D2.2 Report on challenges for SCIs

Report Title:	*D2.2 Report on challenges for SCIs*		
Author(s):	G. Walther, M. Jovanovic, M. Vollmer, G. Desmond, A. Choudhary, Z. Székely, J. Sanne, P. Klimek, D. Bezrukov, R. Koivisto, R. Molarius, I. Macsári, I. Stumphauser, T. Knape, L. Bergfors, K. Buhr, A. Jovanovic, N. Albrecht, S. Warkentin, J. Devarajan, K. Tetlak, P. Auerkari, S. Tuurna, R. Pohja, N. Santamaria, M. Nikolic, D. Blazevic, S. Eremic		
Responsible Project Partner:	FhG-INT	Contributing Project Partners:	AIA, BZN, CCC, CoL, EU-VRI, HNP, IVL, MUW, NIS, R-Tech, SWH, VTT

Document data:	File name / Release:	SmartResilience_D2 2-Challenges_v12bc24022017		Release No.: 1
	Pages:	85	No. of annexes:	-
	Status:	Final	Dissemination level:	Public
Project title:	**SmartResilience**: Smart Resilience Indicators for Smart Critical Infrastructures		Grant Agreement No.:	700621
			Project No.:	12135
WP title:	Challenges and interdependencies of Smart City Infrastructures (SCIs)		Deliverable No:	D2.2
Date:	Due date:	Jan. 31, 2017	Submission date:	Feb. 24, 2017
Keywords:	smart critical infrastructure, challenges, threats, resilience			
Reviewed by:	L. Bodsberg		Review date:	January 26, 2017
	R. Schneider		Review date:	January 30, 2017
Approved by Coordinator:	A. Jovanovic		Approval date:	February 24, 2017

Stuttgart, February 2017

Report E0044
ISBN 978-91-7883-430-3

Release History

Release No.	Date	Change
0.5	Jan. 17, 2017	Draft for reviewers
1.0	Feb. 16, 2017	Final deliverable

Project Contact

EU-VRi – European Virtual Institute for Integrated Risk Management
Haus der Wirtschaft, Willi-Bleicher-Straße 19, 70174 Stuttgart, Germany
Visiting/Mailing address: Lange Str. 54, 70174 Stuttgart, Germany
Tel: +49 711 410041 27, Fax: +49 711 410041 24 – www.eu-vri.eu – info@eu-vri.eu
Registered in Stuttgart, Germany under HRA 720578

SmartResilience Project

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

These are the main questions tackled by SmartResilience project.

The project envisages answering the above questions in several steps (#1) By identifying existing indicators suitable for assessing resilience of SCIs (#2) By identifying new smart resilience indicators including those from Big Data (#3) By developing, a new advanced resilience assessment methodology based on smart RIs and the resilience indicators cube, including the resilience matrix (#4) By developing the interactive SCI Dashboard tool (#5) By applying the methodology/tools in 8 case studies, integrated under one virtual, smart-city-like, European case study. The SCIs considered (in 8 European countries!) deal with energy, transportation, health, and water.

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

Executive Summary

This report discusses the challenges posed by four types of threats – terrorist attacks, cyber-attacks, extreme weather and social unrest – on the following eight smart critical infrastructure systems:

a. ALPHA - Finance (financial system): The analysis focuses on disturbed information flow and disabling/manipulating IT and communication systems, including attacks on the "physical layer" using the example of IEMI/HPEM threats, as well as the software layer.

b. BRAVO - Energy supply (system): The analysis focuses on disruption of "smart" energy supply in a "smart city", caused by natural hazards, in this case flooding, leading to cascading effects and severe consequences for other energy-depending SCIs.

c. CHARLIE - Health care (system): Focus of the analysis is on all threats that might cause large increases in the numbers of injuries or sick patients within a densely populated area. This will include indirect impacts, e.g. large numbers of injuries caused by a disaster or terrorist attacks or disease epidemics, but also direct impacts, e.g. service disruptions in critical health infrastructures, such as hospitals, due to attacks or disasters hitting the infrastructure itself.

d. DELTA - Transportation (system) – airports: According to the framework situation, threats on Smart Airports will be assessed under circumstances of (i) blocked traffic, (ii) passenger and airplane traffic exceeding capacity (iii) flood.

e. ECHO - Industry (in zones in cities) "Industrial Production Plants": The analysis focuses mainly on technological accidents within the refinery complex, but also accidents caused by natural hazards affecting refinery property outside the main refinery complex, e.g. accident on jetty belonging to refinery on the river Danube during unloading/loading oil products from barge to a tank, damages by a gale or storm on process installations (pipes, hoses) resulting in river pollution. Both scenarios could lead to cascading effects for other SCIs in close vicinity.

f. FOXTROT - Water supply (systems): The analysis focuses on three cases of local and regional drinking water supply chains, with different kinds of vulnerabilities in terms of climate threats, ICT challenges, security issues and human error.

g. GOLF - Urban flood protection (systems): The analysis focuses in the disruption of water and transport caused through tidal and fluvial flooding events.

h. HOTEL: City of Helsinki - Flooding underground coal storage. Resilience of the energy infrastructure (city environment).

The way this analysis was conducted was by assessing these threats using a 5x5 framework matrix. The two axes of the matrix were phases (understand risks, anticipate/prepare, absorb/withstand, respond/recover, adapt/learn) and dimensions (system/physical, information/data, organizational/business, societal/political, cognitive/decision-making). Each individual matrix block was discussed by subject experts who identified specific challenges and implications for each matrix element and rated its relevance (high, medium, low).

In terms of the results, the system/physical dimension received the highest number of important challenges. Overall, the most important singular element was to understand risks in the organizational/business dimension. The least importance was attributed to the adapt/learn phase.

Table of Contents

List of Tables

List of Acronyms

Acronym	Definition
API	Advanced Passenger Notification
ATC	Air Traffic Control
BCP	Business Contingency Plan
BI	Business Interruption
CCC	Crisis Control Centre
ESD	Emergency Shutdown
ICS	Industrial Information & Control Systems
ICT	Information and Communication Technology
ISMS	Information Security management System
KPI	Key Performance Indicator
MSB	Swedish Civil Contingencies Agency
NOTAM	Notice to Airmen
OPW	Office of Public Works
RTV	Remote and Virtual Towers
SCI	Smart Critical Infrastructure
SWH	Stadtwerke Heidelberg
TWR	Towers

1 Introduction

This deliverable follows up on the identification of challenges that result from the smartness of critical infrastructure that is conducted within T2.1 ("Understanding 'smart' technologies and their role in ensuring resilience of infrastructures"). While in D2.1[1] challenges are presented in more general terms, this deliverable discusses the impact of four types of threats – terrorist attacks, cyber-attacks, extreme weather and events specific to SCIs – on several SCIs, i.e. the SmartResilience case studies. These SCIs cover nine systems: finance, energy, health care, transportation, industry, water, urban flood protection, a city environment (Helsinki) and an integrated case study that is not assessed here but will be a major focus in T2.3 (Table 1). Each case consists of one to three different types of threats that may affect the system's performance. The different types of threats were chosen based on their specific relevance as determined by subject experts. The data provided within each of these cases provides valuable information to anyone working within this sector. In terms of an impact for SmartResilience itself, the data and results will be useful to several work packages: T2.3 will use the data to determine any interdependencies between the systems in order to understand the possible cascading effects any disruptions within a single system may have on others. WP4 will draw on the results to ensure that their development of indicators is in line with the salience of the impact of the threats as discussed in the conclusion section. Finally, WP5 will test the cases from this deliverable while incorporating the indicators from WP4.

Table 1 Overview of threats and SCIs

Infrastructure (SCI) \ Threat	Terrorist attack	Cyber attack	Extreme weather	Specific event relevant to SCI
1. Financial system (financial service firms)	×	✓	×	×
2. Energy supply (municipal service provider)	✓	✓	✓	×
3. Health care (city health care)	×	×	✓	Mass casualty event
4. Transportation (international airport)	×	×	✓	Blocked traffic; traffic exceeds capacity
5. Industrial Production Plants (oil refinery)	×	×	×	Explosion
6. Water supply (local and regional supply)	×	✓	✓	Outbreak of waterborne disease
7. Urban Flood Protection (water supply in city)	×	×	✓	×
8. City environment (underground coal storage)	×	×	✓	Fire

The challenges these threats pose are assessed with the use of a framework that is based on the definition of resilience and its attributes as identified in D1.2[2]. The framework – as discussed in section 5.2 of D1.2 –

consists of two types of variables – dimensions and phases – that enable a systematic exploration of the threats and their potential challenges for the SCIs. The 'dimensions' variable consists of the following values: System/physical, Information/data, Organization/business, Societal/political, Cognitive/decision-making. The second variable pertains to the different temporal phases in relation to an event: understand risks, anticipate/prepare, absorb/withstand, respond/recover, adapt/learn. This 5x5 matrix was then populated with the use of previous case studies and reports as well as in collaboration with specific SCI providers and their experience and knowledge for the following sectors:

a. ALPHA - Finance (financial system): The analysis will focus on disturbed information flow and disabling/manipulating IT and communication systems, including attacks on the "physical layer" using the example of IEMI/HPEM threats, as well as the software layer.
b. BRAVO - Energy supply (system): The analysis will focus on disruption of "smart" energy supply in a "smart city", caused by natural hazards, in this case flooding, leading to cascading effects and severe consequences for other energy-depending SCIs.
c. CHARLIE - Health care (system): Focus of the analysis will be all threats that might cause large increases in the numbers of injuries or sick patients within a densely populated area. This will include indirect impacts, e.g. large numbers of injuries caused by a disaster or terrorist attacks or disease epidemics, but also direct impacts, e.g. service disruptions in critical health infrastructures, such as hospitals, due to attacks or disasters hitting the infrastructure itself.
d. DELTA - Transportation (system) – airports: According to the framework situation, threats on Smart Airports will be assessed under circumstances of (i) blocked traffic, (ii) passenger and airplane traffic exceeding capacity (iii) flood.
e. ECHO - Industry (in zones in cities) "Industrial Production Plants": The analysis will focus mainly on technological accidents within the refinery complex, but also accidents caused by natural hazards affecting refinery property outside the main refinery complex, e.g. accident on jetty belonging to refinery on the river Danube during unloading/loading oil products from barge to a tank, damages by a gale or storm on process installations (pipes, hoses) resulting in river pollution. Both scenarios could lead to cascading effects for other SCIs in close vicinity.
f. FOXTROT - Water supply (systems): We will identify three cases of local and regional drinking water supply chains, with different kinds of vulnerabilities in terms of climate threats, ICT challenges, security issues and human error.
g. GOLF - Urban flood protection (systems): The analysis will focus in the disruption of water and transport caused through tidal and fluvial flooding events.
h. HOTEL: City of Helsinki - Flooding underground coal storage. Resilience of the energy infrastructure (city environment).
i. INDIA: Integrated European virtual Case Study - Framework Scenario "Tainted Flood" Cascading and ripple effects on combined scenarios on of resilience and its indicators.

After the matrix was filled in for these eight scenarios, the subject experts assigned one of three values (red – high; orange – medium; green – low) to each field in the matrix based on the importance and relevance of the disruption. The INDIA case is an integrated study that will be assessed in detail in T2.3.

2 Case studies

2.1 ALPHA

Introduction

Technology is fundamentally transforming the financial services industry at an ever more rapid pace. "FinTech" initiatives – i.e. new financial technologies or new ways of integrating finance and technology – abound.

In this space non-financial players are using technology to offer innovative solutions that mirror the services traditionally offered by financial institutions – such as mobile payment systems developed by tech firms or online peer-to-peer lending platforms.

At the same time, the financial services industry has been driven to rethink its business models. This includes more cost-efficient ways of running their operations. Financial services firms are leveraging their existing networks and using technology much more intensely to enhance their product offerings and service delivery.

This picture is compounded by the fact that as new technologies are adopted in this field, the interactions among related technologies are increasing the complexity of the networks that underpin everyday business activities. This constitutes the background of current and future challenges surrounding the adoption and impact of smart technologies in the specific context of the financial sector.

In this context, the key threats affecting the nexus between financial services and smart critical infrastructure are:

- disruptive technologies which exploit spaces of weaker regulation
- cyber-attacks (both logical and physical) on critical infrastructure that can disrupt both financial infrastructure but also key finance-sector dependencies like electricity or telecoms
- increase speed of autonomous action (for example parametric speed trading) limiting financial authorities' abilities to react to systemic challenges on time

For the purposes of the ALPHA case study, the identification of key challenges was conducted by a core research team from the City of London. The approach employed was an informal literature review to identify key areas of further enquiry. This was then complemented with contributions from subject matter experts from the finance sector industry and the UK financial authorities. The literature review included academic papers and open source information produced by city authorities from other financial centres across the world. The contributors were asked to identify the most pressing concerns for each domain, concentrating on known challenges that have been exposed in their previous work, it is important to note that no new research / work was commissioned as part of this process.

The threat of cyber-attacks (both logical and physical) is the focus of the ALPHA case study, therefore the key challenges identified below have focused on this risk in particular.

System/ physical

In the system/physical dimension the challenges are mainly around understanding the vulnerabilities and weaknesses of the critical systems (which would vary by subsector) – where competition and regulatory oversight make the flow of information harder.

Another key area of challenges is linked to the difficulties of achieving a secure system architecture that is still open and nimble enough to not hinder market operations.

Understand risks

- *Commercial sensitivities make it harder to understand the current risk landscape:* for a lot of the financial sector firms, having a detailed understanding of their own exposures to cyber threats provides them with a competitive advantage – this could turn into a barrier for sharing information on how they identify exposures and vulnerabilities with competitors.

- *Understanding insider threats (including malicious actor infiltration, blackmailing and employee fraud for personal gain):* technical aspects of the threats are simpler to understand; human factors make the threat landscape harder to measure and model.
- *Regular evaluation of the protection of critical systems*
- *Identifying weaknesses and vulnerabilities on an on-going basis*
- *New technologies interact with existing systems in unexpected ways:* this includes disruptive technologies that are introduced into the already complex systems that underpin the sector.

Anticipate/prepare

- *Embedding security and resilience in the lifecycle of assets (from procurement to decommissioning)*
- *Regular technical security evaluation of the critical systems*
- *Developing fall backs / backups with adequate separation from live systems*

Absorb/withstand

- *Cross-domain protective activity (physical security and information security sometimes operate in silos):* this is compounded by the fact that logical and physical assets are assessed differently.
- *Reliance on distributed infrastructure (instead of a large provider) the components of which are not seen as critical infrastructure in their own right*

Respond/recover

- *Establish system back-ups and recovery plans*

Adapt/learn

- *Reviewing the adequacy of existing control measures*

Information/ data

In the information/data dimension the challenges are mainly around the level of data that is available – in some instances (like incident reporting across the sector) the datasets seem to be incomplete; in other cases the data overwhelms the capacity of the analysts looking at it (too much noise in automated reports could be an example where this is the case). These challenges are magnified by pressures on firms created by the reputational and regulatory impacts of acknowledging a breach.

Understand risks

- *Data needed for probabilistic models of potential cyber risks is not readily available / not regularly collated*
- *Being able to make sense / process live information on system performance and status*

Anticipate/prepare

- *Complex landscape of proprietary data, customer data and the businesses own data*

Absorb/withstand

- *Data on real-time or near-real-time indicators of breaches / compromise of systems tends to be commercially sensitive and not shared outside own organization*

Respond/recover

- *Information on incidents / breaches tends to not be shared because of client sensitivities or fear of regulatory penalties*

Adapt/learn

- *Evaluate data availability and quality and adequacy*
- *Information on incidents / breaches tends to not be shared because of client sensitivities or fear of regulatory penalties*

Organizational/business

In the organizational/business dimension the challenges are surrounding institutional capacity (or rather potential gaps or weaknesses in said capacity).

The following apply across all phases

- *skills-base gaps (specialists are needed in greater numbers than are being produced by the education system)*
- *Complex supply chains are difficult to understand*
- *High level of board level interest does not always match their level of technical expertise*

Understand risks

- *Understanding the business risks and maintaining processes for system mapping and risk management for critical systems and key dependencies*

Anticipate/prepare

- *Updating/upgrading complex legacy systems is not always economically viable*

Absorb/withstand

- *Adequate risk transfer tools in the market (cyber insurance is not well developed)*

Respond/recover

- *Lack of established response capabilities*
- *Costs associated with highly specialized technical expertise for post incident investigation*

Adapt/learn

- *Systematic consequence analysis of changes, upgrades and new installations*
- *New protective measures could provide a competitive advantage making it harder to socialize innovation*

Societal/ political

In the societal/ political dimension the challenges are surrounding the risk appetite of society and how it manifests itself in legislation and regulatory requirements in this space.

