PUBLIC DELIVERABLE

H2020 Project: Smart Resilience Indicators for Smart Critical Infrastructure

D5.4 - Resilience Joint Evaluation and Test Report (JET report) for the case study "SmartResilience Project: BRAVO: Smart city"

Coordinator: Aleksandar Jovanovic EU-VRi

Project Manager: Bastien Caillard EU-VRi

European Virtual Institute for Integrated Risk Management

Haus der Wirtschaft, Willi-Bleicher-Straße 19, 70174 Stuttgart

Contact: smartResilience-CORE@eu-vri.eu

Resilience Joint Evaluation and Test Report (JET report) for the case study "SmartResilience Project: BRAVO: Smart city"

Author(s):	Ruben Roque, Nils Albrecht, Florian Brauner, Christian Becker
Responsible Project Partner:	Stadtwerke Heidelberg
Contributing Project Partners:	Stadtwerke Heidelberg, SRH University, University of Wuppertal
Deliverable No:	D5.3
Due date:	September 30, 2018
Submission date:	

Summary / Main facts & findings

In summary, the JET report from the BRAVO case study based in Heidelberg Germany shows how based on a table top exercise the energy critical infrastructure would handle a serious cyber security threat to their smart meters. The table top exercise included stakeholders from leadership positions throughout the critical infrastructure.

The participants believed that the resilience indicators are serving their purpose, but as digitalization continues, and new technologies become more widely accepted, the resilience indicators will need to evolve smartly. The suggestions focus on the importance of change in critical infrastructures to manage the threats that emerging technologies will induce.

Cyber-security was a major part of the table-top exercise. The majority of the discussion surrounded cyber-security. The result was new information on what critical infrastructures in Germany are dealing with. An interesting note was that cyber incident occurs every second day. The most likely cause is by human error. Also, new law regulations in Germany for IT-security (IT-Sicherheitsgesetz und BSI-KRITIS-Verordnung), all critical infrastructures of Germany are demanded to join in an information platform and report critical events such as hacking and cyber-attacks. In the discussion about IT-security, several major challenges developed:

- *Seeking isolated IT-systems (island systems) which are independent of each other, especially for systems that are part of the operation monitoring and steering system.*
- *Reduction of interfaces between systems.*
- *Demanding the updating of firewalls and anti-virus systems on all devices.*
- *Different roles for data access, reducing the number of accessibilities.*
- *Sensitivity of own employers to reduce the risk of inner attacks*

The experts felt that new technologies often provide more ports and gateways into the already secured system and therefore makes the system more vulnerable and prone to attacks. The complexity increases with the combination of different systems and interfaces. Therefore, new technologies should be tested carefully according to their risk and benefit.

1. Introduction

Today, cities are facing challenges that could very well bring them to their knees. Overpopulation, extreme weather events, and rapid digitalization are all threats that cities must face. The backbone of these cities are the critical infrastructures that supply energy, water, and finances. This study will consider the developing field of risk resilience in critical infrastructures, with the focus of digitalization and smart cities.

2. Assessed Critical infrastructure

2.1. General description of the assessed critical infrastructure

The Stadtwerke Heidelberg GmbH is divided into nine different private companies. The companies cover the regions of Heidelberg and Neckargemünd. The nine companies cover the main activities of providing electricity, gas, water, heating, public pools, and the mountain tram. The companies under the Stadtwerke Heidelberg GmbH umbrella are:

- *Stadtwerke Heidelberg Energie (Energy)*
- *Stadtwerke Heidelberg Netze (Network)*
- *Stadtwerke Heidelberg Technische Dienste (Technical Services)*
- *Stadtwerke Heidelberg Bäder (Pools)*
- *Stadtwerke Heidelberg Umwelt (Environment)*
- *Stadtwerke Heidelberg Garagen (Garages)*
- *Heidelberger Straßen und Bergbahn (Streets & Mountain Tram)*
- *Stadtwerke Neckargemünd*
- *Stromnetz Neckargemünd (Electricity Network)*

The umbrella company Stadtwerke Heidelberg GmbH employs 214 people who generated 30 million euros in revenue in 2016. Stadtwerke Heidelberg Energie employs 31 employees that generate 190 million euros in revenue in 2016. Stadtwerke Heidelberg Technische Dienste employs 87 people who generate 3 million euros in revenue in 2016.The Stadtwerke Heidelberg Bäder employs 27 people while generating a revenue of 1.8 million euros in revenue. Stadtwerke Heidelberg Environment employs 25 people with a revenue generation of 31.8 million euros. Lastly, the Stadtwerke Heidelberg Garagen employs 2 people with total revenue in 2016 of 3.1 million revenue. In Heidelberg, the Stadtwerke is one of the largest employers with over 1,000 employees and 270.1 million euros in sales for 2016 (Stadtwerke Heidelberg, 2016).

Recently as a joint-venture between the city of Heidelberg and Stadtwerke Heidelberg, the Digital Agentur Heidelberg GmbH was founded to drive the smart city developments in Heidelberg.

2.2. Smart critical infrastructure features

The Stadtwerke Heidelberg is a critical infrastructure in the beginning of its digital transformation process. Examples of smart technologies being used include the integration of solar tiles and building integrated PV, voltage stability analysis application, smart lighting in a developing neighborhood, fiber optics, and smart metering. The use of an IoT infrastructure is in the early proof of concept stage. Most of these technologies are relatively new for the Stadtwerke Heidelberg and the CI.

3. Assessment Setup

3.1. Threat

The final threat identified in the Bravo case study in Smart Resilience project was cyber-attacks. In the past years, cyber-attacks have become more famous. The data breaches at American Retailers like Target and TJ Maxx or in the Government sector where the Clinton Foundation was breached and even the Internal Revenue Service, where the tax data of American citizens are held. Just this year, Equifax had a data breach where 143 million American had their personal data exposed. Equifax is one of the three largest credit companies in the United States of America. There are also major cases of Malware, Spyware, viruses, and Ransomware. The WannaCry Ransomware was one of the worst examples in recent history. There were over 200,000 victims and more than 300,000 computers infected by the WannaCry worm. These threats cause global concern for companies, especially critical infrastructures.

According to the Allianz Annual Risk report, the main causes of cyber incidents are a hacker attack/organized crime, data or security breach, malware and other viruses, and errors or mistakes made by employees. These incidents cause economic loss through business interruption, reputational loss, liability claims after data breaches, and data restoration costs. This has caused data protection rules becoming increasingly strong to strengthen cyber-security (Allianz, 2012-2017).

3.2. Scenario

1. Stadtwerke Heidelberg IT & Energy notice higher energy consumption in the Bahnstadt district of Heidelberg.

2. It was confirmed by the Stadtwerke Heidelberg IT that the Smart Meter system was hacked, which led to an extremely high energy demand.

