarified.

"9. Resilience evaluation should invite to continuous reflection and analysis" – is it supposed to be a living document?

Peer review /auditing/comparing the system or during the evaluation process? Provide strict criteria/evidence for evaluation (against other cases/infrastructure). Need to have a circular evaluation process/review/update. Engage the management to be held responsible to keep the system alive with the operators. Check ISO 55000 (Asset management) – many similarities. This ensures that management works, which could be useful for the framework.

Group 2 summary:

User-friendly: In order to call something user friendly, it needs to be tested by users, and have them test it all the way. If you succeed then you can say that it is user friendly; if used, it works. But be careful, if is too user-friendly something might be missing, as the assessment is complex.

In this case, we can't call the framework user-friendly; it is the tool that can be user friendly. Adoption might be the adjective for the framework. If you change the question to "The resilience assessment-methodology should be user-friendly"- it's easier to relate to what is supposed to be user friendly.

Self-assessment: It was mentioned that the assessment should be something the operators wants to do rather than something that they are obliged to do, not having to show the results to authorities. But the

operators must also feel that they need it. The motivation factor is to deliver a better service. However, resilience is not a priority because of the lack of time and resources.

It seems that resilience could be a country specific concept, as for water providers in the UK, resilience must be provided; it is law regulated.

Self-assessment can help operators to find gaps and critical parts of their organization that needs to be improved, which is very much related to business continuity. It can help to remember important aspects and good if it builds on what already exists.

Relative resilience measurement: Since companies and operators face different threats and their needs are different it can be difficult to compare different infrastructures. It could be more relevant to compare with yourself, to see if year after year, you improve, are stable or get worse.

Not for publishing, too unrevealing and creates vulnerability.

Adoption: a good indicator for user-friendliness shows if people want to use it. Use to create better service and self-improve, become more sustainable in the future. When resources are limited, legal requirements may however be needed, making it a "duty" to apply resilience.

Secure: Important criterion. A good indicator for organizations could be how the mindset of the employees is being maintained, and for instance, how exercises are carried out. How they train is important (not only if they train). A good indicator is how you consider "near misses", so if you almost got into a situation but you managed to save it. Do you see this as like a learning opportunity or like no problem because nothing happened?

It was mentioned that it is important that the framework is applicable to all CI, but should be possible to tailor (considering that CIs do very different things).

Effective and coherent crisis and disaster resilience management: How do you measure this unless you actually have a crisis?

Includes human factor resilience: resilience must include human factors, one participant meant. It's difficult to distinguish between the contribution of human resilience due to training and "just reaction". Retain the resilience mind-set amongst the people. Don't just ask "Do you train?" but rather "How often, How?" Discussion on the matter of nemesis, -learning, what does it mean? The difference from "potential incidence".

Applicable to all types of CI: The difficulty now lies in figuring out which indicators to choose, which are relevant to you organization?

Quantitative, qualitative and semi-qualitative assessment: The framework shall *enable* qualitative, quantitative and semi-quantitative assessment. A qualitative assessment is required in order to perform a quantitative assessment. Again important to define! Define what you are assessing.

Group 3 summary:

The most important success criteria would be that the framework is user-friendly, that it is easy to implement and that the results are easy to understand. Comments on individual criteria below:

The framework shall be user-friendly: User-friendliness is important for all participants. The framework should be applicable without a lot of expertise about the tool/framework. It must be clear what input is needed.

The framework shall provide self-assessment: All participants agree that self-assessment is important. It would be useful to have a checklist to show decision makers, and for end users to quickly see if the procedures they already have in place are compatible with the framework.

The approach shall provide relative resilience measurements: All participants think that it is important to be able to monitor over time within their own organization as well as comparing externally to other organizations in the same sector. It could be used as a basis for benchmarking. You would need to be aware that you are not comparing apples and apples but it would be a great thing if you would be able to compare with other organizations. A lot of companies use external consulting companies to do KPI's and risk analysis and they tend to be a bit unreal and manipulated. It would therefore be important to be explicit about the ambiguity of the framework if using it to benchmark, that would increase the level of accuracy.

Using the framework is secure: All participants agree that this is important. You must be able to follow local legislation so e.g. classification should be optional, at least. It is also useful for decision makers to be able to say that it is a protected tool that can handle sensitive information.

The framework provides efficient adoption of risk assessments: Absolutely, if it makes the work easier or if it's a prolongation of the risk assessments, that's great. It is not important that it follows a given standard, but that it follows a standard in general is good.

The framework include the human factor of resilience, examining the ties between people, technology and the organization: All partners agree that this is very important. This is currently missing in a lot of other resilience work and should definitely be included. It will probably be more and more important in the years to come.

The framework shall take dependencies and interdependencies into account: Interdependencies are important to consider, there are a lot of dependencies in CI. Cascading effects are also important to take into account. Some of the participants consider cascading effects and interdependencies today in their risk management work but they all agree that it is a topic that needs to be worked more on. For example, the railways can also be used as an evacuation tool, and you can imagine all sorts of scenarios, so this is definitely a topic that railways are interested in.

The framework shall balance the level of risk that CI is exposed to, with the level that resilience operators and society are willing to accept: All participants: This might not be a good success criterion.

The approach shall be low-cost: The costs are always important, but it would not necessarily have to be low cost – the results and gains are more important. It is a cost-benefit situation; if the benefit is large the cost can also be higher.

Success criteria 17: All participants - Delete this criterion.

Q: Do you have experience with pilot implementation and would like to share information about the process or lessons learned?

Group 1 summary:

They have practical exercises (e.g. simulate fire exercises on a bridge).

Q: Based on what you know now: Do you have any comments or suggestions regarding our plan for pilot implementation of the resilience management framework?

Group 1 summary:

Difficult to answer this question due to lack of available details at this time. It needs to be demonstrated.