Understand risks

- *Political appetite for increasing the level of engagement could drive greater funding for law enforcement in this space or increased regulatory burden*

Anticipate/prepare

- *Perception of potential for commercial gains from successful exploits provides a strong incentive for attackers*

Absorb/withstand

- *Public appetite for accepting an outage or a breach is changing rapidly*
- *Concept of what is deemed too sensitive to put in the public domain is shifting on a longer timescale*

Respond/recover

- *Public outrage / market impacts could require shorter response and recovery timeframes*

Adapt/learn

- *Fear of regulatory action limits appetite for disclosing security vulnerabilities/breaches*

Cognitive/ decision-making

In the cognitive/ decision-making dimension the challenges are closely linked to the risk appetite of society and firms as well. In this case, these challenges shape how the needs for security are balanced with the needs for a greater understanding of the threats and the systemic exposures.

The following apply across all phases

- *Security considerations limit academic field of enquiry:* fear of disclosing existing vulnerabilities or providing potential attackers with sensitive information on targets or attack modes.
- *Availability bias and other cognitive biases strongly influence decision makers and researchers:* this is the flip side of the point above – for example, limits on the information available make researchers concentrate on what is available / observable without attracting security concerns.

Understand risks

- *Understanding of the full extent of system interdependencies and single points of failure*

Respond/recover

- *Practicing cyber-incident management and response capabilities going beyond ICT incident management*

Adapt/learn

- *Evaluating awareness levels and the outcomes of post incident reviews and exercises*

Table 2: ALPHA – Cyber attack

Phases Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
System/ physical	Commercial sensitivities make it harder to understand the current risk landscape Understanding insider threats (including malicious actor infiltration, blackmailing and employee fraud for personal gain) Regular evaluation of the protection of critical systems Identifying weaknesses and vulnerabilities on an on-going basis New technologies interact with existing systems in unexpected ways	Embedding security and resilience in the lifecycle of assets (from procurement to decommissioning) Regular technical security evaluation of the critical systems Developing fall-backs / backups with adequate separation from live systems	Cross-domain protective activity (physical security and information security sometimes operate in silos) Reliance on distributed infrastructure (instead of a large provider) the components of which are not seen as critical infrastructure in their own right	Establish system back-ups and recovery plans	Reviewing the adequacy of existing control measures
Information/ data	Data needed for probabilistic models of potential cyber risks is not readily available / not regularly collated Being able to make sense / process live information on system performance and status	Complex landscape of proprietary data, customer data and the businesses own data	Data on real-time or near-real-time indicators of breaches / compromise of systems tends to be commercially sensitive and not shared outside own organisation	Information on incidents / breaches tends to not be shared because of client sensitivities or fear of regulatory penalties	Evaluate data availability and quality and adequacy Information on incidents / breaches tends to not be shared because of client sensitivities or fear of regulatory penalties

Phases Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
Organizational/business	High level of board level interest does not always match their level of technical expertise Skills-base gaps (specialists are needed in greater numbers than are being produced by the education system) Complex supply chains are difficult to understand Understanding the business risks and maintaining processes for system mapping and risk management for critical systems and key dependencies	Skills-base gaps Updating/upgrading complex legacy systems is not always economically viable Complex supply chains with limited ability to influence protective behaviours	Skills-base gaps Adequate risk transfer tools in the market (cyber insurance is not well developed) Complex supply chains with limited ability to influence protective behaviours	Skills-base gaps Lack of established response capabilities Costs associated with Highly specialised technical expertise for post incident investigation	Skills-base gaps Systematic consequence analysis of changes, upgrades and new installations New protective measures could provide a competitive advantage making it harder to socialise innovation
Societal/ political	Political appetite for increasing the level of engagement could drive greater funding for law enforcement in this space or increased regulatory burden	Perception of potential for commercial gains from successful exploits provides a strong incentive for attackers	Public appetite for accepting an outage or a breach is changing rapidly Concept of what is deemed too sensitive to put in the public domain is shifting on a longer timescale	Public outrage / market impacts could require shorter response and recovery timeframes	Fear of regulatory action limits appetite for disclosing security vulnerabilities/breaches
Cognitive/ decision-making	Security considerations limit academic field of enquiry Availability bias and other cognitive biases strongly influence decision makers and researchers Understanding of the full extent of system interdependencies and single points of failure	Security considerations limit academic field of enquiry Availability bias and other cognitive biases strongly influence decision makers and researchers	Security considerations limit academic field of enquiry Availability bias and other cognitive biases strongly influence decision makers and researchers	Security considerations limit academic field of enquiry Availability bias and other cognitive biases strongly influence decision makers and researchers Practicing cyber-incident management and response capabilities going beyond ICT incident management	Security considerations limit academic field of enquiry Availability bias and other cognitive biases strongly influence decision makers and researchers Evaluating awareness levels and the outcomes of post incident reviews and exercises

Colours indicate the level of relevance:	High	Medium	Low

2.2 BRAVO

Bahnstadt in Heidelberg is one of Germany's largest urban development projects. It is designed to be Heidelberg's first smart neighbourhood. Bahnstadt is located in the south-western part of Heidelberg's city centre and shares a border with the main station. The energy concept consists of passive house standards as a universal construction method, district heating supply to be covered in the medium term by renewable energies, and intelligent control of power consumption using smart metering. Bahnstadt being the first smart neighbourhood is dependent on the critical infrastructure: Stadtwerke Heidelberg (SWH) [4].

SWH identified three main hazards as potential risk factors:

1. Cyber Security Breach
2. Terrorist Attack
3. Flash Flood

Furthermore, with the increasing use of smart technologies in the infrastructures such as smart grids, interconnected systems enabled with internet, efforts to globalize the economy, increased automation, inconsistent adoption of the smart technologies the smart critical infrastructures such as SWH also faces challenges related to increasing vulnerability to the new and emerging risks [5].

Data collection involved the end-users of the BRAVO case study. They were asked to report on the specific challenges for each of the identified threats and prioritize them basis the level of relevance to the SWH infrastructure. Also the SmartResilience task 1.3 report was analysed to derive the previously challenges identified by the end users in the case study. This two- fold approach ensured that all relevant challenges are covered in this task. With this background, the following sections focus on identifying these challenges.

2.2.1 Cyber Security Breach

Heidelberg, being a smart city, uses smart technologies such as smart grids to harness the potential of the new technologies. In this process, it is imperative to employ ICT resources and alternatively, making it vulnerable, too. Attacks through criminals hacking into the SWH data system (servers etc.) are increasing with the increased interconnectivity and globalization. These are driving greater frequency and severity of cyber incidents. The focus of SWH is mainly to prevent these attacks. In order deal with the challenges related to this threat, several physical measure are taken such as installation of security systems, firewalls for IT systems, security surveillance of fire walls which have resisted well so far. This process requires, mobilizing the organization to take the resilience oriented measures, information sharing with the key stakeholders. Hence, the main focus is to develop strategies to address challenges for all the dimensions with more emphasis on system/ physical dimension of the resilience cycle. Also, to understand the cyber security risks, which are primarily unknown due to the fast changing technology in cyber domain, is a major challenge for SWH.

There are many challenges when dealing with ICT-security threats such as a cyber-attack. These challenges are described in **Error! Reference source not found.**.

<u>System/ physical dimension</u>

Understand risk

- The first phase is to understand risk, the attacks caused through criminals hacking the SWH data system (servers etc.) are important to consider. Increasing interconnectivity and globalization are the main factors leading to greater frequency and severity of cyber incidents and hence are challenges for the SWH system. An attack or incident can result in huge data loss.

Anticipate/prepare

- In order to prevent an attack by hackers, SWH's IT-Systems have to be protected by state-of-the art firewalls, while the control room for the infrastructure must be under special security surveillance. Under the system/physical dimension the main focus is on preventive measures.

Absorb/withstand

- Each external attack in the dimension system/physical has to be recognized and monitored by special security surveillance. The firewall has to fulfil its purpose.

Respond/recover

- In case an event escalates further, the system has to be re-established physically. According to the severity of the attack and on the basis of different parameters, further actions have to be initiated.

Adapt/learn

- Each time an event causes any damage, it is mandatory to adjust the physical system. It is necessary to implement actions to adapt the organization to new situations and prevent the recurrence of such an event. Also, elimination of 'blind spots' in the system is crucial.

Information/data dimension

Understand risks

- The objective of these attacks is to get access to information/data which violates its privacy. In addition to damages paid due to loss of customer, loss of reputation can also be significant making data privacy a huge challenge.

Anticipate/prepare

- Within this phase, the impact on the dimensions Information/data is reduced by storing data in a decentralized manner.

Absorb/withstand

- As information/data is decentralized, parts of the system have to shut down automatically / immediately to protect the whole system.

Respond/recover

- Regarding the dimension of information/data, redundant data values must be present in case of a risk threatening data loss.

Adapt/learn

- The information/data that has been compromised by the attack has to be analysed and, based on this analysis, new routines have to be developed.

Organizational/business dimension

Understand risks

- An attack normally leads to business interruption (BI). This BI could be equal to or even exceed financial direct loss from data breach. SWH needs to identify key assets at risks and weaknesses in its organization. Employees can also cause large IT security or privacy breaches inadvertently or even deliberately.

Anticipate/prepare

- Under the dimension of organizational/business, focus is on measuring the safety culture among employees at SWH (Monitoring policies and procedures for all networks and systems). In addition, user education and awareness training has to be offered.

Absorb/withstand

- The dimension organizational/business includes incident management procedures and network security policies and procedures such as creating assets inventory and prioritizing them based on their importance to the organization.

Respond/recover

- Based on the priority list of assets, the organizations develop incident management procedures and network security policies and procedures.

Adapt/learn

- In order to adapt and learn from an incident, SWH considers to alter the priority and to adapt it to the needs of the organization, e.g. considering further training of employees.

Societal/political dimension

Understand risks

- From a societal/political perspective, SWH needs to create a cyber-security culture and adopt a "think-tank" approach to tackle risks. Different stakeholders from the business need to share knowledge.

Anticipate/prepare

- In terms of dimension societal/political, for SWH it is imperative to implement a crisis or breach response plan and test it.

Absorb/withstand

- In order to be able to absorb a shock and withstand in a crises situation, SWH considers it as crucial to know when to inform the public about potential dangers and risks.

Respond/recover

- Involving the public to respond to and recover from a disruptive event, SWH foresees it is crucial to inform the public about the potential dangers and risks.

Adapt/learn

- Further to adapt and learn from the event and related impacts SWH considers learning as a challenges and prioritizes strategies such as informing and exchanging opinions based on lessons learned with all relevant stakeholders.

Cognitive/decision-making dimension: In the cognitive/decision making dimension, it is the decision making challenges that are emphasized more.

Understand risks

- No less important is the dimension cognitive/decision-making. Availability of clear data is a challenge in decision making. Sound decisions have to be taken based on clear data. Therefore KPIs have to be implemented at SWH, which have to be made available to the decision-makers.

Anticipate/prepare

- In order to anticipate a risk, it is necessary to have a system in place to exchange relevant information with top management that will help them to make right decisions. This will be related to the dimension cognitive/decision-making.

Absorb/withstand

- Under the cognitive/decision-making dimension, the top-management has to get the information when incidents happen. They also have to be informed about the number of incidents as well as the severity of each cyber-attack.

Respond/recover

- Under the cognitive/decision-making dimension, the top-management has to carry out an analysis of all the circumstances and the potential consequences that has caused the initial event. They must take appropriate decisions to report the event to important stakeholders such as the insurance company in order to be reimbursed for the damage.

Adapt/learn

- In order to learn from the event, SWH focuses to reconsider the decisions taken in past and to carry out a review of the management plan and definition of an adjusted action plan.

Table 3: BRAVO – Cyber Security Breach

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
System/ physical	Attacks through criminals hacking into the SWH data system (servers etc.). Increasing interconnectivity and globalization are driving greater frequency and severity of cyber incidents.	In order to prevent an attack by hackers SWH's IT-Systems have to be protected by state-of-the art firewalls, while the control room for the infrastructure must be under special security surveillance.	Each external attack has to be recognized and monitored by special security surveillance. The firewall has to fulfil its purpose.	In case an event escalated further the system has to be re-established physically. According to the severity of the attack – based on different parameters – further actions have to be initiated.	Each time an event caused any damage it is mandatory to adjust the physical system. It is necessary to implement actions to adapt the organization to the new situation and prevent the recurrence of such an event. Those measures could be e.g. the set-up of a new firewall.
Information/ data	Access to Information/data. Violating the data privacy. Damages paid due to loss of customer. Loss of reputation can be significant.	Storing data decentralized.	As Information/data is decentralized parts of the system have to shut down automatically / immediately to protect the whole system.	Regarding the dimension of Information/data risk in case of data loss from smart metering routines have to be in place to create replacement values. The control room must have full redundancy in a remote place.	It has to be analysed data was compromised by the attack. Based on this analysis new routines have to be developed.
Organizational/ business	Business interruption (BI). This BI could be equal to or even exceed financial direct loss from data breach. SWH needs to identify key assets at risk and weaknesses in their organization. Employees can cause large IT security or loss of privacy events, either inadvertently or deliberately.	Measuring the safety culture among employees at SWH (Monitoring policies and procedures for all networks and systems). In addition user education and awareness training	Incident management procedures and network security policies and procedures. The assets have to be known. Based on that list those assets have to be prioritized.	Based on the priority list of assets incident management procedures and network security policies and procedures have to be implemented. The assets have to be known.	The priority list has to be altered. Further training of employees has to be considered.

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
Societal/ political	Creation of a cyber-security culture and adopt a "think-tank" approach to tackling risk. Different stakeholders from the business need to share knowledge.	Implementation of a crisis or breach response plan. Testing of the plan.	Plan to inform the public about the potential dangers and risks.	Inform the public about the potential dangers and risks.	Informing and exchanging opinions based on lessons learned with all relevant stakeholders.
Cognitive/ decision-making	Availability of clear data for decision-making	System to exchange relevant information with top management	Information to the top-management about the incident, number of incidents and their severity for decision-.making	The top-management has to carry out an analysis of all the circumstances and the potential consequences that has caused the initial event. They make a decision to report the event to the insurance company in order to reimburse the damage.	Carry on review of the management and definition of an adjusted action plan.

Colours indicate the level of relevance: High Medium Low

2.2.2 Terrorist Attack

Heidelberg is a tourist attraction. With the increased terrorist activities in Europe, SWH foresees this as a prime threat as in the recent past such destinations became target of terrorist attacks. Such an attack could result in large loss of infrastructure. Hence multi-fold efforts are undertaken by SWH to deal with the challenges in relation to this threat. The main focus for SWH to address the challenges of ensuring that the physical infrastructure is well equipped to deal with any physical terrorist attack on the infrastructure or any cascading effects related to the disruptions in this scenario. Some of the challenges in other dimensions are similar to the cyber-attack such as data security in the information/ data dimension or communication with the external stakeholders in the societal/ political dimension and decision making challenges as these attacks cause disruptions which may have similar consequences/impacts.

These challenges related to the terrorist attack are described in **Error! Reference source not found.**.

System/ physical dimension

Understand risk

- The first dimension system/physical is caused by terrorist attacks on Heidelberg's infrastructure. Heidelberg, being a tourist attraction, has in recent years been susceptible to terrorist attacks. A terrorist attack can result in a huge loss of infrastructure.

Anticipate/prepare

- In order to prevent an attack, the installation of security cameras, electronic keys to substations to allow entry to only some personnel have to be ordered. Under the system/physical dimension, the main focus is on preventive measures.

Absorb/withstand

- Each external attack in the dimension system/physical has to be recognized and monitored by special security surveillance. Object protection in the main building and in substations (bullet proof windows and roof windows, fencing around the building) is a further measure.

Respond/recover

- In case an event escalates further, good communication with the control room is necessary, especially in case of a power supply cut from any of the substations.

Adapt/learn

- Each time an event causes any damage, it is mandatory to adjust the physical system. It is necessary to implement actions to adapt the organization to new situations and prevent the recurrence of such an event. Those measures could for example be to set up a new firewall.

Information/data dimension

Understand risk

- In a cascading effect, the outcome of these attacks could result in the loss of information/data.

Anticipate/prepare

- Security of the important information for SWH is crucial and the impact is reduced by storing data in a decentralized way.

Absorb/withstand

- As information/data is decentralized, parts of the system have to shut down automatically / immediately to protect the whole system.

Respond/recover

- Regarding the dimension of information/data, redundant data values must be present in case of a risk threatening data loss. The control room must have full redundancy in a remote place.

Adapt/learn

- The information/data compromised by the attack has to be analysed and, based on this analysis, new routines have to be developed.

Organizational/business dimension

Understand risk

- An attack normally leads to business interruption (BI). This BI could be equal to or even exceed financial direct loss from the attack itself.

Anticipate/prepare

- Under the dimension of organizational/business, focus is on measuring the safety culture among employees at SWH (Monitoring policies and procedures for all networks and systems). In addition, user education and awareness training has to be offered.

Absorb/withstand

- The dimension organizational/business includes incident management procedures and network security policies and procedures. The assets have to be known and prioritized.