3. Hacking caused a power failure in all houses using smart meter technologies.

3.3. Issues/elements/indicators refinement

3.3.1. Selection of issues/elements/indicators

I. Understand risks
I.1. Company Safety Culture; ID-579
I.1.1. How many safety education and awareness trainings are done yearly?; ID-580
I.1.2. Are firewalls updated frequently?; ID-586
I.1.3. Are there drills in place in case of emergency?; ID-600
II. Anticipate/prepare
II.1. Decision-Making; ID-618
II.1.1. Are there plans for communication in times of shut-down?; ID-633
II.2. Data storage; ID-582
II.2.1. How many locations is the operations data being held?; ID-584
III. Absorb/withstand
III.1. Business interruption (BI); ID-576
III.1.1. Are there automatic functioning shut-down mechanisms? ; ID-592
IV. Respond/recover
IV.1. Interconnections (grid); ID-630
IV.1.1. Is the overall system structured in a mesh?; ID-631
V. Adapt/transform
V.1. Continuous improvement; ID-585
V.1.1. Is there an incident reporting procedure in place?; ID-605
V.1.2. Are overall reviews required after crisis situations?; ID-643

4. Description of the exercise method (type of event) and other practical details

4.1. Exercise method

The ISO 22398 describes six different exercise methods. This table was extracted from their informative annex to have a readable chart comparing the different methods. Through this chart, there is a better picture of the scope, aim, benefits, performance objectives, and safety for each type of exercise. As seen from the tabletop test that it should be practical or simulated, it should evaluate procedures, should benefit by practicing team building and problem-solving, there should be at least three performance objectives, and finally that for the participant's safety it is relatively low risk to execute.

	Seminar	*Workshop*	*Tabletop*	*Simulation*	*Drill/Functional*	*Full scale*
Scope	*Introductory, overview or Education Sessions*	*Introductory, Overview or Education Sessions*	*Practical or simulated*	*Games and Gaming*	*Walk-through or Specialized Exercise*	*Live or real-life exercise*
Aim	*Provide an overview of Plan. Designed to orient participants to new or updated plans, policies, or procedure*	*Intended to build the specific product. Example draft plan*	*Evaluate plans, procedures, coordination, and assignment of resources*	*Provide practice in decision required during a disruptive incident*	*Simulate a scenario as realistically as possible in a controlled environment. Testing communication, preparedness, and availability of resources*	*Deploys personnel, equipment, and resources to a specific location for the real time, real life simulation of a scenario.*
Benefits	*Informal, easy to conduct and low stress*	*Informal, easy to conduct and low stress. More participant's involvement*	*Practices team building and problem-solving. Medium stress level*	*Decisions and actions generate simulated responses and consequences. Involves more participant, simulators, and evaluators*	*Decisions and actions occur in real time. Generate responses and consequences*	*Evaluates operational capabilities in an interactive manner, facilities communication and coordination across organization and public-private sector*
Performance objectives	*Specific objective*	*Specific objective that identifies the "product" of the workshop*	*At least 3 performance objectives*	*At least 5 performance objectives*	*Number of exercise performance objectives depending upon the number of functions involved. No less than 3 objectives per function*	*Number of exercise performance objectives depending upon the number of functions involved. No less than 3 objectives per function*
Safety	*Low Risk*	*Low Risk*	*Low Risk*	*Low Risk*	*Medium Risk*	*High Risk*

4.2. Stakeholders involved in the exercise

The Smart Resilience team in attendance were:

- *two exercise coordinators*
    - *Professor from Heidelberg University of Applied Sciences*
    - *Leader of New Technologies at Stadtwerke Heidelberg*
- *one documentation coordinator*
    - *research assistant for both Stadtwerke Heidelberg & Heidelberg University of Applied Sciences*
- *three observers*
    - *a research assistant at University of Wuppertal*
    - *innovation manager for Stadtwerke Heidelberg*
    - *regulatory manager*

The job titles of the participants of the Stadtwerke Heidelberg were as follows:

- *Group Leader Planning Power Systems*
- *Group Leader Central Management*
- *Area Coordinator IT Infrastructure & Security*
- *Staff Leader Occupational Safety*
- *Department Manager Network Information*
- *Staff Leader Company Communications*

4.3. Planning of the exercise

The planning of the table-top exercise began at the end of April 2017 as part of the Smart Resilience Task 5.2. For this task, it was requested that a test environment is created to validate the indicator-based assessment. This should be done by the development of a dynamic scenario. The results of Task 5.2 will be accumulated into a Test and Evaluation Manual. Eventually, this task will evolve into Task 5.4 where the tabletop test will be executed.

The start of the Smart Resilience project was in May 2016. The next milestone was the identification of the contact relevant persons and their roles from Heidelberg. This task was executed by the professors at the SRH Heidelberg University of Applied Sciences. The next relevant milestone was the identification of threats to the critical infrastructure Stadtwerke Heidelberg. The objective was completed by joint-work between the SRH Heidelberg University of Applied Sciences. The following milestone of the developed method of for identifying issues and indicators for resilience was presented to all project partners by SINTEF, which is a research company based in Norway, and Steinbeis Advanced Risk Technologies based in Stuttgart, Germany. This presentation was held at the end of January 2017 in Stuttgart, Germany. The next milestone was completed as joint-work from the SRH Heidelberg University of Applied Sciences and Stadtwerke Heidelberg, to identify the initial issues and indicators that can be used to measure resilience in critical infrastructures in the energy sector. This milestone was completed in the middle of February 2017. The completion of the stress-test framework for the Bravo case study began the period of planning for the stress-test. April 25th, 2017 the idea for a stress-test framework for a critical infrastructure in the energy sector was presented to the Smart Resilience partners and accepted by them. From the time between this milestone and the next one for the stress-test planning group meeting, was where research was completed on the different types of tests, exercises, and how to execute a proper table-top exercise was executed. The research process will be later in the chapter. In the middle of June 2017 was the group meeting with the newly constructed Smart Resilience team for the stress-test in Stadtwerke Heidelberg. The group meeting set-up and results will be discussed in detail later in the chapter. Then the execution of the stress-test at Stadtwerke Heidelberg was completed on August 2nd, 2017. In between the group meeting and the execution of the stress-test was coordination between parties Stadtwerke to get the right space, devices, and tools at the location. Also, finalizing the plan for the stress-test ended just minutes before the exercise participants entered the room on August 2nd because the aim to have a dynamic discussion and exercise environment was the highest priority. Finally, at the end of August was the final evaluation of the stress-test results. Members of the University of Wuppertal and Stadtwerke Heidelberg completed the evaluation of the results.

4.4. Informed consent

The participants provided consent that their ideas would be used for the study. No consent was given for personal information.

5. Results

5.1. Main results

The end of the table-top test can be reviewed in terms of the scenario, smartness, cyber security, crisis operation procedures, and finally the resilience indicators. The results of the exercise were developed with the help of the Smart Resilience Bravo team.

The experts in the exercise had issues discussing all three scenarios due to the different levels of complexity. The result from the discussion of the scenarios was that the experts felt that their current procedures according to the Business Continuity Plan and the Emergency Plan could hand each scenario. This is because the procedures provide detailed guidelines on how to handle and disturbance in the energy power supply. Even when the exercise coordinator pushed the experts to think of the worst-case scenario, the experts still concluded that their current plan is complete enough that it could deal with every scenario.