Respond/recover

- Based on the priority list of assets, the organizational/business includes incident management procedures and network security policies and procedures. The assets have to be known.

Adapt/learn

- The priority list of the organizational/business has to be altered. Further training of employees has to be considered.

Societal/political dimension

Understand risk

- From a societal/political perspective, loss of water, heating and gas could escalate into vandalism, as people could try to take advantage of the incident while at the same time feeling insecure and afraid.

Anticipate/prepare

- In terms of societal/political dimension, it is imperative to implement a crisis or breach response plan and test it.

Absorb/withstand

- Under the societal/political dimension, it is crucial to know when to inform the public about the potential dangers and risks. Especially businesses have to have their own protection mechanism and fall back plans. Communication to the city police have to be installed.

Respond/recover

- Under the societal/political dimension, it is crucial to inform the public about the potential dangers and risks. City police have to intervene in case of assaults, violations or infringements.

Adapt/learn

- The societal/political dimension is focused on informing and exchanging opinions based on lessons learned with all relevant stakeholders.

Cognitive/decision-making dimension

Understand risk

- No less important is the dimension cognitive/decision-making. Sound decisions have to be based on clear data. Therefore KPIs' have to be implemented at SWH, which are made available to the decision-makers.

Anticipate/prepare

- It is necessary to have a system in place to exchange relevant information with top management that will help them make the right decision. This will be related to the dimension cognitive decision-making.

Absorb/withstand

- Under the cognitive/decision-making dimension, the police have to get the information when an incident occurs. Hence, communication during the event is crucial.

Respond/recover

- Under the cognitive/decision-making dimension, the top-management has to carry out an analysis of all circumstances and potential consequences that has caused the initial event.

Adapt/learn

- Cognitive/decision-making will carry on review of the management and definition of an adjusted action plan.

Table 4: BRAVO – Terrorist Attack

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
System/ physical	Heidelberg is a tourist attraction. In the recent past those destinations became target of terrorist attacks. Such an attack could result in large loss of infrastructure.	Security of the infrastructure -	Object protection in the main building and in substations	Good communication with the control room in case of cut of power supply from any of the substations.	Initiation of crisis management training program for employees
Information/ data	Due to a physical act information and data could be destroyed or get lost.	Storing data decentralized.	As information/data is decentralized parts of the system have to shut down automatically / immediately to protect the whole system.	Risk in case of data loss from smart metering routines	Analyse compromised data and develop new routines.
Organizational/ business	Business interruption (BI). This BI could be equal to or even exceed financial direct loss from the attack itself.	Measuring the safety culture among employees at SWH	Procedures and network security policies and procedures.	Procedures and network security policies and procedures	The priority list has to be altered. Further training of employees has to be considered.
Societal/ political	Loss of water, heating, gas could escalate in vandalism as people could try to get an advantage out of the incident. People will feel unsecure and will be frightened.	Implementation of a crisis or breach response plan. Testing of the plan.	Communication with key stakeholders and fall back plans	City police have to intervene in case of assaults / violations / infringements	Informing and exchanging opinions based on lessons learned with all relevant stakeholders.
Cognitive/ decision-making	Availability of clear data for decision-making.	System to exchange relevant information with city police	The police needs to get the information that incidents occur.	Analysis of all the circumstances and the potential consequences that has caused the initial event.	Carry on review of the management and definition of an adjusted action plan.

Colours indicate the level of relevance: High Medium Low

2.2.1 Flash flood

Heidelberg is a smart city in south-west Germany that lies on the River Neckar in a steep valley in the Odenwald. When the torrential rain occurs, the main challenge which city has to deal with is how to proceed with downfall without damage for infrastructure or systems crucial to functioning of the city. The core activities to prevent the city against total destruction and disruption of the systems focus mainly on the first two phases - understanding risk and anticipate/prepare. Also, challenges are foreseen in all the dimensions, however, more emphasizes is given to the system/physical, organizational/business and societal/political dimensions. These challenges are summarized in **Error! Reference source not found.**.

System/Physical dimension

In the system/physical dimension, the challenges are to understand the vulnerabilities and weaknesses of the water drainage system improve it and establish an efficient pre-warning system that can minimalize the possible damage caused by flash floods.

Understand risks

- Awareness about city sewer system efficiency will help in understanding the impact of the flood risk.

Anticipate/prepare

- Improvement of water drainage system. Installation of pre-warning systems.

Absorb/withstand

- Adverse event (e.g. flash flood) has to be recognized and monitored by special security surveillance. Interconnections via a meshed system have to be established to provide power to the affected region.

Respond/recover

- In case an event escalated further the system has to be re-established physically. Grid restoration procedures have to be executed.

Adapt/learn

- Each time it is mandatory to adjust the physical system. Continuous adjustment of the old systems with "state of the art" is necessary.

Information dimension

The challenges of the information/data dimension are to avoid loss of data.

Understand risks

- Due to a flash flood information and data could be destroyed or get lost, that's why the procedures about data protection should be established and known

Anticipate/prepare

- To prepare for the challenges of loss of data, data should be stored in decentralized locations.

Absorb/withstand

- As information/data is decentralized parts of the system have to shut down automatically / immediately to protect the whole system

Respond/recover

- Redundancies in case of data loss from smart metering routines have to be in place to create replacement values. The control room must have full redundancy in a remote place.

Organizational/business dimension

The main challenge of the organizational/business dimension is to create a safety culture with implementation of network security policies and procedures. Prioritization within those assets is recommended.

Understand risks

- As a cascading effect a flash flood could leads to BI. This BI could be equal to or even exceed financial direct loss from the flash flood itself.

Anticipate/prepare

- Under the dimension of organizational/business focus is on measuring the safety culture among employees at SWH (Monitoring policies and procedures for all networks and systems). In addition user education and awareness training has to be offered.

Absorb/withstand

- The dimension organizational/business includes incident management procedures and network security policies and procedures. The assets have to be known. Based on that list those assets have to be prioritized

Respond/recover

- Based on the priority list of assets the organizational/business includes incident management procedures and network security policies and procedures. The assets have to be known.

Adapt/learn

- It has to be analysed what information/data was compromised by the flash flood. Based on this analysis new routines have to be developed.

Societal/political dimension

Understand risks

- A flash flood can have cascading effects that could influence the societal/political dimension. Loss of water, heating, gas could result in vandalism as people try to get an advantage out of the incident.

Anticipate/prepare

- It is imperative to implement a crisis or breach response plan and test it.

Absorb/withstand

- It is crucial to know when to inform the public about the potential dangers and risks. Especially businesses have to have their own protection mechanism and fall back plans. Communication to the city police and the fire department has to be established.

Respond/recover

- It is crucial to inform the public about the potential dangers and risks. City police have to intervene in case of assaults / violations / infringements. Fire department and other squads have to support the public.

Adapt/learn

- The main focus is on informing and exchanging opinions based on lessons learned with all relevant stakeholders.

Cognitive/decision-making

Understand risks

- Sound decisions have to be based on clear data. Therefore KPIs have to be implemented at SWH. Those KPIs have to be available to the decision-makers.

Anticipate / Prepare

- It is necessary to have a system in place to exchange relevant information with city police and fire department that will help them to make right decision.

Absorb/withstand

- The police and the fire department have to get the information that incidents occur.

Respond/recover

- The top-management has to carry out an analysis of all the circumstances and the potential consequences that has caused the initial event.

Adapt/learn

- Cognitive/decision-making will carry on review of the management and definition of an adjusted action plan.

Table 5: BRAVO – Flash Flood

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
System/ physical	Heidelberg is crossed by the river Neckar. Understanding the impact of increased rains on Necker and possible flood scenarios	Good city infrastructure. Better water drainage systems. Pre-warning systems	Presence of interconnections via a meshed system to provide power to the affected region.	Grid restoration procedures	Modernization of old systems. Continuous adjustment of the systems with "state of the art" features.
Information/ data	Due to a flash flood information and data could be destroyed or get lost.	Storing data decentralized.	Automatic/ immediate shutdown of parts of the system to protect the whole system	Creation of replacement values for smart metering	It has to be analysed data what was compromised by the flash flood. Based on this analysis new routines have to be developed.
Organizational/ business	Business interruption (BI). This BI could be equal to or even exceed financial direct loss from the flash flood itself	Measuring the safety culture among employees at SWH (Monitoring policies and procedures for all networks and systems). In addition user education and awareness training.	Incident management procedures and network security policies and procedures. The assets have to be known.	Procedures and network security policies and procedures	The priority list has to be altered. Further training of employees
Societal/ political	A flash flood can have a cascading effect. Loss of water, heating, gas could escalate in vandalism as people could try to get an advantage out of the incident	Implementation of a crisis or breach response plan. Testing of the plan	Communication with key stakeholders and fall back plans	City police have to intervene in case of assaults / violations / infringements. Fire department and other squads have to support the public.	Informing and exchanging opinions based on lessons learned with all relevant stakeholders
Cognitive/ decision-making	Availability of clear data for decision-making	System to exchange relevant information with city police and fire department	The police and the fire departments have to get the information that incidents happens	Analysis of all the circumstances and the potential consequences that has caused the initial event enabling top-management decision making.	Carry on review of the management and definition of an adjusted action plan.

Colours indicate the level of relevance:	High	Medium	Low

2.3 CHARLIE

The SmartResilience project assumes that the resilience of the health care system plays a key role in assessing the overall resilience of several different critical infrastructures. In this sense, case study CHARLIE is an "integrative" case study: it is not primarily concerned with a single scenario but with a particular threat that is central to most of the scenarios that are studied in other case studies in the project. This is the threat of a sudden and/or unexpected surge of patients or injured people due to either a mass casualty incident (e.g. water contamination, disasters), or due to an event that renders a substantial fraction of health care provider inoperable (e.g. through an urban flood or solar storm). An Austrian city's health care system is used as a test case. SmartResilience focuses in particular on the possibilities that open up due to an on-going shift towards electronically stored medical claims data and electronic health records in an increasing number of European countries, which enables the development of novel, data-driven ways of assessing the resilience of health care systems. Experts from the technical direction of Europe's largest hospital, as well as experts for a data-driven and evidence-based benchmarking and performance measurement of health care systems evaluated the threats and provided advice.

System/physical

Understand risks

- The physical dimension that is relevant for a resilience assessment of the health care system corresponds to a city-spanning network of different types of health care providers – from hospitals over physicians and medical specialists to pharmacies. In order to provide effective care for patients, multiple of these health care providers need to coordinate themselves in their treatments.

Anticipate / prepare

- In the normal mode of operation this system can be characterized by flows of patients between their homes or work places and through different types of providers. To understand risks for such a system means to understand how such these flows change under the particular scenario. Anticipation and preparation on this dimension means to adjust the densities of certain types of provider in specific regions such that the system has a sufficient capacity to provide for the population even in the case of adverse events.

Absorb / withstand and respond / recover

- In the case of emergency response this requires an effective system for triaging patients and routing them according to their level of urgency through the health care system following the rules implemented in a so-called patient guidance system.

Adapt / learn

- The procedures in this system need to be continuously adapted and adjusted in order to reflect the "lessons-learned" from past events.

Information/data

Understand risks

- For a quantitative and data-driven understanding of risks in a regional health care system, the implementation of a shared, nation-wide system for electronic health records is necessary.

Anticipate / prepare

- This allows to anticipate and to prepare for adverse events through a moment-by-moment quantification of population health and the characterization of the status quo of the utilization of certain types of health care providers. From this it is possible to derive key performance indicators that are informative on where potential vulnerabilities exist in the system.

Absorb / withstand and respond / recover.

- In the case of an event itself, a permanent monitoring of patient flows at the sites of individual health care provider, in particular those involved in emergency response, is key.

Adapt / learn

- These experiences can then be used to refine and update the performance indicator in order to have a "smart" and resilient health care system.

Organizational/business

Understand risks

- On an organizational level, such quantitative approaches to risk analysis need to be complemented by suitable qualitative approaches, in particular scenario analysis.

Anticipate / prepare

- In order to anticipate and prepare it is crucial to formulate a plan of action that clearly assigns roles, competences and also hierarchies to different organizations as well as key staff within these organizations. In case of an event the personnel need to follow the procedures set out in the corresponding plan of action.

Absorb / withstand

- In these plans, response measures are typically implemented through extensive checklists.

Respond / recover and adapt / learn

- Regular training and simulation exercises for the key staff are necessary for an adaptive and in this sense learning system.

Societal/political

Understand

- To ensure an efficient and suitable allocation of resources and investments in relevant infrastructures is fundamental in the societal/political dimension. An important characteristic of the health care system is that a large number of stakeholders are involved on this level (representatives of the inpatient and outpatient sector on a state and federal level, private companies, social security institutions, public and private carrier organizations for hospitals, and so on).

Anticipate / prepare

- In order to understand the risks and prepare plans of action accordingly it is therefore necessary to coordinate all these involved stakeholders.

Absorb / withstand and respond / recover

- In the case of an event and in its wake one of the main priorities for this dimension is to efficiently distribute information to the media, medical staff, but also to relatives.

Adapt / learn

- An adaptation and learning on this level can only be achieved through a redistribution of -mostly public- funds.

Cognitive/decision-making

Understand risks

- The first step in understanding risks is to note that there are crucial differences between the routine mode of operation in the health care system and procedures in the case of adverse events.

Anticipate / prepare

- In anticipating and preparing for such events this means to understand which types of mass casualties or disruptions in the operation of certain types of health care providers are to be expected.

Absorb / withstand

- In the case of an event the first priority is to identify the relevant threats and then follow the checklists and agreed-upon procedures.

Respond / recover and adapt / learn

- Increased adaptability and learning can be achieved through increasing the coordination between different health care provider and stakeholder organizations.

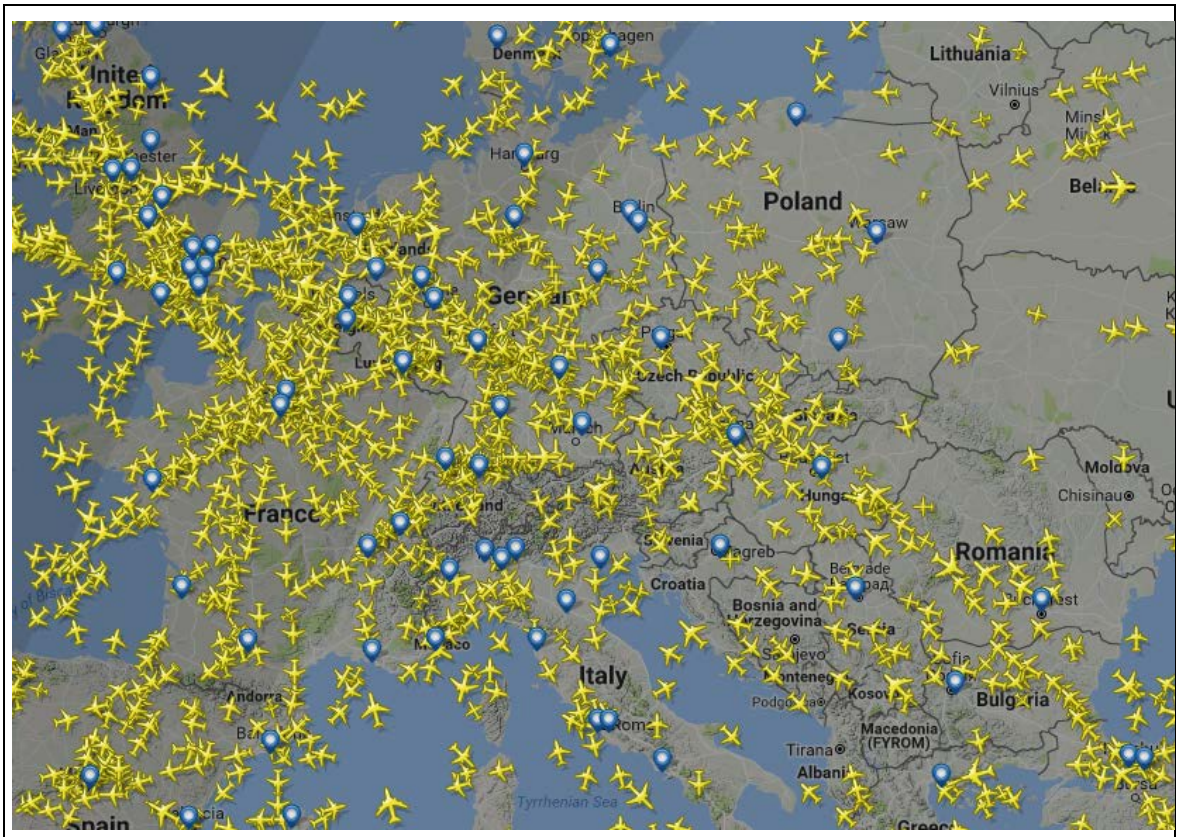
Table 6: CHARLIE

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
System/ physical	Treatment pathways of patients. System given by transport flows of patients between different types of health care providers (physicians, hospitals, pharmacies)	Adjust the density of certain types of provider in a certain region to ensure that needs of the population are met in case of an event.	Triaging of patients to distinguish between different levels of urgency	Care and transport of the patients following the patient guidance system for patients with a given triage level	Review of the management system and adjust plans of action
Information/ data	Implementation of a nation-wide shared system of electronic health records	Moment-by-moment quantification of population health as a function of demographic variables and place of residence	Permanent monitoring of patient flows on HCP level	Permanent monitoring of patient flows on HCP level	Continually update relevant key performance indicator - "smart critical infrastructure"!
Organizational/ business	Quantitative and qualitative risk analysis	Assign roles, competences, and hierarchies to the involved organizations and their key staff	Implementation of a plan of action on the level of individual health care provider (internal events) and on a regional level (external events)	Follow checklists	Regular scenario exercises and training for key staff
Societal/ political	investments in infrastructure, political discussions and negotiation among different stakeholder	Formulate joint plans of actions and provide resources necessary for their execution	Distribute relevant information to media, relatives, and staff	Distribute relevant information to media, relatives, and staff	Redistribute funds and investments
Cognitive/ decision-making	Understand differences between emergency procedures and the routine mode of operation	Anticipation of events that have the potential to either lead to mass casualties or to reduce the number of operational health care provider drastically	Identify relevant threats	Follow checklists and agreed-upon procedures	Increase coordination between different health care provider and other, relevant organizations

Colours indicate the level of relevance: High Medium Low

2.4 DELTA

Air transportation industry has two main pillars, one is the air traffic, and the other is the ground handling of aircrafts. Issues that result in a failure of one pillar seriously impact the other pillar as well. In the following three scenarios, we present permutations of failures: in 3.4.1 air traffic fails, in 3.4.2 both pillars fail, in 3.4.3 ground handling fails. In case of commercial civil aviation, both is heavily relying on airports as base infrastructure, as an airport does not only consist of a passenger terminal, but a complex facility usually housing air traffic control (ATC) of the nearby flight areas, covering ground movement planning and local control (for approaching, landing, taxiing and taking off). At most airports, it is housed in an integrated system placed in a tall building called tower (TWR), ensuring good view on the airport surface and aircrafts within visual range. Some, low traffic airports in remote areas may have remote and virtual towers (RVT) meaning their airspace is controlled from another location, while busier airports have separate control units for air traffic, local control and ground movements. BUD airport, model airport for case study DELTA has separated control units and a medium amount of passengers and aircrafts every year, as detailed in D1.3 [3]. At the current technology level, commercial aircrafts have a limited time of staying in the air therefore the usability of nearby airports (destination airport and diversion airports) is life critical for the passengers aboard. Aviation is a key sector of transportation. Nowadays around 6000 planes are in flight worldwide in every second during daytime.



Early morning commercial air traffic over Europe on 2017.01.17 08:19 as shown of FlightRadar24.com

"By 2034 total passenger numbers are projected to reach 7.3 billion, more than double the 3.3 billion passengers expected to take to the air this year. Recently McKinsey estimated the investment in airports required to support GDP growth will need to be some $2 trillion by 2030. Aviation already has a significant economic footprint. Alone, airline revenues of some $750 billion account for about 1% of global GDP. When combined with aviation-related tourism, aviation accounts for 58 million jobs globally and some $2.4 trillion of economic activity (3.4% of global GDP).Allowing fast and safe travel between cities in considerable distance from each other, in almost every weather condition, airplanes are playing a crucial role in mobility, economy and also in resilience. […] However, airports are very vulnerable critical infrastructures; their huge capacity

can be crippled easily, although by this time there is a considerable program run by IATA to upgrade airports into Smart Airports, focused on response capability out of resilience." states the Smart Resilience proposal.

In case of airport as Smart Critical Infrastructures, the biggest threat is the complete halt of systems or exceeding capacity resulting from a large scale, unexpected event radically changing traffic for a given period. More than a decade before we could handle such situations by reverting to manual controls, but nowadays the number of passengers and planes are so high that most of the airport are not able to keep up their standard level of operation when their smart systems fail.

According to running development projects, strategic foresights, like the Airport 4.0 concept (see End-user needs and requirements in D1.3) and reports (ENISA report on Securing Smart Airports, December 2016), number of cyber-threats on airport IT systems, including conventional "grey" and "smart" systems, are increasing. At this time, failure of services due to loss of power and/or connections is the most frequent kind of SCI incident, but for the future, we expect more refined cyber -attacks, we expect malware, ransomware, and information theft and payment fraud against airport systems. However, it has to be pointed out that our priority is the aviation safety and security, therefore cybercrimes committed against individuals or group of individuals (passengers) resulting in damage of their property (including information) is second to saving lives.

Three experts were participating in completing section DELTA, with 15-30 years of experience in airport operations. One expert has been responsible for aviation security for more than 10 years, leading the national competent unit for supervising aviation security at all Hungarian civilian airports. The other expert has been the lead security expert of the airport operator company for more than 20 years, before he was first responder at the airport. The third expert has first responder and first line command experience of 10 years. Each of the experts had already been in charge of solving airport crises, including ones threatening life of passengers and heavily impacting facility operations and European air traffic. All of them were distinguished at least once for merit in service. Two of them are active sworn senior officers of the Airport Police Directorate; the third is a retired senior officer now working as lead security expert for the airport operator company.

2.4.1 Blocked Traffic

On the 7th of December, 2012, TWR systems, including reserve systems, halted due to an electricity fault. This rendered BUD airport unable to control arriving and departing air traffic. NOTAM was issued, all airmen were instructed on ETOPS to use diversion airports. All other systems, including passenger terminals stayed operational, but passengers were stuck at the airport as planes on airport ground were not allowed to launch and inflight aircrafts were not allowed to attempt landing.

<u>System/physical dimension</u>

Understand risks - Critical dependencies

- However the airport has redundant systems, environmental or other effects can render critical system elements inoperable, forcing the airport to stop, especially in case of *vis major*. Dependency of system elements should be considered during risk assessment.

Anticipate/prepare - Systems durability

- Systems shall be robust and redundant by design, having warm and cold reserves, spare parts and repair toolkits, if these are not available, system failures can hit the infrastructure at any time.

Absorb/withstand – Physical resistance

- A shutdown in local power grid leaves vital systems without power, rendering smart systems into "smart bricks"; the facility has to be able to localize the failure minimizing area of effect then restore power in as many zones as possible.

Respond/recover – Repairing

- Inability to swiftly repair utilities damaged, change broken parts delays re-establishment of operation.

Adapt/learn – Re-evaluation of design

- Check performance of current design during the incident and determine if water systems need to be re-designed, otherwise an incident arising from design error will reappear from time to time.

Information/data dimension

Understand risks - Insufficient foresight

- Insufficient data gathered and analysed of previous incidents of the same kind hinders effective risk assessment.

Anticipate/prepare - Emergency communication channels

- When there are no communication channels reserved for emergency communication and early warning, everyday business communication and emergency communication will mix and disturb each other.

Absorb/withstand – NOTAM

- In a case of disaster or danger, Notice to Airmen (NOTAM) has to be disseminated immediately to inform all aviation participants on the situation to absorb effects. It can also be understood as capability for prevention of escalation.

Respond/recover – Incident tracking

- Gathering and assessing maintenance and incident information, including system logs, repair logs, checklists, replacement compatibility standards to determine repair and maintenance needs and set priority order only in digital format may cripple repair operations when the digital system itself lost power or fail on another reason.

Adapt/learn – Reporting

- Investigate incident, assess lessons learned and update relevant data analysis methods, extend communication channels etc. Effective reporting procedure on outcome of the investigation with recommendations on resilience development is needed as otherwise the lessons will not be learned.

Organization/business dimension

Understand risks - Staff training

- Lack of proper training in risk awareness and use of foresight systems prevents achieving high resilience, increases the chance of panicking and bad decisions as well as insufficient human resources available at critical moments.

Anticipate/prepare - Emergency Planning and BCP

- If there are no Emergency Procedures and Business Continuity Plans (BCPs) covering the case of blocked traffic, a lot of time will be lost on making self-understanding decisions, slowing down overall reaction time (affecting absorption and response capacity).

Absorb/withstand – Operational endurance

- Management shall be able to immediately determine current operational level by assessing business critical procedures remaining operational to minimize damage.

Respond/recover – Restoration

- Missing or outdated BCP with parts on how to raise back to standard operational level by restoring business critical procedures step-by-step delays reaching standard business operation level, which is a critical indicator for resilience

Adapt/learn – Re-training and quality control

- Quality control airport facilities to achieve better resilience for similar cases. Without this, cascade or ripple effects may follow. Update and develop training covering new modus operandi as necessary.

Societal/political dimension

Understand risks - Communication plans

- Missing or outdated communication plans covering risks can misinform the wider society, resulting in negligent or unaware behaviour leading to incidents.

Anticipate/prepare - Premade infopacks and manuals

- If there are no clear, pre-written information packages and manuals for staff at home, affected passengers and mass media, important information may not reach target groups or become distorted.

Absorb/withstand – Alerting

- Failing to release communication through mass media as well as on individual basis based on Advanced Passenger Information (API) where available to inform passengers affected may result in more people arriving to the airport, hardening the situation even more.

Respond/recover – Flow of information

- Failing in keeping passengers well informed to avoid stress or panic on the passenger terminals results in endangered, angry and discomforted passengers, having enduring negative impact on business results. Immediately communicate restoration of operational level.

Adapt/learn - Feedback gathering

- Gather feedback on reaction on societal and political level, to initiate additional measures to achieve better resilience.

Cognitive/decision making

Understand risks – Bloated bureaucracy

- Too high or too low number and unclear area of responsibility of manager posts create erratic decisions due to overload against time pressure or creates a bloated, top-heavy bureaucracy in risk management, which will not make decisions and always try to push responsibility away to other, overlapping areas of responsibility, resulting in bad quality of risk assessment.

Anticipate/prepare - Chain of Command

- Lack of clear tasks, responsibilities and reporting system set in documents ensure optimal performance for the entire staff creates “islands of resistance” with natural leaders stepping forward, lowering effectiveness of response.

Absorb/withstand – Forward line command

- It is critical to have competent managers on duty to the spot, initiate pre-defined commands in the Emergency plan, competence based decision in case of aspects not covered by plan.

Respond/recover – Control Center

- Managers on duty and selected managers gather in the Crisis Control Center (CCC) to facilitate quick and effective cooperation and decision making. Lack of such temporary organization burdens already endangered communication (especially when power systems fail, there will be no radio or cell phones at all or for not long) and delays vital decisions.

Adapt/learn - Decision tree upgrading

- Update tasks, responsibilities, revise competences and internal training system for managers.

Table 7: DELTA – Blocked traffic

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
System/ physical	Critical dependencies	System durability	Physical resistance	Repairing	Re-evaluation of design
Information/ data	Foresight	Emergency communication channels	NOTAM	Incident tracking	Reporting
Organizational/ business	Staff training	Emergency Planning and BCP	Operational endurance	Restoration	Re-training and quality control
Societal/ political	Communication plans	Premade infopacks and manuals	Alerting	Flow of information	Feedback gathering
Cognitive/ decision-making	Bloated, top-heavy bureaucracy	Chain of Command	Forward line command	Control Center	Decision tree upgrading

Colours indicate the level of relevance: High Medium Low

2.4.2 Passenger and airplane traffic exceeding capacity

On the 3rd of February, 2012, a national airline with spreading role between Europe, Asia and Africa suddenly ceased operation without previous warning, due to bankruptcy. Transfer and departing passengers got stuck on the terminal, as operating flight companies were unable to re-book and board everyone. About 3600 extra-Schengen passengers were stranded in the transit area, most of them visa-obliged TCN without a valid visa to enter the Schengen Area.

Explanation for indicators used in passenger and airplane traffic exceeding capacity

System/physical dimension

Understand risks - Capacity awareness

- Lack of pre-assessment of passenger capacity of terminal passenger lounge services (restrooms, benches, food shops etc.) renders to sudden overload of terminal. Even when there are no incidents, it takes years to extend those facilities.

Anticipate/prepare - Spare capacity

- Airport systems and infrastructure has to be designed to be capable of temporary handling passenger overflow.

Absorb/withstand – Flexibility

- Search for facility areas usually closed from passengers but capable of operating temporarily as passenger terminal or lounge.

Respond/recover – Extension

- Temporary extension of capacity by using other facilities as terminal or lounge.

Adapt/learn – Re-evaluation of design

- Check performance of current design during the incident and determine if terminal and smart passenger handling systems need to be re-designed.

Information/data dimension

Understand risks - Monitoring capacity

- Not following terminal and air traffic capacity based on digital and IRL check-in desk throughput plus arriving transit passenger estimation, leading to late detection of terminal overload.

Anticipate/prepare - Emergency communication channels

- When there are no communication channels reserved for emergency communication and early warning, everyday business communication and emergency communication will mix and disturb each other.

Absorb/withstand – Information Exchange

- Continuous information flow among involved entities (airlines, ground handling, airport operator, authorities) to solve the overflow as soon as possible.

Respond/recover – Incident tracking

- Gather data on affected passengers and destinations. Setting up priorities for vulnerable passenger categories.

Adapt/learn – Reporting

- Investigate incident, assess lessons learned and update relevant data analysis methods, extend communication channels etc. Effective reporting procedure on outcome of the investigation with recommendations on resilience development is needed as otherwise the lessons will not be learned.

Organization/business dimension

Understand risks - Staff training

- Improper staff training for handling passenger overflow, failures in emotional sensitivity, clear communication and calming nervous passengers may lead to risk of unwanted and unnecessary consequences or even more incidents.

Anticipate/prepare - Emergency Planning and BCP – Emergency Planning and BCP

- If there are no Emergency Procedures and Business Continuity Plans (BCPs) covering the case, a lot of time will be lost on making self-understanding decisions, slowing down overall reaction time (affecting absorption and response capacity).

Absorb/withstand – Transport modalities

- Establish ground transfer connection with other airports in the region, to hand over passengers via bus transfer. Attempt booking transfers to free capacities of operating airlines. Accommodate passengers in nearby hotels.

Respond/recover – Restoration

- Assume possibilities to rebalance passenger load among airlines, to achieve capacity through optimization and booking transfer.

Adapt/learn – Re-planning

- Expand capacity by adopting new passenger handling solutions. Update business continuity plans and market research to better forecast.

Societal/political dimension

Understand risks - Communication plans

- Missing or outdated communication plans covering risks can misinform the wider society, resulting in negligent or unaware behaviour leading to incidents.

Anticipate/prepare - Premade infopacks and manuals

- If there are no clear, pre-written information packages and manuals for staff at home, affected passengers and mass media, important information may not reach target groups or become distorted.

Absorb/withstand – Alerting

- Failing to release communication through mass media as well as on individual basis based on Advanced Passenger Information (API) where available to inform passengers affected may result in more people arriving to the airport, hardening the situation even more.

Respond/recover – Flow of information

- Failing in keeping passengers well informed to avoid stress or panic on the passenger terminals results in endangered, angry and discomforted passengers, having enduring negative impact on business results. Immediately communicate restoration of operational level.

Adapt/learn - Feedback gathering

- Gather feedback on reaction on societal and political level, to initiate additional measures to achieve better resilience.

Cognitive/decision making

Understand risks – Bloated bureaucracy

- Too high or too low number and unclear area of responsibility of manager posts create erratic decisions due to overload against time pressure or creates a bloated, top-heavy bureaucracy in risk management, which will not make decisions and always try to push responsibility away to other, overlapping areas of responsibility, resulting in bad quality of risk assessment.

Anticipate/prepare - Chain of Command

- Lack of clear tasks, responsibilities and reporting system set in documents ensure optimal performance for the entire staff creates “islands of resistance” with natural leaders stepping forward, lowering effectiveness of response.

Absorb/withstand – Forward line command

- It is critical to have competent managers on duty to the spot, initiate pre-defined commands in the Emergency plan, competence based decision in case of aspects not covered by plan.

Respond/recover – Control Center

- Managers on duty and selected managers gather in the Crisis Control Center (CCC) to facilitate quick and effective cooperation and decision making. Lack of such temporary organization burdens already endangered communication (especially when power systems fail, there will be no radio or cell phones at all or for not long) and delays vital decisions.

Adapt/learn - Decision tree upgrading

- Update tasks, responsibilities, revise competences and internal training system for managers.