In terms of smartness, the exercise exposed a great interest in the experts' desire to work with new technologies in the energy supply. For example, areas across Heidelberg are using smart grid technologies including smart meters. The challenge, however, is to get the full potential out of this technology. The experts agreed that they are currently not using their smart technology developments to their full potential. One example is that smart grids should provide electricity consumption data two ways. However, as of now, the data only goes to Stadtwerke Heidelberg. Customers have no way currently to view their consumption via an app or website. Also, the digitalized self-regulated power supply is not currently being used. Many issues that occur in the grid must be handled mechanically. Therefore, the use of smart resilience indicators is not feasible.

Cyber-security was a major part of the table-top exercise. The majority of the discussion surrounded cyber-security. The result was new information on what critical infrastructures in Germany are dealing with. An interesting note was that cyber incident occurs every second day. The most likely cause is by human error. Also, new law regulations in Germany for IT-security (IT-Sicherheitsgesetz und BSI-KRITIS-Verordnung), all critical infrastructures of Germany are demanded to join in an information platform and report critical events such as hacking and cyber-attacks. In the discussion about IT-security, several major challenges developed:

- *Seeking isolated IT-systems (island systems) which are independent of each other, especially for systems that are part of the operation monitoring and steering system.*
- *Reduction of interfaces between systems.*
- *Demanding the updating of firewalls and anti-virus systems on all devices.*
- *Different roles for data access, reducing the number of accessibilities.*
- *Sensitivity of own employers to reduce the risk of inner attacks*

The experts felt that new technologies often provide more ports and gateways into the already secured system and therefore makes the system more vulnerable and prone to attacks. The complexity increases with the combination of different systems and interfaces. Therefore, new technologies should be tested carefully according to their risk and benefit.

5.2. Other information

In terms of the resilience indicators, Stadtwerke Heidelberg is already using conventional indicators throughout the company. For example, if a disturbance occurs that affects more than 30 households, the communication department will be informed. If the buildings affected are of special interest, law enforcement will be informed. If the number of affected households reached near 500 households, the CEO of Stadtwerke Heidelberg will be involved in the crisis management too. There is also a special crisis management team that is informed when different indicators thresholds are reached like deaths, injuries, special interests, or high consequences. Also, in the control room in Stadtwerke Heidelberg performance indicators such as load/demand curves are used to stabilize the energy network and control the right balance of production and distribution.

6. Recommendations

For future reports, this topic can be built on further. More testing of indicators can be completed. Also, looking at the advancement in critical infrastructures smartness could be done as well. The best way to continue advance this study to the next level is to work with a company that is dealing with smart technologies and track how they are progressing as a company, where are the benefits and where are the pain points. Furthermore one point was crucial. So far the entire grid is not smart. That means that the indicators which are used successfully today could be less useful in the near future. Therefore, a regular evaluation of the used indicators has to be done.

ANNEXES

1	BRAVO Functionality Level Cyber Attack;ID-277 (Cyber attack)
2	BRAVO Resilience Index Level Cyber Attack;ID-276 (Cyber attack)

RESILIENCE ASSESSMENT REPORT FORM

The template is proposed in the EU funded project: SmartResilience (the Grant Agreement No. 700621)
see more: http://smartresilience.eu-vri.eu/

Scenario name & ID:	**Cyber attack; ID-29**
DCL name & ID:	**Bravo Smart City Heidelberg Cyber Attack; ID-79**
Assessment name & ID:	**BRAVO Functionality Level Cyber Attack; ID-277**
Date:	**06.04.2018**

Executive summary of the exercise:

Historical data/ situational reporting of the similar events (real or simulated):

There have been fears that how connected cities' critical infrastructures are becoming that the energy grid could be a clear target for those trying to do harm. One familiar story throughout the energy provider industry is told from a book called "Blackout" where an entire energy grid was shut down through the entry point of smart meters (energy monitoring meters connected to the internet). The question that needs to be answered is, "what are the steps to the quickest recovery if this type of cyber attack where to occur?"

Main objectives and challenges of the exercise:

The main objective of this exercise was to collect usable existing data for resilience and functionality indicators. The focus was to confirm existing resilience/functionality indicators and identify new potential indicators especially for cyber threats.

Description of the conducted exercise:

Start Time	Content
10:30	Introduction of Participants
10:35	SMART-City Heidelberg
10:40	Existing Process of Stadtwerke
10:45	Goal of the Workshop – Table Top Test (TTX)
10:47	Question Catalogue of Indicators (Individual Work)
11:10	Use of Indicators (Group Work)
11:40	Summary Sheet

12:00	Adaptations to Existing Processes of Stadtwerke
12:25	Next Steps

Main findings after the exercise:

The end of the table-top test can be reviewed in terms of the scenario, smartness, cyber security, crisis operation procedures, and finally the resilience indicators. The results of the exercise were developed with the help of the Smart Resilience Bravo team.

The experts in the exercise had issues discussing all three scenarios due to the different levels of complexity. The result from the discussion of the scenarios was that the experts felt that their current procedures according to the Business Continuity Plan and the Emergency Plan could hand each scenario. This is because the procedures provide detailed guidelines on how to handle and disturbance in the energy power supply. Even when the exercise coordinator pushed the experts to think of the worst-case scenario, the experts still concluded that their current plan is complete enough that it could deal with every scenario.

In terms of smartness, the exercise exposed a great interest in the experts' desire to work with new technologies in the energy supply. For example, areas across Heidelberg are using smart grid technologies including smart meters. The challenge, however, is to get the full potential out of this technology. The experts agreed that they are currently not using their smart technology developments to their full potential. One example is that smart grids should provide electricity consumption data two ways. However, as of now, the data only goes to Stadtwerke Heidelberg. Customers have no way currently to view their consumption via an app or website. Also, the digitalized self-regulated power supply is not currently being used. Many issues that occur in the grid must be handled mechanically. Therefore, the use of smart resilience indicators is not feasible.

Cyber-security was a major part of the table-top exercise. The majority of the discussion surrounded cyber-security. The result was new information on what critical infrastructures in Germany are dealing with. An interesting note was that cyber incident occurs every second day. The most likely cause is by human error. Also, new law regulations in Germany for IT-security (IT-Sicherheitsgesetz und BSI-KRITIS-Verordnung), all critical infrastructures of Germany are demanded to join in an information platform and report critical events such as hacking and cyber-attacks. In the discussion about IT-security, several major challenges developed:

- Seeking isolated IT-systems (island systems) which are independent of each other, especially for systems that are part of the operation monitoring and steering system.
- Reduction of interfaces between systems.
- Demanding the updating of firewalls and anti-virus systems on all devices.
- Different roles for data access, reducing the number of accessibilities.
- Sensitivity of own employers to reduce the risk of inner attacks

The experts felt that new technologies often provide more ports and gateways into the already secured system and therefore makes the system more vulnerable and prone to attacks. The complexity increases with the combination of different systems and interfaces. Therefore, new technologies should be tested carefully according to their risk and benefit.

Part A: Basic info

I. Resilience assessment/stress-test team member's information: Requestor		
I.1 Requestor's initials & last name: NAlbrecht	I.2 Requestor's organization: SRH Heidelberg	I.3 Requestor's position: Professor
I.4 Requestor's phone number:	I.5 Requestor's email address:	
II. Resilience assessment/stress-test team member's information: Resilience Assessment Exercise (RAE) Manager		
II.1 RAE Manager's initials & last name: RRoque	II.2 RAE Manager's organization: Stadtwerke Heidelberg	II.3 RAE Manager's position: Business Development New Technolog
II.4 RAE Manager's phone number:	II.5 RAE Manager's email address:	
III. Resilience assessment/stress-test team member's information: Executive Team		
III.1 Main Analyst's initial & last name: FBrauner	III.2 Main Analyst's organization: University Wuppertal	III.3 Main Analyst's position: Dr. Engineering
III.4 Liaison Officer/Security Liaison Officer's initials & last name (if applicable):	III.5 Liaison Officer/ Security Liaison Officer's organization (if applicable):	III.6 Liaison Officer/ Security Liaison Officer's position (if applicable):
III.7 Resilience Tool Operator's initials & last name (if applicable):	III.8 Resilience Tool Operator's organization (if applicable):	III.9 Resilience Tool Operator's position (if applicable):
IV. Resilience assessment/stress-test team member's information: Team Members		
IV.1 Infrastructure Specialist's initials & last name (if applicable): SWarkentin	IV.2 Infrastructure Specialist's organization (if applicable): Stadtwerke Heidelberg	IV.3 Infrastructure Specialist's position (if applicable): Head of New Technologies
IV.4 Other Experts' initials & last name (if applicable):	IV.5 Safety & Security/ Rescue Specialists' initials & last name (if applicable):	IV.6 IT/SCADA/data specialists' initials & last name (if applicable):
V. Scenario information (to be completed by the Resilience Assessment Exercise Manager)		
V.1 Scenario name: Cyber attack	V.2 Scenario description: Attack launched from one computer or more computers against another computer, multiple computers or networks. Cyber attacks might be broken down into two broad types: attacks where the goal is to disable the target computer or knock it offline, or attacks where the goal is to get access to the target computer's data and	

V.3 Type(s) of (smart) critical infrastructure involved:	☐ All/any infrastuctures ☐ Financial Systems ☐ Energy Supply Systems ☐ Health Care Systems ☐ Transportation System ☐ Industrial Production Systems ☐ Water Supply Systems ☐ ICT Systems ☑ Other SCIs
V.4 Particular substructures (parts of infrastructures) involved in the exercise:	
V.5 Provide details on the smartness level of the selected infrastructure:	The Stadtwerke Heidelberg is a critical infrastructure in the beginning of its digital transformation process. Examples of smart technologies being
V.7 Other CI(s) possibly affected:	
V.8 Type(s) of threats:	☐ All/any threats ☐ Terrorist attack ☑ Cyber attack ☐ Natural threats ☐ Social Unrest ☐ New Technology Accident ☐ Cascading Effects ☐ Other Threats
Other (description/details):	
V.9 Task Nr.:	V.7 Case Study "identifier" and name: SmartResilience Project: BRAVO: Smart city

VI. EXCERCISE INFORMATION (to be completed by Resilience Assessment Exercise Manager)		
VI.1 Start date, time: 02.08.2017; 10:30	VI.2 End date, time: 02.08.2017; 12:30	VI.3 Event place/venue: Stadtwerke Heidelberg
VI.4 Type event (cf. FEMA 2013):	☐ Seminar ☐ Workshop ☑ Table-top ☐ Game ☐ Drill ☐ Functional Exercise ☐ Full-Scale Exercise ☐ Other (describe)	
Other (description/details):		

Part B: Resilience Assessment Setup

VII. SmartResilience analysis setup (to be completed by the Exercise coordinator)	
VII.1 Type of resilience analysis:	☐ resilience level assessment (RL) ☑ stress-text / functionality assessment (FL) ☐ other (describe)
VII.2 Other (description/ details):	
VII.3 Dynamic Check-List (DCL) ID: 79	VII.4 DCL name: Bravo Smart City Heidelberg Cyber Attack
VII.5 Elements and indicators for Functionality Level assessment (FL)* with theirs IDs: * - alternatively attach the full list as Appendix	Element, indicator (at given points in scenario time) **Functionality** 1. Production performance; ID-1234 1.1. Alternative site exists; ID-1042 1.2. Alternative site capacity?; ID-1043 2. Electicity Supply; ID-2401 2.1. Percentage of households supplied with electricity; ID-2402 2.2. Grid supply (KwH) annually; ID-3326 3. Loss of income; ID-2181 3.1. Total income from all activities (€) annually; ID-3327 4. Terveys-, turvallisuus- ja ympäristövaikutukset - HSE impact; ID-3273 4.1. Number of HSE training/year; ID-1269
VII.6 Functionality parameters:	Downtime (minutes, days, etc.): Within an hour
	Recovery time (minutes, days, etc.): Within a day
	Recovery rate (% over time):
	Improvement/adaptation/transformation (%):

Part C: Resilience Assessment Results

VIII. Functionality level assessment/stress-test results		
VIII.1 Resilience level assessment/stress-test performance date: 06.04.2018	VIII.2 Location: Stadtwerke Heidelberg GmbH	
VIII.3 Functionality Level assessment / stress-test results:	See: Annex 1: Functionality Level assessment results for BRAVO Functionalit	
VIII.4 Evaluation of Functionality Level assessment /stress-test results:		
VIII.5 Evaluation of the results compared to minimum / critical level of functionality / Stress-test limits:	Downtime (minutes, days, etc.):	Is it equal/ above threshold:
	Recovery time (minutes, days, etc.):	Is it equal/ above threshold:

	Recovery rate (% over time):	Is it equal/ above threshold:
	Improvement/adaptation/transformation (%):	Is it equal/ above threshold:
VIII.6 Preventative/ protective/ corrective measures to be implemented:		
VIII.7 MCDM results:	N/A	
VIII.8 Selected alternative:		
VIII.9 Other relevant information:		
VIII.10 Approved by (name, affiliation): Ruben Roque, Stadtwerke Heidelberg	VIII.11 Date: 11/5/2018	

VIII.12 List of attachments:

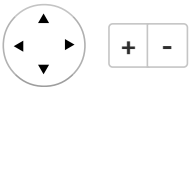
File Name	Download	Delete
No records to display.		