Table 8: DELTA – Exceeding capacity

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
System/ physical	Capacity awareness	Spare capacity	Flexibility	Extension	Re-evaluation of design
Information/ data	Monitoring capacity	Emergency communication channels	Information Exchange	Incident tracking	Reporting
Organizational/ business	Staff training	Emergency planning and BCP	Transport modalities	Restoration	Re-planning
Societal/ political	Communication plans	Premade infopacks and manuals	Alerting	Flow of information	Feedback gathering
Cognitive/ decision-making	Bloated, top-heavy bureaucracy	Chain of Command	Forward line command	Control Center	Decision tree upgrading

Colours indicate the level of relevance: High Medium Low

2.4.3 DELTA – GOLF

On the 23rd of July, 2006, a hurricane hit BUD with 23.6 mm rain in 1.5 hours, causing pluvial flood hitting RWY1 on BUD airport. About 1.5 meter deep ponds emerged and the water found way to the high-voltage electrical system, forcing a shutdown. Due to the strong wind and rain, passengers could not be evacuated easily but protected on the spot until bus transport could be arranged.

System/physical dimension

Understand risks - Considering *vis major* in risk assessment

- Although the airport has redundant systems, flood can render critical system elements inoperable, forcing the airport to stop, therefore it is important to cover this area in risk assessment.

Anticipate/prepare - Systems durability

- Systems shall be robust and redundant by design, having warm and cold reserves, spare parts and repair toolkits, if these are not available, system failures can hit the infrastructure at any time.

Absorb/withstand – Physical resistance

- Try to remove as much water as possible, protect RWY, APRON, TWY and passenger terminal buildings with sandbags to absorb flood impact.

Respond/recover – Repairing

- Remove water, repair utilities damaged, change broken parts, and re-establish operation.

Adapt/learn – Re-evaluation of design

- Check performance of current design during the incident and determine if water systems need to be re-designed.

Information/data dimension

Understand risks - Monitoring early warning systems

- Monitoring weather forecasts and other disaster early warning systems can greatly help to understand risks arising.

Anticipate/prepare - Emergency communication channels

- When there are no communication channels reserved for emergency communication and early warning, everyday business communication and emergency communication will mix and disturb each other.

Absorb/withstand – NOTAM

- In a case of disaster or danger, Notice to Airmen (NOTAM) has to be disseminated immediately to inform all aviation participants on the situation to absorb effects. It can also be understood as capability for prevention of escalation.

Respond/recover – Incident tracking

- Gathering and assessing maintenance and incident information, including system logs, repair logs, checklists, replacement compatibility standards to determine repair and maintenance needs and set priority order only in digital format may cripple repair operations when the digital system itself lost power or fail on another reason.

Adapt/learn – Reporting

- Investigate incident, assess lessons learned and update relevant data analysis methods, extend communication channels etc. Effective reporting procedure on outcome of the investigation with recommendations on resilience development is needed as otherwise the lessons will not be learned.

Organization/business dimension

Understand risks - Staff training

- Lack of proper training in risk awareness and use of foresight systems prevents achieving high resilience, increases the chance of panicking and bad decisions as well as insufficient human resources available at critical moments.

Anticipate/prepare - Emergency Planning and BCP

- Emergency Procedures and Business Continuity Plans (BCPs) for airport operators, airlines and authorities shall cover the case of flood (flood protection and evacuation).

Absorb/withstand – Operational endurance

- Management shall be able to immediately determine current operational level by assessing business critical procedures remaining operational to minimize damage.

Respond/recover – Restoration

- Missing or outdated BCP with parts on how to raise back to standard operational level by restoring business critical procedures step-by-step delays reaching standard business operation level, which is a critical indicator for resilience

Adapt/learn – Re-training and quality control

- Quality control airport facilities to achieve better resilience for similar cases. Without this, cascade or ripple effects may follow. Update and develop training covering new modus operandi as necessary.

Societal/political dimension

Understand risks - Communication plans

- Missing or outdated communication plans covering risks can misinform the wider society, resulting in negligent or unaware behaviour leading to incidents.

Anticipate/prepare - Premade infopacks and manuals

- If there are no clear, pre-written information packages and manuals for staff at home, affected passengers and mass media, important information may not reach target groups or become distorted.

Absorb/withstand – Alerting

- Failing to release communication through mass media as well as on individual basis based on Advanced Passenger Information (API) where available to inform passengers affected may result in more people arriving to the airport, hardening the situation even more.

Respond/recover – Flow of information

- Failing in keeping passengers well informed to avoid stress or panic on the passenger terminals results in endangered, angry and discomforted passengers, having enduring negative impact on business results. Immediately communicate restoration of operational level.

Adapt/learn - Feedback gathering

- Gather feedback on reaction on societal and political level, to initiate additional measures to achieve better resilience.

Cognitive/decision making

Understand risks – Bloated Bureaucracy

- Too high or too low number and unclear area of responsibility of manager posts create erratic decisions due to overload against time pressure or creates a bloated, top-heavy bureaucracy in risk management, which will not make decisions and always try to push responsibility away to other, overlapping areas of responsibility, resulting in bad quality of risk assessment.

Anticipate/prepare - Chain of Command

- Lack of clear tasks, responsibilities and reporting system set in documents ensure optimal performance for the entire staff creates “islands of resistance” with natural leaders stepping forward, lowering effectiveness of response.

Absorb/withstand – Forward line command

- It is critical to have competent managers on duty to the spot, initiate pre-defined commands in the Emergency plan, competence based decision in case of aspects not covered by plan.

Respond/recover – Control Center

- Managers on duty and selected managers gather in the Crisis Control Center (CCC) to facilitate quick and effective cooperation and decision making. Lack of such temporary organization burdens already endangered communication (especially when power systems fail, there will be no radio or cell phones at all or for not long) and delays vital decisions.

Adapt/learn - Decision tree upgrading

- Update tasks, responsibilities, revise competences and internal training system for managers.

Table 9: DELTA – GOLF

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
System/ physical	Considering vis major in risk assessment	System durability	Physical resistance	Repairing	Re-evaluation of design
Information/ data	Monitoring early warning systems	Emergency communication channels	NOTAM	Incident tracking	Reporting
Organizational/ business	Training staff in risk awareness	Emergency Planning and BCP	Operational endurance	Restoration	Re-training and quality control
Societal/ political	Communication plan	Premade infopacks and manuals	Alerting	Flow of information	Feedback gathering
Cognitive/ decision-making	Bloated, top-heavy bureaucracy	Chain of Command	Forward line command	Control Center	Decision tree upgrade

Colours indicate the level of relevance: High Medium Low

2.5 ECHO

The NIS Pancevo Oil Refinery is located in the immediate vicinity to the city of Pancevo. According to the official census of the year 2011, the city of Pancevo has 123,414 inhabitants. City of Pancevo is located 20 km away from Belgrade, the capital of Serbia. Due to this fact, the refinery pays great attention to its operational risks and to implement corrective / preventive measures in order to prevent undesirable events that can potentially have serious consequences for the functioning of the Pancevo city. The threat analysed in this case study is a boiling liquid expanding vapour explosion (BLEVE) in a spherical storage tank installation.

Many efforts are aimed at reducing the technological risks considering the nature of refinery activities. Resilience is not just assured by the behaviour of people but also by the consistent application of processes and procedures as well as the functionality of safety critical equipment. Presented in Table 10 and described in the text below are assessed the phases within each of the dimensions:

System/Physical dimension

The challenges of the System/Physical dimension are to identify hazards, primarily related to process safety considering the nature of the technological process with presence of hydrocarbons.

Understand risks

- Periodically carry out risk assessment at the technological units and primarily containments.
- Update risk registry related primarily to process safety.

Anticipate/prepare

- Timely planning of periodic preventive inspection of the fire alarm system, a system for the detection of flammable vapours and gases and the cooling system, hydro test of pressure vessels, testing of safety equipment, valves, etc.

Absorb/withstand

- Major role in absorbing the event have process alarm and ESD (Emergency shutdown) activation and for exceeding certain parameters in the process (pressure, temperature, flow, level of fluid), activation of the fire alarm system (calibrated to less temperature).

Respond/recover

- Operatively mobilize and activate a preparedness and response team, interventions of fire brigades, stop key processes by the operator of the plant, the rehabilitation plan, and the evacuation of all employees to a safe place.

Adapt/learn

- Develop a rehabilitation plan and form a commission to investigate the event.

Information dimension

The challenges of the information/data dimension are to provide unique database with relevant and updated information that will be available to operators in any required moment

Understand risks

- Ensure the collection of relevant information for getting the key indicators of reliability of the equipment (e.g. number of Hi-Hi level alarm activated, activation of safety equipment, unplanned shutdowns, required replacement/reparation of LOPC equipment caused as results of testing/inspection, exceeding of safe operating limits etc.).

Anticipate/prepare

- Conduct periodic analysis of performance indicators (weekly, monthly, quarterly and annually), an analysis of all alarms and process deviations, such as pressure, temperature and flow rate that

arrived in the control room, the analysis of the implemented measures imposed both by state inspection and by internal audits carried out by the refinery.

Absorb/withstand

- Timely warn process engineer about potential critical information crucial for further moves. Risk can imagine situations that limit values of process indicators are not adequately adjusted or personnel did not noticed oncoming warning about safe operating limits. This entails carrying out checks, tests and subsequent modification of thresholds.

Respond/recover

- Gather key information emerged about the consequences and preparing information for the public.

Adapt/learn

- Analyse the findings, defining actions, implementing measures, and monitoring their effectiveness.

Organizational/business dimension

The challenges of the organizational/business dimension are to develop the ability to actively learn from its own mistakes, which is fundamental to maturing the culture.

Understand risks

- Regroup of organization units or forming new ones in order to meet the requirements on safe and reliable run of production plants,
- Engagement of consultants to conduct independent audit.

Anticipate/prepare

- Measure the safety culture among employees at the plants.

Absorb/withstand

- Timely engagement of specialized service companies to perform non-standard operations (Formanite method, hot tapping, and remediation of spills) may affect the future course of event.

Respond/recover

- Define a new or redefining existing responsibilities and their allocation to relevant work positions.

Adapt/learn

- Develop ability to actively learn from its own mistakes is fundamental in maturing the culture.

Societal/political dimension

The challenges of the societal/political dimension are to demonstrate commitments and readiness to act proactively in order to prevent major chemical accident.

Understand risks

- Establish communication with all operators in the immediate vicinity of Seveso establishment.

Anticipate/prepare

- Organize joint exercises with neighbouring operators,
- Periodically inform the public about the potential dangers and risks.

Absorb/withstand

- Adequately maintain audio means for alerting the dangers and means for communication with the neighbouring operators. All these means, in the event of emergency will mitigate the consequences by timely alerting and evacuation of people.

Respond/recover

- Notify the public through the media and other communication means.

Adapt/learn

- Inform and exchange of experiences based on lessons learned with state authorities and other relevant stakeholders.

Cognitive/decision-making dimension

It is incumbent on NIS that they actively manage and where possible eliminate the most significant risks within their business. It is crucial that those who plan and manage activities understand the importance of maintenance, inspection, verification and testing on the continued integrity of assets. Also they need to understand cumulative risk and the use of barrier management thinking and operational application in defending high hazard activities.

Understand risks

- Company executives make a decision on restart or shut down of the plant.

Anticipate/prepare

- Exchange relevant information on the regular basis with the top management that will help them to make right decision.

Absorb/withstand

- Conduct an analysis of all circumstances and potential consequences that could cause the initial event.

Respond/recover

- Consider a damage made by an accident, required funds for recovery and potential.

Adapt/learn

- Review of the management system and defining actions for improvements.

Table 10: ECHO

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
System/ physical	Periodically carry out risk assessment and when it is necessary update risk registry	Conduct periodic preventive inspections (fire alarm system, system for the detection of combustible gases and vapours, cooling system, hydro test, inspection of pressure vessels, testing of safety equipment (valves, etc.), periodic testing of DCS (distributed control system)	ESD activation, activation of the alarm for the process parameters (pressure, temperature, flow, level of fluid), activation of the gas alarm	Mobilize and activate team for preparedness and response to extraordinary events, the intervention of fire brigades, stop key processes by the operator of the plant, the rehabilitation plan, the evacuation of all employees in a safe place	Develop a rehabilitation plan, form a commission to investigate the event
Information/ data	Key indicators of process safety and reliability of equipment	Periodic analysis of the key indicators, analysis of all alarms that arrived in the control room and other process deviations (pressure, temperature flow rate)	Defined threshold values of key performance indicators	Collect key information emerged about the consequences and preparing information for the public	Analyse the findings, defining actions and implementation measures and monitoring their effectiveness
Organizational/ business	Regroup of organization units or forming new ones and engagement of consultants to conduct independent audit	Measure the safety culture among employees at the plant, audits and safety visits	Engage specialized service companies to perform non-standard operations (Formanite, hot-tapping, spill remediation)	Define new or redefine existing responsibilities and their allocation to relevant work positions	Develop ability to actively learn from its own mistakes
Societal/ political	Establish communication with all operators in the immediate vicinity of Seveso establishment	Organize joint exercises, inform the public about the potential dangers and risks	Maintain audio means for alerting the dangers and means for communication with the neighbouring operators	Notify the public through the media	Exchange information and experiences of lessons learned with state authority and other relevant stakeholders
Cognitive/ decision-making	Company executives make decisions regarding the functioning of the plant to start up or shut down	Regularly share all relevant information with the top management	Conduct an analysis of all circumstances and a potential consequences that could cause the initial event	Consider the damage made by accident, required funds for recovery and potential impact on the company's reputation caused by accident	Review of the management system and defining actions for improvements

Colours indicate the level of relevance:	High	Medium	Low

2.6 FOXTROT

The FOXTROT case focused on the threats cyber-attack, outbreak of waterborne disease cause by microbial contamination and water shortage. Cyber-attack is linked to the vast digitalization of industrial processes, including drinking water production, causing new challenges for the producers to prevent vulnerabilities in the systems. Waterborne disease and water shortage are both linked to climate change and are predicted to be more frequent in the future as described in each threat description.

To help us describe these threats we have been in contact with the subject experts from the National Food Agency of Sweden, the Swedish Water & Wastewater Association, the Swedish Civil Contingencies Agency and Chalmers University.

2.6.1 Cyber-attack

All industrial production sites today are using ICT systems to enhance production performance, reliability and robustness, and while ICT-systems can contribute to immense advantages in product quality and profit, it could also pose a threat to the production process due to failure in the ICT-systems. This could be caused by cyber-attacks. In the past many cyber-attacks focused on weaknesses in the ICT infrastructure, getting through firewalls etc., whereas today the use of malicious code such as worms, viruses and Trojans has grown increasingly common.

When a cyber-attack targets a control system of a critical infrastructure such as a drinking water production facility, the effects of the attack are leaving the cyber realm and entering the physical world with the potential to cause physical damage and casualties. A successful attack would pose a threat to the process equipment as well as human well-being. Imagine for instance an attack on a traffic signal control system where an attack would suddenly change the light to green from all directions that could cause a serious traffic accident. In water production, if an attacker would disable the chemical precipitation of the process while telling the operators that the process is running normal with the effects of thousands of people getting bad drinking water. The most famous example of this kind of attack is Stuxnet, which was discovered in 2010, and targeted specific PLCs (Programmable Logic Controller) made by Siemens. Since Stuxnet, there has been a number of malicious software, such as Duqu and Flame, acting in a similar manner to attack industrial control systems.

The most common protective action is to create an *Air gap*, which essentially is to ensure that there is no communication between the control system network and the outside world, i.e. no wired or wireless connections allowed. However, there are always bridges over an air gap such as computer and equipment upgrades and log files extraction, through which malicious software may infect the system.

There are many challenges when dealing with the ICT-security threats such as a cyber-attack. Much of the work focusses on preventing incidents to occur and is therefore located in the early phases of the resilience matrix. When considering the dimensions, challenges in the system/physical and the organizational/business dimensions are dominating. The challenges described in the following are summarized in Table 11.

<u>System/Physical dimension</u>

In the system/physical dimension the challenges are to understand the vulnerabilities and weaknesses of the ICS (Industrial Information and Control System), and to construct a secure system architecture, which prevents intrusions and minimizes the possible damage caused by an attack.

Understand risks

- *Regularly scan the system to identify weaknesses and map administrative IT-architecture and ICS*: Additions and alteration of the ICS and surrounding systems are continually made at a production site. It is important to have an updated overview of the system. Special attention should be paid to external connections to the ICS.

- *Regular evaluation of the physical protection of the ICS*: It is not only the virtual security that needs to be considered also the physical protection needs to be addressed.

Anticipate/prepare

- *Include security requirements in equipment and system purchase process*: Having well established requirements of ICT-security when purchasing new or additions to the production system is important to maintain a secure system.
- *Perform regular technical security evaluation of the ICS*: A secure system needs to be up to date with new threats that arise. There are no systems that will remain secure forever.

Absorb/withstand

- *Create "Air-gap" between administrative IT-systems and the ICS*: This is essential in ICS security. Keeping external connections to a minimum effectively decreases the risks by simply minimizing the possible access point.
- *Divide control system in zones*: Control system zones with implemented depth defence minimize the exposed equipment by not making it possible to access further equipment within the site. We want to prevent an intruder to able to move from one part of the site to another by removing interconnections between the zones.

Respond/recover

- *Establish system back-ups and recovery plans*: When the system fails we need to have available back-ups to quickly get up and running again.