IX. Feedback from the resilience assessment exercise
IX.1 Issues/ suggestion methodologies:
IX.2 Issues / suggestions tools:
IX.3 Resilience of the SCI in the DCL based test compared another resilience or risk assessment method:
IX.4 New indicators which have been derived from the dataset:
IX.5 Other suggestions/general feedback:

Dynamic Checklist Assessment Results

Assessment Basic Information

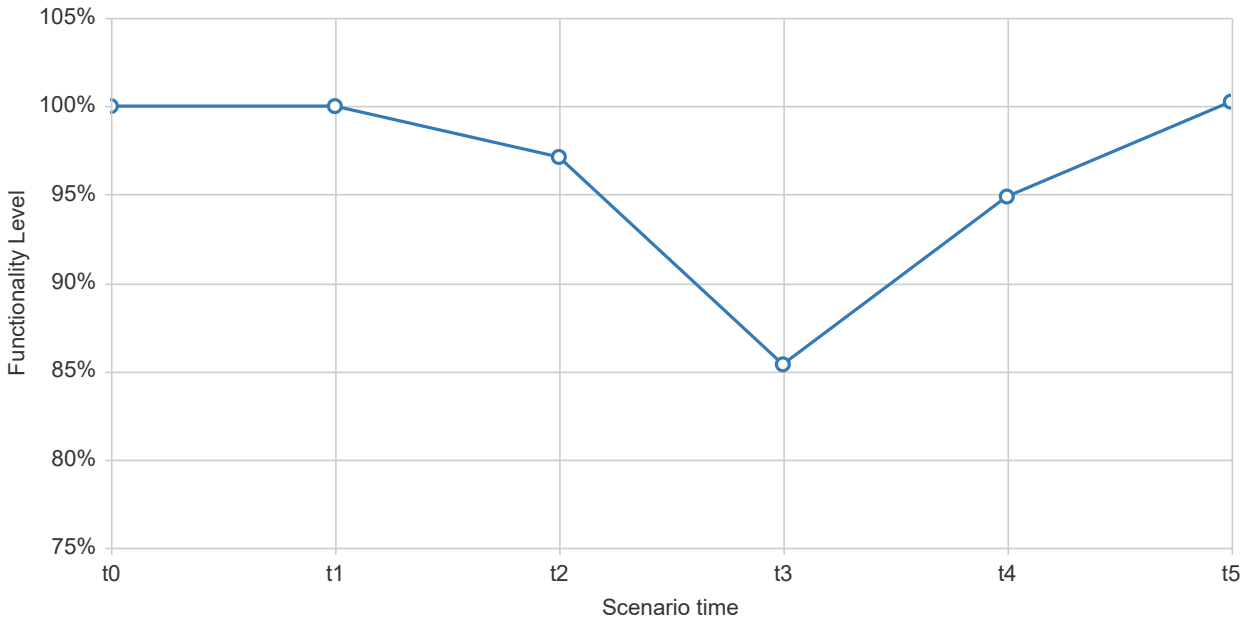
Name:	**BRAVO Functionality Level Cyber Attack**
On:	4/6/2018 10:05:49 AM
By:	Roque Ruben (SWH)
Scanario:	Cyber attack
DCL:	Bravo Smart City Heidelberg Cyber Attack



Approved by Rosen Tal / 06.11.2018

Time: Equidistant time

Show legend



Functionality Time Series

Point	Real Time	Relative Time (h)	Acceptance Level (%)	Description	New Injuries	New Deaths	New Economic Loss
t0	01.05.2018 06:00	0					
t1	02.05.2018 09:00	27					
t2	09.05.2018 11:00	197					
t3	12.06.2018 15:00	1017					
t4	10.07.2018 18:00	1692					
t5	07.08.2018 21:00	2367					
				Total:	0	0	0

Name	Type	t0	t1	t2	t3	t4	t5
Functionality level	**Root**	**100.00**	**100.00**	**97.12**	**85.38**	**94.88**	**100.25**

Name	Type	t0	t1	t2	t3	t4	t5
1. Production performance; ID-1234	**Element**	**100.00**	**100.00**	**99.00**	**68.00**	**90.00**	**101.00**
1.1. Alternative site exists; ID-1042	Indicator	100.00	100.00	99.00	70.00	90.00	101.00
1.2. Alternative site capacity?; ID-1043	Indicator	100.00	100.00	99.00	66.00	90.00	101.00
2. Electicity Supply; ID-2401	**Element**	**100.00**	**100.00**	**94.50**	**83.50**	**94.50**	**100.00**
2.1. Percentage of households supplied with electricity; ID-2402	Indicator	100.00	100.00	90.00	70.00	90.00	100.00
2.2. Grid supply (KwH) annually; ID-3326	Indicator	100.00	100.00	99.00	97.00	99.00	100.00
3. Loss of income; ID-2181	**Element**	**100.00**	**100.00**	**95.00**	**90.00**	**95.00**	**100.00**
3.1. Total income from all activities (€) annually; ID-3327	Indicator	100.00	100.00	95.00	90.00	95.00	100.00
4. Terveys-, turvallisuus- ja ympäristövaikutukset - HSE impact; ID-3273	**Element**	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**
4.1. Number of HSE training/year; ID-1269	Indicator	100.00	100.00	100.00	100.00	100.00	100.00

RESILIENCE ASSESSMENT REPORT FORM

The template is proposed in the EU funded project: SmartResilience (the Grant Agreement No. 700621)
see more: http://smartresilience.eu-vri.eu/

Scenario name & ID:	**Cyber attack; ID-29**
DCL name & ID:	**BRAVO Cyber Attack on Stadtwerke Heidelberg; ID-78**
Assessment name & ID:	**BRAVO Resilience Index Level Cyber Attack; ID-276**
Date:	**06.04.2018**

Executive summary of the exercise:

On August 2nd 2017 a table-top exercise was led by the SRH Heidelberg and the University of Wuppertal at the Stadtwerke Heidelberg GmbH to examine how this specific critical infrastructure is dealing with emerging threats with the focus on cyber threats. Decision makers including company safety leader, electrical network control, IT security, and communications where all present in the exercise. The exercise lasted about 2 hours long. The results of the exercise were that the Stadtwerke Heidelberg follows all of the laws and guidelines for critical infrastructures and these guidelines would be enough to manage the threats of today. In the end, it was confirmed that the Stadtwerke Heidelberg at the time was not using many Smart technologies for operations, however, they are aware that this will change in the near future. The indicators used by the Stadtwerke Heidelberg suffice today, however with the use of more Smart technologies there was a belief among members of the exercise that new indicators will need to be used.

Part A: Basic info

I. Resilience assessment/stress-test team member's information: Requestor		
I.1 Requestor's initials & last name: NAlbrecht	I.2 Requestor's organization: SRH Heidelberg	I.3 Requestor's position: Professor
I.4 Requestor's phone number:	I.5 Requestor's email address:	
II. Resilience assessment/stress-test team member's information: Resilience Assessment Exercise (RAE) Manager		
II.1 RAE Manager's initials & last name: RRoque	II.2 RAE Manager's organization: Stadtwerke Heidelberg	II.3 RAE Manager's position: Business Development New Technolog

II.4 RAE Manager's phone number:	II.5 RAE Manager's email address: ruben.roque@swhd.de	
III. Resilience assessment/stress-test team member's information: Executive Team		
III.1 Main Analyst's initial & last name: FBrauner	III.2 Main Analyst's organization: University Wuppertal	III.3 Main Analyst's position: Dr. Engineering
III.4 Liaison Officer/Security Liaison Officer's initials & last name (if applicable):	III.5 Liaison Officer/ Security Liaison Officer's organization (if applicable):	III.6 Liaison Officer/ Security Liaison Officer's position (if applicable):
III.7 Resilience Tool Operator's initials & last name (if applicable):	III.8 Resilience Tool Operator's organization (if applicable):	III.9 Resilience Tool Operator's position (if applicable):
IV. Resilience assessment/stress-test team member's information: Team Members		
IV.1 Infrastructure Specialist's initials & last name (if applicable): SWarkentin	IV.2 Infrastructure Specialist's organization (if applicable): Stadtwerke Heidelberg	IV.3 Infrastructure Specialist's position (if applicable): Head of New Technologies
IV.4 Other Experts' initials & last name (if applicable):	IV.5 Safety & Security/ Rescue Specialists' initials & last name (if applicable):	IV.6 IT/SCADA/data specialists' initials & last name (if applicable):
V. Scenario information (to be completed by the Resilience Assessment Exercise Manager)		
V.1 Scenario name: Cyber attack	V.2 Scenario description: Attack launched from one computer or more computers against another computer, multiple computers or networks. Cyber attacks might be broken down into two broad types: attacks where the goal is to disable the target computer or knock it offline, or attacks where the goal is to get access to the target computer's data and	
V.3 Type(s) of (smart) critical infrastructure involved:	☐ All/any infrastuctures ☐ Financial Systems ☐ Energy Supply Systems ☐ Health Care Systems ☐ Transportation System ☐ Industrial Production Systems ☐ Water Supply Systems ☐ ICT Systems ☑ Other SCIs	
V.4 Particular substructures (parts of infrastructures) involved in the exercise:		
V.5 Provide details on the smartness level of the selected infrastructure:	The Stadtwerke Heidelberg is a critical infrastructure in the beginning of its digital transformation process. Examples of smart technologies being	
V.7 Other CI(s) possibly affected:		

V.8 Type(s) of threats:	☐ All/any threats ☐ Terrorist attack ☑ Cyber attack ☐ Natural threats ☐ Social Unrest ☐ New Technology Accident ☐ Cascading Effects ☐ Other Threats
Other (description/details):	Resilience Indicators Question Catalogue Indicator Where can it be
V.9 Task Nr.: 5.4	V.7 Case Study "identifier" and name: SmartResilience Project: BRAVO: Smart city

VI. EXCERCISE INFORMATION (to be completed by Resilience Assessment Exercise Manager)		
VI.1 Start date, time: 02.08.2017; 10:30	VI.2 End date, time: 02.08.2017; 12:30	VI.3 Event place/venue: Stadtwerke Heidelberg
VI.4 Type event (cf. FEMA 2013):	☐ Seminar ☐ Workshop ☑ Table-top ☐ Game ☐ Drill ☐ Functional Exercise ☐ Full-Scale Exercise ☐ Other (describe)	
Other (description/details):		

Part B: Resilience Assessment Setup

VII. SmartResilience analysis setup (to be completed by the Exercise coordinator)	
VII.1 Type of resilience analysis:	☑ resilience level assessment (RL) ☐ stress-text / functionality assessment (FL) ☐ other (describe)
VII.2 Other (description/ details):	The start of the tabletop exercise started on time on August 2nd, 2017. There were slight preparations and adjustments made just in the morning before the start. On the day, there was a decision to focus on the threat dealing mostly with smartness. That was the cyber-security attack. All invited participants were in attendance. Represented as participants were: □ Group Leader Planning Power Systems □ Group Leader Central Management □ Area Coordinator IT Infrastructure & Security □ Staff Leader Occupational Safety □ Department Manager Network Information □ Staff Leader Company Communications. The participants were provided with: □ agenda of the exercise □ a written copy of scenarios □ copy of

□ agenda of the exercise □ a written copy of scenarios □ copy of the relevant policies and plans □ pens and notepads □ list of participants □ individual resilience indicator worksheet □ coffee, water, and snacks

The Smart Resilience team in attendance were:
□ two exercise coordinators □ Professor from Heidelberg University of Applied Sciences □ Leader of New Technologies at Stadtwerke Heidelberg □ one documentation coordinator □ research assistant for both Stadtwerke Heidelberg & Heidelberg University of Applied Sciences □ three observers □ a research assistant at University of Wuppertal □ innovation manager for Stadtwerke Heidelberg □ regulatory manager The observers were provided with pre-prepared forms to guide their notetaking.

The exercise coordinators were provided with the procedure, scenarios, and the agenda. They were also briefed earlier in the week of the procedure and agenda. The main goal of the exercise was to have applicable data to validate the resilience indicators from the Smart Resilience project. An additional goal was to be able to identify gaps in the current crisis response procedures. Finally, there was a goal to have a deep discussion on the effect of cyber threats on the company. As mentioned previously the entire exercise was done in the German language to encourage free and open discussion. The exercise began with an introduction of the Smart Resilience Bravo team, and the participants lasting only a brief few minutes. Then the presentation shifted to what makes Stadtwerke Heidelberg smart. The neighborhood of Bahnstadt and the upcoming Heidelberg Innovation Park (HIP) in the Patton Barracks were shown as examples. After this, the disruption management processes were discussed in a story-telling format. First, the definition of a catastrophe was shown from the disruption management handbook. Then came the example of a natural disaster being a flash flood. The handbook also mentioned the terrorist attack on September 11th, 2001. As an example, the exercise coordinator made the point that this was a form of sabotage per definition in the handbook. Next, the first connection of cyber-attack and sabotage was made. Finally, the relation between catastrophe, sabotage and the working situation was visualized. For example, whether the company is performing at full strength or at a slower rate because of a catastrophe or sabotage. Next, the goal of the tabletop exercise was shared with the participants. Collect usable / existing data for resilience indicators defined in the SR project. The focus is on the confirmation of existing resilience indicators and the identification of new potential resilience indicators-, especially for cyber-attacks. Followed by the sharing of the goal of the exercise, there was individual work given. This work consisted of 18 questions symbolizing the resilience indicators developed in Smart Resilience for the energy sector. These 18 indicators were pre-selected by both research assistants on the Smart Resilience Bravo Team. During the time where the participants were going through the individual work, the observers and exercise coordinator walked around the room to clarify when necessary. Also, this time was used for individual conversations with participants on the status of risk resilience at the company. The individual work lasted about 40 minutes because conversations continued to be interesting for the exercise. The next subject was the first scenario. The first two scenarios were quickly discussed because they were not of high interest in terms of smartness of the critical infrastructure. The scenarios where a flash flood and a terrorist attack. The final scenario was the cyber-security attack. This led to a deep discussion among all participants. The exercise coordinator mediated the conversation and encouraged all participants to give their expertise on the situation. The question was asked to the participants if they felt that their current disruption management processes would hold up with new threats like cyber-attacks. This led to a focused conversation on the current processes. Next, the entire discussion of scenarios was summarized for about 15 minutes on a flipchart. Finally, the exercise ended in the next steps section.