Adapt/learn

- *Strengthen and upgrade the ICS security*: This should be performed in cooperation with system distributers.

Information dimension

The challenges of the information/data dimension are to secure data storage and detect attacks.

Anticipate/prepare

- *Implement monitoring and detection of intrusion attempts*: We need to have an understanding of where most attacks are made and how to minimize the vulnerability.
- *Regularly inspect that only secure connection to the ICS exists*: Less connections means less access points for possible intrusion.

Respond/recover

- *Create redundant data storage*: In order not to lose data at a system failure it is important to have redundant and mirrored data storage.

Organizational/business dimension

The main challenge of the organizational/business dimension is to create a culture where IT-security issues are taken seriously and that the principles of IT-security stated in the Information Safety Management System imbibes the day-to-day business. It is also a challenge to understand and prevent the business related risks caused by attacks on the ICS as well as on the administrative systems.

Understand risks

- *Secure management engagement*: Management needs take responsibility for security of the ICS and administrative systems.
- *Understand the business risks*: Management needs to understand the risks and maintain processes for system mapping and risk management of ICS.

Anticipate/prepare

- *Assign responsibilities*: There is a need to assign persons responsible for ICS security and to implement an Information Security Management System (ISMS) (ISO 27001 and ISO 27002).

Absorb/withstand

- *Continuity planning*: It is important to perform systematic continuity planning and incident handling in ICS.

Respond/recover

- *Establish response capabilities*: Quick responses to intrusions are important to minimize the damage cause during the attack.

Adapt/learn

- *Upgrades and installations*: Perform systematic consequence analysis of changes, upgrades and new installations in the industrial information and control system and stay up to date on ICS incidents and monitor security issues in world.

Societal/political dimension

In the societal/political dimension, the challenge is mainly to stay up-date with development within the field and take part of the preventive work performed in different communities. Regulations have been passed on the political level to force organizations to assess their vulnerabilities.

Understand risks

- *Regulations*: There are regulations forcing the producers to perform risk assessment focused on IT-security.

Anticipate/prepare

- *Guidelines*: The Swedish Civil Contingencies Agency has developed guidelines to handle cyber security and secure industrial production systems.

Adapt/learn

- Cooperation: Communities, networks and standardization organizations concerning security in ICS are play an important role in today and future cyber security.

Cognitive/decision-making dimension

In the cognitive dimension, the challenge is to educate and raise awareness of the issues and the possible consequences of cyber-attacks and risks involved with inadequate IT-security.

Understand risks

- *Increase awareness*: Work is being made to increase the awareness of security importance in industrial information and control systems.

Anticipate/prepare

- *Education*: Education, exercises and stress tests has been in IT-security in ICS in many places including drinking water production sites.

Respond/recover

- *Education*: Practices in IT-incident management and response capabilities are important to prepare for cyber-attacks.

Table 11: FOXTROT – Cyber attack

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
System/ physical	• Regularly scan the system to identify weaknesses and map administrative IT-architecture and ICS. Special attention should be paid to external connections to the ICS. • Regular evaluation of the physical protection of the ICS.	• Include security requirements in equipment and system purchase process. • Perform regular technical security evaluation of the ICS.	• Create "Air-gap" between administrative IT-systems and the ICS. Keep external connections to a minimum. • Divide control system in zones with implemented depth defence in order to minimize exposed equipment.	• Establish system back-ups and recovery plans.	• Strengthen and upgrade the ICS security in cooperation with system distributers.
Information/ data		• Implement monitoring and detection of intrusion attempts. • Regularly inspect that only secure connection to the ICS exists.		• Create redundant data storage	* Evaluate data availability and quality and adequacy
Organizational/ business	• Understand the business risks and maintain processes for system mapping and risk management of ICS.	• Assign responsible persons for ICS security. • Implement an Information Security Management System (ISMS) (ISO 27001 and ISO 27002. • Secure management engagement and responsibility for security of the ICS and administrative systems.	• Perform systematic continuity planning and incident handling in ICS.	• Establish response capabilities	• Perform systematic consequence analysis of changes, upgrades and new installations in the industrial information and control system. • Stay up to date on ICS incidents and monitor security issues in world. * Evaluate business plans and recover systems
Societal/ political	• Regulations demanding risk assessment	• Development of guidelines to handle cyber security			• Cooperate in communities, networks and standardization organizations concerning security in ICS.

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
Cognitive/ decision-making	• Increase awareness of security importance in industrial information and control systems	• Perform education and exercises in IT-security in ICS.		• Practice IT-incident management and response capabilities.	* Evaluate awareness level, exercises etc.

Colours indicate the level of relevance: High Medium Low

2.6.2 Outbreak of waterborne disease

A serious future threat to drinking water supply is outbreak of diseases due to drinking water being contaminated with pathogens. Heavy rain and flooding can cause sewage systems to release untreated waste water-to-water protection areas, both from the sewage network and from the wastewater treatment plant; this causes natural occurring microorganisms to be flushed into drinking water sources. Higher temperatures could also increase microbial growth rates for some microbes. Due to climate change, more extreme weather and higher temperatures are anticipated in the future. Furthermore, a more dense population due to urbanization trends will put additional pressure on the existing wastewater treatment systems that may have similar effects on drinking water production.

The most common microbial contaminations in drinking water have been *Campylobacter* and *Norovirus* and according to the Public Health Agency of Sweden the cases of outbreaks has increased in recent years. Furthermore, due to climate change it is expected that the outbreaks of diseases caused by viruses and protozoans such as *Cryptosporidium* will increase in Sweden. The most common source to contaminated drinking water is contamination of the raw water by human or animal faeces.

A lot of attention has been giving to the issue of microbial outbreaks since the event in Östersund in 2010 where approximately 3, 000–9, 000 people were infected by *Cryptosporidium*. It has not been established how the raw water was contaminated. After the discovery of the outbreak, the inhabitants were recommended to boil the drinking water for ten minutes before using it. The following year there was a similar outbreak in Skellefteå.

The main action to ensure drinking water production in case of an event affecting the raw water quality such as microbial outbreak is to have redundant systems and adequate water reserves. Listed below are some actions connected to the five dimensions of the resilience matrix. The challenges described in the following are summarized in Table 12.

System/Physical dimension

When risk analysis suggest that additional measure should be taken many Swedish water treatment plants are considering to introduce new treatment units as part of the process such as an extra microbial barrier e.g. ultra-filtration in combination with further chemical precipitation. Most water treatment plants work with redundant systems as the main action in case of an event e.g. connections in the distribution system to other drinking water distributers, for instance in Stockholm the two largest producers have connections between their distribution systems so that they can help each other in case of an emergency.

Understand risks:

- *Risk assessment*: Regular inspections of state and capability of equipment and process and analyse the raw water microbiological quality is important. It is also important to map harmful contamination sources affecting raw water source and to perform a microbial risk assessment

Anticipate/prepare:

- *Barriers and sources*: To create additional barriers focused on microbial activity (ozone, UV, chlorine, UF) is an effective way to increase the system capability. In combination with alternative water intakes and redundant systems, such as cooperation with other producers and alternative water sources, the system can be even better. There is also the possibility to increase water storage in distribution system to manage short interruptions

Absorb/withstand:

- *Over* capacity: By adding barriers an "over-capacity" is added to the system which isn't needed under normal circumstances but is crucial in case of microbial contamination.

Respond/recover

- *Barriers and sources*: Additional barriers, switch water intake (resource), use redundant system (other producers) and use water stored in distribution system are possible actions to respond in case of events.

Adapt/learn

- *System and process adjustments*: To adapt to occurred incidents it may be necessary to perform system and process adjustments and introduce new technologies

Information dimension

There is a possibility to subscribe to indicative data on epidemic outbreak from the regional health care system. This is a "slow" indicator since there could be several days of delay before an indication of outbreak is recognized and the geographical resolution is not precise enough to locate the outbreak source. However, this information could also be used to anticipate when contamination to the raw water from human sources is more likely and the producer may take precautionary actions.

There are on-going research activities and investments in on-line sensors for to detect microbes (bacteria, virus and parasites) at the water resource intake.

Understand risks:

- *Data analysis*: Store and analyse historical data are important to understand the risks and vulnerabilities of the system or organization.

Anticipate/prepare:

Monitoring and predictions: Many producers are trying to establish data driven predictions and monitor process values to find process anomalies. Further action is to develop new sensors to detect harmful pathogens, which is performed in several Swedish research projects. It is also possible to get feedback from Swedish health care system.

Absorb/withstand:

- *Real-time assessment*: Many producers try to perform real-time assessment of process status and monitor process values to find anomalies and possible counteractions.

Respond/recover

- *Monitor*: To monitor the recovery of the process and the process response to the counteractions are important to improve the recovery process.

Adapt/learn

- *Data analysis and evaluation*: Perform data analysis and evaluate the system performance, which are an important input in order to increase future resilience.

Organizational/business dimension

All organizations work with risk analysis where microbial outbreak has been on the agenda for especially surface water plants since the outbreak of cryptosporidium in Östersund (2010) and Skellefteå (2011). It is also on the political agenda resulting in regulations, guidelines and performance goals, which the organizations need to address.

Understand risks:

- *Business continuity plan*: Risk and vulnerability analysis and decision analysis of preventive counteractions such as installation of additional barriers are important aspects when establishing the continuity plan.

Anticipate/prepare:

- *Business continuity plan*: Incorporate business continuity plan addressing regulations, goals, guidelines, contingency plans, activities and responsibilities

Absorb/withstand:

- *Business continuity plan*: Activate business continuity plan and take actions according to it

Respond/recover

- *Business continuity plan*: Follow business continuity plan

Adapt/learn

- *Business continuity plan*: Evaluate organization response and adjust business continuity plan
- *Business impact analysis*: Evaluate financial impact and consider investments to strengthen system resilience.

Societal/political dimension

On a societal and political level, investments are made in infrastructure and research to protect water resources from the effects of climate change. Regulations and standards for risk analysis and management have been prepared and resulted in goals e.g. in terms of the amount of emergency water to inhabitants of municipality within 24 hours have been constructed to stimulate the actors in drinking water to work with process continuity. Research in new technologies to detect harmful microorganisms in real-time is also being performed. The methods available today are not fast enough to be implemented in real-time process control.

Understand risks:

- *Societal risk analysis:* Societal financial risk analysis and human risk assessment are critical to understand the risks involved and direct appropriate research funding and regulations on the subject.

Anticipate/prepare:

- *Regulations and guidelines*: Set-up of national regulations, guidelines, goals and evaluation for the producers and to increase water resource protection are critical preventive actions on a societal level.
- *Investments:* Regional and national crisis management resources (laboratories, support functions, etc.) and investments in redundant infrastructure as well as research funding of development of new detection methods that are fast enough to alert producers of harmful microbes at an early stage are other measures taken by society.

Absorb/withstand:

- *Communication and crisis resources*: Crisis contact and social/political information as well as warning systems are important to keep the public informed on how to act in a crisis. The available crisis resources such as catastrophe water supply are important to withstand an event of contaminated drinking water.

Respond/recover

- *Communication and crisis resources*: Catastrophe water supply needs to be distributed and a prioritization of help receivers such as health care and risk groups is performed. Societal crisis support and information to the public is another important aspect.

Adapt/learn

- *Reporting and* evaluation: The societal effects needs to be analysed and evaluated to decide on further preventive actions such as investments in infrastructure, crisis resources and further water resource protection.

Cognitive/decision-making dimension

Water treatment plants are working with updating the system design to cope with new threats but are impaired by old technology in the process, which causes high investments costs. Work is performed across organizations, society and dimensions of the process to raise awareness and readiness in case of an incident.

Understand risks:

- *Awareness*: Raise awareness through education and guidelines to the public and the producers

Anticipate/prepare:

- *Training*: Event training and exercises for the producers

Absorb/withstand:

- *Prioritize*: Plans to prioritize in the use of crisis management resource and improve decision making.

Respond/recover

- *Recovery and communication plans*: Plans to help and improve the decisions made during the recovery phase are important as well as public communication of the recovery process.

Adapt/learn

Evaluate: Evaluate and improve the crisis management and adapt the measures in earlier phases.

Table 12: FOXTROT – Outbreak of waterborne disease

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
System/ physical	• State and capability of equipment and process. • Raw water microbiological quality • Map harmful contamination sources affecting raw water source • Microbial risk assessment	• Create additional barriers focused on microbial activity (ozone, UV, chlorine, UF) • Establish alternative water intakes • Create redundant systems (such as cooperation with other producers and alternative water sources) • Increase water storage in distribution system to manage short interruptions	• Create over-capacity through additional barriers.	• Use additional barriers • Switch water intake (resource) • Use redundant system (other producers) • Use water stored in distribution system	• Perform system and process adjustments • Introduce new technologies
Information/ data	• Store historical data, • Perform process data analysis	• Try to establish data driven predictions • Monitor process values to find anomalies • Development of new sensors to detect harmful pathogens • Feedback from health care system	• Perform real-time assessment of process status, • Monitor process values to find anomalies and possible counteractions	• Monitor recovery and responses of counteractions	• Perform data analysis • Evaluate system performance
Organizational/ business	• Risk and vulnerability analysis • Decision analysis of preventive counteractions such as installation of additional barriers	• Incorporate business continuity plan addressing regulations, goals, guidelines, contingency plans, activities and responsibilities	• Activate business continuity plan	• Follow business continuity plan	• Evaluate organization response and adjust business continuity plan • Evaluate financial impact • Consider investments to strengthen system resilience

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
Societal/ political	• Research funding, • Societal risk analysis, • Societal financial risk analysis, • Human risk analysis	• Set-up of national regulations, guidelines, goals and evaluation, • Increase Water resource protection, • Research in detection of microbes (fast enough not available today). • Investment in redundant infrastructure • Regional and national crisis management resources (laboratories, support functions, etc.)	• Crisis contact and social/political information, • Warning systems • Use of crisis management resources	• Catastrophe water supply • Societal crisis support and information to the public • Prioritize available water (health care, risk groups)	• Reporting and evaluating societal effects • Further water resource protection
Cognitive/ decision-making	• Raise awareness through education and guidelines.	• Event training and exercises	• Priority decision-making	• Recovery decision-making • Communication of recovery process	• Evaluate event management and decisions made

Colours indicate the level of relevance: High Medium Low

2.6.3 Water shortage

Water shortage is a significant threat to produce sufficient amounts of drinking water. In Sweden, this is particularly visible in the southern parts of the country. Climate change is expected to lead to less rainfall and more frequent droughts in these areas. In the winter, snowfall will become less frequent than rainfall, which means that the water quickly runs off rather than contributing to groundwater recharge. This adds to the problem of water shortage.

Gotland is the biggest island of Sweden with approximately 57,000 inhabitants. However, being one of Sweden's most popular tourist destinations, the population increases dramatically in the summer, which puts increasing pressure on the available water resources. Gotland has few alternative drinking water sources and is an interesting case to illustrate the threat and challenges of climate change in the drinking water infrastructure.

The threat of water shortage does not illustrate a sudden disruption to the drinking water infrastructure, but rather an evolving crisis, which is developed over time. If groundwater recharge has been limited for a long time, it can develop into an even bigger problem when the population increases during the tourist season, leading to an acute situation in drinking water supply.

In the summer of 2016, there were record-low ground water levels throughout South-eastern and Southern Sweden, due to little rain and snowfall in the previous winter. In Gotland, the equal of one year's rain- and snowfall was missing and the situation was the worst since 1964.

The challenges described in the following, are summarized in Table 13.

System/Physical dimension

Understand risks:

- *Identify risks in the technical system, which could affect the production capacity:* Such risk identification should include the entire chain, from raw water supply to preparation and distribution of processed drinking water. It includes the technical system, but also the natural conditions and the impacts following climate change. A challenge here is to identify alternative resources, as a basis for planning how drinking water supply can be secured during normal circumstances as well as in emergencies.

Anticipate/prepare:

- *Desalination plant:* The regional government on Gotland has invested in a new desalination plant, where saltwater from the sea is desalinated to produce water suitable for human consumption or irrigation. This water source is independent of rainfall. However, challenges include high energy consumption, which is generally more costly than producing drinking water from fresh water sources (rivers or groundwater), water recycling and water conservation. In addition, the quality of the drinking water is sometimes questioned although the drinking water produced through desalination in Gotland meets the standards from the National Food Agency. Finally, the process of desalination produces a by-product of concentrated salt, which is released back into the sea, and may have a negative impact on the marine environment. However, the desalination plant in Gotland is small and the environmental impact is considered to be limited.
- *Urban planning to ensure that sufficient amounts of rainwater reach the ground water.* While the amount of rainwater cannot be affected, it is possible to allow for more rain water to reach the ground water through urban planning. Having less impervious surfaces in urban areas means that more rain can infiltrate. Planning for more ponds, reservoirs and wetlands gives water the chance and the time to reach down to the ground. Challenges that arise here are linked to urban planning, such as making decision-makers and urban planners aware of these factors.
- *Build infrastructure to transport water from the mainland by boat.* To be able to receive water from the mainland by boat, it is necessary that the right capacity is available at harbours and that it is possible to connect the water tanks with the public water supply network. Transporting water also has an environmental impact, which should be taken into consideration.

Absorb/withstand:

- *Decrease the pressure in the water conduits:* This measure requires that the pressure in the water distribution system is not decreased to such an extent that other issues arise. Significant decreases in the pressure can, worst case, trigger pollutants to penetrate the pipelines if the drinking water pipelines are located next to sewage pipelines.

Respond/recover:

- *Transport water from the mainland by boat.* Sufficient amounts needs to be transported at the right points in time.
- *Set up emergency water tankers.* Challenges may include that emergency water is directed to where it is most needed.

Adapt/learn:

- *Plan for additional technical measures. S*uch measures can include planning for additional desalination plants. Each technical measure may bring its own challenges. For desalination, challenges include financing, since desalination is a relatively costly way to produce drinking water.

Information/data dimension

Understand risks:

- *Understanding the status of water supply:* A situation analysis of the water supply is a key factor in the information/data dimension.
- *Information management linked to the production process.*
- *Estimating amounts of rainfall and snowfall:* This should provide input to the production planning process.
- *Forecasting future water shortages through hydrological and hydrogeological data and other forecasts.*

Anticipate/prepare:

- *Monitoring of groundwater levels.*
- *Data simulations and estimates on drinking water consumption (private and commercial):* Such simulations and estimates can be based on historical records, but it can be a challenge to make such estimates sufficiently precise.

Absorb/withstand:

- *Monitoring of groundwater levels:* See above.

Respond/recover:

- *Monitoring of groundwater levels:* See above.

Adapt/learn:

- *Evaluation of previous crisis.*

Organizational/business dimension

In Sweden, the 290 municipalities are each responsible for the local drinking water supply. To cope better with this task, some municipalities cooperate through for example municipal associations or jointly owned water and sanitation companies. In Gotland, Region Gotland is the only municipality on the island. In addition, it has an extended responsibility that covers county council operations and regional development.

Understand risks

- *Risk analysis at organizational level:* An analysis to identify the most relevant and pressing risks for the municipality.

Anticipate/prepare

- *Analysis of the identified risks in the information/data dimension:* This type of data include understanding the status of water supply, information management linked to the production process and estimating amounts of rainfall and snowfall.
- *Risk management, training and exercises:* Local actors often highlight lack of time, skills and financial resources for adequate risk management procedures.
- *Business continuity plans:* In the process of creating systems of prevention and recovery to deal with potential threats to a company, it is important to take into account all dimensions of such a plan and employ appropriate exercises to test it. It is also important that it is made clear what resources are available.
- *Adequate pricing levels and appropriate financial management:* In general, pricing is a powerful mechanism to influence supply and demand. However, drinking water in Sweden is relatively cheap and a challenge is to find a balanced price level that meets current and future needs while making sure that it is affordable.

Absorb/withstand

- *Activate crisis management plan:* A challenge here is making sure that all aspects of the crisis management plan works and that a possible "weak link" does not hinder effective crisis management.

Respond/recover

- *Monitor responses:* The organization needs to make sure that the responses to the disruptive event have the desired effect.

Adapt/learn

- *Evaluation and adjustments of crisis management plan:* After a significant disruptive event, the crisis management plan needs to be evaluated and adjusted. A challenge here may be to agree on what the functioning parts are.
- *Examine conditions for collaboration across municipalities:* Research shows that conditions exist for increased municipal collaboration and there is a widespread willingness to cooperate among the relevant administrative organizations in many of Sweden's municipalities.

Societal/political dimension

Understand risks:

- *National risk and capability assessments and climate change vulnerability assessments:* Appropriate assessments needs to be done at the national, regional and local level.
- *Research funding:* Sufficient amounts of resources should be spent on research on all aspects of water availability.
- *Investments in infrastructure:* This should be done taking estimates of future water supply into account. It is a challenge that such estimates are uncertain.

Anticipate/prepare:

- *MSB (Swedish Civil Contingencies Agency) goals for protection of vital societal functions and critical infrastructure:* These goals are an important inspiration for the drinking water sector and the goals are developed in a way that they are possible to evaluate. It may be a challenge to identify the relevant goals and adapt them to the appropriate context.
- *Regulation and policies:* These are important tools in preparing for a disruptive event, and a challenge is to identify the most effective policy instruments and be attentive for possible impacts from combining them.
- *Urban planning:* When planning for new districts, there is a need to make sure that political decisions are taken to make sure that sufficient amounts of water can be supplied to that district.

- *Dialogue and awareness-raising with the public and significant commercial consumers of water:* It is of crucial importance to raise awareness about water shortage among water consumers, including what consequences there may be and what can be done to save water.

Absorb/withstand:

- *Governmental support:* In the event of a disruptive event – an acute water supply crisis – it may be relevant to call for governmental short-term support. A challenge here is to implement the right measures at the right point in time and place.
- *Volunteers:* Volunteers may play an important role in an acute water supply situation, but volunteers must never replace the public responsibility.
- *Limit the use of water through bans, rationing or political priorities:* This can be done through, for example, bans on using water for sprinklers and hoses, guidelines with priorities for what water should be used for (such as health care), and rationing. Facilities such as swimming halls may be closed down for a period of time. A challenge related to this is balancing interests and needs between, for example, local businesses, such as agriculture or tourism, and households.
- *Information to the public and significant commercial consumers about how to save water.* Such information includes putting bricks in the toilet's water tank and replace old showerheads.

Respond/recover:

- *Governmental support:* See above.
- *Volunteers:* See above.
- *Limit the use of water through bans, rationing or political priorities:* See above.

Adapt/learn:

- *Regulation and policies:* See above.
- *Urban planning:* See above.

Cognitive/decision-making dimension

Understand risks:

- *Inform the public and significant commercial users about the risks of water shortage:* Such information emphasizes the risks in particular.

Anticipate/prepare:

- *Training and exercise at organizational and political level:* Challenges may include financial resources and skilled personnel to carry out appropriate training and exercise.

Absorb/withstand:

- *Inform the public and significant commercial consumers about how to save water:* Such information emphasizes advice to save water in particular.
- *Public and industrial acceptance of saving water:* Several of the challenges mentioned in the previous dimensions above will require widespread acceptance among the public and other stakeholders such as industry. Acceptance issues may arise for challenges such as limit the use of water through bans, rationing or priorities, or desalination plants (the technology can be controversial).

Respond/recover:

- *Inform the public and large industrial consumers about how to save water:* See above.
- *Public acceptance of saving water:* See above.

Adapt/learn:

- *Research on the cognitive aspects of the crisis, including decision-making.*

Table 13: FOXTROT – Water shortage

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
System/ physical	Identify risks in the technical system that could affect the production capacity.	Desalination plants. Urban planning to ensure that sufficient amounts of rainwater reach the ground water. Build infrastructure to transport water from the mainland by boat.	Decrease the pressure in the water conduits.	Transport water from mainland by boat. Set up emergency water tankers.	Plan for additional technical measures.
Information/ data	Understanding the status of water supply. Information management linked to the production process. Estimating amounts of rainfall and snowfall. Forecasting future water shortages through hydrological and hydrogeological data and other forecasts.	Monitoring of groundwater levels. Data simulations and estimates on drinking water consumption (private and commercial).	Monitoring of groundwater levels.	Monitoring of ground water levels.	Collecting data to evaluate the previous crisis.
Organizational/ business	Risk analysis at organizational level.	Analysis of the identified risks in the information/data dimension. Risk management, training and exercises. Business continuity plans. Adequate pricing levels and appropriate financial management.	Activate crisis management plan.	Monitor responses.	Evaluation and adjustments of crisis management plan. Examine conditions for collaboration across municipalities.

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
Societal/ political	National risk and capability assessments and climate change vulnerability assessments. Research funding. Investments in infrastructure.	MSB (Swedish Civil Contingencies Agency) goals for protection of vital societal functions and critical infrastructure. Regulation and policies. Urban Planning. Dialogue and awareness raising with the public and significant commercial consumers of water.	Governmental support. Volunteers. Limit the use of water through bans, rationing or political priorities. Information to the public and significant commercial consumers about how to save water.	Governmental support. Volunteers. Limit the use of water through bans, rationing or political priorities.	Evaluating and revising regulation and policies as well as urban planning.
Cognitive/ decision-making	Inform the public and significant commercial consumers about the risks of water shortage.	Training and exercise at organizational and political level.	Inform the public and significant commercial consumers about how to save water. Public and industrial acceptance of saving water.	Inform the public and significant commercial consumers about how to save water. Public acceptance of saving water.	Research or investigation on the cognitive aspects of the crisis, including decision-making.

Colours indicate the level of relevance: High Medium Low

2.7 GOLF

Cork City, located at the head of a tidal estuary and at the downstream end of a large river catchment is prone to both tidal and fluvial flooding. Cork City is the second city of the Irish Republic with a population of 125,622 as per the 2016 census. A serious tidal flood can affect the Water supply to over 50,000 houses and businesses. Disruption to public transport, hospitals, energy supply and local government services can also occur. Cork City Council will be the lead flood response agency for any flood emergency within Cork City. Assistance will be provided by other response organizations including: Civil Defence, ESB, Police, Army and HSE. The subjects experts that have and will contribute to this project including the Director or Environment and Recreation, Assistant Chief Fire Officer, Senior Engineer Water & Drainage and Senior Executive Officer in ICT.

System/Physical dimension

Understanding Risk

- Cork City, located at the head of a tidal estuary and at the downstream end of a large river catchment is prone to both tidal and fluvial flooding. Flood risk is assessed on the likely probability of varying degrees of severity occurring. This probability is designated as the % probability of the event in any one year i.e. % annual exceedance (%AEP).

Anticipate/prepare

- Cork City Council is constantly monitoring for potential flood events. We also organize major emergency training where various emergencies such as flooding are re-enacted to ensure we are prepared for such an event.

Absorb/Withstand

- Work with the Office of Public Works (OPW) to develop flood defences under the Lower Lee Draining Scheme is due to commence in 2017 and be completed in five years. We will ensure the Major Emergency Plan is well practiced so it operates efficiently when required.

Respond/Recover

- Declaration of Major Emergency (Flooding) as per set procedures and criteria. Ensure that flood defences are in place. Culverts and drains are cleared and that worse affected areas are evacuated. Cancellation of sporting and social events.

Adapt/Learn

- The Lower Lee Drainage Scheme will raise the key walls in the city along with demountable flood gates. A review of defences that failed should be undertaken and improvements identified.

Information/Data dimension

Understanding Risk

- Early identification of a potential flooding event is critical and Cork City Council currently achieve this by monitoring Met Eireann weather alerts and reports received from other sources on current weather conditions. Analysing any reports received from staff monitoring Flood Early Warning Systems. Determining the potential effect of spilling notifications from the ESB Inniscarra Dam on Cork City as the rate of discharge directly affects the height of the river Lee. Analysing data on storm surge forecasts from the OPW

Anticipate/prepare

- Monitoring and recording of water levels and reviews of storm surge models. A project to develop a Tidal Flood Event Advisory System will aid greatly in predicting when and where flooding may occur.

Absorb/Withstand

- Review Flood forecasting information, storm surges and weather information to best determine the course and level of action required. Work with the OPW to develop better flood forecasting systems.

Respond/Recover

- Communicate with the public effectively using alert systems, social and traditional media. Determine the worse affected areas and time of flood events. Monitor water and electricity supply and ensure essential health services and functioning.

Adapt/Learn

- Reasons as to why the tidal flooding occurred are recorded and reviewed against criteria in the lower lee drainage. Cork is striving to improve our flood defences and early warning systems through the Lower Lee Drainage Scheme. Analytic tools are being developed and investments in smart meters on tidal and fluvial indicators are being put in place.

Organizational/business dimension

Understanding Risk

- Flood events are a corporate risk for Cork City Council and are managed through the Major Emergency Plan. Businesses and citizens subscribe to a system called Cork Now which will alert on flood and other emergency issues.

Anticipate/prepare

- The council reviews and tests our major emergency plan, we are enhancing our alerting systems and learning from the experience of other areas affected by flooding

Absorb/Withstand

- Ensure that all stakeholders and aware of their roles and responsibilities in a serious flooding event.

Respond/Recover

- Evacuations of flood area where a threat to life exists. Regular and specific area based alerts. Work with insurance companies to ensure speedy corrective action. Ensure essential services are back in operation once safe to do so.

Adapt/Learn

- Review data and predictive modelling against actual outcomes to determine performance.

Societal/political dimension

Understanding Risk

- Cork has experience a major flooding event in the past in 2009 and has learnt from this event. A detailed and practiced major emergency plan is in place which deals with determining if a major emergency has occurred. It contains key staff from the entire major relevant stakeholders in the City and tools have been developed to disseminate information to the public

Anticipate/prepare

- Liaise with other key stakeholders such as Police and Civil Defence. Improve communication systems with the public and engage with central government on public works to enhance flood defences.

Absorb/Withstand

- Alert stakeholders of potential flood events and to be on standby. Build public confidence that a plan is in place to manage and mitigate the effect of the flood.

Respond/Recover

- Evacuation of flood area where a threat to life exists. Regular and specific area based alerts. Work with insurance companies to ensure speedy corrective action. Ensure essential services are back in operation once safe to do so.

Adapt/Learn

- Implement lessons learnt in revised Major Emergency Plan and predictive models. Implement flood defences to withstand future predicted flood events. Avoid development in floodplains, wetlands and coastal areas prone to flooding.

Cognitive/decision-making dimension

Understanding Risk

- Should indicators inform that a serious flooding event is likely the steering group of the major emergency team will meet and if applicable declare a major emergency and activate the plan.

Anticipate/prepare

- Outcomes of Major Emergency drills reviewed and reported to senior management and stake holders.

Absorb/Withstand

- Gather the Major Emergency Steering Group to review the data and models and determine the best course of action including the activation of a Flooding Major Emergency.

Respond/Recover

- Regular daily review of crisis by Major Emergency group. Once flood threat has abated stand down the major emergency team and resume normal operations.

Adapt/Learn

- Review Major Emergency Plan and predictive models. Invest in infrastructural works such as flood protection and storm water attenuation. The city's historic core will be protected from flood risk by new and improved defence structures, as part of the OPW's Draft Lower Lee Relief Scheme. The scheme will provide.

Table 14: GOLF

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
System/ physical	A severe Tidal Flooding event caused by spring tides and low pressure.	Notifications from Met Eireann if severe weather is due. Review of surge models and tidal gauges to determine likely breaches of key walls.	Alert Major Emergency stakeholders to review the severity of the flooding threat; i.e. Civil Defence, ESB, Police, Army and HSE. Improve Flood defences with OPW/	Declaration of Major Emergency (Flooding) as per set procedures and criteria.	On stand down of Major Emergency a review process on how the stakeholders performed and lessons learnt are documented and a revised Plan issued. Works with the OPW on flood defences will be informed by findings.
Information/ data	Tidal Gauges, Surge Modelling, Met Eireann Weather Forecast and discharge levels from Inniscarra dam.	Regular Analysis of surge models and river levels. A project to develop a Tidal Flood Event Advisory System will aid greatly in predicting when and where flooding may occur.	Review Flood forecasting information, storm surges and weather information to best determine the course and level of action required.	Alert public via Cork Now and social and traditional media. Outlining probable flood areas and extent.	Reasons as to why the tidal flooding occurred are recorded and reviewed against criteria in the lower lee drainage
Organizational/ business	Should a Major Emergency be called Cork City Council will be the lead agency and operations to increase the resilience and recovery of the City will be put into action in conjunction with other key stakeholders.	Ensure regular review of flood threats occur and that Major Emergency exercises occur and are reviewed.	Ensure the Major emergency Plan is optimal and well-rehearsed.	Cork City Council to liaise with key stakeholders: Civil Defence, ESB, Police, Army and HSE.	Review data and predictive modelling against actual outcomes to determine performance.
Societal/ political	Failure /contamination of water supplies, evacuation of vulnerable people from dwellings and potential threat of loss of life. Reduction in economic and transport activity in the area and issue with insurance.	Conduct periodical Major Emergency drills and development of alerting systems.	Alert stake holders of potential flood events and to be on standby.	Evacuations of flood area where a threat to life exists. Regular and specific area based alerts.	Implement lessons learnt in revised Major Emergency Plan and predictive models. Work with OPWon implementing flood defences.

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
Cognitive/ decision-making	Major Emergency Team made up of key stakeholders such as police, army, local authority and health workers to manage and maintain the crisis.	Outcomes of Major Emergency drills reviewed and reported to senior management and stake holders.	Gather the Major Emergency Steering Group to review the data and models and determine the best course of action.	Regular daily review of crisis by Major Emergency group.	Review Major Emergency Plan and predictive models.