The next steps included: □ Evaluation of exercise results in the form of: □ Existing indicators □ New potential indicators □ Results of the current processes analysis □ Send the results of the analysis to interest parties at

	Stadtwerke Heidelberg Adjustments to the disruption management handbook. The entirety of the tabletop exercise lasted just under two hours. Afterwards, the Smart Resilience Bravo team met together to discuss the outcome and the future of Smart Resilience at Stadtwerke Heidelberg.
VII.3 Dynamic Check-List (DCL) ID: 78	VII.4 DCL name: BRAVO Cyber Attack on Stadtwerke Heidelberg
VII.5 Issues and indicators for Resilience Level assessment (RL)* with theirs IDs: * - alternatively attach the full list as Appendix	Phase, issue, indicator **I. Understand risks** I.1. Company Safety Culture; ID-579 I.1.1. How many safety education and awareness trainings are done yearly?; ID-580 I.1.2. Are firewalls updated frequently?; ID-586 I.1.3. Are there drills in place in case of emergency?; ID-600 **II. Anticipate/prepare** II.1. Decision-Making; ID-618 II.1.1. Are there plans for communication in times of shut-down?; ID-633 II.2. Data storage; ID-582 II.2.1. How many locations is the operations data being held?; ID-584 **III. Absorb/withstand** III.1. Business interruption (BI); ID-576 III.1.1. Are there automatic functioning shut-down mechanisms? ; ID-592 **IV. Respond/recover** IV.1. Interconnections (grid); ID-630 IV.1.1. Is the overall system structured in a mesh?; ID-631 **V. Adapt/transform** V.1. Continuous improvement; ID-585 V.1.1. Is there an incident reporting procedure in place?; ID-605 V.1.2. Are overall reviews required after crisis situations?; ID-643
VII.6 Resilience Level (RL) critical limits:	Safe zone:
	Alert zone:
	Alarm zone:
	Critical zone:

Part C: Resilience Assessment Results

VIII. Resilience level assessment results	
VIII.1 Resilience level assessment performance date: 06.04.2018	VIII.2 Location: Stadtwerke Heidelberg
VIII.3 Resilience Level assessment : * - alternatively attach the full list as Appendix	See: Annex 1: Resilience Level assessment results for BRAVO Resilience Inde

VIII.4 Evaluation of Resilience Level assessment: * - alternatively attach as Annex	The end of the table-top test can be reviewed in terms of the scenario, smartness, cyber security, crisis operation procedures, and finally the resilience indicators. The results of the exercise were developed with the help of the Smart Resilience Bravo team. The experts in the exercise had issues discussing all three scenarios due to the different levels of complexity. The result from the discussion of the scenarios was that the experts felt that their current procedures according to the Business Continuity Plan and the Emergency Plan could hand each scenario. This is because the procedures provide detailed guidelines on how to handle and disturbance in the energy power supply. Even when the exercise coordinator pushed the experts to think of the worst-case scenario, the experts still concluded that their current plan is complete enough that it could deal with every scenario. In terms of smartness, the exercise exposed a great interest in the experts' desire to work with new technologies in the energy supply. For example, areas across Heidelberg are using smart grid technologies including smart meters. The challenge, however, is to get the full potential out of this technology. The experts agreed that they are currently not using their smart technology developments to their full potential. One example is that smart grids should provide electricity consumption data two ways. However, as of now, the data only goes to Stadtwerke Heidelberg. Customers have no way currently to view their consumption via an app or website. Also, the digitalized self-regulated power supply is not currently being used. Many issues that occur in the grid must be handled mechanically. Therefore, the use of smart resilience indicators is not feasible. Cyber-security was a major part of the table-top exercise. The majority of the discussion surrounded cyber-security. The result was new information on what critical infrastructures in Germany are dealing with. An interesting note was that cyber incident occurs every second day. The most likely cause is by human error. Also, new law regulations in Germany for IT-security (IT-Sicherheitsgesetz und BSI-KRITIS-Verordnung), all critical infrastructures of Germany are demanded to join in an information platform and report critical events such as hacking and cyber-attacks. In the discussion about IT-security, several major challenges developed: • Seeking isolated IT-systems (island systems) which are independent of each other, especially for systems that are part of the operation monitoring and steering system. • Reduction of interfaces between systems. • Demanding the updating of firewalls and anti-virus systems on all devices. • Different roles for data access, reducing the number of accessibilities. • Sensitivity of own employers to reduce the risk of inner attacks The experts felt that new technologies often provide more ports and gateways into the already secured system and therefore makes the system more vulnerable and prone to attacks. The complexity increases with the combination of different systems and interfaces. Therefore, new technologies should be tested carefully according to their risk and benefit. In terms of the resilience indicators, Stadtwerke Heidelberg is already using conventional indicators throughout the company. For example, if a disturbance occurs that affects more than 30 households, the communication department will be informed. If the buildings affected are of special interest, law enforcement will be informed. If the number of affected households reached near 500 households, the CEO of Stadtwerke Heidelberg will be involved in the crisis management too. There is also a special crisis management team that is informed when different indicators thresholds are reached like deaths, injuries, special interests, or high consequences. Also, in the control room in Stadtwerke Heidelberg performance indicators such as load/demand curves are used to stabilize the energy network and control the right balance of production and distribution. With the help of the research questions and the table-top test, the hypothesis can be proved or disproved. Through the work of this thesis, the hypothesis: Existing resilience indicators are no longer valid as cities are becoming increasingly interconnected and data-driven, was proven to be false. According to the experts in the table-top exercise, the current

	false. According to the experts in the table-top exercise, the current conventional indicators are serving their purpose. However, while critical infrastructures continue to utilize smart technologies, the result will be a change in the resilience indicators to smart resilience indicators.

VIII.5 Evaluation of the results compared to the critical levels:	Resilience Level: 4.27	Critical zone to which belongs the results:

VIII.6 Preventative/ protective/ corrective measures to be implemented:	
VIII.7 MCDM results: * - if applicable	N/A
VIII.8 Selected alternative:	
VIII.9 Other relevant information:	
VIII.10 Approved by (name, affiliation):	VIII.11 Date:

VIII.12 List of attachments:

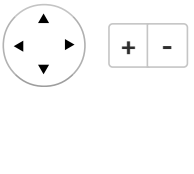
File Name	Download	Delete
No records to display.		

IX. Feedback from the resilience assessment exercise
IX.1 Issues/ suggestion methodologies:
IX.2 Issues / suggestions tools:
IX.3 Resilience of the SCI in the DCL based test compared another resilience or risk assessment method:
IX.4 New indicators which have been derived from the dataset:
IX.5 Other suggestions/general feedback:

Dynamic Checklist Assessment Results

Assessment Basic Information

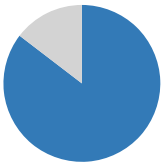
Name:	**BRAVO Resilience Index Level Cyber Attack**
On:	4/6/2018 9:23:45 AM
By:	Roque Ruben (SWH)
Scanario:	Cyber attack
DCL:	BRAVO Cyber Attack on Stadtwerke Heidelberg



Approved by Roque Ruben / 19.11.2018

R_{IL}=4.27

Excellent



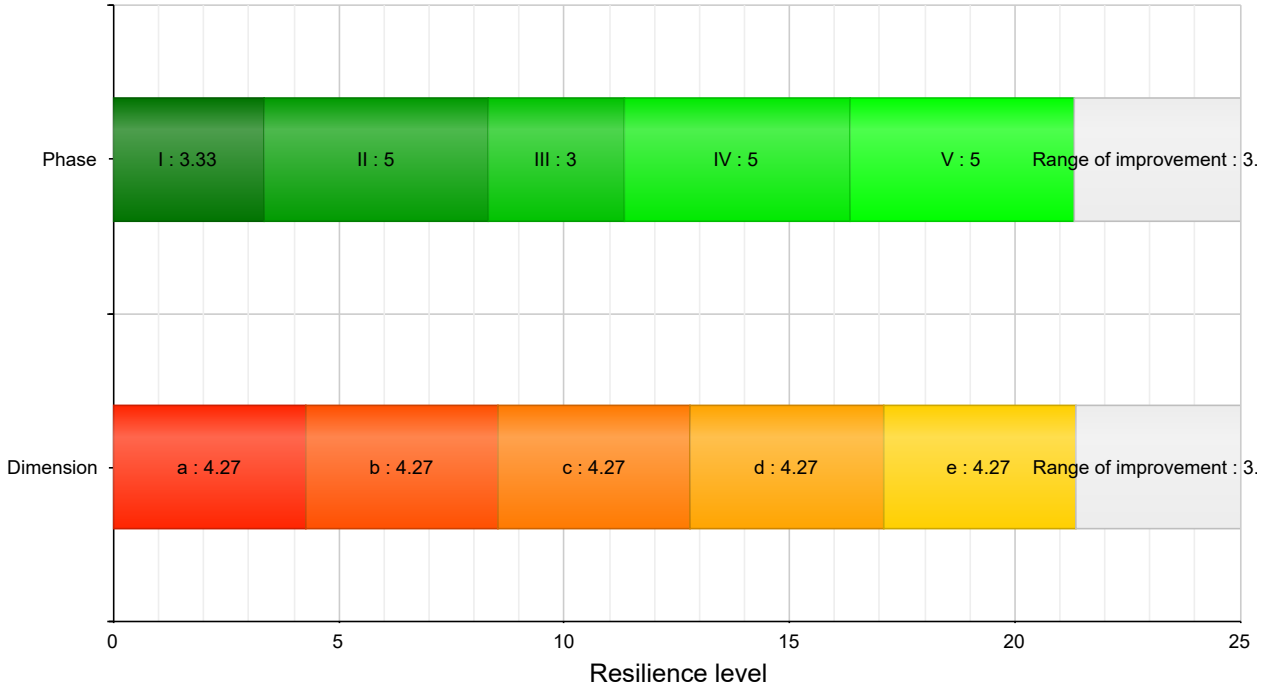
Number of indicators per cell

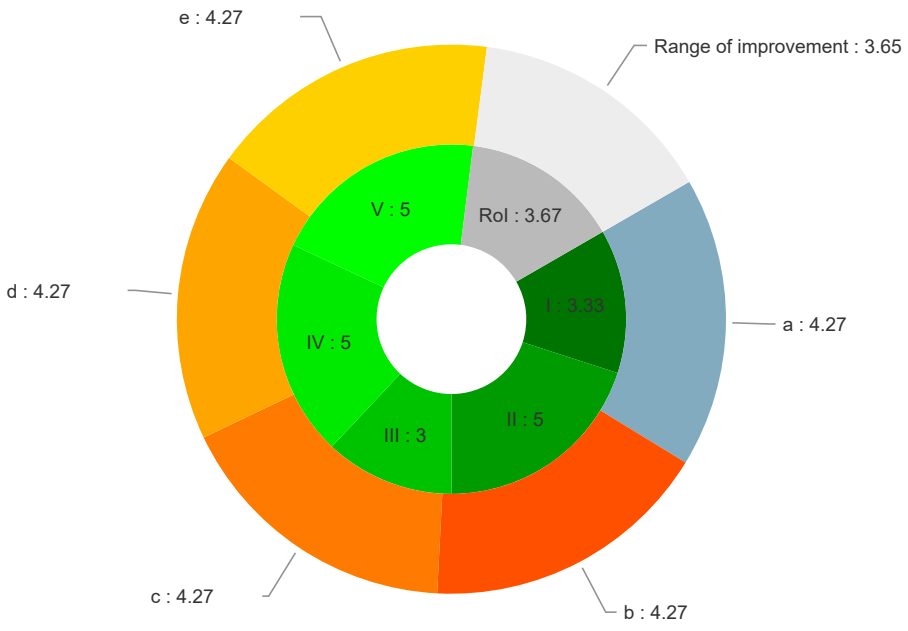
Phase Dim\	I.Understand Risk	II.Anticipate/ prepare	III.Absorb/ withstand	IV.Respond/ recover	VAdapt/ trandform
a. System/ physical	3	1	1	1	2
b. Information/ smartness	3	1	1	1	2
c. Organization/ business	3	1	1	1	2
d. Societal/ political	3	1	1	1	2
e. Cognitive/ decision making	3	1	1	1	2

Resilience level matrix

Phase Dim\	I.Understand Risk	II.Anticipate/ prepare	III.Absorb/ withstand	IV.Respond/ recover	V.Adapt/ trandform
a. System/ physical	3.33	5	3	5	5
b. Information/ smartness	3.33	5	3	5	5
c. Organization/ business	3.33	5	3	5	5
d. Societal/ political	3.33	5	3	5	5
e. Cognitive/ decision making	3.33	5	3	5	5

Resilience level per phase and dimension





Name	Type	Syst a	Info b	Org c	Soc d	DeM e	Score	Resilience Level
Resilience index level	**Root**						**4.27**	**Excellent**
I.Understand risks	**Phase**						**3.33**	**Good**
I.1. Company Safety Culture; ID-579	**Issue**	✓	✓	✓	✓	✓	**3.33**	**Good**
I.1.1. How many safety education and awareness trainings are done yearly?; ID-580	Indicator						1	Critical
I.1.2. Are firewalls updated frequently?; ID-586	Indicator						5	Excellent
I.1.3. Are there drills in place in case of emergency?; ID-600	Indicator						4	Good
II.Anticipate/prepare	**Phase**						**5**	**Excellent**
II.1. Decision-Making; ID-618	**Issue**	✓	✓	✓	✓	✓	**5**	**Excellent**
II.1.1. Are there plans for communication in times of shut-down?; ID-633	Indicator						5	Excellent
II.2. Data storage; ID-582	**Issue**	✓	✓	✓	✓	✓	**5**	**Excellent**
II.2.1. How many locations is the operations data being held?; ID-584	Indicator						5	Excellent
III.Absorb/withstand	**Phase**						**3**	**Average**
III.1. Business interruption (BI); ID-576	**Issue**	✓	✓	✓	✓	✓	**3**	**Average**
III.1.1. Are there automatic functioning shut-down mechanisms? ; ID-592	Indicator						3	Average
IV.Respond/recover	**Phase**						**5**	**Excellent**
IV.1. Interconnections (grid); ID-630	**Issue**	✓	✓	✓	✓	✓	**5**	**Excellent**

Name	Type	Syst a	Info b	Org c	Soc d	DeM e	Score	Resilience Level
IV.1.1. Is the overall system structured in a mesh?; ID-631	Indicator						5	Excellent
V.Adapt/transform	**Phase**						**5**	**Excellent**
V.1. Continuous improvement; ID-585	**Issue**	✓	✓	✓	✓	✓	**5**	**Excellent**
V.1.1. Is there an incident reporting procedure in place?; ID-605	Indicator						5	Excellent
V.1.2. Are overall reviews required after crisis situations?; ID-643	Indicator						5	Excellent