Colours indicate the level of relevance: High Medium Low

2.8 HOTEL

The energy infrastructure in Helsinki is producing and distributing district heating, district cooling and electricity. The supply system provides major welfare services to the citizens, such as comfortable indoor temperature, lighting, and power for private and public needs including those of the city water and wastewater systems, hospitals and elderly peoples' homes, for example. For electricity, there are alternative sources and feeds from outside the city, and cooling is generally less critical due to the climate. However, most buildings of the city rely on the district heating system that includes few power plants as main sources, and an underground pipeline network for distribution. The system has additional peak load sources from local small heat plants, but not significantly from external sources, and it is not designed to cover sustained load approaching the record cold in Helsinki (-34°C in 1987). Breakdown in the major heat sources or in the distribution during cold spells in winter represents a threat to the heating function, and in extreme cases, it might endanger public health. The section is based on the interviews and background information provided by the responsible management of the power plant operating company, including information on available risk assessment.

The HOTEL case focuses on two scenarios that could significantly disrupt the district heating supply or distribution in Helsinki, namely on

- fires in the underground fuel storage of a power plant (supply node for district heating), and
- flooding of the underground tunnel of a trunk pipeline for distribution of district heating.

Both scenarios can be initiated by a sudden or short term disruption, but will take some time to develop into a crisis, depending on weather and functionality of the backup resources. There is more experience on the initiation of the first scenario, as smaller scale fires in solid fuel storages are not uncommon. This scenario may have gradually decreasing impact due to global warming, but more challenges with increasing share of biomass-derived solid fuels in storage. The latter scenario may become more important in time with increasing probability of flooding by storm surges in the north-eastern Baltic Sea, assuming rising sea water level due to global warming.

2.8.1 Fires in (underground) fuel storage site at a main supply node

Solid organic fuel (coal) of a downtown power plant is being stored in closed underground silos. In time, exothermic reactions in the stored fuel bed will gradually raise the bed temperature, potentially leading to auto-ignition and a fire.

System/Physical dimension

Understand risks

- The likelihood of auto-ignition of solid fuel in a closed storage mainly depends on the fuel composition, bed size and geometry (thermal properties), air ingress, initial temperature, and time in storage. Minor consequences beyond the lost fuel value from small pockets of heating or fires at locations with easy access for rapid response are expected. Fires that are more extensive can emit unpleasant odour for public nuisance, with loss of reputation, and may result in structural damage of the facility. In the worst case of limited availability of fuel from other silos or damage to the conveyor system, a fire can result in significant plant derating (reduced production).

Anticipate / prepare

- To reduce the chance of autoignition and fire, the fuel grade (composition, size distribution) of the delivered fuel batches is kept within controlled specifications, air leaks to silos are minimized and initial fuel temperatures monitored, and all silos are made nearly empty every year by the end of the main heating season. Several silos are available in parallel. Sensors and alarm systems are in place and functional to detect indications of heating, ignition and smouldering fires. Training of personnel includes the appropriate preventive and containing measures and actions.

Absorb / withstand

- Fuel from a not too overheated bed can be directed to immediate combustion.

Respond / recover

- When excessively overheated or ignited, or the plant is not operating, the fuel may need to be extinguished/cooled before transporting it out. If necessary, fuel from other available silos (or from another site) can then be used for plant operation.

Adapt / learn

- Review and update the specifications for fuel selection, storage and removal. Review and update sensor options and options for other possible technical opportunities.

Information dimension

Understand risks

- Delayed detection of the time and location of the ignition/fire by sensors, as self-heating and ignition usually start deep inside the bed; the same thermal properties also limit bed-cooling rates. Information about the storage time at different layers in the silos (delivered fuel batches) is related to self-heating and time to ignition.

Anticipate / prepare

- Transfer, analysis and interpretation of sensor data and records of grades, batches and fuel levels in the silos can be used to assess the likelihood of heating/ignition; the routines mainly aim to establish the degree of compatibility with guidelines/specifications.

Absorb / withstand

- Independent measurements to indicate time, location and extent of heating can be used for comparing them to established guidelines or tolerances of acceptability.

Respond / recover

- Sensor data, other records and tools used for situational picture can indicate need, urgency, and performance in the responses, and provide data on recovery.

Adapt / learn

- To adapt and learn about the situation it is important to review and update the sensors, software and analysis tools, and compare assessed and observed heating/ignition behaviour.

Organizational / business dimension

Understand risks

- Normally the storage is unmanned. Human actions are taken only in case of alarm, deviation or maintenance. System changes and observed events are subjected to the district heating system-related risk analysis of the organization.

Anticipate / prepare

- Continuity plans are applied in case of deviations and interventions.

Absorb / withstand

- Redundancy is normally available by using parallel silos, but if not, by fuel transport from another plant site (at reduced production rate).

Respond / recover

- Evaluate the rates of response and recovery. Review need and contents for response cooperation and training.

Adapt / learn

- To adapt and learn there is a need to adjustment of financial evaluation and plans of crisis management, investment and training.

Societal / political dimension

Understand risks

- Fire emissions can be nuisance or burden for citizens in the nearby city environment and may alarm the wider public. Loss of local heating service would be expected to launch a public enquiry. Rising share of solid biomass-derived fuels will increase the fire risk when similarly stored. Major service disruption would be an issue on city and national level, as all cities in the country make use of district heating from power stations.

Anticipate / prepare

- There is emphasis on measures to reduce emissions and other inconvenience to the society. Policy is in place for timely and open communication to the society and media.

Absorb / withstand

- To inform the general public and the local population, provide timely and open communication.

Respond / recover

- There is a need for support of rescue services and open communication to respond to and recover from the situation.

Adapt / learn

- To adapt and learn it is important to review and update environmental, human protection and crisis management plans.

Cognitive / decision-making dimension

Understand risks

- The perception of the fire risk may affect the social acceptance of the plant and other plans of the owner/operator. The public and other stakeholders need to be informed about the general associated risks.

Anticipate / prepare

- To anticipate and prepare for crisis there is a need to implement policy for timely and open communication as well as training of the organization.

Absorb / withstand

- Follow contingency protocols, including timely and open communication.

Respond / recover

- Follow contingency protocols.

Adapt / learn

- Review and update communication and contingency plans and protocols, lessons for decision-making.

Table 15: HOTEL – Fires in (underground) fuel storage at a main supply node

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
System/ physical	The risk of autoignition of solid fuel mainly depends on the fuel composition, bed size and geometry, air ingress, initial temperature, and time in storage.	The fuel grade is kept within specifications and silos made nearly empty by the end of main heating season. Several silos available in parallel. Functional sensors in place.	Heated fuel to be transported to combustion.	Extensive overheating or fire may require extinguishing/cooling before fuel removal. Other available silos can be used for plant operation.	Review and update the specifications for fuel selection, storage and removal. Review and update sensor options.
Information/ data	Delayed detection of the time and location of the ignition/fire by sensors. Time in storage at a given silo layer is related to the expected time of ignition.	Transfer, analysis and interpretation of sensor data and records of grades, batches and fuel levels in the silos, to assess likelihood and timing of ignition.	Independent measurements to indicate time, location and extent of heating, in comparison to tolerances of acceptability.	Sensor data, other records and tool used for situational picture, to indicate need, urgency and type of response taken, and to provide data on recovery.	Review and update the sensors, software and analysis tools, and compare assessed and observed heating/ignition behaviour.
Organizational/business	Normally the storage is unmanned. Human action taken only in case of alarm/deviation/maintenance.	Continuity plans in case of deviations and interventions.	Redundancy by using alternative silos, or if necessary by fuel transport from another plant site.	Evaluate the rates of response and recovery. Review need and contents for response cooperation and training.	Adjustments of crisis management plan, financial evaluation, investment needs and plans, training plans.
Societal/ political	Fire emissions can be inconvenient for citizens in the nearby city environment and may alarm the wider public and media.	Emphasis on measures to reduce emissions and other inconvenience to the society. Policy for timely and open communication to the society.	Timely and open communication to the public and media.	Support of rescue services.	Review and update of environmental and human protection plans.
Cognitive/ decision-making	The perception of fire risk may affect the acceptance of the plant and other plans of the owner/operator.	Policy for timely and open communication.	Follow contingency protocols.	Follow contingency protocols.	Review and update communication and contingency plans and protocols.

Colours indicate the level of relevance:	High	Medium	Low

2.8.2 Flooding in the district heating pipeline tunnels

The district heating pipelines are placed in underground tunnels, sometimes together with other infrastructure equipment. Very high seawater level due to extreme weather conditions such as storm surge, for example, may cause flooding in these tunnels. The flooding risk is gradually increasing with global warming, and only partly compensated by bedrock lift by about 25 cm/century in Helsinki. Flooding can cool the pipelines to result in a loss of heating power, and may interrupt the heating service if rapid corrosion in seawater will lead to pipe burst or major leaks within already aged main trunk lines.

<u>System/Physical dimension</u>

Understand risks

Risk consists of two different hazardous events which may exist alone or parallel.

- 1) Reduced delivery of heating power.
- 2) Pipe rupture/leak by fast external corrosion at ageing sections.

Anticipate / prepare

- At least two alternatives for feed and return flow of the district heating water

Absorb / withstand

- A short term impact of flooding can be absorbed by the system redundancies.

Respond / recover

- Remedial actions to stop flooding and repair damage

Adapt / learn

- Review and update remedial actions to stop flooding and repair damage.

<u>Information dimension</u>

Understand risks

- No direct data source - information via other stakeholders (on expected/current status of indicators).

Anticipate / prepare

- Communication with end-users & collaboration with the infrastructure owner (status, indicators).

Absorb / withstand

- Timely communication on expected and current status of pipelines, indicators and preventive/remedial capacity.

Respond / recover

- Mapping of flooding penetration and damage, timely communication on requirements and extent of response and repairs (with end-users, owner, rescue services).

Adapt / learn

- Review and update flooding indicators, measures and communication plans.

<u>Organizational / business dimension</u>

Understand risks

- Risk of interruption or reduction of the heat delivery, loss of reputation in the customer base, possible customer shift to alternatives, cost of prevention & repairs.

Anticipate / prepare

- For each customer there are at least two alternative feed and return flow options for the district heating water that supports conditions for maintenance of pipelines.

Absorb / withstand

- A short term impact of flooding can be absorbed by the system redundancies.

Respond / recover

- Remedial actions to stop the flooding and repair damage.

Adapt / learn

- Review and update guidelines and responsibilities of remedial and preventive measures.

Societal / political dimension

- None.

Cognitive / decision-making dimension

Understand risks

- Perception of future sea rise, flooding and cost of rebuilding may affect the competitive position of district heating vs. local heat pumps. There is a need for deep communication with the tunnel infrastructure owner.

Anticipate / prepare

- Policy for open communication with the tunnel infrastructure owner on measures to avoid or reduce the impact of flooding.

Absorb / withstand

- Cooperation with owner and rescue services for proper preventive/remedial capacity.

Respond / recover

- Implementation of remedial actions and communication with the infrastructure owner.

Adapt / learn

- Review and update guidelines and responsibilities preventive and remedial actions

Table 16: HOTEL – Flooding in the transmission pipeline tunnels

Phases / Dimensions	Understand risks	Anticipate/prepare	Absorb/withstand	Respond/recover	Adapt/learn
System/ physical	1) Reduced delivery of heating power. 2) Pipe rupture/leak by fast pipeline corrosion	1) Alternative feed & return flow options for district heating water	A short term impact of flooding can be absorbed by the system redundancies.	Remedial actions to stop flooding and repair damage.	Review and update remedial actions to stop flooding and repair damage.
Information/ data	No direct data source - information via other stake-holders (on expected/current status of indicators).	Communication with end-users & collaboration with the infrastructure owner (status, indicators).	Timely communication on status of pipelines, indicators and preventive/remedial capacity.	Mapping of flooding penetration and damage, timely communication on response and repairs (owner, rescue services).	Review and update flooding indicators, measures and communication plans
Organizational/ business	Risk of interruption of the heat delivery, loss of reputation, cost of prevention & repairs.	1) Alternative flow options for district heating water, condition maintenance	A short term impact of flooding can be absorbed by system redundancies.	Remedial actions to stop the flooding and to repair damage.	Review and update guidelines and responsibilities of preventive and remedial actions.
Societal/ political					
Cognitive/ decision-making	Perception of risk and cost may affect customer preference. Communication with the tunnel infrastructure owner.	Policy for open communication with the infrastructure owner on measures to avoid or reduce the flooding impact.	Cooperation with owner & rescue services for proper preventive/remedial capacity	Implementation of remedial actions and communication with the infrastructure owner.	Review and update guidelines and responsibilities of preventive and remedial actions.

Colours indicate the level of relevance: High Medium Low

3 Conclusion

As individual conclusions have already been reached within the specific sections on the eight systems, this conclusion section will provide a quantitative analysis of the overall data in order to identify possible trends that may hold true for all systems. Table 15 summarizes the results from all 14 tables. While this table provides a detailed account of the distribution of the three relevancy levels, it may be more useful to quantify the results by weighting the data. This was done by attributing values to the colours (red = 2 point, yellow = 1 point; green = 0 points). Table 16 shows the results. The average score was 20.72 and the median 20, which indicates that outliers among the higher end are slightly more dominant.

Table 17: Combined data from all matrices.

		Phases														
		Understand risks			Anticipate/ prepare			Absorb/ withstand			Respond/ recover			Adapt/ learn		
Dimensions	System/physical	12	3	0	12	3	0	13	2	0	13	1	1	8	4	3
	Information/ data	8	3	4	9	5	1	5	8	2	6	7	2	6	4	5
	Organizational/business	15	0	0	8	7	0	8	7	0	7	6	2	4	11	0
	Societal/ political	8	2	5	6	4	5	6	6	3	9	2	4	2	9	4
	Cognitive/ decision-making	11	1	3	6	4	5	6	6	3	6	9	0	5	6	4

Table 18: Weighted data of all matrices. Top five values marked with red and bottom five values marked with green.

		Phases					
		Understand risks	Anticipate/ prepare	Absorb/ withstand	Respond/ recover	Adapt/ learn	*Average*
Dimensions	System/physical	27	27	28	27	20	25.8
	Information/ data	19	23	18	19	16	19.0
	Organizational/business	30	23	23	20	19	23.0
	Societal/ political	18	16	18	20	13	17.0
	Cognitive/ decision-making	23	16	18	21	16	18.8
	Average	23.4	21.0	21.0	21.4	16.8	

As can be seen, nearly all phases within the system/physical dimension have been considered extremely important and relevant. The average score of 25.8 is close to three points ahead of the second placed dimension (Organization/business with 23.0). Only the adapt/learn phase in this dimension has not been highly important, which is unsurprising given that three out of the five values for this phase have been among the lowest five scores in total. With an average of 16.8 the adapt/learn phase was scored over 4 points below the next lowest phase (anticipate/prepare and absorb/withstand with an average of 21.0). In terms of the other dimensions, only organization/business stood out besides the system/physical dimension one. The remaining three show very similar results. As already indicated, the adapt/learn phase was considered the least important phase. All other phases had a score of more than 21.0 with understand risks leading with an average score of 23.4.

Several of these findings are noteworthy for the overall SmartResilience project.

First, the high score of the understand risk phase is interesting as there has been an on-going debate to what degree this task is part of resilience. In the analysis and overview of concepts of resilience in D1.1 understanding risk was only incorporated infrequently. Our data indicate that understanding risks is a crucial element for dealing with threats and thus contributing to resilience, thus supporting the initial conclusion in D1.1 that "[u]nderstanding the risks you are facing is obviously a prerequisite for knowing what to do about them" (D1.1, p. 31).

Second, even though threats in these cases were quite varied, 'system/physical' is on average the most important dimension. This finding should be hardly surprising given that all of the system under investigation belong to infrastructure. It may be useful for WP4 pay particular attention to this dimension when identifying and developing indicators.

Third, the single most important effort is to understand risk in the organization/business dimension. In every one of the fourteen cases, this was deemed highly relevant. In D1.2 the dimension organization/business was defined as "includ[ing] business-related aspects, financial and HR aspects as well as different types of respective organizational networks". Taking this definition into account, it may not be unsurprising that understanding risk rates very high as anything that might negatively impact on the financial health of the organization could be a threat to the survival of the organization.

References

[1] SmartResilience (2016). Deliverable D2.1: Understanding "smart" technologies and their role in ensuring resilience of infrastructures. [in progress]

[2] SmartResilience (2016). Deliverable D1.2: Analysis of existing assessment resilience approaches, indicators and data sources. http://www.smartresilience.eu-vri.eu/sites/default/files/publications/SmartResD1.2.pdf

[3] SmartResilience (2016). End-users' challenges, needs and requirements for assessing resilience. http://www.smartresilience.eu-vri.eu/sites/default/files/publications/SmartResD1.3.pdf

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

[5] US Department of Homeland Security (2015). The Future of Smart Cities: Cyber-Physical Infrastructure Risk. https://ics-cert.us-cert.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf