University of Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study program/ Specialization: Risk Management	Spring semester, 20..... Open / Restricted access
Writer: Thale Wilson Losnedal	..... (Writer's signature)
Faculty supervisor: Roger Flage External supervisor(s): Lars Bodsberg	
Thesis title: Assuming a future with "smarter" water supply (more adaptive and more intelligent); chart the risk aspects, capacity to handle deviations and breakdowns, resilience to threats and how this could be measured by the use of resilience indicators, having in mind the new technology (using the method developed/suggested by SINTEF in the SmartResiliene Project)	
Credits (ECTS): 30	
Key words: Critical infrastructure ICT Resilience Resilience indicators Resilience assessment Water supply Case study	Pages: 136..... + enclosure: 19..... Stavanger, 13 June 2017 Date/year

ACKNOWLEDGEMENT

I would like to express my gratitude to my external supervisor Lars Bodsberg at SINTEF for providing me with this topic as well for the support on the way. Furthermore I would like to thank my internal supervisor Roger Flage at the University of Stavanger for useful comments and remarks throughout the process. Also, I like to thank the participants in my surveys and interviews, who have willingly shared their precious time and expertise. These are Jarle Furre (municipality of Stavanger), Karl-Olav Gjerstad (IVAR), Kjetil Birkedal Pedersen (IVAR) and Leif Ydstebø (IVAR and University of Stavanger). In addition, I would like to thank Ole Christian Olsen (Profitbase) for his time and contribution regarding important ICT security measures.

Abstract

Proper functioning of Critical Infrastructures (CIs) is crucial for the welfare of society. However, as for other natural and man-made systems, disruptive events and disasters occur from time to time. Major catastrophes can leave large-scale CI systems devastated, defenseless and non-functioning. Such breakdowns have proven rather rare, but as demonstrated after disasters like Hurricane Katrina in 2005 and the September 11 in 2001, the coping ability is lacking.

As a result of the incidents referred to above, there has been a significant emphasis on understanding the concept of resilience, and how this could be implemented in large-scale infrastructure systems. This thesis explores a new methodology developed by SINTEF that attempts to measure infrastructure resilience by the use of resilience indicators. This is a holistic framework that considers an integrated view on resilience assessment, addressing a broad variety of issues including human factors, sociology, security, economy, etc., and the increased vulnerability due to changing threats. This holistic approach considers both conventional indicators obtained from a top-down manner, and new indicators delivered out of big and open data sources, making it suitable to assess resilience of "smart" critical infrastructure as well. The framework consists of a series of steps/levels that include the identification of area, CIs, threats, phases, issues and indicators.

The ability of the proposed framework in assessing resilience is demonstrated by applying (parts of) the methodology to a case study representing one critical infrastructure - the water supply in the city of Stavanger. The case study identifies relevant threats towards the water supply through interviews and literature reviews. However, for simplicity, only two threats were considered when issues and corresponding indicators were identified. These threats were chosen on the basis of probability of occurrence and associated consequences. Thus, the methodology was applied to a high probability, low consequence kind of threat and a low probability, high consequence kind of threat, presented by water leakages and hacking attack respectively.

Table of content

List of figures

List of tables

Abbreviations

CARL – Current annual real losses
CERT – Computer Emergency Response Team
CI – Critical Infrastructure
CSIRT – Computer Security Incident Response Team
EU-VRi – European Virtual Institute for Integrated Risk Management
ICT – Information & Communication Technology
IDS – Intrusion detection system
IVAR - Interkommunalt vann, avløp og renovasjon
NOU – Norges offentlige utredninger
NSM – Nasjonal sikkerhetsmyndighet
QoS – Quality of Service
RI – Resilience Indicator
RIL – Resilience Level
SCADA - Supervisory Control And Data Acquisition
SCI – Smart Critical Infrastructure
SOP – Standard operating procedure
SRA - Society for Risk Analysis
UARL – Unavoidable annual real losses
WP – Work Package

1 Introduction

1.1 Background

The background for the following work is the modern society`s increased dependency on Information & Communication Technology/Systems (ICT/ICS) and the integrated use of such technology in critical infrastructures. ICT makes new and better (?) solutions possible and the day-to-day life becomes easier by making the critical infrastructures smarter (more adaptive, more intelligent, etc.) in their normal operation and use. In relation to this expanding trend a number of questions are raised among a wide range of scientists and experts within different fields of interest. The concerns vary from the smart critical infrastructures (SCI) resilience towards extreme threats, such as extreme weather disasters and terrorist attacks, to their possible increased vulnerability due to more complex systems. Is it possible to determine resilience indicators in order to anticipate, prepare for, adapt and withstand, respond to, and recover from external and internal threats?

The SmartResilience Project was initiated through the European Virtual Institute for Integrated Risk Management (EU-VRi). They recognize a need for a system of resilience management going beyond the conventional risk management, in order to address the complexities of large integrated systems and the uncertainty of future threats (SmartResilience, The project 2016). The critical infrastructures in a modern society (energy grids, transportation, government, water, etc.) are the systems that determine resilience of the society. The SmartResilience Project aims to provide an innovative "holistic" methodology for assessing resilience that is based on resilience indicators. The project envisages answering the questions and concerns stated above in several steps, presented in their objectives (SmartResilience, The project 2016):

1) By identifying existing suitable indicators for assessing resilience of SCIs.
2) By identifying new smart resilience indicators
3) By developing a new resilience assessment methodology
4) By developing a SCI Dashboard tool
5) By applying the methodology and tools developed in 8 case studies. The SCIs considered deal with energy, transportation, health, and water.

SmartResilience is expected to significantly improve the resilience of SCIs by providing a uniform and comprehensive methodology of risk and resilient assessment.

The project is structured around seven work packages (WP), where SINTEF is the lead partner for WP 3. In WP 3, the SmartResilience indicators based methodology and an integrated tool (SCI Dashboard) for assessing, predicting and monitoring resilience of SCI are developed (Buhr et al. 2016). With such methodology and its tools, the SmartResilience project attempts to support and enable end users (authorities, operators and owners of critical infrastructures) to better assess the resilience of their respective critical infrastructures and, hence, significantly improve the resilience of the same (Buhr et al. 2016).

In SmartResilience the resilience attributes are based on the definition of resilience used

in the project. The definition of resilience of critical infrastructures is (currently) (Jovanovic et al. 2016):

"Resilience of an infrastructure is the ability to anticipate possible adverse scenarios/events (including the new/emerging ones) representing threats and leading to possible disruptions in operation/functionality of the infrastructure, prepare for them, withstand/absorb their impacts, recover from disruptions caused by them and adapt to the changing conditions."

This definition of resilience will be the basis for the following thesis and work. From this background, chapter 2 comprises relevant theory needed in order to understand and use the method. The different phases and dimensions of resilience, and the relation to the concepts as vulnerability and risk are derived. The methodology developed by SINTEF will be presented in chapter 3. In the fourth chapter a case study related to a specific critical infrastructure will be presented in order to discuss the actions needed to provide a resilient system. In chapter five the case study will be analyzed in relation to the method presented in the third chapter. The discussion in chapter 6 will include, amongst other, a critical review of the methodology, already existing resilience indicators (RI) provided for the chosen critical infrastructure and new RIs suggested by the author of this thesis. Conclusions and final recommendations will be established in the final chapter.

1.2 Objective, scope and limitations

The objective and point of departure for this work is the following:

"Assuming a future with "smarter" water supply (more adaptive and more intelligent); chart the risk aspects, capacity to handle deviations and breakdowns, resilience to threats and how this could be measured by the use of resilience indicators, having in mind the new technology (using the method developed/suggested by SINTEF in the SmartResiliene Project)".

As stated above, the critical infrastructure chosen for further discussion is the drinking water supply, limited to the municipality of Stavanger. Literature reviews and interviews will be performed in order to assess the new technology for making the water supply "smarter". The interview objects will be relevant end-users.

In Stavanger, 99 percent of the citizens are connected with the municipal water supply. Private water supply will not be considered in this thesis.

1.3 Working methodology and approach

For this master thesis a deductive approach is utilized in order to describe and discuss the problem thoroughly, and use the theory and empirical data obtained from interviews and literature study to produce new insights and knowledge. The working methodology is a qualitative approach, which is based on a comprehensive literature review and interviews of relevant people in order to obtain the necessary information enabling the author to answer the objective stated above. The information revealed through this process will give the foundation needed in order to perform a case study

and a following analysis. Through the analysis of the case study, important issues necessary for maintaining a robust and resilient water supply will be identified. These issues will be based on the answers provided by interviewees, vulnerabilities identified through the literature review and subjective proposals provided by the author of this thesis. In order to make these issues measurable, suitable indicators will be utilized. The issues and corresponding resilience indicators obtained will be systemized according to a framework established by SINTEF.

The methodology is suitable in order to gain increased understanding. By analyzing the theory obtained through the literature review and interviews, qualified arguments will be systematically provided. Hopefully, this master thesis will establish a useful supplement to the already well-established conventional risk assessments used today.

2 Theory

The following sub-chapters will provide the reader with relevant and necessary information in order to understand important aspects of critical infrastructures; as the use of ICT systems, interdependencies and cascading effects. Also, the concept of resilience and its relation to risk and vulnerability will be presented, focusing on the SmartResilience understanding.

2.1 Conventional Critical Infrastructures vs. Smart Critical Infrastructures

Infrastructures are man-made, large-scale dynamic systems that work interdependently in order to produce and distribute essential goods (such as water, energy and data) and services (such as transportation, health care and banking) (Zio, 2016). An infrastructure is termed critical if its destruction or incapacity has a significant impact on "vital societal functions, health, safety, security, economic- or social well-being" (EU Commission, 2008 p. 77). A failure in such an infrastructure can be damaging to a single society and its economy, while it could also cause a "domino effect" across boundaries causing failures in multiple infrastructures with the possibility for catastrophic consequences (Zio, 2016).

Critical infrastructures (CI) are diverse by operational context (legal/political/institutional, economic, etc.), and by nature (physical-engineered, organizational or cybernetic) and by environment (geographical, natural). Examples are those providing services of (Zio, 2016):

- Transportation (including rail, roads, waterways and aviation)
- Energy (including generation, transmission, distribution and storage, regarding electricity-, water-, oil- and gas supply).
- Information and telecommunication (including Internet, information systems and fixed and mobile communication and broadcasting).

CIs are designed to function for long periods of time, through maintenance, updating and integration of new technologies (Zio, 2016). An increased capacity is also often required to meet the changing and growing demands. This challenge leads to the need of injecting adaptability and flexibility to the system engineering design, in order to respond to the constantly changing domains of technology, economy, legislation, society and politics, which are determining the profiles of service demand and the corresponding expected performance (Zio, 2016).

The complexity of CIs is reflected by the many components interacting in a network structure. With the increasing use of ICT the ubiquity of digitalization is emerging as a new paradigm which will have a unique impact on the future developments and re-engineering of CIs and on their complicated dependencies (Gheorghe & Schläpfer, 2006). This development leads to the more suitable "Smart Critical Infrastructure" (SCI) referring to the higher degree of complexity due to the integration of ICT. A comparison of conventional critical infrastructures with the SCI is obtained in table 2.1 below (Jovanovic et al., 2016). The table does also provide an overview of characteristics that make an infrastructure smart.

Table 2.1: SCIs in comparison with conventional CIs (Jovanovic et al., 2016).

Infrastructure characteristics	Conventional CI	Smart CI
Stakeholder involvement	Stakeholders are not actively involved in the project design and operation traditional engineering. However, they are often engaged with the aim to create local support for the project.	Extended stakeholders are often required to support the project in addition to an active and ongoing role in the project design and operation.
Engineering approach	Standardization and replication of solutions enables reduced project costs and delivery times.	SCI solutions require a custom made, location-specific design and do not lend themselves to standardization and replication.
Environmental footprint	Often increased environmental footprint due to material and energy intensive processes (manufacturing, distribution, operation)	Often reduced environmental footprint due to the solutions being nature-based and self-regenerating
Susceptibility to external factors	Susceptible to loss of power, mechanical failure of industrial equipment and price volatility	SCI solutions are susceptible to extreme weather, seasonal temperature changes or rainfall and disease and similar
Monitoring and control	Conventional	SCI are complex and living systems that can be monitored and effectively managed by a deep understanding of the key control variables

2.1.1 Information and Communication Technology in CIs

The pervasive use of ICT within other infrastructures provides many benefits that become indispensable for the operation of today's interconnected systems, especially with respect to automation, efficiencies and availability of information (Eusgeld, Nan & Dietz, 2011). However, the fusion of critical infrastructures with ICT has added complexity to an already complex field. ICT is becoming increasingly important as communication within industrial, social and economic systems is becoming increasingly digital. It is, perhaps, the most internationally interconnected infrastructure of today's society, and while physical infrastructures may be hosted locally, transfer of data and storage could take place internationally (Guthrie & Konaris, 2012). From a resilience perspective, while it could offer additional capacity and security of data in the likelihood of local disruption, it can also make local infrastructures vulnerable to entirely different, and not yet considered, natural and human threats.

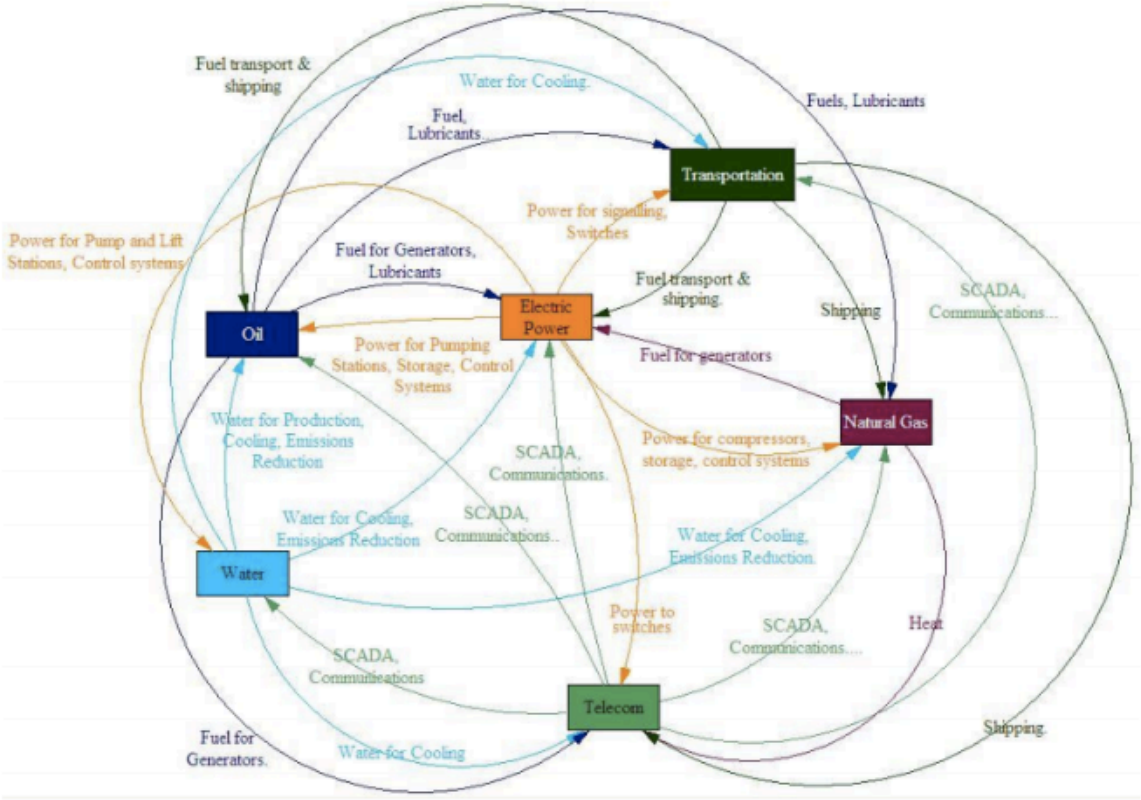

Figure 2.1: Overview of different interdependencies between CI systems (Guthrie & Konaris, 2012).

According to Guthrie & Konaris (2012), and as presented in figure 2.1, ICT (telecom) infrastructure seems to be the most interconnected infrastructure on multiple levels, and its use for making operations more productive and efficient is expected to increase. However, they also stress that the increased reliance on ICT to increase efficiency can cause an emerging risk due to decreased focus on the development of additional physical capacity. This can result in decreased resilience of such systems, which operate closer to full capacity, and are hence vulnerable in the case of ICT failure.

The increased integration of ICT in conventional CI is making operations more efficient and easier to monitor. However, the vulnerability towards cascading failures is expected to increase accordingly. This will be discussed in the following.

2.1.2 Interdependencies and cascading effects

The notion that our modern society's CIs are highly interconnected and mutually dependent in complex ways, both physically and through a host of ICT (or so-called "cyber based systems"), is more than an abstract, theoretical concept (e.g. see figure 2.1) (Rinaldi, Peerenboom & Kelly, 2001). As shown after Hurricane Katrina in 2005, causing an interruption in the supply of crude oil and refined petroleum products due to loss of electric power (O'Rourke, 2007), or the power outage in northern Ohio in 2003 which caused the largest blackout in the history of North America affecting amongst others, water supply, telecommunications and transportation (Guthrie & Konaris, 2012). Hence, what happens to one infrastructure can both directly and indirectly affect other infrastructures, impact large geographic regions, and cause ripples throughout the

national and global economy. In the case of the power outage in Ohio for example, the failure cost $10 billion in losses.

In order to outline the complexity of infrastructure interdependencies the framework developed by Rinaldi et al. (2001) is presented in figure 2.2. This framework enables the characterization of interdependence between infrastructures according to the environmental factor, the nature of their connectivity and the current state of operations.

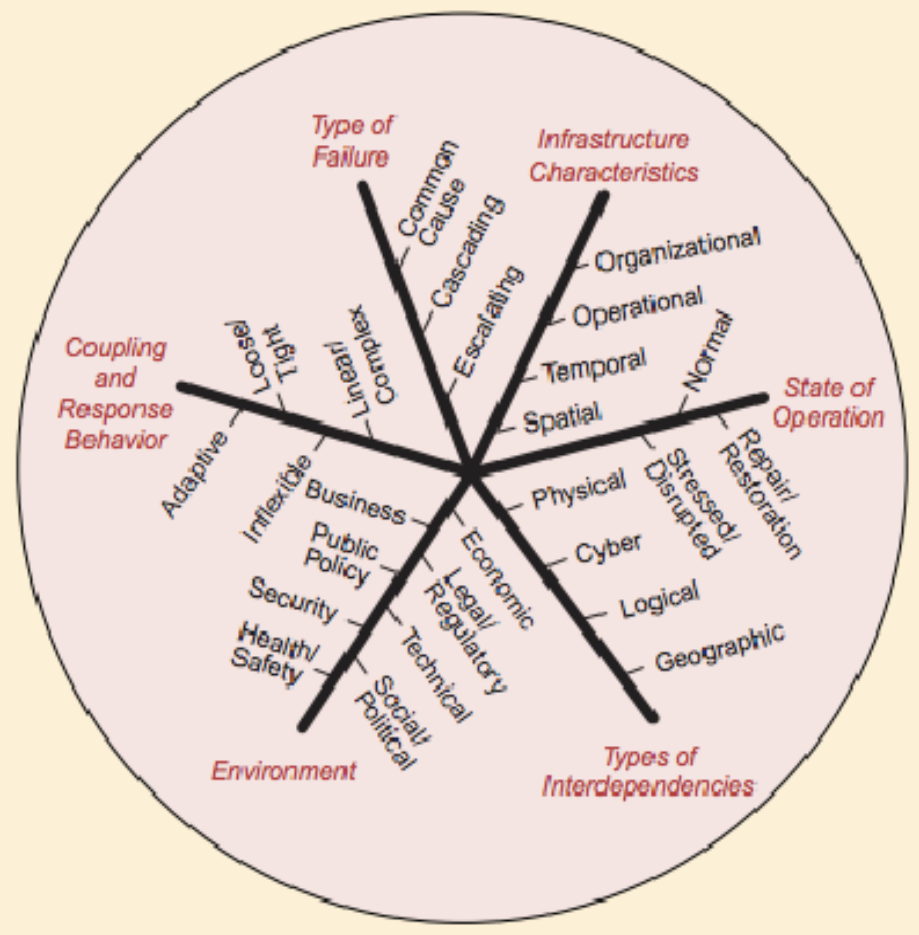

Figure 2.2: Schematic overview of infrastructure interdependencies (Rinaldi et al., 2001).

Three kinds of failures or outages can be found in CI (Rinaldi et al., 2001):

1. Escalating failures: Occur when an existing failure in one infrastructure worsen an independent disturbance of a second infrastructure, generally in the form of increased severity or the time for recovery/restoration of the second failure. For example, a breakdown in an underground metro is significantly worse if a main road is unavailable due to a fire in a tunnel (example from Vatn, Hokstad & Utne, 2012).
2. Cascading failure: Occur when a failure in one infrastructure causes a failure in a second infrastructure. In such situations, there is a functional relationship between two or more infrastructures. For example, water treatment is dependent of electricity in order to function.

3. Common-cause failures: Occur when two or more infrastructures are affected at the same time because of an external and common cause. For example a natural disaster, like an earthquake or a tornado, may cause interruption of electricity, water and telecom at the same time.

These failures consequently show that the infrastructures are subjected to an increased risk from direct connectivity or spatial proximity. Hence, CI seems to have strong interdependencies, of which there are four types (see figure 2.2): physical, cyber, logical and geographic (Rinaldi et al. 2001). These are thoroughly explained by Rinaldi et al. (2001), and will be summarized in the following:

- Physical interdependency arises from a physical linkage between the outputs and inputs of two agents: an output produced or modified by one infrastructure is required by another infrastructure (an input) in order to operate. The state of one infrastructure directly influences the state of the other and vice versa.
- Cyber interdependency is a relatively new phenomenon and is a result of the pervasive computerization and automation of infrastructures. If the state of an infrastructure depends on information transmitted through the information infrastructure, there is a cyber interdependency. Cyber interdependencies are connecting infrastructures to one another by the use of electronic, informational links; the outputs of the information infrastructure are inputs to the other infrastructure, meaning that the "commodity" passing between the infrastructures is information.
- Geographic interdependency occurs when components of multiple infrastructures are in close spatial proximity, meaning that a local environmental event (e.g. explosion or fire) can create changes in all of the infrastructures. The interdependency in these cases is simply due to proximity; the state of one infrastructure is not influencing the state of another.
- Logical interdependency is when the state of one infrastructure depends on the state of another infrastructure via a mechanism that is not physical, cyber or geographic connected. E.g. logical interdependency due to human decisions and actions.

The integration of ICT in physical infrastructures is expected to increase the environmental and economic efficiencies, in addition to improving the overall quality of people's lives. The benefits of the use of ICT and cyber technologies are well recognized, but the risks associated with cyber-physical system integration in urban critical infrastructures' are not well understood due to the lack of competence and fast developing technologies (Duvall, 2016). All the information generated due to this fast development are a part of the generic term "Big data", which, if utilized properly, have the potential to change the way we interact with the world today.

2.1.3 Big data

Over the past two decades, data has increased in a large scale in various fields. The amount of stored information grows four times faster than the world economy, while the computers processing power grows nine times faster (Mayer-Schönberger & Cukier, 2013). Big data is an abstract concept and no rigorous definition of big data exists. In general, "big data shall mean the datasets that could not be perceived, acquired, managed, and processed by traditional IT and software/hardware tools within a

tolerable time" (Chen, Mao & Liu, 2014, p. 173). Hence, the era of big data challenges the way we live and the way we interact with the world. It overturns centuries of established practices and challenges the most basic understanding on how we make decisions and comprehends reality (Mayer-Schönberger & Cukier, 2013).

More and more business activity is digitized and large amounts of digital information exist on virtually any topic of interest to a business. Mobile phones, credit cards, social networks, electronic communication, sensors, GPS, and instrumented machinery all produce big torrents of data as a by-product of their ordinary operations (McAfee, Brynjolfsson, Davenport, Patil & Barton, 2012). At the same time, the steadily declining costs of all the elements of computing (storing, memory capacity, processing, etc) mean that the data-intensive approaches, which previously were expensive, are quickly becoming economical. The benefits of this in relation to productivity growth and ability to cope with new tasks are obvious.

Big data has it strength within predictive analyses, meaning anticipating incidents or human actions. These systems of algorithms perform well because they are constantly fed with lots of data on which to base their predictions. However, such information could easily be misused. When analyzing large amounts of data could single parts of information that, separately, is not sensitive and without reason to protect, be systematized and put together to sensitive information (Nasjonal sikkerhetsmyndighet (NSM), 2015).

2.1.4 Information security (ICT security)

Information is an asset that, in addition to other important business assets, is of great value for an organization and needs to be protected in an appropriate manner. Information security (ICT security) protects information against a wide range of threats in order to ensure business continuity, reduce damage and maximize the profit of investments and possibilities (NS-ISO/EC 17799).

As previously discussed, information can exists in many forms. It can be written on paper, stored electronically, transferred via mail, communicated orally, etc. No matter what form the information has or how the information is communicated or transferred, it should always be reasonable protected. The NS-ISO/EC 17799 standard defines security as measures (politics, routines, procedures, software functions, etc.) to protect the information's confidentiality, integrity and availability:

- Confidentiality: the information should only be available for authorized personnel. Example on loss of confidentiality is if hackers get access to information stored in the operational control system.
- Integrity: make sure the information is accurate, precise and relevant, in other words: cannot be manipulated by unauthorized persons. Example on loss of integrity is if hackers get access to a water treatment facility through the operational control system and changes the dose of chemicals.
- Availability: make sure that authorized personnel have access to the information, and the related services, when needed. Example on loss of availability is if the operators are unable to access the system when demanded.

Information and other support functions, systems and networks are important business assets. Confidentiality, integrity and availability could be crucial in order to maintain competitive advantage, cash flow, profitability, compliance of regulations and public reputation (NS-ISO/EC 17799).

The standard referred to above further explains why information security is necessary due to the increasing number of threats against organizations and their operational control systems identified, e.g. computer fraud, espionage, sabotage, vandalism, fires, and floods. Harmful activities, as propagation of data viruses, cybercrime and blocking of services, are becoming more and more comprehensive, ambitious and sophisticated making them harder to detect and counter act.

Organizations are becoming increasingly dependent on their information- and operational control systems, making them more vulnerable towards security threats. The interdependencies between public and private networks and the sharing of information are making it increasingly difficult to secure access control. Another prominent problem is that many information systems are not designed focusing on safety. The security obtained by the use of technical means is limited and should be supplemented by the use of appropriate management and procedures. This requires careful planning in order to decide what types of safety measures to implement.

In the next chapter, a CI will be presented as an SCI. The use of operational control systems will be discussed and critical aspects with this increased use of ICT will be identified.

2.1.5 Water supply as an SCI

The society expects the water supply to be sufficiently robust in order to deliver enough, high quality drinking water, even if the distribution system is exposed to various types of threats and stress. This also applies if the threats are related to digital vulnerabilities. Hence, safe and secure water supply is increasingly dependent on robust digital systems (NOU 2015:13).

The water supply is today managed and controlled by the use of Supervisory Control And Data Acquisition (SCADA) systems, databases, access control and a number of other ICT based systems. The increasing use of operational control (SCADA systems) within the water supply and water distribution improves the management and monitoring of the system and, hence, increases efficiency, reliability and productivity (NOU 2015:13). Simultaneously, this increased digitalization will make the water sector vulnerable to new and unknown incidents and threats.

2.1.5.1 Use of operational control systems

As already mentioned, the increased dependency on ICT and digital systems makes the CIs more complex and vulnerable to new scenarios and threats. This also applies to the water supply. ICT has become an integrated part of the water supply system and appears as a separate infrastructure in the water infrastructure.

The increased use of operational control systems in the water supply have contributed to more efficient facilities, decreased costs and fewer personnel needed. Furthermore,

this development has led to better services provided, decreased the time needed to respond (if/when incidents occur) and better monitoring of facilities. However, this extensive use of such ICT based systems has increased the vulnerability towards new types of threats. Hence, the operational control systems used to manage and monitor the facilities are said to be one of the most vulnerable aspects of the water supply (NOU 2015:13). Such systems have developed from being closed systems that only worked on certain computers, to be integrated systems that are connected to office support and Internet, making them accessible and easy to manipulate.

Due to the different ICT based solutions implemented; the monitoring of pumps and valves is much easier than before. Bigger facilities, as water treatment plants, are becoming increasingly complicated, and require more advanced control of the different integrated processes, components, signals, etc. included in the water treatment plant and distribution system. Manual operation of the most complicated plants is not possible for long periods of time. By rapid changes in input data, such as changes in the untreated water from the water source (e.g. during periods of flooding), there is a need for sudden changes in the operating conditions. This presumes the ability to control the plant by the use of operational control systems.

As mentioned above, the operational control systems have gone from being closed systems to becoming increasingly integrated with traditional office support systems and Internet connection. Hence, the operational control systems are no longer independent systems, but integrated solutions, making them vulnerable towards computer viruses and hacking-attacks (NOU 2015:13). ICT security of operational control systems used at water treatment facilities and in the following water distribution has, traditionally, not been devoted much attention. The focus of the risk and vulnerability analyses is mostly based on the process engineering issues. There is a lack of knowledge among the water engineers regarding the ICT based operational control systems (NOU 2015:13). The Norwegian Food Safety Authority has also paid little attention towards this issue, and it seems to be little or no competence regarding information security present in the organization (Mattilsynet, 2006). This is also reflected in the available regulations (see "Drikkevannsforskriften").

2.1.5.2 Smart water meters

The aim of increased efficiency and reduction in the number of leakages are important issues to address in the water industry. These desires bring along an increased use of ICT solutions. Smart water meters are in a testing phase in a number of Norwegian water facilities. Smart water-metering technology can enable water utility companies to track the consumers' water usages more accurately, and encourage water-conservation by implementing water-pricing plans. In addition to reduce the water consumption by 10 per cent (due to the consumers awareness about how much water they are using), the consumers will be able to track their water usage in real time and thus be able to take action much earlier in case of leakages (ITU, 2017). The introduction of smart water meters and, hence, a more active control of the operating conditions on the water distribution system will, most likely, claim an increased attention to the ICT- and information security comparing to todays practice.

Uncritical implementation of functionality that link smart water meters closer together with the operational control systems, will lead to increased vulnerability and severe damage potential.

2.2 Resilience

During a risk assessment study, the primary questions normally asked are: (1) what can go wrong, (2) what is the likelihood of such a disruptive scenario, and (3) what are the associated consequences of such a scenario (Kaplan & Garrick, 1981). The main focus of risk management strategies has traditionally been on likelihood reduction of disruptive events and reducing the potential consequences of the events. Thus, risk management strategies often emphasized mitigation measures in the form of protection and prevention (Hosseini, Barker & Ramirez-Marquez, 2016). The main objectives of protection and prevention strategies are to detect the potential threat early and defer the threat long enough for an appropriate response, and to prevent undesired events or consequences from happening, respectively (Hosseini et al., 2016). An example of such a strategy is the well-known CO_2 –reduction measures taken to reduce the emissions and, hence, the potential associated consequences related to a warming climate. However, plenty of recent disruptive events have highlighted that not all undesired events could be prevented. Hurricanes, like Sandy in 2012 and Isabel in 2003, earthquakes and tsunamis are examples of large-scale events causing varying degree of disruptions and emergency responses that influences CIs. Hence, the emphasis placed on resilience of systems through preparedness, response and recovery, are increasing, especially as it relates to complex systems vulnerability to multiple or cascading failures (Park, Seager, Rao, Convertino & Linkov, 2012).

In the following, the concept of resilience will be explained both in a general manner and in relation to the SmartResilience project.

2.2.1 The concept of resilience

The word ”resilience” comes from *resilire, resilio,* Latin for ”bounce” – hence the idea of ”bouncing back”. This denotes a system attribute characterized by the ability to recover from disruptive events and challenges (Alexander, 2013).

The meaning of resilience is contested in different contexts. In general, “resilience is understood to mean the capacity to adapt to changing conditions without catastrophic loss of form or function” (Park et al., 2012). This is a broad definition that applies to different fields such as ecology, materials science, psychology, economics and engineering (Hosseini et al., 2016). The degree of resilience in between the different fields vary, e.g. the human body is more resilient in its ability to preserve through infections than our society’s critical infrastructures are to adverse events (Linkov et al., 2014). Hence, applicable definitions of resilience within different fields are developed in order to cover the complexities and characteristics of the different systems with the general interpretation of resilience used as basis.

As already mentioned, the concept of resilience used in practice varies from application and discipline. In the following, a selection of different understandings of the term is presented. (Zio, 2016):

Resilience can be understood as…

- … the system's ability to reduce the chances of a shock occurring, to absorb the shock if it occurs and to quickly recover after a shock (re-establish normal performance). This is characterized be four properties (robustness, redundancy, resourcefulness, rapidity) and four interrelated dimensions (technical, organizational, social, economic) (Bruneau et al., 2003).
- … a new paradigm for safety engineering, which proactively integrates the accident preventive tasks of anticipation and monitoring, the in-accident tasks of responding and learning, the mitigating tasks of absorbing and the recovery tasks of adaptation and restoration (Hollnagel, Woods & Leveson, 2007).
- … the system's capacity of surviving shocks and aggressions by rebuilding itself and changing its non-essential attributes (Manyena, 2006).
- … the system's ability to withstand severe/major disruptions within acceptable degradation parameters and to recover within an acceptable amount of time, costs and risks (Haimes, 2009).
- … as a structural property, meaning the ability to resist to internal operations and cascading failures, and recover to initial operational state (Alessandri & Filippini, 2012).

Hence, the above definitions and understandings capture more or less the same ideas and could be summarized; in order to be resilient, a system or an organization must have the following four qualities (Steen & Aven, 2011): the ability to (i) respond to both regular and irregular threats in a robust, yet flexible manner, (ii) monitor what is going on (also its own performance), (iii) anticipate opportunities and risks, and (iv) learn from experience. These are often called the "four cornerstones of resilience" as presented in figure 2.3 below (Hollnagel, 2011).

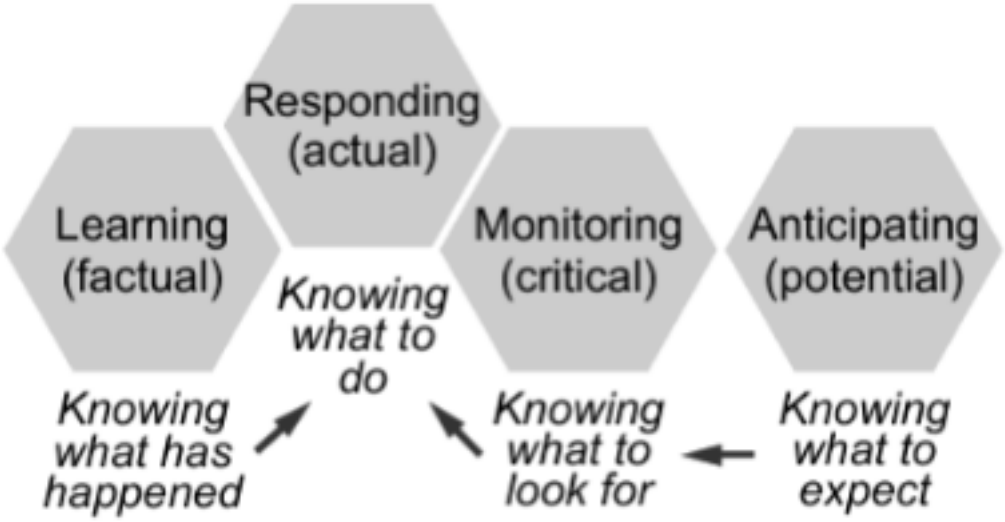

Figure 2.3: The four cornerstones of resilience: i) knowing what to do (how to respond to regular and irregular disruptions and disturbances), ii) knowing what to look for (how to monitor that which is, or can become, a threat in the near term), iii) knowing what to expect (how to anticipate developments, threats and opportunities), and iv) knowing what has happened (learn from experience) (Hollnagel, 2011).

Various methods, models and frameworks for analyzing and measuring resilience have been proposed and presented in the literature. In this thesis, the method developed by SINTEF in the SmartResilience project is to be presented. Concepts like risk and vulnerability in relation to resilience will be discussed based on the resilience definition established in that project.

2.2.2 Development through the SmartResilience project

It seems critical to build resilience into today's complex infrastructures in order to sustain the daily functioning of society and its ability to withstand and recover from natural disasters, epidemics and cyber-threats (Ganin et al., 2016). The objectives of this thesis are limited to critical infrastructures and the definition of resilience used in the SmartResilience project, the following will therefore be based on the terms and concepts relevant in that context.

As mentioned in the introduction, the SmartResilience project is targeting an advanced methodology to analyze the resilience of smart critical infrastructures by the use of (smart) indicators. This approach requires a robust frame regarding terminology and concept, especially when considering the amount and variety of usages of the term, different concepts, including different attributes of resilience, and the different considerations on the relation to other terms such as risk and vulnerability (Vollmer et al., 2016).

The SmartResilience project developed through a comprehensive study of different resilience definitions and concepts from selected organizations/sources (see Vollmer et al., 2016 and Jovanovic et al., 2016)). The preliminary definition of resilience used in the project proposal was adapted from Linkov et al. (2014) and was stated as follows:

"Resilience of an infrastructure is the ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruption".

In this phase of the work, resilience management was understood to go beyond risk management to address the complexities of large integrated systems and the uncertainty of future threats, as it included risk analysis as a central component (this understanding was later changed as explained in the following two chapters) (Vollmer et al., 2016). In the resilience management framework suggested by Linkov et al. (2014), risk analysis quantifies the probability that the system will reach the lowest point of the critical functionality profile. Fig. 2.4 presented below shows this conceptually.

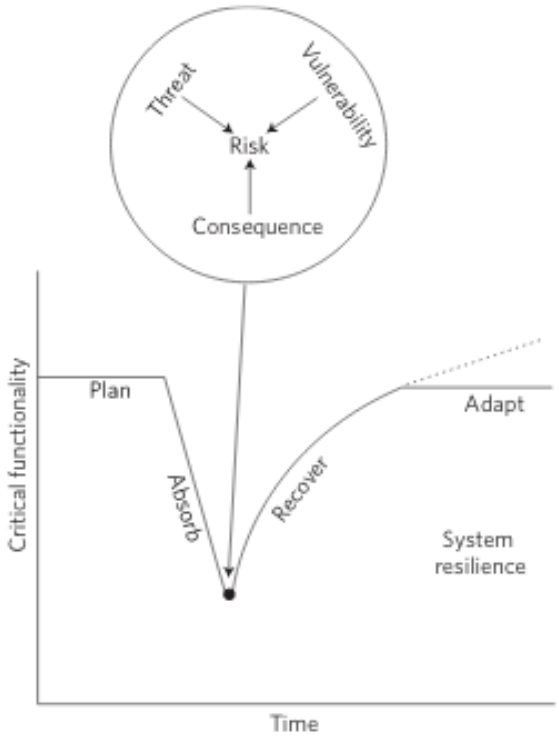

Fig. 2.4: Resilience management framework suggested by Linkov et al. (2014), where risk analysis is included as a central component.

Following this framework, risk management helps the system to prepare and plan for adverse events, while resilience management goes further by integrating the temporal capacity of a system to adsorb (the slope of the absorption curve) and recover (the shape of the recovery curve) from adverse events, and then adapt (see figure 2.4) (Linkov et al., 2014). The dotted line presented in the figure indicates that highly resilient systems can adapt in a way that improve the initial functionality of the system, enhancing the system's resilience to future adverse events and the concept of resilience stresses upon these aspects (Vollmer et al., 2016). The resilience framework suggested by Linkov et al. (2014) was "the point of departure" as the concept and ideas was developed further by the SmartResilience project.

Several scientific disciplines characterize the functionality as a more or less smooth V-curve (as the one presented in figure 2.4) or U-curve. The V-model/curve is a graphical representation suitable in mechanics, when stressing materials. If the stress does not go beyond the yield point, it will return to ("recover") its original state. There is no response phase in such manners, as the time it potentially stays in the stressed state is not important as long as it does not exceed the yield point. The resilience of critical infrastructures on the other hand is more representable by the U-curve due to the relevance of the response phase and the time spent in this phase (Jovanovic et al. 2016). This dimension was not considered in the resilience framework presented by Linkov et al. (2014).

In some disciplines, it tends to be paid particular attention to the curve itself, e.g. the steepness of the absorption curve and/or the slope of the recover curve (Vollmer et al., 2016). In the SmartResilience project, this curve is not of main interest as a measure of resilience. Resilience indicators are used for the purpose of measuring resilience indirectly through the status of the resilience dimensions/phases. In the initial

framework for resilience assessment presented in the SmartResilience project, eight resilience dimensions/phases where identified, including the four resilience dimensions/phases proposed in figure 2.4 above:

- Understand risks
- Anticipate
- Prepare/adapt
- Be aware/attentive
- Absorb
- Respond
- Recover
- Adapt

The focus of the SmartResilience project is smart functionality, not just system functionality; thus, the functionality axis was adjusted accordingly. This, and the eight resilience dimensions/phases are illustrated in figure 2.5.

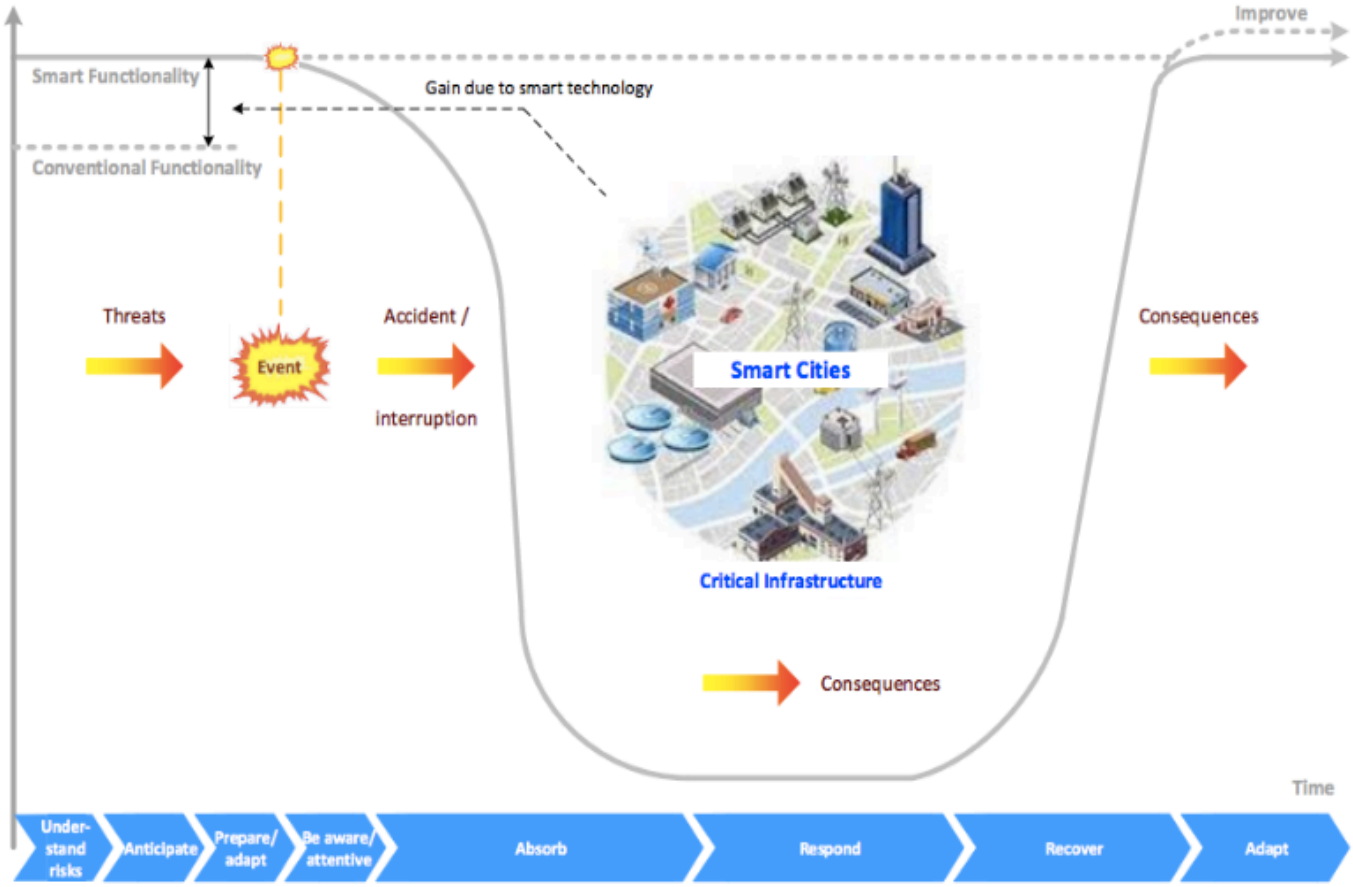

Figure 2.5: System functionality curve for SCI. The functionality axis is adjusted in order to reflect the smart functionality (Vollmer et al., 2016).

Smart critical infrastructures seems to increase the functionality of the system (from conventional to smart functionality as shown in figure 2.5), however, the smart technology may increase the vulnerability of the infrastructure system. This is indicated in the following figure (figure 2.6).

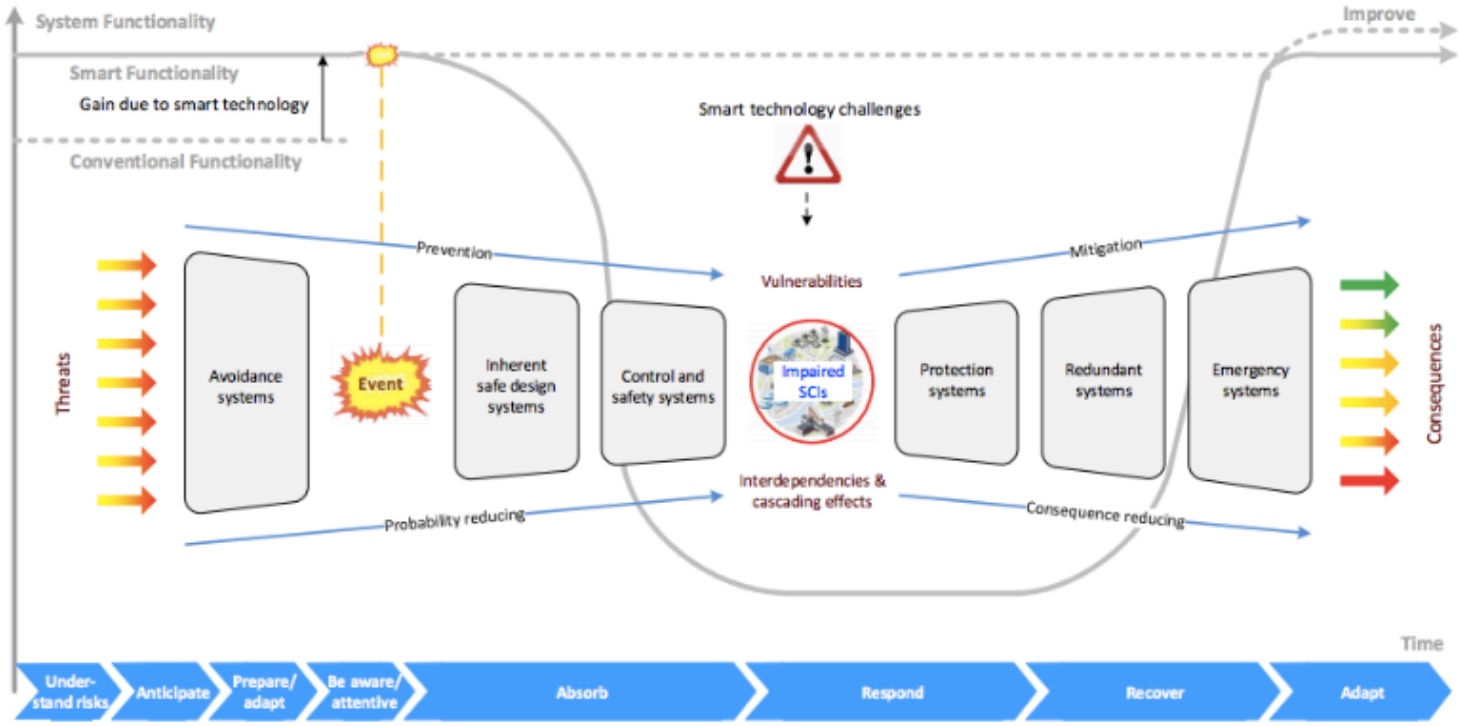

Figure 2.6: Smart functionality and smart technology vulnerabilities (Vollmer et al., 2016).

In addition to providing an overview of smart technology vulnerabilities, figure 2.6 also illustrates general types of barrier systems that contribute to the resilience of the SCIs. The potential increase in vulnerability due to smart technology can be expressed through either increased inclination for failures/events or through less reliable barriers, both leading to reduced functionality (Vollmer et al., 2016).

It is important to notify that the U-curve in figure 2.6 is a simplified conceptual curve that is representative for a single event or disruption affecting a single critical infrastructure and, hence, not representative for smart critical infrastructures (Vollmer et al., 2016). Since many critical infrastructures, particularly the SCIs, are interconnected these systems also need to be resilient with respect to interdependencies and cascading effects. This is indicated in figure 2.6, but as already mentioned, not represented by the single U-curve.

If a second critical infrastructure is affected, the phases will displace compared to the first affected infrastructure, e.g. the respond phase of the second may coincide with the recovery phase of the first. Also, if the functionality axis represents the total functionality (of several CIs), the slope of the absorb curve will not be straight downward, but it will have several "plateaus" on its way to the bottom of the curve (Vollmer et al., 2016). The difficulty of representing this by a single U-curve is one reason why the curve itself will not be used for the measuring of the resilience (Vollmer et al., 2016). Hence, the measurement of resilience is done by the use of indirect resilience indicators measuring the resilience dimensions/phases through "issues", not direct measures of the curve (or slope) of functionality. Meaning, important issues for

the success of the dimension are defined (e.g. the success of response). These issues are in turn measured by indicators. This will be explained further in a later chapter.

A final comment to figure 2.6 provided in the "Initial Framework for Resilience Assessment" by Vollmer et al. (2016) is related to the U-curve's visualization of consequences in terms of loss of functionality. The disruptive event may also lead to other consequences not visualized, like loss of lives. This can be illustrated through an example; in addition to loss of subway transportation for a certain period, a terrorist attack on a subway could lead to immediate deaths and injuries. Only the loss of subway transportation is reflected by the U-curve.

Following the work done by Vollmer et al. (2016) the initial definition of resilience adapted from Linkov et al. (2014) was amended in order to include the importance of risk understanding. Understanding the risks you are facing is obviously a prerequisite for knowing what to do about them. Hence, the updated definition of resilience became:

"Resilience is the ability to understand risks, anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruption".

2.2.2.1 Definition of resilience and its main phases and dimensions

The SmartResilience project does not claim to provide a universal answer to what resilience is and how it can be assessed. In the SmartResilience project, the definition of resilience is supposed to evolve with the work done in the project (literature reviews, interviews, workshops etc.). From the "Initial Framework for Resilience Assessment", the definition of resilience was developed a step further. The main reason for this amendment was the need to bring the definition more in line with the other elements of the overall framework, namely:

- Indicators
- Resilience matrix
- Risk analysis
- Results of the work in "Initial Framework for Resilience Assessment by Vollmer et al. (2016)

In the report and study performed by Jovanovic et al. (2016) over 450 resilience indicators was collected and over 40 case studies and over 20 approaches was analyzed. Hence, a framework where the resilience indicators could be structured and the case studies and approaches could be compared was necessary from the practical point of view. This was also creating the basis for the further work in WP3.

Further, a clear differentiation between the phases and dimensions was established; phases of resilience are related to the timeline i.e. which aspects are important before, during and after an incident. The important aspects identified are to be grouped in relation to "dimensions". Also, the eight phases identified above was updated and reduced to five, in addition five dimensions was suggested; 1) System/physical (technical aspects, physical/technical networks, interconnectedness), 2) Information/data (technical systems dealing with information/data), 3)

Organizational/business (business-related, financial and HR aspects and organizational networks), 4) Societal/political (the broader societal/social context, indirect stakeholders), and 5) Cognitive/decision-making (perception aspects of e.g. threats and vulnerabilities) (Buhr et al., 2016). The final and current proposal of phases of the resilience cycle and the dimensions of resilience results in the SmartResilience "Resilience Matrix" represented in figure 2.7.

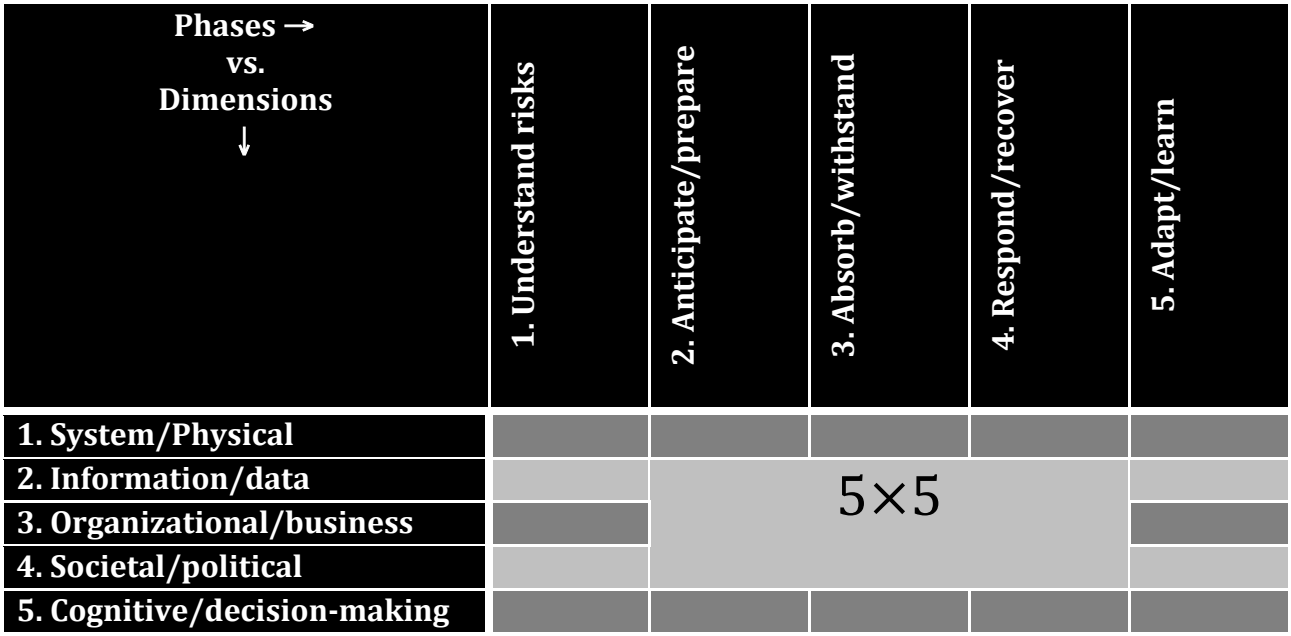

Figure 2.7: The "5 x 5 Resilience Matrix" of SmartResilience project (Jovanovic et al. 2016).

These updates/amendments lead to a new, and currently used, definition of resilience applied in the SmartResilience project (Jovanovic et al. 2016):

"Resilience of an infrastructure is the ability to anticipate possible adverse scenarios/events (including the new/emerging ones) representing threats and leading to possible disruptions in operation/functionality of the infrastructure, prepare for them, withstand/absorb their impacts, recover from disruptions caused by them and adapt to the changing conditions."

2.3 Resilience in relation to vulnerability

There exist different understandings regarding the relation of resilience to vulnerability, mainly due to the variety of definitions of the two terms. In general, and in line with the Society for Risk Analysis (SRA), vulnerability is understood as the degree a system is affected by a risk source or its ability to withstand specific loads (SRA, 2015). Depending on the risk source or event, the vulnerability of an asset or system is normally described by the use of the following metrics (SRA, 2015):

- Expected loss given a failure of a single component/multiple components
- Expected number of fatalities given the occurrence of a specific event
- Expected system loss under conditions of stress

- The probability that the capacity of the system is not able to cover/withstand a specific load
- A probability distribution for the loss given the occurrence of a risk source

(The suitability of these metrics depends on the situation).

Hence, as shown by the metrics presented by SRA, key parameters of vulnerability are seen in the exposure, susceptibility, and coping/adaptive capacity of elements.

Scholarly discussions and debates on resilience and vulnerability have, independently of each other, developed over decades (Fekete, Hufschmidt & Kruse, 2014). Despite this independent development, there are a number of recent works that discuss the two concepts as interlinked, as communicated by Menoni, Molinari, Parker, Ballio & Tapsell (2012). Some conceptualize resilience and vulnerability as positive and negative poles on the same continuum, while others think of them as completely different concepts. The authors following the "two poles" approach, amongst other conclude that vulnerability of a system results from reduced resilience. However, other authors see an overlap between the two concepts, assuming that there are many characteristics influencing only the vulnerability or only the resilience of a system, while other characteristics influence both (Vollmer et al. 2016).

The SmartResilience understanding

In the context of the SmartResilience Project the understanding of the relation between vulnerability and resilience follows the overlap approach, due to the partial overlap of the components of resilience (the phases presented in the currently used resilience definition) with the parameters of vulnerability.

2.4 Resilience in relation to risk management

The conventional risk and safety management methods efforts to improve the safety of systems have often been dominated by hindsight. Approaches to risk and safety prediction are developing in an incremental manner, i.e., the well-established and trusted approaches are only changed when they fail and then usually by adding one additional element or factor to account for the unexplained variability (e.g. "human error", "organizational failures", etc) (Woods & Hollnagel, 2006). Conventional risk management considers variability (of any kind) in the system's performance as a threat and something that should be avoided, which results in the use of constraining means such as barriers, rules, procedures and the use of automation (Hollnagel, referred to by Steen & Aven, 2010). In contrast, in resilience engineering performance variability is considered both necessary and normal. Variability is the source of both positive and negative outcomes. As explained by Woods & Hollnagel (2006), safety cannot be obtained by constraining variability in the system's performance, since that would also affect the ability to achieve desired outcomes. The suggested solution is instead to reduce the variability that may lead to negative outcomes and, at the same time, to strengthen the variability that may lead to positive outcomes (Hollnagel, referred to by Steen & Aven, 2010).

In many ways, resilience engineering represents an alternative to conventional risk management approaches (Steen & Aven, 2010). While conventional risk management is based on hindsight knowledge, reporting of failures, and risk assessments calculating

historical data based probabilities in order to avoid (expected) failures (Steen & Aven, 2010), resilience engineering focuses on the systems ability to function under both expected and unexpected conditions (Hollnagel, 2011). The proponents of resilience engineering consider conventional risk assessment methods to be inadequate for present-day systems due to the fact that socio-technical systems are developing continuously, while risk assessment methods are not (Steen & Aven, 2010). Hence, conventional risk assessments are not considered adequate for analyzing socio-technical systems. The conventional approach to risk and safety assumes tractable systems (meaning that the principles of functioning are known, simple descriptions with few details, and that a system is not changing while being described), but this is not a reasonable assumption today (Hollnagel, referred to by Steen & Aven, 2010). Hollnagel et al. (2007) are presenting a comprehensive argumentation to why resilience engineering is a solution in order to satisfy the need for a new method for addressing safety issues related to the fast developing socio-technical systems.

Linkov et al. (2014) do partly follow this argumentation. They argue that resilience, as a property of a system, must be incorporated into system management. Current methods of risk analysis identify the vulnerabilities of specific system components towards an expected adverse event and quantify the loss in system functionality as a consequence of the event occurring. Referring to the argumentation above, subsequent risk management will thus focus on hardening of these specific system components in order to withstand the identified threats to an acceptable level and to prevent overall system failure. Linkov et al. (2014) states that this form of protection is unrealistic for many systems, due to (i) social and technical systems become more and more complex and interconnected making the risk analysis of many individual components cost and time prohibitive and (ii) the uncertainties associated with the vulnerabilities of these systems, combined with the unpredictability of certain threats, challenges our ability to understand and manage them. To address these challenges, Linkov et al. (2014) suggest that "risk analysis should be used where possible to help prepare for and prevent consequences of foreseeable events, but resilience must be built into systems to help them quickly recover and adapt when adverse events do occur". Resilience is, hence, not a substitute for risk management, but a complementary attribute that uses adaptation and mitigation strategies to improve traditional risk management.

According to Hollnagel, referred to by Steen & Aven (2010), for an organization or system to be defined as resilient, it should fulfill the four cornerstones (ref. figure 2.3) of resilience. Conventional risk assessments are not suitable for the use in resilience engineering due to the traditional risk perspective (the main component of risk is probability, and this probability is interpreted as an objective property of the current activity), but other risk perspectives exist (see e.g. Aven & Renn, 2009). Steen & Aven (2010) argues that by replacing probability by uncertainty in the definition of risk, the basic ideas of resilience engineering can be supported. This category of perspectives is referred to as the (A, C, U) risk perspective (Aven & Renn, 2009, Steen & Aven, 2010). In this view, A represent threats (events), C the consequences of A, and U the associated uncertainties related to the occurrence of A and the value of C. Following this perspective, uncertainty replaces probability in the risk definition. Steen & Aven (2010) argues that risk assessments need to see beyond the computed probabilities by describing the more or less "hidden" uncertainties in the background knowledge that the probabilities are based on. This would provide a solution that sees qualitative

aspects as equally important as assigned probability figures. In their article, they present a framework based on this risk perspective that both provides a structure for linking the concepts of risk and resilience, and a conceptual basis for resilience engineering (Steen & Aven, 2010). However, as the risk metrics used in Steen & Aven (2010) are outdated, the updated metrics are presented below (SRA, 2015):

Extended Risk Assessment:

- Identification of initiating events A
- Cause analysis
- Vulnerability analysis expressing vulnerability (C', Q, K | A)
- Resilience analysis expressing resilience (C', Q, K | any A, including new types of A)
- Risk description and characterization)

Here, C' is some specific consequences, Q a measure of uncertainty associated with C' (e.g. probability), and K the background knowledge that supports C' and Q.

The four cornerstones for obtaining a resilient system seems to be better supported by a (A, C, U) type of perspective compared to a traditional perspective (see the Discussion by Steen & Aven, 2010).

Resilience is increasingly considered as a capacity of CI. The Realising European ReSILiencE for Critical INfraStructure (RESILENS) project (May 2015 – April 2018) will develop a European Resilience Management Guideline to assist in the application of resilience to critical infrastructure. As already discussed, different perspectives on resilience and risk management can be identified. In this context the RESILENS project have presented an overview of four different "perspectives" on risk and resilience as currently practiced by CI sectors; see table 2.2, below (Suter, referred to by Clarke et al., 2015). The table below summarizes the most common perspectives on the relation between resilience and risk management. The ones presented above can be recognized.

Table 2.2: Overview of different perspectives on resilience and risk management, together with related comments provided by the RESILENS project (Clarke et al., 2015).

Perspective	Resilience as…	Definition	RESILENS comments
1	A goal of risk management	Many documents describe resilience as the overarching goal of protection policies and risk management as the method to achieve this goal. Resilience replaces or complements the concept of protection, which was previously defined as the goal of risk management activities.	Understands resilience as the outcome of risk management. This perspective is the traditional, normative approach to risk and resilience within CI's, and thus one that is easily integrated into existing policies. It is, however, challenged by the complexity, the uncertainty related to unpredictable events, as well as the interdependency of sectors and thus the cascading effects of impacts.
2	A part of risk management	Resilience is understood as a part of risk management. Activities to strengthen resilience are needed in order to deal with the so-called "remaining risks", i.e. risks that have not been identified or underestimated and are not been identified or underestimated and are this not covered by appropriate protection (preventive) measures.	This perspective views resilience as part of existing risk management approaches and brings together probabilistic analysis with coping strategies. The resilience of a system is about having sufficient capacity to address any residual risks. Within this perspective, however, resilience is difficult to define. It is suggested that it is still somewhat normative and could stifle innovation or more transformational change.

3	An extension of risk management	This transitionary perspective recognizes the importance of risk management to CI operation, but proposes that these practices need to be extended to encompass resilience practice that integrates social and organizational factors, as well as building capacity to change.	This perspective has been formulated for the RESILENS project and recognizes that while risk assessment is fundamental to CI practice at present, that there is a requirement to extend this process to consider resilience as part of a more dynamic system that includes social, technical and organizational factors.
4	An alternative to risk management	Challenges the traditional methods of risk management and promotes resilience as a new way of dealing with risks in a complex environment. It is argued that a probabilistic risk analysis is not an adequate approach for socio-technical systems that are confronted with non-linear and dynamic risks and are themselves characterized by a high degree of complexity. Instead of preventing risks and protecting the status quo, such systems should enhance their resilience by increasing their adaptive capacities.	Resilience is presented as a transformative alternative to risk management. It is based on the principle that probabilistic risk analysis is inadequate for the complex, non-linear and dynamic, socio-technical nature of today's challenges, and that probabilistic approaches will always fail to assess the risks of "The Black Swan" appropriately. This perspective, however, is slippery and underdeveloped, but advocates redundancy, flexibility and self-organization rather than risk assessment. It is further suggested that in a resilient society, there should be few CI's. This perspective presents a challenge to CI approaches and is unlikely to be widely accepted.

The SmartResilience understanding

The SmartResilience understanding of resilience in relation to risk management sits somewhere between the third and fourth perspective (from table 2.2). They argue: "on the one hand, resilience does not comprise everything of what risk management covers, but on the other hand also cannot replace risk management, since e.g. risk analysis is seen as important basis for resilience, however not included in resilience" (Vollmer et al., 2016).

2.5 Resilience indicators

One of the four cornerstones of Resilience Engineering is monitoring. Measurement of the processes is an essential part of any organization. Every organization has one or more metrics that are used to judge whether the levels of performance, safety, etc. in the organization are acceptable or not. The problem with common metrics used to day is that they rely on events happened in the past (e.g. the number or rate of accidents or injuries over some period of time, the time between events, etc.) (Wreathall, 2011). They measure the absence, rather than the presence of safety. Such measures are of little use in preparing for foreseen and unforeseen adversity or in managing the proactive processes in order to achieve safe and efficient performance.

The adage, "You can't manage what you don't measure" is a well-known and established phrase, applicable for different kinds of organizations (Wreathall, 2011). Resilience of a system is referring to a quality (rather than a quantity) to something that the system does rather than to something that the system has. Due to this, managing resilience can be seen as a kind of process control (Hollnagel, 2011). A resilient system must be able to monitor its own performance as well as changes in the environment. By the use of monitoring, the system becomes able to address possible near-term threats and opportunities before they become reality.

The aspect of reality – also termed the theoretical variable – may be resilience issues, risk factors, etc. These cannot be measured directly, thus an operational definition of the factor/issue that represents the theoretical variable is needed (Jovanovic et al., 2016). This operational variable is what is denoted an indicator. This is shown in figure 2.8 below. The figure also illustrates that there may be a need for several indicators in order to represent one factor or issue. The indicator are typically described by the use of numbers, ratios, scores, or similar. This type of specification/operationalization is necessary in order to provide suitable indicators.

There are both leading and lagging indicators, where leading indicators seems to be of particular interest (Øien, Utne & Herrera, 2011). Leading indicators can be used as valid precursors for changes and events that are about to happen (Hollnagel, 2015). However, the main difficulty related to leading indicators is that the interpretation requires an articulated description/model of how the system functions. In the absence of such descriptions or models, leading indicators are defined by association or spurious correlations (Hollnagel, 2015). This is why most systems seem to rely on lagging indicators, such as accident statistics. The dilemma of lagging indicators, however, is that while the likelihood of success increases the smaller the lag is, the validity/certainty of the indicator increases the longer the lag (or sampling period) is (Hollnagel, 2015).

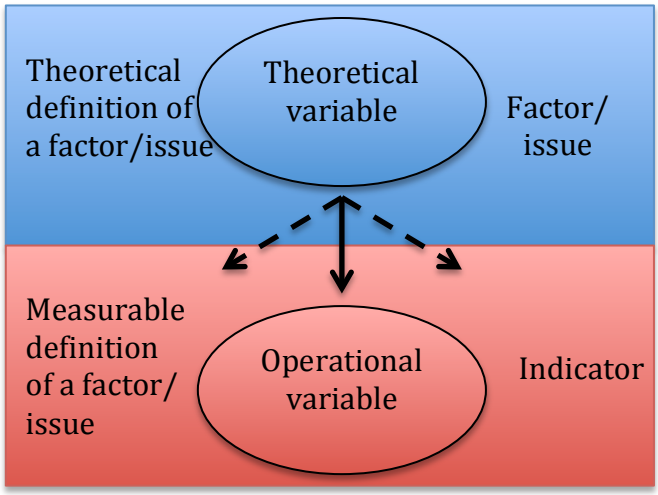

Figure 2.8: General measurement model. The factors, issues, etc. what is desired to measure, and the indicators used to measure the facotrs/issues, are two different things (Jovanovic et al., 2016, p. 40).

2.6 SmartResilience: Indicators for Smart Critical Infrastructures

In the SmartResilience project, indicators are considered as important for measurement of resilience. The definition of an indicator applied in the project is as follows (Øien, referred to by Jovancovic et al., 2016, p. 40):

"An indicator is a measurable/operational variable that can be used to describe the condition of a broader phenomenon or aspect of reality"

The following information is obtained from the third chapter in the report provided by Jovanovic et al. (2016), thus references is only stated if there are exceptions.
In SmartResilience, focusing on resilience, the dimensions and phases included in the current definition of resilience are the "aspects" supposed to be measured; however, the dimensions are not measured directly. First, important issues for the success during phases of resilience, e.g. the success of response, needs to be defined. These issues are in turn measured by indicators. The issues (and the corresponding indicators) may also be grouped in a set of dimension (the five dimensions presented in the "Resilience Matrix, ref. figure 2.7).

When resilience is measured and assessed, it is crucial to capture the most important resilience abilities (through phases, dimensions and issue). The indicators can never be better than the relevance/suitability/representativeness of the phases, dimensions and issues supposed to be measured.

Two different approaches for obtaining indicators are used in the SmartResilience project. The first is a top-down approach where the indicators are identified by asking domain experts certain questions related to status of the issue and level of performance of the corresponding resilience dimension. The second is a bottom-up approach where both existing and new potentially relevant indicators are collected through data mining, e.g. using big data or open data sources. Relevant conventional indicators identified by

the top-down approach should cover most/all relevant issues, meaning that the indicators from big data or open data sources will be additional, and hence, especially useful for capturing smart technology issues that supplements the conventional indicators. This means that not every issue and every dimension are dependent on indicators provided from big data or open data sources. This makes it possible to assign resilience levels for both SCIs and other critical infrastructures that are not especially advanced with respect to the use of smart technologies.

2.6.1 Indicators requirements

To obtain valid indicators is a challenge, especially when considering the leading indicators providing early warnings. Quantitative measures that are individually valid and collectively have adequate coverage could be difficult to obtain due to complex underlying causes and contributing factors (Bodsberg et al., 2017, pp. vii).

High reliability and validity are scientific requirements; however, there are also several non-scientific requirements to indicators. In the SmartResilience project, the following requirements are stated (Bodsberg et al., 2017, pp. vii):

The indicators should be:

- clear,
- realistic,
- measurable,
- tangible,
- standardized,
- harmonized an performing

Ideally, evaluation of indicators should be made on the basis of both scientific and non-scientific requirements. However, it is impossible to fulfill all. This is why it is beneficial to include users in the identification, evaluation and selection of indicators. It will always be a matter of trade-off between competing properties/requirements. When this trade-off is made by the users, a beneficial ownership towards the selected indicators will be established (Bodsberg et al., 2017, pp. viii).

It is of great importance to be able to distinguish between “issues” and “indicators”. As help in the work with defining good issues and indicators, a short guideline is provided in appendix 1. These guidelines are the same as given in Bodsberg et al. (2017, pp. xvii).
.

3 Resilience assessment methodology (SINTEF)

It is of common understanding that guidelines and frameworks for resilience are particularly important for areas of ICT security and related CIs, e.g. "smart infrastructures". As already mentioned, in addition to providing more and more possibilities to make critical infrastructures "smarter", information technology also creates more risks and vulnerabilities. The SmartResilience project makes an attempt to combine a common framework for resilience with the need to adapt this framework to new technology related risks and opportunities (Jovanovic, Schmid & Klimek, 2015). The basic idea for the developed approach is that as modern CIs increases their "smartness", the amount of available data is increasing accordingly and, hence, providing the possibility to measure resilience by using big and open data indicators.

The method proposal developed by SINTEF should be able to demonstrate that a set of common and thoroughly validated indicators could be applied to CIs in order to assess the resilience level by the use of a scale approach, and furthermore make it possible to develop a resilience level based on summations of the various indicators. The method should cover all attributes of resilience for SCIs (Øien et al., 2017a). The resilience attributes in the SmartResilience project are covered in the definition of resilience used in the project, as presented in the last section of sub-chapter 2.2.2.1, and explicitly given by the five phases in the resilience matrix (figure 2.7).

The assessment methodology presented in the following does not have specific end-users in mind, it should rather be a generic approach that is adaptable to different users and which proactively target the needs and requirements of public bodies (Øien et al., 2017a). However, the example provided is based on the drinking water supply in Stavanger.

3.1 Point of departure

Several resilience assessment approaches using indicators exists. Some of them were presented in the literature review performed by Jovanovic et al. (2016). The approaches found most relevant, and furthermore used as references for the SmartResilience project are shortly presented in the following:

- ANL/Argonne method:
  In order to enhance the resilience of CIs it is necessary to determine the ability of the system to withstand specific threats and to return to normal operations after degradation. Thus, a methodology for assessing resilience requires comprehensive considerations of all part of CI systems – from threats to consequences. The method must further generate reproducible results that can support decision-making in risk management, response to disasters, and business continuity (Fisher et al., 2010). Having in mind these issues, a comprehensive methodology that uses uniform and consistent data to develop a resilience index (RI) was developed. The RI is derived from three categories: i) robustness, ii) resourcefulness and iii) recovery and ranges from 0 (low resilience) to 100 (high resilience). The RI compares the level of resilience at CIs and guides prioritization of limited resources for improving resilience (Fisher et

al., 2010). The ANL/Argonne method for assessing a RI is structured in five levels, for providing indicators on the lowest level. A similar hierarchy is used in the SmartResilience project for assessing resilience levels.

- Leading Indicators of Organizational Health (LIOH):
  The LIOH method is a method based on contributions from the users of the indicators. The users take part in workshops and define their own issues (general and nuclear power plant specific) for each of the seven identified themes (1. Management commitment, 2. Awareness of safety performance, 3. Preparedness for problems, 4. Flexibility built in for responding to problems, 5. Just culture (to promote reporting of errors and failures), 6. Learning culture (to promote fixing of problems), and 7. Transparency (visibility of safety performance)), and for each issue they define indicators (Øien, Massaiu, Tinmannsvik & Størseth, 2010). There are no predefined examples of issues or candidate indicators in place prior to the workshops. The LIOH method uses three distinct terms for the levels in their method structure (from top to bottom). These are themes, issues, and indicators, respectively.

- Resilience Early Warning Indicator (REWI):
  The REWI method consists of eight contributing success factors (CSFs) being attributes of resilience. There is a set of issues, for each CSF, contributing to the fulfillment of the goals of the CSF. There is only one level of issues (denoted general issues) for which indicators are developed. A literature review and an empirical study on successful recovery of high-risk incidents was the basis for the CSFs development (Øien et al., 2010). The general issues and proposed candidate indicators were developed based on a number of workshops with scientists covering various fields including engineering, psychology, organizational theory and human factors. These predefined sets of general issues and candidate indicators are first of all a foundation for the triggering of suitable indicators, but at the same time it forces the participants to assess the a priori set of general issues and candidate indicators. Thus, it counteracts the tendency during workshops to identify random "indicators of the day" (Øien et al., 2010). The REWI method uses three levels in the method structure (from top to bottom). These are CSFs, issues, and indicators, respectively.

3.2 Method development

The resilience attributes in SmartResilience are the five resilience phases – Understand risk, Anticipate/prepare, Absorb/withstand, Respond/recover and Adapt/learn – corresponding to the CSFs and themes in REWI and LIOH, respectively. The issues (the factors, functions/tasks that are important in order to be resilient against a given threat for a specific CI) that are important for each of these phases are identified, and indicators to measure those issues are developed (Øien et al., 2017a). Thus, the three lowest levels in the SmartResilience structure are phases, issues and indicators. Furthermore, the issues and the corresponding indicators are structured according to the five dimensions – system/physical, information/data, organizational/business, societal/political and cognitive/decision-making. The five phases and dimensions form the Resilience Matrix illustrated in figure 2.7 above. It is to be noticed that the dimensions are only used for structuring the issues and indicators, and to support the

identification of issues. It is the phases, which are important. It is neither necessary to fill every cell in the matrix with issues and corresponding indicators. The cells themselves have no part in the calculations of the resilience levels (Øien et al., 2017a).

3.2.1 Levels of assessment

The overall structure of the resilience assessment methodology in the SmartResilience project consists of six levels. In addition to the three lower levels mentioned above (i.e. phases, issues and indicators), three more levels are included. Starting from the top, the first level is the area level, e.g. a city. The second level consists of the critical infrastructures, and the third level deals with the threats. This six level structure of the resilience assessment methodology is illustrated in figure 3.1 below.

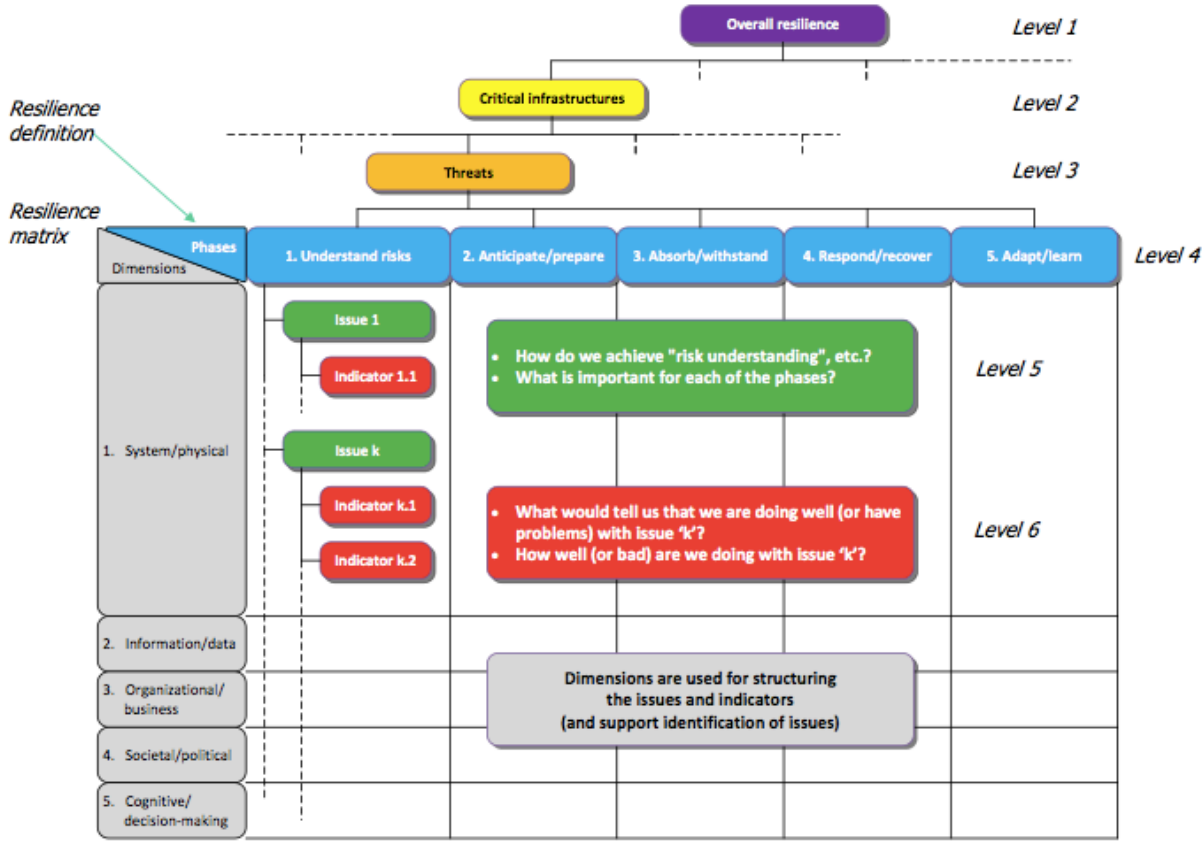

Figure 3.1: The six level structure of the resilience assessment methodology in SmartResilience. The phases, issues and indicators represent level 4, 5 and 6 respectively (Øien et al., 2017a).

The methodology is kept simple, transparent and as easily understandable as possible. This is due to the users basis or knowledge regarding resilience or risk. The users performing resilience assessments of their area/city, CIs and/or specific threats are not assumed to be resilience or risk experts. That all models are simplifications of the real world are a well established understanding, hence it will always be a balance between having a model that is easy to use/understand and transparent on one hand, and being sufficiently realistic on the other hand (Øien et al., 2017a).

Within the six level structure, three specific features are treated. These features are related to how to deal with the ICT infrastructure as an overarching infrastructure, how to deal with interdependencies, interactions and cascading effects, and finally, how to deal with the potential vulnerability and opportunities of smart features that are increasingly introduced in CIs. The solutions are indicated in figure 3.2 illustrating the overall structure of the SmartResilience methodology.

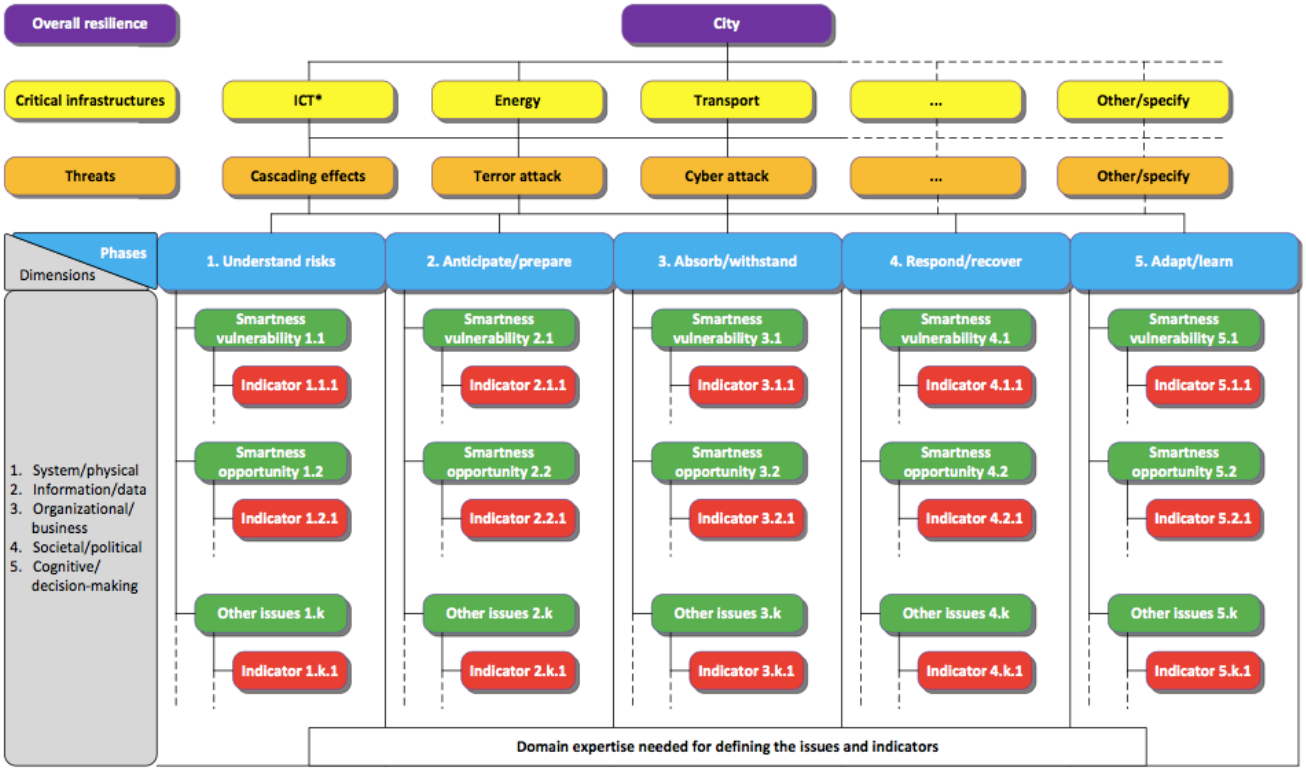

Figure 3.2: Overall structure of the SmartResilience methodology (Øien et al., 2017a).

As the ICT infrastructure could potentially affect the other CIs, this needs to be explicitly considered as a potential issue when issues are defined in the resilience matrix for the ICT infrastructure. In figure 3.2 this is indicated by adding an asterisk, i.e. ICT*. Cascading effects are treated as a specific type of threat. Other types of interdependencies and interactions could also be treated as specific threats, and added as indicated by "others/specify" in figure 3.2. The "smartness" of CIs is explicitly included as smartness vulnerability and smartness opportunity on issue level. These are default issues, for which the relevance should be considered for all phases in all types of assessments (Øien et al., 2017a).

Øien et al. (2017a) points out two important general features of the methodology - its flexibility and its demand for domain expertise in "configuring" the resilience model for a specific area/city or CI. It is up to each city/area using the methodology to decide which infrastructures that are critical for them and which threats they consider relevant. This is indicated with "others/specify" both for CIs and threats in figure 3.2. The domain experts are needed in order to define important issues and how these issues can be measured by identifying the indicators.

3.2.2 Method steps

The SmartResilience method is carried out through ten steps as presented in table 3.1. Starting from level 1, the steps are as follows (Øien et al., 2017a):

Table 3.1: Method steps, from "the top of the model". Steps 1-6 are considerations and selections related to the six levels of the methodology, whereas steps 7-10 are related to the calculations and the utilization of the results (Øien et al., 2017a).

Step #	
1	Select the area (Level 1)
2	Select the relevant CIs for the area (Level 2)
3	Select relevant threats for each CI (Level 3)
4	Consider each phase (in the resilience matrix) for each threat (Level 4)
5	Define the issues within each phase (structured according to the dimensions) (Level 5).
6	Search for the appropriate indicators for each issue (Level 6)
7	The range of values (best and worst values) for each indicator are to be determined
8	Assign values to the indicators
9	Perform the calculations (scores and resilience levels (RILs))
10	Utilize the results for e.g comparison/trending, benchmarking and "stress-testing".

The methodology can be performed at different levels, assessing resilience for an entire city, a specific area, for one or more CIs, and for one ore more threats. The term "scenario" is used for a specific selection of CIs and threats for a given city or area.

There are no limitations to what format the indicators provided could have. They can be yes/no questions, percentages, numbers, rates, etc. Their real values, no matter of what type, are collected and transformed to a score/rating on a scale from 1 (worst) to 5 (best). This is taken care of in the seventh step (ref. table 3.1). The score is obtained by interpolation between the best and worst values (Øien et al., 2017a).

When the resilience assessment is performed, the indicators' real values are entered into the calculations (Step 8), and the average weighted scores of the indicator scores can determine the issue scores. Thus, both issues and indicators are measured using scores on a scale from 1 to 5 (Øien et al., 2017a). It is also possible to have "knock out indicators" which could overrule the effect of the other indicators.

Further, for level 4 – the phases – the scores are transformed to a scale from 0 to 10, providing resilience levels (RILs). This scale is kept unchanged through the rest of the structure i.e. for threats (level 3), CIs (level 2) and areas (level 1).

Øien et al. (2017a) explains the reasoning behind the selected scales and argue that a scale from 1 to 5 for indicators and issues are sufficiently broad, especially in cases of lack of data where expert judgments are needed to provide scores for the indicators (or directly for the issues) (e.g. using a scale: very low – low – medium – high – very high). It is not easy for experts to distinguish between scores on a very fine graded scale. A main

goal of the SmartResilience project is to develop a method for assessing resilience levels using a scale approach. The resilience levels are provided from a scale ranging from 0 to 10, which is considered to provide sufficient differentiation, and at the same time not give the illusion of an extremely accurate assessment.

In the ninth step, the calculation is performed in a database and the assessment for the given case/scenario is saved. The results obtained, which in the case of a full scope assessment for a smart city covers all the relevant CIs, all relevant threats for each CI, all five phases of the resilience cycle, all relevant issues for each phase and all indicators for measuring the issues, can be utilized in various ways (Step 10) e.g. comparing previous assessments, providing trends, and showing progressions. Since the calculation is performed on all levels, it is possible to identify the reason for an increase/decrease in resilience compared to the previous assessment. Another use is to benchmark against other areas or CIs. This provides an opportunity to learn from others. It is also possible to assess the resilience of a city/area or a CI by imposing a set of threats (including defined challenges such as interactions and cascading effects), i.e. stress testing the resilience ability of the chosen area/city/CI, and compare the results with a predefined criteria (Øien et al., 2017a).

3.3 Example of calculations

The following calculations are representing a simplified example, inspired by Øien et al. (2017a), of how the method assesses the RILs. The water supply in Stavanger will be the point of departure for the calculations, i.e. the area (level 1) is Stavanger and the SCI (level 2) is the water supply. The threat, level 3, considered is a cyber attack. All of the phases (level 4) are included in the calculations. However, only the second phase (anticipate/prepare) is represented by a calculated value. The remaining phases are assigned random values for this simplified example. To be able to anticipate and prepare for a cyber attack, two issues (level 5) are included in this example; redundancy (functions/systems) and cyber entrance control. The indicators used (level 6) are related to the performance of these issues.

The basic rules for the calculations will be summarized below.

Summary of the basic rules for the calculations:

1. The indicators' real values, no matter of what type, are collected and transformed to a score on a scale from 1 (worst) to 5 (best). The score is obtained by interpolation between the best and worst values.
2. The average weighted scores of the indicator scores determine the issue scores (on a scale from 1 to 5).
3. "Knock out indicators" could overrule the effect of other indicators (i.e. not averaging away the effect on issue level).
4. The issue scores are transformed to a scale from 0 to 10, providing RILs for each of the phases. This scale is kept unchanged through the rest of the structure, i.e. for threats, critical infrastructures and areas.

3.3.1 Level 6 – Indicators

Table 3.2 below provides an overview of four indicators relevant for assessing the resilience of the second phase (anticipate/prepare). The example shows the flexibility of

the method in terms of what format the indicators may have (yes/no, hours, numbers, etc). A short explanation of the chosen indicators (in this simplified example) are provided in the following:

- Redundant telecom lines are recommended in order to secure a robust communication system. This is indicated by either yes of no.
- For the water work to provide a safe and reliable water supply they are dependent on a predictable operational control systems. By having more than one telecom supplier will make the communication system more resilient as if one breaks down, another network is present to keep the operation going. This is indicated by number of suppliers.
- To secure a sufficiently safe cyber entrance control password requirements are needed. A personal password should be a requirement. This is indicated by yes or no.
- Procedures related to frequency of password renewal should be implemented. E.g. renewal of password once a year. This is indicated by average number of years between each password renewal.

Table 3.2: Indicator values

Level 6: Indicators	
Indicator name	**Real value**
Redundant telecom lines	Y
No. of telecom suppliers	2
Personal password	y
Frequency of password renewal	2

3.3.2 Level 5 – Issues

The issues are given scores based on the indicator scores. This requires a conversion of the real values of the indicators scores. This is illustrated in table 3.3 below.

Table 3.3: The conversion of the indicator scores provides the issue scores and the final weighted score of issues.

Level 5: Issue scores for resilience phase 2 (Anticipate/prepare)								Weights of issues	Weighted score for issues
Issue 1 (Dimension - System/physical)	**Indicator name**	**Real value**	**Best value (score = 5)**	**Worst value (score = 1)**	**Score**	**Weight**	**Weighted score**		
Redundancy (functions/systems)	Redundant telecom lines	y	5	1	5	0,5	2,5		
	No. of telecom suppliers	2	2	1	5	0,5	2,5		
						Issue score	5	0,5	2,5
Issue 2 (Dimension - Information/data)									
Cyber entrance control	Personal password	y	5	1	5	0,5	2,5		
	Frequency of password renewal	2	1	5	4	0,5	2		
						Issue score	4,5	0,5	2,25

In this example redundant telecom lines are in place, thus the best value of the score was obtained. It is recommended to have two telecom suppliers to sustain a redundant and robust system, which is also the case for this example, resulting in the highest score possible for this issue. Personal passwords are recommended when accessing the operational control systems. The frequency of password renewal is in this example intended to be once a year, but as indicated in the table above this is only done every other year, resulting in a reduced score for cyber entrance control issue.

The real values ”y” and ”n” are converted to scores on the scale 1 to 5. It is, however, not given that “y” is the desired outcome (e.g. when smell is used as an indicator for water quality, “n” is the desired outcome). Hence, the best and worst value (5 or 1 respectively) is dependent on the desired outcome.

Individual weights can be assigned to the indicators; however, it is recommended to use equal weights (due to simplicity and transparency) (Øien et al., 2017a). Thus, with two indicators the weight is 0,5 for each. For each indicator, weighted scores are calculated (indicator score * weight of indicator), and the issue score is calculated as the sum of the weighted indicator scores. In addition, weights can be assigned to the issues representing a phase (in this example: phase 2 –Anticipate/prepare). Also here it is recommended to use equal weights (Øien et al., 2017a).

The sum of weighted scores for the issues are obtained by adding the individual weighted issue scores, hence the total score for phase 2 is 4,75. This score is brought to the next level.

3.3.3 Level 4 – Phases

As summarized above, the resilience levels are represented by a scale from 0 to 10. In table 3.4 below the total scores for each phase is provided. The only calculated value in this example is the score for phase 2 (Anticipate/prepare). The other values are random, for the sake of the calculations (indicated by the red color).

Table 3.4: The resilience levels for each phase in the resilience matrix. Level 4 is the stage at which the scores (scale 1 to 5) are transformed to RILs on a scale from 0-10.

Level 4: Resilience level for phases					
	Understand risk	Anticipate/ prepare	Absorb/with-stand	Respond/ recover	Adapt/learn
System/physical Information/data Organizational/business Societal/political Cognitive/decision-making	5	4,75	4.5	3	3
Resilience level for phase (Transformed value)	10	9	9	5	5

The transformation from scores (scale 1 to 5) into RILs (scale 0 to 10) are obtained by the equation RIL = (Score – 1)*2,5 and using standard round-off rules (Øien et al., 2017a). E.g. for anticipate/prepare: (4,75 – 1)*2,5 = 3,75*2,5 = 9,4 ≈ 9.

3.3.4 Level 3 – Threats

The RIL values for each phase, calculated above, are transferred to table 3.5 below.

Table 3.5: The resilience level for a cyber attack is calculated by summing the weighted scores for each phase.

Level 3: Resilience level for relevant threat (cyber attack)						
	Understand Risk	Anticipate/ prepare	Absorb/with-stand	Respond/ recover	Adapt/learn	
Resilience level for phase (Transformed value)	10	9	9	5	5	
Weights for each phase	0,2	0,2	0,2	0,2	0,2	
Resilience level for cyber attack	2	2	2	1	1	8

As discussed previously, individual weights for each phase could be assigned, however, it is recommended to use equal weights as shown in table 3.5. The resilience level for the given threat is obtained as the sum of weighted resilience levels for the phases, here RIL = 8. Also at this level standard round-off rules are used.

3.3.5 Level 2 – Smart Critical Infrastructure

The resilience levels for each identified threat are entered into a table covering all relevant threats for the water supply. Table 3.6 below illustrates the idea. It is possible to assign weights to the various threats considered relevant for the given SCI. In this example, only one threat is considered. Therefore, the resilience level of the SCI is equal to the resilience level of the threat, i.e. RIL = 8. In general, however, the resilience level for the considered SCI is obtained as the sum of weighted resilience levels for the threats. It is, as usual, recommended to use equal weights in the case of more than one threat (due to simplicity and transparency).

Table 3.6: Resilience level for the CI water supply.

Level 2: Resilience level for the CI water supply			
Threat	**Weights**	**Resilience level for relevant threats**	
Terrorist attacks			
Cyber-attacks	1	8	
Climate changes			
Internal conflicts			
Technical failures			
Other/specify			
Total number of relevant threats	1		
Resilience level for the CI water supply	8		

3.3.6 Level 1 – Smart city or area

The resilience level for Stavanger is obtained as the sum of weighted resilience levels for the SCIs. This is illustrated in table 3.7 below. However, this is out of the scope of this thesis, but illustrated in order to understand the principle of the model and the opportunities it provides.

Table 3.7: The resilience level for Stavanger. The resilience level for each CI is weighted and summarized.

Level 1: Resilience level for Stavanger		
Critical infrastructures	**Weights**	**Resilience level for relevant Cis**
Energy		
Healthcare		
Water	1	8
Transport		
Production		
Financial		
Other/specify		
Total number of relevant CIs	1	
Resilience level for Stavanger	8	

4 Case-study: Drinking water supply in Stavanger

Through this case study and the following analysis, the risk aspects and vulnerabilities of the water supply in Stavanger will be identified. Also the capacity to handle deviations from normal operation will be addressed. Furthermore, resilience indicators covering relevant issues and factors will be suggested.

4.1 Introduction and current practice

A well-functioning water supply is, and always has been, essential for all urban development and for the creation of an efficient society. Water is an important resource that should cover domestic consumption and industrial water needs. In Stavanger, treated drinking water is supplied from IVAR (Interkommunalt vann, avløp og renovasjon) to the municipality, which in turn distributes water to the consumers.

Stavanger municipality includes the mainland and the inhabited islands Hundvåg/Buøy, Austre Åmøy, Langøy, Bjørnøy, Roaldsøy, Ormøy, Steinsøy, Engøy, Sølyst, Grasholmen, Vassøy, Lindøy, Hellesøy and Kalvøy. Figure 4.1 illustrates the extent.

Figure 4.1: Map of the municipality of Stavanger (Stavanger kommune, 2013).

In 2010, "Hovedplan for vannforsyning, vannmiljø og avløp 2011-2022" (main plan for water and aquatic environment 2011-2022) was passed and signed by the mayor (at the time) in Stavanger and the head of the political secretariat (Stavanger kommune, 2010a). This provides an overview of current practice and future plans regarding water quality, capacity, needs, etc. The following summary is based on this document if nothing else is stated.

For the people living in Stavanger, high quality drinking water straight from the tap is expected. The total annual water consumption in Stavanger (including loss from leakage) was 21 million m^3 (in 2010), which corresponds to approximately 470 liters per citizen per twenty-four hours. Comparing to other critical infrastructures, the water supply is in an overall good state and provides plenty of supply (capacity), good quality, high reliability and good risk knowledge/understanding. In order to take care of and address these concerns the following goals are set to maintain a secure and proper water distribution and supply (Stavanger kommune, 2010a):

- The drinking water must be hygienically reassuring, approved according to the drinking water regulations and satisfy all quality requirements.
- A good useable water quality, without prominent taste, smell or color, where acidity (pH) and color are used as indicators.
- Unplanned interruptions should not exceed 0,5 hours per citizen per year and in total (i.e. including planned shutdowns and flush-related interruptions) less than 1 hour per citizen per year.
- A good alternative water supply should be available and able to handle a 3 months use of drinking water.
- "Water not accounted for" (leakage indicator) should be less than 20% of the total volume delivered.

It is also important, in addition to the bullet points mentioned above, that the people living in and close to Stavanger is satisfied with the services provided in relation to the water supply. The strategies developed in order to achieve this involve both IVAR and the municipality.

The supplied drinking water is surface water from Stølsvatn and Romsvatn in Bjerkreim municipality and Storevatn in Gjesdal municipality. Langevatn in Gjesdal and Hagavatn in HÅ are working as reserve water sources (see fig. 4.2).

Figure 4.2: Main water supply infrastructure provided by IVAR (Stavanger kommune, 2010a).

The water is treated at IVAR's treatment facility stationed at Langevatn (Langevatn vannbehandlingsanlegg in figure 4.2). After treatment, the water is transported through two large transmission pipes to an elevated water reservoir in Stavanger which capacity volume is around 24-hours water consumption. The municipality buys the water as it passes the installed water meters close to Stavanger.

In the next section the current status regarding resilience work and assessments will be provided.

4.2 Current status regarding resilience work and assessments

In recent years, a number of threats towards the good established and well-known practice regarding drinking water supply in Stavanger have been identified. The possible threats include among others population growth, climate change (extreme weather events, temperature changes, etc.), leakages and erosion of pipes. The increased number of threats towards the drinking water in Stavanger have been increasingly acknowledged, and resilience of drinking water distribution related to some of the threats are considered in the 11 year plan mentioned above. IVAR on the other hand revised their main plan (see Kjellesvik & Gjerstad, 2011) in 2011 in order to include their long-term development goals, which could be related to resilience[1]: 1) Sustainable capacity – to be able to produce enough water to cover the city's needs, (2) Redundancy – provide water from different water sources when needed and (3) To be able to cope with future changes in raw water quality.

This chapter builds on a summary of interviews made with experts from IVAR and the municipality of Stavanger. The interview questions are provided in appendix 2. In addition to the answers obtained, the "Hovedplan for vannforsyning, vannmiljø og avløp 2011-2022" are used as supplementation. Deviations from this will be stated.

Neither the municipality nor IVAR were familiar with the term "resilience". However, they could very much relate to the term "robustness", which they interpreted to be more or less the same as resilience in this context.

Enough water from IVAR

The facility at Langevatn, operated by IVAR, was initially (in 2004) supposed to/estimated to deliver enough water until 2050. In the main plan issued by the municipality in 2011, the population projections and prognosis on that time showed that the current water supply capacity could be too small already in 2025, based on the increased population growth during the years before. However, in recent years this prognosis has stagnated. This could be just a momentary recession considering a longer perspective (e.g. 10- 20 years), or a prolonged development. According to IVAR, the possible lack in capacity is considered in their future plans and an expansion of the treatment facility at Langevatn has already started (finished in 2018). IVAR is also considering new water reserves in order to cope with increasing population and the need of more capacity (IVAR, 2016). However, due to the temporary stagnation in population growth, the capacity increase is not as urgent as first presumed. In addition to the capacity expansion, the treatment facility will increase the strength and number of hygienic barriers by including ozone-treatment and bio-filtration.

The elevated water reservoir in Stavanger is also under expansion and the transmission lines transporting the water from the treatment facility are under restoration. A brand new transmission line is under consideration, in order to replace the oldest and most vulnerable of the two lines used to day. The new transmission line will follow a different

[1] The term "resilience" is not applied, but the author interpret the established goals to be based on a resilient mindset.

path in order to make the system more robust. These transmission lines are of glass fiber, meaning that they do not corrode.

These measures together will make the system robust and flexible with plenty of capacity when all systems and components are working satisfactory.

Satisfactory water quality

The quality of the water delivered by IVAR fulfills the demands stated in the regulations (Drikkevannsforskriften). The treatment is based on well-established, conventional treatment technologies. IVAR seems to be aware of the possible problems (corrosive water, contaminated water due to pathogens and heavy rainfall, etc.) that could occur and the precautious measures needed are taken. Their main challenge is related to the esthetic quality of the water (no smell, taste or color). In the expansion of the treatment facility at Langevatn, this is taken care of by adding ozone treatment as the first treatment step. Following the ozone treatment, the water flows through a marble filter that makes the water less corrosive by increasing the pH and calcium content (buffer effect against changes in pH). Downstream the marble filter, the bio-filtration (also a barrier newly added to the treatment chain) removes the potentially remaining smell and smallest molecules that could cause bacterial growth. Furthermore, the water passes the UV-lights killing the microorganisms. The last step in the treatment chain is to add chlorine. This is considered a robust process with no requirement of physical supervision. The water flows due to gravity and no pumps are needed. The process goes automatically (retention time, chlorine dosing, etc.). If something goes wrong or stop working, alarms goes off and notifications are sent instantaneously to present or "on duty" personnel. The process could also, in practice, be controlled manually. The water could follow two parallel paths through the treatment process, making the system extra robust if one of the paths stops functioning or maintenance is required.

However, new and better water sources are investigated, considering capacity, smell and temperature. In recent years the quality of the water source used today has deteriorated (higher concentrations of E.coli bacteria (indicator bacteria), higher humus content and increased temperatures), also periods of drought have been experienced. This development is assumed to continue, based on heavy rain and temperature prognosis. IVAR is considering moving the water intake to another water source. The source considered (Birkelandsvannet in Bjerkreim municipality) is bigger and deeper compared to the water used for drinking water today, hence the detention time increases and the temperature is more stable during the year (Kjellesvik & Gjerstad, 2011). Also, due to its depth, Birkelandsvannet will not be especially affected by extreme weather as heavy rain and wind conditions. Thereby, both a functioning hygienic safety barrier in the source itself, and a stable water quality are obtained. This option was considered to costly for imminent future, thus the treatment facility at Langevatn was expanded instead. The expansion included, in addition to the extra treatment steps mentioned above, a back-up reservoir in order to increase the robustness of the facility's delivery potential. Birkelandsvannet is still considered as a possible main drinking source for the future when increased capacity is needed.

The water quality, water flow and water treatment are continuously monitored by the use of different indicators (pH, smell, taste, contaminations, volume of flow, water level,

etc), and water samples are analyzed both before and after treatment. If something differentiates from predefined criteria, alarms go off and personnel get notified.

The city of Stavanger, on the other hand, is stressing that they should become more active in relation to IVAR as their water provider concerning changing of water source due to temperature fluctuations and climate change. Routine checks will be established as well as checks due to complaints (Stavanger Kommune, 2010b).

Safe and reliable water supply from IVAR

The safety is taken care of both through preventive measures; in order to reduce the probability for mistakes, and through a well established emergency preparedness system; in order to reduce the possible consequences of mistakes. The safety is discussed in two "dimensions": security of supply and water quality.

The security of supply is taken care of in all stages through:

- High technical quality and high level of security at the facilities
- High level of expertise throughout the company
- Frequently performed risk assessments and analyses in order to update possible threats and probabilities/consequences.
- A new and better intake at Storevatn was installed in order to improve the flexibility and safety of the source.
- Elevated water reservoirs with reserves that can cover a maximum of 24 hours shut down. This is considered sufficient in order to repair possible damages on the transmission lines. The reservoirs constitute a total volume of 50 000 m^3, which correspond to 24-hours of water supply.
- IVAR provides the possibility to take water from Langevatn, and even Store Stokkavatnet in emergency situations (if Store Stokkavatnet is to be used, a boiling notice needs to be sent out to the consumers, as chlorine is the only treatment step). The probability that Store Stokkavatnet is to be used in the first place, is considered very low.
- The water treatment facility and the distribution system have several parallel lines and ring connections. This makes it possible to disconnect parts of the system under maintenance and repairs if necessary. It is estimated that 75 % of the normal water supply can be maintained for at least 3 month if needed.
- The whole water treatment process and delivery can, in practice, be performed manually if the IT systems should fail. If power outage, the emergency generator unit have enough capacity to last for a considerable amount of time (for exactly how long is confidential).
- IVAR is also providing a regional arrangement regarding emergency water supply. This includes 5 huge tanks (15 000 liters each), 20 smaller tanks (1000 liters each), 4-5000 plastic cans (10 liters each) and access to groundwater sources to fill the tanks if the surface water is impaired.

The estimated capacity of 75% of normal water supply if a longer shut down should occur is a problem, hence it is important to focus on a reduction on the number of leakages. The leakage percentage is currently almost 40%. The goal is to reduce this to less than 20%. Considerable resources have been used on reducing leakages. The

frequency of pipe ruptures are mapped and systematized in relation to pipe material and pipe lifetime. Strategic replacement plans are prepared with regard to replacement rate, area assessments and pipe materials (Stavanger kommune, 2010b). Further focus is placed on following up the measures, installations of more online water meters on the network/distribution system and organization of nightly leakage listening. The population growth in the region makes it necessary with a new review of the emergency preparedness situation in order to assess the consequences of extreme and exceptionally rare events and, thus, the possible increase in the emergency water supply. A consequence may be to use Store Stokkavatnet, which is defined as emergency source (with a boiling notice). This means that the overall risk may be acceptable and that costly measures can be compromised in advantage to renewals of old distribution lines.

The water quality are taken care of through:

- The criteria of at least two hygienic safety barriers through the choice of water source, depth of water intake and disinfection are fulfilled.
- Improvement of the hygienic safety barrier is considered. This consideration involves the choice of a new main drinking water source and/or augmented water treatment[2].
- The security in the transmission system is firstly in the combination of distribution lines, ring mains and reservoirs, in order to maintain the overpressure in the water supply system. Stavanger has a robust system, where even bigger shut downs will normally result in small or no consequences for the consumers.

Safe and reliable water distribution by the municipality

The municipality of Stavanger is responsible for the water distribution to the consumers, meaning that they should deliver sufficient, reliable and high quality water. The threats and scenarios identified, and well known as especially focused on for the water distribution in Stavanger, are contamination in the distribution lines and interruptions in the water supply for long periods of time and over large areas. In order to cope with such unwanted scenarios, emergency preparedness plans and trainings are frequently performed. These plans and rehearsals are executed on the basis of a conventional risk- and vulnerability analysis, which are regularly updated when new threats are identified and if new technology is to be utilized.

The municipality does not consider the network, in it self, constituting the water supply in Stavanger especially vulnerable. The variety of districts is well covered by loop systems, making it easy to sustain the water supply during maintenance or if something should go wrong. Measures have also been taken regarding the areas considered especially vulnerable by building additional supply lines in to the district in order to secure safe water distribution throughout the municipality. However, the condition of the pipes constituting the distribution network is considered a problem. The average age of the water pipes in Stavanger is yet just 34 years, due to the elaboration started in

[2] As mentioned above, these considerations resulted in an expansion of the treatment facility at Langevatn (finished in 2018). However, a new drinking source will be further discussed in order to increase capacity in the future.

the post-war period. Figure 4.3 below shows an overview of the age distribution of Stavanger's water pipes. The water pipes from the post-war period and up to late 1970s is characterized by low quality iron (gray cast iron) and/or bad or no protection towards ne. Today, the distribution of materials constituting the water pipe network is 67 % spheroidal iron, 26 % gray cast iron, 6 % plastic compounds and 1 % other materials. In the main plan for water and aquatic environment 2011-2022, a goal of minimum 1 % renewal of water pipes each year (a total of 12 % during that period) is stated in order to provide a secure and reliable water supply and reduce the number of leakages.
An overview of the water distribution network in Stavanger is presented in appendix 4.

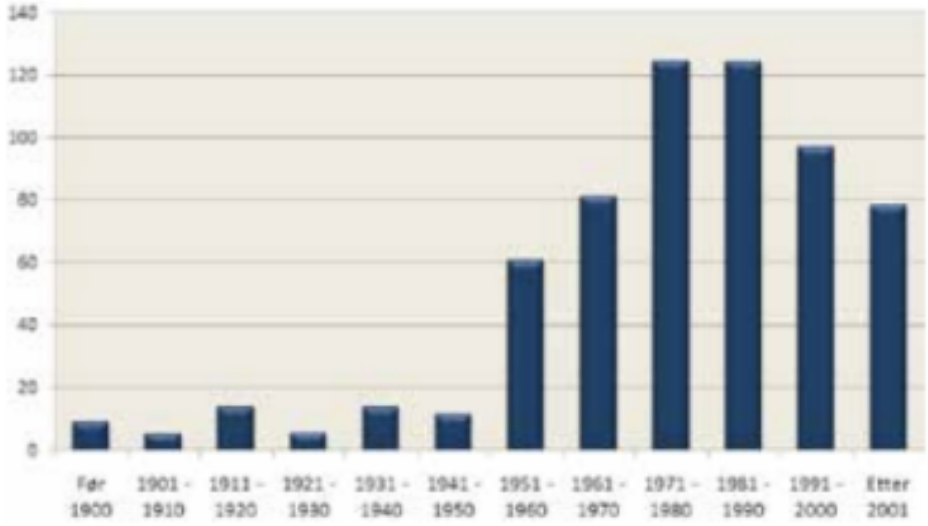

Figure 4.3: Number of kilometers existing water pipeline laid in different periods of time (Stavanger commune, 2010a).

The water consumption is constantly monitored making it easier to detect deviations from normal use. The water consumption could mainly be divided into two categories: 1) real/true water consumption and 2) leakages/waste. The capacity to deliver enough water is not infinite and the leakages are contributing to the increased challenges related to the region's resources. However, through comprehensive leakage control and systematic renovation of the distribution system, the municipality's total water consumption are reduced from 29 mill m^3 in 1981 to 21 mill m^3 in 2010. Figure 4.3 shows an overview of the water consumption the last 40 years.

Figure 4.3: The water consumption presented as number of liters per person per 24 hours. The specific consumption has been relatively stable for the last decade (Stavanger kommune, 2010a).

The age of the distribution pipes are also constantly considered, as old and vulnerable pipes can lead to sudden disruptions. The municipality of Stavanger is actively searching for new ways/new technology to discover corrosion on water pipes.
The emergency preparedness related to "common" disruptions in the water distribution is considered efficient and well established. If a disruption occurs, the localization of the problem, subsequent pipe disconnection and installation of temporary supply lines, and the following repairing, is normally a quick and efficient process (normal operation are restored during hours). The experience and knowledge gained following such disruptions are always considered in order to improve the measures taken and to update the emergency preparedness plan. The reporting of such events also makes it possible to establish trends, and hence, uncover vulnerable areas.

There is an overview in the emergency preparedness plan related to response and procedures to follow for each of the unwanted scenarios and relevant threats identified in the risk- and vulnerability analysis. The training of personnel is crucial in order to sustain the robustness of the water distribution in Stavanger. The risk- and vulnerability analysis and the emergency preparedness plan have so far been satisfying in relation to the municipality's requirements. The threats identified with the possibility of large consequences (terror attack/sabotages, hacking or other disruptions of ICT systems, etc) are included, but no such events have ever happened. Having in mind the challenges and uncertainties related to new technologies, social developments, climate changes, etc in the future, the municipality states that the risk- and vulnerability analysis should be a "living document". The events/threats identified in this analysis are arranged in a risk matrix according to consequences and probabilities.

The municipality is focusing on increased smartness of the water distribution when planning future projects. In this work, they will use the already existing information, which is not properly utilized as the system is today. This information would preferably

be used to reduce the consequences and downtime related to incidents/events. However, this is currently a future matter.

bedreVANN (Better water)

bedreVANN is a great tool for communicating the relationship between the standard of services, investments needs and the development of costs. With bedreVANN, the municipalities and their suppliers can measure their own performance over time and the effects of the measures implemented (bedreVANN.no). The results are summarized in a yearly report covering the following five categories (the weighted percentage in the brackets):

- Hygienically reassuring drinking water (40%)
- Useable water quality (15%)
- Security of supply (15%)
- Alternative water supply (10%)
- Functionality of distribution network (20%)

Each of the five categories listed are weighted differently, corresponding to their importance. The possible outcomes for each category are "good" (4 points in the quality index), "insufficient" (2 points in the quality index) and "bad" (0 points in the quality index), represented by the colors green, yellow and red respectively. The assessment criteria regarding the standard of the water supply is listed below (bedreVANN, 2015, pp.4):

Good: 4 points in the quality index

- Hygienically reassuring: 100 % of the citizens connected to the municipal water supply have hygienically reassuring drinking water. The water supply is protected against pollution of the source and though water treatment, and have proven good hygienic quality.
- Usable water quality: 100 % of the citizens connected to the municipal water supply are provided with drinking water of good usable quality. Meaning, the requirements related to pH and color are fulfilled.
- Security of supply: Unplanned interruptions should not exceed an average of 0,5 hours per citizen per year, and total interruption should be less than an average of 1,0 hour per citizen per year.
- Alternative water supply: 100 % of the citizens, receiving water from waterworks providing more than 1000 people with drinking water, have good supply alternatives available for up to three months.
- Distribution network: Estimated water loss are less than 20 % of the total amount of water produced and delivered to the distribution network.

Bad: 0 points in the quality index

- Hygienically reassuring: More than 10 % of the citizens connected to the municipal water supply (or more than 1000 people) do not have hygienically reassuring drinking water. The protection against pollution of the water source and the treatment of the water are too bad and/or several water samples taken from the distribution network shows intestinal bacteria.

- Usable water quality: More than 25 % of the citizens connected to the municipal drinking water (or more than 5000 people) are provided with bad usable water quality. The requirements related to pH and/or color are generally not met throughout the year.
- Security of supply: Unplanned interruptions are exceeding an average of 1,0 hour per citizen per year.
- Alternative water supply: More than 25 % of the citizens (or more than 5000 people) receiving water from waterworks providing more than 1000 people with drinking water, have no alternative water supply or an alternative water supply of bad quality.
- Distribution network: Less than 0,5 % of the distribution network are renovated yearly (estimated as the average from the last three years) and estimated water loss are over 40 % or the number of network repairs due to leakages are more than 0,10 per km per year.

Insufficient: 2 points in the quality index

- Lies between the criteria for "good" and "bad".

The quality index (KI) is calculated by summing each of the products of the individual weights and scores. The table below shows the current status for the drinking water supply in Stavanger. Top scores in four out of five categories are obtained, resulting in a KI of 3,6 (bedreVANN, 2015, pp. 4).

Table 4.1: The quality index obtained for the drinking water supply in Stavanger is 3,6. This was more or less as expected due to the potential for improvement already identified related to the distribution network.

Assessment category	Code	Weight (%)	Points in the quality index according to assessment				
			Good	Insufficient	Bad	No documentation required	Missing data
			4	2	0	4	0
Hygienically reassuring drinking water	H	40 %					
Useable water quality	B	15 %					
Security of supply	S	15 %					
Alternative water supply	A	10 %					
Functionality of distribution network	L	20 %					
Quality index (KI):	H 40%*4 + B 15%*4 + S 15%*4 + A 10%*4 + L 20%*2 = 3,6						

4.3 The "smartness" of the water supply in Stavanger

In order to address the "smartness" of the water supply and water distribution in Stavanger the whole process/chain from the water source to the tap needs to be analyzed. This process is supervised and monitored by the use of operational control systems and connected sensors.

For IVAR to be able to operate the facility as efficient and reliable as possible, the whole treatment process is remotely monitored and distance-controlled by the use of computer-based operational control systems. These systems control the pumps and valves, and monitor the water quality, water level in the reservoir, the detention times, chlorine doses, flow and pressure. Such systems also make it possible for operators to

control the treatment process by the use of laptops and telecom outside working hours. In addition to the water treatment, the operational control systems also controls the security at the facility, e.g. cameras, access, etc.

As for IVAR, the municipality also relies on its operational control system for safe and reliable water distribution. The operational control system controls the pressure increase stations (10 in total around the municipality) (see appendix 4), the stop and start up of water before and after maintenance and leakage, monitor the water usage throughout the municipality (55 water meters are situated on strategic points on the distribution network) and the safety valves securing the distribution systems towards backlash. The operational control system is considered crucial in order to maintain an efficient water distribution. However, the valves could also be turned on and of manually, but this is not an optimal solution.

The municipality relies on IVAR to deliver safe, hygienic and drinkable water. However, the municipality is manually monitoring the bacteria content/contamination by the use of weekly measurements. Water samples are taken from five different places on the distribution network each week. The spots where the samples are taken, rotates and are not systematic. If the water is judged to be hygienically not drinkable, either by IVAR or by the municipality, text messages with warnings are automatically sent out to people's mobile phones.

The use of water meters in private homes is voluntary and not very common in Stavanger, meaning that most of the leakages are located by manual leakage detection during the night or when the leak is obvious due to water on the surface (e.g. flooding due to bigger pipe disruptions) or pressure drop (detected by monitoring). The desire of increased efficiency and reduction in number of leakages leads to increased use of ICT. The municipality is currently considering a new technology provided by Powel AS (2017). This new technology analyzes different sources of data (e.g. hydraulic models, operational control systems and population figures and statistics). The system further assigns each water pipe a risk-based grade considering the conditions, making the replacement of pipes a more efficient process. The condition of the pipes is based on estimated probabilities regarding pipe disruptions and corresponding consequences. This solution, however, is of future concern and not a part of the scope of this thesis.

4.4 Security of the Operational control systems

In the water industry in general little attention have traditionally been given to the security related to the operational control systems, despite the fact that they are more or less dependent on a robust and reliable ICT solutions. For operational control systems to stay robust and reliable they should be designed in a way that makes it difficult to put them completely out of function, and if cessation of the system it should still be possible to deliver a satisfying demand. In recent years, the focus on ICT security has increased for the water supply in Stavanger. The following information is based on interviews with both IVAR and the municipality. Due to the criticality related to the operational control systems the discussion will be on a general and "advisory" level. IVAR and the municipality will not be presented separately in order to provide some sort of anonymity. The interviewee representing IVAR was the operational control

system responsible at the wastewater department, as he was the one available. However, he ensured that the practice was the same as for drinking water department. The interview questions are given in appendix 3.

The operational control systems should be custom-made in order to fit the needs and requirements for the relevant organization. All access passwords should be personal and linked to individual users, hence "default" passwords should not be used. The operational control system and the office network should be two separate networks connected through a firewall. The remote access procedures were different for the two organizations, however the focus on security seemed more or less the same. Both were focusing on multi-authentication with personal passwords in all steps. The systems were regularly tested towards known attacks. This was especially considered important by one of the organizations.

The reporting routines regarding logging of interruptions (e.g. interruptions in communication between servers, nodes, etc.) and breakdowns were established in order to develop trends and tendencies. However, the two does not equally focus upon reporting of spam-mails not detected by the spam filter. One of the organizations has established routines for this purpose as well, but for the other this seemed more personnel dependent. Measurable solutions towards unusual account activities on both the office network and the operational control system are provided. There is also a focus on risk awareness among employees regarding the possible threats towards the ICT systems, and it is recommended to provide a yearly e-learning course for this purpose. Traffic against not open gates should be monitored, either by the organization itself or by the supplier of the telecom system.

The access to the systems and to the various critical functions is restricted in the sense that only the personnel needing access have access. Due to the different roles IVAR and the municipality provide in the water supply chain, there is some differentiation on what is possible to control from home. The municipality seemed to have more restrictions regarding remote control and home based possibilities on their systems than IVAR. At IVAR, there were no restrictions in what was possible to control from home, but it was segmented in order to take care of the safety related to the most critical parts of the treatment system. The responsible for the operational control system at IVAR works as the administrator and can provide access to not-available functions to the operators if needed. Employees who quit or change work internally will have access removed. This should be followed up if this is not already done.

Extra safety measures should be established regarding critical functions as electricity and telecom system. This could be provided by redundant telecom lines delivered by different suppliers in order to sustain the traffic. Also, a separate network that is administrative should be in place, meaning that if the external firewall breaks down it will still be possible to operate from the facility. Emergency electricity generators should be present in case of power outage.

The operational control system and the Internet is recommended to not be connected, meaning that is should not be possible to reach the Internet through the control system network. The firewalls should be regularly revised. As both the municipality and IVAR are big organizations with different departments, it is recommended to separate the

networks as much as possible to not be influenced by other networks weaknesses. E.g. as IVAR consist of both a wastewater department and a drinking water department, it should not be possible to take a "short cut" between the two.

A risk- and vulnerability analysis and corresponding emergency preparedness plans are established by both organizations. Actually, IVAR also performed an ICT adapted risk- and vulnerability analysis last year as a measure towards a more robust and resilient system. This analysis was based on the template suggested and recommended by Johnsen & Røstum (2015). In this analysis a value assessment related to secure confidentiality, integrity and availability was discussed.

It is believed that both IVAR and the municipality has taken their decisions and evaluations related to ICT security measures on the basis of the identified risks related to a possible disturbance/attack towards the operational control systems. It is also believed that these measures are considered sufficient for the current situation. It is, however, recommended to stay updated on the constant development happening in the hacking-world, considering more advance methods used for gaining access and causing harm.

5 Analysis of case-study

In the following sub-chapters the case study presented above will be analyzed and vulnerabilities will be identified, revealing uncovered needs. In order to make the water supply more resilient towards future scenarios and threats, resilience indicators will be suggested and discussed in accordance with the resilience matrix presented in figure 2.7.

5.1 Vulnerabilities identified

As mentioned previously, IVAR provides the treatment of the drinking water while the municipality distributes the drinking water out to the consumers. This is a continuous process, which is expected to be reliable and robust for both planned and unplanned interruptions. The risk- and vulnerability analysis and the emergency preparedness plans are anticipated to prevent big disasters and water outages for long period of times, and so far this have worked sufficiently. However, because of the escalation of generated data from the water industry, climate changes and in general a more interdependent society, the increasing amount of threats towards the water supply are expected to require new and/or modified methodologies in order to assess risks and robustness.

Vulnerabilities identified for both IVAR and the municipality will be separately discussed in the following.

5.1.1 IVAR

The currently used drinking water source is relatively shallow, which implies vulnerability towards changes in the water quality (e.g. periods of intensive rain, high temperatures during summer). Higher temperatures are expected to increase the humus content and worsen microbial quality and intensive periods of rain could stir up the mud on the bottom of the lake. Also, periods of drought could occur (as experienced in 2010), making the already shallow water source shallower. The expansion of the treatment facility at Langevatn will be able to cope with these challenges; however, this is not optimal considering the potentially increased use of chlorine and wear and tear on equipment. In addition to the hygienic challenges related to the current drinking source, the capacity is also considered a problem. The water delivered by IVAR has increased by almost 10 mill m^3 during the last decade (Kjellesvik & Gjerstad, 2011), and population prognosis shows that the capacity limit could be reached in a shorter time frame than first considered. The elaboration of a new water source will take time (years), thus an immediate clarification regarding the new source considered is expected. Birkelandsvannet will not be affected by heavy rain or warm periods, and the capacity required will be covered.

Neither the currently used drinking water source nor the new source considered is/will be particularly exposed to natural phenomenon as earthquakes and hurricanes. Strokes of lightning could occur, but measures to prevent severe consequences are taken.

The expanded treatment facility is based on conventional and well-established treatment processes. The system is robust, considering the parallel treatment lines and the number of hygienic barriers. However, the process is dependent on electricity and

the operational control system to function optimally. If electricity should fail, there are emergency generators present at the facility. If the operational control system should break down the process must be controlled manually. This is in theory possible, but has never been tested for longer periods of time, making the facility vulnerable towards the telecommunication system provided. However, due to the high lying water source, the water flows through the treatment steps due to gravity, hence no pumping are needed (except for the adding of chlorine). The water could actually be delivered and will be hygienically reassuring when treated only by UV lights (if for example the rest of the treatment steps stops working), but this assumes that the water source works as a hygienic barrier in it self. This is only periodically the case due to the increased E.coli and humus content registered in recent years.

The operational control systems, which controls and monitors the treatment process, are accessible for "on-duty" personnel after working hours. It is known that such systems can be manipulated, if the security mechanisms are not good enough, which means that the systems in themself can pose a security risk caused by failure in the water supply or contaminations. This influences the integrity and the confidentiality of the systems. However, at IVAR the security awareness towards the operational control system has increased in recent years by, among other, regularly revision of the firewalls and segmentation of the different networks. In 2016, a risk and vulnerability analysis especially adapted to ICT was performed, reflecting an increased consciousness regarding the dependency related to ICT solutions in the water industry. It could be discussable that the operational control system responsible was not aware of the traffic against not open gates, and relied on the suppliers of the networks to give warnings if there were deviations from normal activities. The suppliers have many clients to follow-up, meaning that there is a chance that threats could be overlooked. Also the ICT-manager at IVAR was supposed to keep an overview of such abnormal traffic, however, how thorough this is followed-up and how the communication is between the supplier, the ICT-manager and the operational control system responsible is not known.

Emergency preparedness plans adapted to ICT was not established following the risk and vulnerability analysis regarding the ICT solutions performed in 2016. This could represent a problem, as the organization gets very dependent on a limited number of ICT-competent personnel if something unexpected should occur. However, IVAR arrange yearly e-learning courses in order to increase the knowledge regarding vulnerabilities, attitude towards ICT security, training and risk communication (spam mails, strength of passwords, etc.). The focus seems to be on maintaining the functionality, and less on what to do if the functionality fails.

5.1.2 Stavanger Municipality

The distribution network (considering its layout and coverage ratio) was not considered especially vulnerable in it self. However, it is discussable that a simplistic map is exposed and easily found online with no restrictions (e.g. log-in password or request) required what so ever. It is not a detailed map showing the size and dimensions of the water pipes, but it is both possible and easy to designate critical areas, pumping stations and particularly vulnerable districts (e.g. not covered with ring mains) for people with bad intentions.

The risk and vulnerability analysis performed for the water/wastewater department is not available online, but a relatively new summary report covering the overall risk and vulnerability analysis for the municipality of Stavanger is available (see Stavanger kommune, 2013). This summary report is showing a brief overview of undesired events and threats related to different social factors and infrastructures, including the water supply. The risk matrices showing the estimated probabilities and the corresponding consequences towards life, health and social stability are especially considered relevant for the water supply. This report also focuses on the interdependency between a break down in the ICT infrastructure and a failure in the electricity supply, and how this affects other critical infrastructures. Even though this report is not particularly performed in order to assess risk and vulnerabilities towards the drinking water supply in Stavanger, it contributes to awareness about the possible consequences and cascading effects if a long lasting interruption in the drinking water should occur. This information could be planting thoughts in the wrong people heads, however the provided information is very general and could be found elsewhere.

In addition to the vulnerability related to having the distribution network layout available online, the condition of the water pipes constituting this network are not satisfying. Due to poor quality iron and bad protection against corrosion, the leakage rate is very high. This was also focused upon in the main plan for water and aquatic environment 2011-2022 (Stavanger kommune, 2010a). However, after this was paid more attention to the water consumption have decreased from 470 liters per citizen per twenty-four hours in 2010 till 371 liters per citizen per twenty-four hours in 2016 (Stavanger kommune, 2016). This decrease is due to better work on following up the leakage plans. The replacement rate of old water pipes was 0,81 % in 2016 (Stavanger kommune, 2016). Even though the goal is 1 % per year, this was an improvement compared to the year before, when the rate was 66 % (Stavanger kommune, 2015). The problem by not reaching the goal of 1 % replacement rate yearly is the resulting "replacement lag". This may lead to a slower leakage reduction (over a longer period of time) than originally estimated.

From the annual report provided by Stavanger kommune (2016), some statistics are provided showing trends and developments from the five previous years. It seems to be an over all positive and stable development in the water supply in Stavanger. However, one of the factors did deviate considerable from the predefined goal and from the years before. It was reported 99 pipe ruptures in 2016, compared to the predefined goal of less than 65 and 60 the year before. These numbers are misleading because the increase in ruptures are due to an increase in the amount of resources applied in leak detection, hence more leakages are detected. The numbers are not comparable.

Even though the municipality is depending on IVAR to deliver high quality drinking water, water samples are taken and tested regularly by the municipality (as explained in the case study). These water samples are vulnerable towards human mistakes and "carelessness" as they are taken manually.

The municipality of Stavanger does also have twenty-four hours available personnel with access to the operational control system from private computers. However, only a few authorized personnel provides the possibility to actual "do something" when logged

on to the system. The focus on security awareness regarding their ICT systems have also increased lately, and measures are considered.

5.2 Threats considered

The severity of the threats relevant for the drinking water supply in Stavanger is ranging from low probability - high consequences kind of threats (terror attacks, hacking) to high probability – low consequences kind of threats (e.g. small pipe ruptures, minor leakages, esthetic water quality, etc.). The latter is dealt with on a day-to-day basis, and the preparedness routines towards these kinds of threats are well established and implemented throughout the infrastructure. However, in recent years the focus on the more severe threats, like terror attacks, extreme weather events and hacking of the ICT systems, has increased. These threats have the potential to cause serious consequences towards the drinking water supply in Stavanger.

Due to confidentiality reasons and to the limited timeframe given for a master thesis, the threats considered for the following representation of the SmartResilience method are general threats relevant for drinking water supply anywhere, however both of the chosen threats were mentioned during the interviews. The method is flexible, meaning that more specific threats towards the drinking water supply in Stavanger could also be included when assessing the overall resilience level. The threats chosen for the following assessment are:

- Water leakage in the distribution network
- Hacker attack against the operational control systems

The threats considered are covering both of the extreme points of the severity range presented above. The threat chosen to represent the potential of severe consequences (e.g. interruptions in the water supply for long periods of time and over large areas) is a hacker attack, while the threat chosen to represent the low consequence kind of threat is water leakages. From this point, IVAR and the municipality of Stavanger will not be considered separately as it is the total resilience of the drinking water supply that is supposed to be assessed. Also, as risk and vulnerability analysis is considered as an important basis for resilience in this context (ref. the theory presented above), it will not be possible for the author of this thesis to give a complete picture of resilience in each phase of the resilience cycle. It is up to the users to define a required number of issues (and corresponding indicators) to provide a sufficiently complete resilience picture. Guidelines regarding the completeness of the selected issues and indicators relevant for the quality of the process of identifying and selecting issues and indicators are provided in appendix 1. However, in the following, a number of identified issues and indicators relevant for the chosen threats will be presented and organized according to the resilience phases in order to present the essence of the method. Some recommendations will also be presented.

5.3 Resilience assessment

In this section issues and indicators relevant for the two chosen threats; hacking and water leakage, will be presented and systemized according to the five phases of resilience. First the relevance of the five phases will be presented.

5.3.1 The relevance of the five phases

Before presenting systematized lists and tables with overviews of issues and indicators relevant for the selected threats, a more thorough representation of the idea behind the different phases will be presented. A hacker attack, the system functionality curve presented in figure 2.5 and the five phases of resilience will be the point of departure for the following example.

A group of hackers are trying to harm the water supply in Stavanger by sending spam mails to different personnel. Considering this scenario, how do IVAR and the municipality handle this situation and how are the abilities to detect the virus and stop/adapt the water supply if necessary? What are the barriers present in order to limit the consequences in the first place? If the water supply has to be stopped due to this attack, how long does it take to restore normal activity? What processes exists in order to learn from such undesired events and to be more prepared to handle the next one?

The questions stated above could be grouped according to the five resilience phases, and it is important to clarify the measures taken in between each phase in order to identify potential gaps. E.g. a lot of measures are implemented, representing easily measurable factors, in the anticipate/prepare phase, but no (or few) measures are implemented in order to be resilient in the respond/recover phase. Such a process could display how resilient the system is today, and where the gaps are.

The information provided from the interviews will be used as input in the following simplified illustration of the relevance of the five phases. As the scenario presented is very specific, only measures relevant for the specific threat will be considered. This is only a very simplified example with the purpose of illustrating the meaning of the phases, thus only a few factors will be included in each phase. A comprehensive overview of issues and indicators will be given in later tables.

Let us first consider the first phase, understanding risk. In this phase issues on how to achieve knowledge and experience about risk and hazards are to be included. This phase is applicable prior to an adverse event. This is obtained by raising risk awareness among employers through e-learning courses where employers are provided with information about suspicious e-mails and how to react when such e-mails are received. Further, the quality of the spam filter is assessed by testing it towards known spamming techniques. Clear procedures related to upgrading and maintaining the systems should also be in place.

In the second phase, anticipate/prepare, measures implemented in order to anticipate what to look for and how to prepare for possible attacks are to be included. Also this

phase is applicable before the occurrence of an adverse event. Both IVAR and the municipality have performed a risk- and vulnerability analysis and corresponding emergency preparedness plans. Further, early warning systems are implemented to give information about potentially deteriorating safety before this is manifested in trends. Both IVAR and the municipality focus on very high degree of competence among the personnel. This is taken care of through comprehensive training and exercise plans targeting the actual threat.

In the third phase, absorb/withstand, the abilities to detect, absorb and withstand the consequences of a virus is to be measured. This phase comes into action during the initial phase of the event. Hence, following the rationale behind figure 2.5, measures implemented should prevent loss of functionality as far as possible. In this phase, measures implemented to increase the ability to detect the attack and the ability to adapt the water supply accordingly, should be included. Both passive and active safety systems, in addition to combat plans and required resources should be included when assessing the resilience in this phase.

In the phase respond/recover, available factors to get control over the situation and keep the downtime and consequences as low as possible are included. In this case, initiate emergency response resources, keep the consumers regularly updated on the drinking water situation (if necessary), obtain an overview of impacts and repair damages. Both IVAR and the municipality have the possibility to send out text messages with information about the severity of the situation (drinkable/not drinkable, drinkable if boiled, etc.). Response capacity, regarding number of personnel available, should be kept at a certain level. The amount of time needed in order to be "up and running", is dependent on the type and degree of virus and consequences. The communication between the different actors is essential throughout this phase and information and communication systems should be available.

The phase adapt/learn is related to the ability to learn from the event in order to improve the level of preparedness towards similar threats in the future. This phase encompass all kinds of improvements made on the infrastructure and its environment. Debriefing of the event and the response operation should be provided. Recommended adaptations and resilience improvements should be considered and followed-up. Furthermore, the experience and knowledge gained and the lessons learned from events and response operations should be systemized in order to store knowledge.

The example presented above is very simplistic, and is just meant to illustrate the idea behind the division of phases. The point of this division is to display possible gaps in the ability to either understand the risk and possible consequences, prepare for the considered threat, withstand the impacts and sustain critical functionality, mobilize appropriate responding resources, recover and learn form the event. This could also help decision makers decide where to put their resources. In order to draw such conclusions, a more comprehensive overview of issues and corresponding indicators relevant for each phase is needed. In the following, the two threats mentioned above will be presented with issues and indicators considered relevant for the drinking water supply in Stavanger to stay resilient before, during and after such events.

5.3.2 Generic candidate issues

In the third report released by Øien et al. (2017b), generic candidate issues were collected and described (see appendix 5). These will be the basis when identifying relevant issues, and corresponding indicators, for the chosen threats. Two main constraints when collecting the issues where 1) only internal resilience is covered, i.e. those issues that the SCI itself have control over, and can do something about, and 2) only activity/process type of issues are covered, i.e. not outcome type of issues. The reason for the second constrain is that resilience is to be measured independently on whether or not a crisis have been experienced. It may be misleading to include actual experience of a few and/or minor event in measuring the ability to be resilient against catastrophes.

The generic candidate issues were provided not only by collecting existing issues/"indicators" from the risk, security, safety, crisis management, business continuity and similar domains, but also by capturing typical topics discussed in resilience literature, i.e. those issues that can provide "added value" (Øien et al., 2017b).

The generic candidate issues presented by Øien et al. (2017b) can be reviewed by all critical infrastructures in order to establish their relevance and importance. Only for those selected (i.e. relevant and important), it is necessary to establish indicators. This can be done by checking if some indicators already used cover the selected issues (e.g. risk indicators, safety indicators, etc.), or it can be made a search in the SmartResilience database in order to obtain relevant indicators. Finally, new indicators may be developed with the help from domain experts. The generic candidate issues presented in appendix 5 should be considered when assessing resilience. However, additional issues could be added by end users if necessary. For simplicity reasons, and the limited time frame given for this master thesis, only the generic issues presented in appendix 5 will be considered. This is found to be sufficient for a thoroughly representation of the method.

Furthermore, some final comments to the candidate issues (Øien et al., 2017b): "They [*the candidate issues*] will never be complete; never be completely non-overlapping; and never be precisely correct located with respect to phases".

The following tables will provide issues and corresponding indicators relevant for the considered threats. The generic candidate issues referred to above will be the basis for the identified indicators. This will not be a complete picture of the overall resilience, rather a suggestion of relevant issues and indicators to include.

5.3.3 Threat: Leakage

The reduction of leakage is, as mentioned in the case study, an important objective of the water supply in Stavanger. The work towards detecting leaks and replacing poorly corrosion protected water pipes have been intensified in recent years. In their main plan, the municipality of Stavanger states that the goal is to reduce the leakages from 40 to 20 percent. The benefits of leakage reduction include, but are not limited to the following, which will change in priority depending on local circumstances (EPD Guidance Document, 2007, pp. 3):

- Improved operational efficiency
- Reduced potential for contamination
- Lowered water system operational costs

- Extended life of facilities
- Reduced water outage events
- Improved public relations
- Reduced potential property damage and water system liability

The water supply in Stavanger is aware of these benefits related to reduced leakages, and are constantly evaluating the most vulnerable areas of the distribution network. However, the category of leaks varies in severity – from complete pipe ruptures causing flooding on the surface and water outage, to small underground leaks difficult to detect. In the following, a list with suggested issues (obtained from the generic issues provided by SINTEF and stated in appendix 5) and corresponding indicators, relevant for water leakage, will be given. The indicator marked with an * is found in Bodsberg et al. (2017). A discussion regarding the choice of issues and indicator will be presented in the next chapter.

Table 5.1: Relevant issues and corresponding indicators are identified for each of the five resilience phases. The threat considered is leakage on the distribution network.

Type	Issue name	Issue description
	Phase I - Understand risks	
Issue	System knowledge	Knowledge about how the technical systems work and the interactions between systems, and knowledge about design assumptions and operational conditions. This knowledge provides insight in how systems may fail, and the potential consequences.
Indicator	Distribution network condition	Is the state of the distribution network assessed?
Indicator	Distribution network design	Do the municipality have maps showing a detailed overview of the distribution network design (pipe dimensions, pipe material, pumping stations, valves, water meters, etc.)?
Indicator	Soil characteristics	Is the municipality aware of the soil characteristics (movement, type of soil, acidity, permeability, etc.) throughout the city?
Indicator	Traffic loading	Is the municipality aware of the areas carrying most traffic and causing vibrations and high loading?
Indicator	Leakage control method	Is the chosen method for leakage control considered the most effective?
Issue	Information and knowledge about risk	Risk understanding is enhanced by basic knowledge of the concept of risk, and by specific knowledge about the risk on the particular plant, installation, etc. described in various risk analyses. A certain level of basic knowledge about risk is required in order to utilize the risk analyses information and/or to perform risk analyses.

Type	Issue name	Issue description
Indicator	Communication of vulnerabilities	Is the state of the distribution network communicated to relevant personnel (vulnerabilities, critical areas/zones, etc.)?
Indicator	Vulnerable consumers	Number of consumers considered especially vulnerable (e.g. not covered by ring mains, areas of bad corrosion protected water pipes, etc.)
Issue	Knowledge about context	Knowledge about e.g. the specific threats/hazards and situational factors.
Indicator	Potential socioeconomic impacts	Are potential socioeconomic impacts of operational disruptions on the infrastructure identified and evaluated?
Indicator	Geographic context	Are the geographic context and local circumstances clearly understood? (exposed to earthquakes, ground frost, etc.)
Issue	Knowledge about CI dependencies	Knowledge about dependencies between own CI and other CIs, including unexpected or non-intuitive dependencies.
Indicator	Dependency awareness	Is a systematic process for identifying critical dependencies conducted?*
Issue	Event reports	Information about real incidents and accidents gives knowledge about what have happened in the past, which also provides insight in what may go wrong in the future.
Indicator	Reporting routines	Are reporting routines to follow after an incident established and implemented?
Indicator	Report follow-up	Are the event reports regularly followed-up and analyzed?
Indicator	Efficacy of reporting	Is the efficacy of reporting monitored?
Issue	Failure data gathering	Failure data provides information on the status of the critical infrastructure systems and potential causes of events.
Indicator	Routines for data gathering	Are there established thorough routines for failure data gathering?
Indicator	Database	A common format for information database (making it easy to transfer data) is established?
Indicator	Follow-up failures	Do the municipality has routines to follow-up on failure frequencies?
Issue	Information about quality of barriers	Information about the quality of barriers, e.g. based on test results or real demand, gives knowledge about how well the safe-guards / defenses are protecting against accidental events. It provides insight in the technical systems that prevent the development of an accidental event.

Type	Issue name	Issue description
Indicator	Integrity of distribution system	Is an assessment of the current system been performed?
Indicator	Water balance	Is the municipality calculating and analyzing the water balance on an annual basis?
Indicator	Corrosion protection	Percentage of the water distribution network pipes with sufficient corrosion protection
Indicator	Pipe inspections	Frequency of pipe inspections
Indicator	Consumer complaints	Average no. of consumer complaints during a year
Indicator	System testing	Is a methodology for system testing under various stress-load scenarios and recovery conditions established?
Issue	Information about quality of barrier support functions	Information about the quality of barrier support functions, e.g. preventive maintenance, by-passing, etc. including human and organizational elements, gives knowledge about the operational readiness of the safe-guards / defenses. It provides insight in the operational support systems contributing to the readiness of the barriers.
Indicator	Water meters	Is a preventive maintenance plan established?
Indicator	Pumps	Is a preventive maintenance plan established?
Indicator	Valves	Is a preventive maintenance plan established?
Indicator	Active leakage control	Frequency of leakage listening
Issue	Risk/safety/resilience performance requested by senior management	When risk/safety/resilience performance is requested by senior management it signals the importance of risk/safety/resilience in general and the specific issues that are addressed in particular. It enhances the awareness of the importance of risk/safety/ resilience in the organization.
Indicator	Effective internal controls	Are regular internal controls and risk management practices implemented (to achieve security, reliability, resiliency and recoverability (in accordance with the regulations))?
Indicator	Evaluate threat trajectories	Senior management team is evaluating threat trajectories from a position of risk profiling and business acceptability
Indicator	Leakage management strategy	Is a tailored leakage management strategy developed and communicated to staff?
Indicator	Conservation policy	Is a water conservation policy established and communicated to staff?
	Phase II - Anticipate/prepare	

Type	Issue name	Issue description
Issue	Risk/hazard identification	Systematic risk/hazard identification is a prerequisite in order to anticipate what may go wrong. It expands on the repertoire of incidents/accidents that have been experienced.
Indicator	Risk- and vulnerability analysis	Is a risk- and vulnerability analysis used for planning and decision-making in order to reduce vulnerability or to increase emergency capacity?*
Indicator	Decisions of agents involved	Do the organization consider explicitly integration of the decisions of the relevant agents involved (e.g. policy makers, corporations, operators, and lay people)?
Indicator	Cooperation with experts	Is the risk- and vulnerability analysis performed in cooperation with relevant experts?
Indicator	Hazard identification	Is a systematic approach for hazard identification utilized (e.g. brainstorming, checklists, hazard database, experience from the past)?
Issue	Learning form own events and experiences	The most obvious source of information on what may go wrong (and how to treat such situations) is the experience from incidents and accidents in own organization. It is a particular obligation to any organization to avoid the reoccurrence of events. Learning from success stories, e.g. "what went right", should also be included.
Indicator	Leak repair records	Do the municipality keep records covering exact position of the leak, cause and type of leak, and repair carried out, pipe material and size, and whether pipe replacement was necessary?
Indicator	Use of theoretic models	Is a verified model used that described the steps that a company needs to take in order ot learn from incidents?
Indicator	Dissemination of lessons learnt	The municipality secures dissemination of lessons learnt throughout the organization?
Indicator	Yearly reports	Is the municipality conducting yearly incident/accident reports in order to see development over time?
Issue	Learning from other`s events and experiences	The manifestation of potential events in real occurrences constitutes only a small percentage of the potential events. Therefore, it is important to learn as much as possible also from other's incidents and accidents. Today's accessibility of information makes organizational borders no excuse for learning from outside own organization. Learning from success stories, e.g. "what went right", should also be included.
Indicator	Sharing information and knowledge	Do the municipality actively search for information from available sources?

Type	Issue name	Issue description
Indicator	Exchange of data	Do the municipality encourage exchange of data across water utilities?
Indicator	Cooperative forum	Do the municipality convenes a cooperative forum for internal and external actors in order to share experiences?*
Issue	Status on risk, events, quality of barriers, etc.	The status on risk, events, quality of barriers, etc. compared to thresholds, provides information on where to focus attention.
Indicator	Regular meetings	Is the municipality organizing regular status meetings?
Indicator	Pipeline renewal	Percentage of pipe replacement per year
Indicator	Functionality of distribution network	Quality index provided by bedreVANN
Indicator	Infrastructure Leakage Index (ILI)	Infrastructure Leakage Index number
Issue	Trends in risk, events, quality of barriers, etc.	Increase in reported events or negative development in the quality of barriers are clear indications of the need to take action to remedy the situation.
Indicator	Water meter failures	Frequency of water meter failures
Indicator	Pumping failures	Frequency of pumping failures
Indicator	Valve failure	Frequency of valve failures
Indicator	Frequency of bursts	Frequency of bursts
Issue	Alert systems	Utilization of fixed technical alert systems, identifying threats and/or increased level of threat.
Indicator	Alerts	Are remote sensors and monitoring software installed to alter operators to leaks, fluctuations in pressure, problem with equipment integrity?
Issue	Monitoring	Continuous monitoring of potential threats.
Indicator	Pressure fluctuations	Is the pressure in the distribution network continuously monitored?
Indicator	Flow rate	Is the flow rate in the distribution network continuously monitored?
Indicator	Consumption	Is the water consumption throughout the municipality continuously monitored?
Indicator	Temperatures	Are the temperatures continuously monitored?
Indicator	Condition monitoring	Is condition monitoring of components established (important to know their condition and performance histories)?
Issue	Audits	Regular searching for problems/weaknesses/failures through audits (internal and/or external).
Indicator	Water audit	Is a water audit performed to quantify leakage and prioritize leak management activities?

Type	Issue name	Issue description
Indicator	Audit report	Is an audit report prepared at the completion of each audit?
Issue	Robustness (functions/systems)	Resilience through robust design, e.g. large safety margins.
Indicator	Design requirements	Is each component in the pipe network designed or selected to function correctly under local conditions (also considering the cost)?
Indicator	Diurnal peak demand	Is the pipe network designed to handle diurnal peak demand during seasonal peak demand periods?
Indicator	Water demand patterns and growth	Is the system designed to handle future demands?
Indicator	"Zoning"	Is leakage monitoring in zones or sectors provided throughout the municipality?
Issue	Redundancy (functions/systems)	Resilience through redundant functions and/or systems.
Indicator	Ring mains	No. of consumers covered with ring mains
Indicator	Emergency connection points	Are emergency connection points available at strategic points on the distribution network?
Indicator	Isolation valves	Is an adequate number of isolation valves placed in such a way that they allow for the isolation of sections of the system?
Indicator	Parallel distribution network	Percentage of network covered with parallel distribution lines
Indicator	Redundant telecom lines	Are redundant telecom lines in place to secure communication?
Indicator	No. of telecom suppliers	No. of telecom suppliers
Issue	Back-up/alternative (functions/systems)	Internal back-up systems or alternatives.
Indicator	Emergency water (not depending on the distribution network)	Is an emergency water solution provided (e.g. tanks, bottles, etc.)?
Indicator	Emergency generator unit	For how long can the emergency generator unit provide the facility, plant, etc. with enough electricity to sustain production?
Issue	Emergency preparedness plans (and crisis organization)	Preparing for resilience through emergency preparedness plans, including pre-planned crisis organizations.
Indicator	Emergency preparedness plan/incident protocol	Do the municipality have an emergency plan for extraordinary events? (An emergency plan indicates that there is procedures and processes to follow in case of extraordinary events)*

Type	Issue name	Issue description
Indicator	Requirements analysis	Has the municipality investigated the material and personnel resources most critical to manage extraordinary events?*
Indicator	Capacities within the emergency organization	Do the organization have an overview of capacities within the emergency organizations? *
Indicator	Cooperation in planning	Is the emergency preparedness plan executed in cooperation with relevant actors?
Indicator	Communication plan	Is a communication plan prepared?
Issue	Training plans (table-top, simulator, drills, etc.)	Training plans on how to deal with potential scenarios is essential in order to know what to do, not only with respect to identical or similar scenarios as trained on, but also with respect to response to other (unexpected) scenarios. This includes the use of simulators, table-top exercises, emergency preparedness drills, etc.
Indicator	Training and exercise plan	Are training and exercise plans, considering emergency preparedness drills, developed and adjusted according to level of threat?
Indicator	Communication training plan	Is a training plan provided related to communication procedures during an extraordinary event?
Indicator	Incident management training plan	Is a plan considering incident management training been established?
Issue	Joint exercises plans	Preparing for resilient emergency response through plans for joint exercises with external actors.
Indicator	Coordinated training and exercise	Are training and exercising plans coordinated with relevant external actors?
Issue	Cooperation agreements (external resources)	Pre-planned agreements of use of external resources in crisis situations.
Indicator	Agreements for external supply of resources	Are there contracts with external actors for extra supply in case of an extraordinary event?*
Issue	Planned maintenance	Planned maintenance of critical systems and equipment to ensure adequate functioning.
Indicator	Maintenance schedule	Has the municipality prepared a maintenance schedule based on the state of the distribution network?
Indicator	Maintenance routines	Are there routines that secures that the maintenance is executed according the maintenance schedule?
Indicator	Adequate quantities of network components	Do the municipality has an adequate quantity of network components held in municipal stores for repair and replacement of pipes and other components?

Type	Issue name	Issue description
Indicator	Maintenance requirements	The municipality is carefully following the manufacturer's maintenance requirements?
Indicator	Staff work schedules	Are all maintenance activities incorporated into the maintenance staff work schedules so that the work is done on time and as required?
Indicator	Maintain or replace	No. of maintenance activities before replacement?
Issue	Financial resources/insurance	Necessary financial resources to maintain resilient operations and being financially prepared for major events/interruptions.
Indicator	Repair cost analysis	Is an analysis of repair cost versus replacement costs been conducted for older pipes?
Indicator	Expenditure plan	Is an expenditure plan established, derived from estimates of current leakage levels, and an economic assessment of alternative measures?
Issue	Smartness vulnerability in the anticipate/prepare phase	Are there any smart features ("smartness") included in the critical infrastructure(s), which makes it more difficult to anticipate what may happen and/or prepare for it, e.g. if failures occur in these smart features?
Indicator	Failure in remote sensors and monitoring software	No. of unplanned interruptions due to failures in remote control sensors and monitoring software
Issue	Smartness opportunity in the anticipate/prepare phase	Are there any smart features ("smartness") included in the critical infrastructure(s), which makes it easier to anticipate what may happen and/or prepare for it, e.g. through the functioning of these smart features?
Indicator	Remote sensor and monitoring software	Is remote sensor and monitoring software installed?
	Phase III - Absorb/withstand	
Issue	Active safety systems	Automatic and/or manual safety systems to detect/prevent/ withstand an event.
Indicator	Active leak detection	Is an active leak detection plan prepared, providing an overview of areas to pritoritize, frequency, approach, etc.?
Indicator	Constant monitoring	Are pressure, flow rate and water consumption constantly monitored?
Indicator	Water meters at the distribution network	Are water meters installed on tactical places on the distribution network?
Issue	Notification/alarm	Notification of an event, e.g. by releasing an alarm, as soon as possible to the responsible unit, e.g. a control center.
Indicator	Telemetry system	Is a telemetry system that raises alarms for conditions such as no-flow, high flow, abnormal temperatures, vibrations, unauthorized access and flood conditions, installed?

Type	Issue name	Issue description
Indicator	Notification from public	Are routines established to follow-up public complaints?
Issue	Confirmation of threat/event	Confirming that the threat/event is real, and what kind of threat/ event it is.
Indicator	Leakage listening	Frequency of nightly leakage listening
Indicator	Logger software	Do the municipality provide a logger software that contains an "error table" for daily scanning?
Indicator	Leakage control team	Do the municipality has a leakage control team that follows-up alarms and deviations?
Issue	Action plan - reaction (availability, familiarity, use)	Availability, familiarity with, and use of pre-planned action plans for immediate reaction to an event.
Indicator	Tailored action plan	Has the municipality constructed an tailored action plan, based on local knowledge, for the relevant threat?
Indicator	Action plan - reaction	Do the action plan includes measures and strategies on how to secure a robust reaction?
Indicator	Available action plan	Is the action plan available for relevant personnel?
Indicator	Familiarity	Are personnel familiar with where to find the action plan?
Issue	Competent personnel	Competent/experienced personnel are required to obtain a resilient reaction to withstand an (expected or unexpected) event.
Indicator	Monitoring competence	Is an overview of competence gained, lost and needed through obtain e.g. trough monitoring of personnel starting and leaving?
Indicator	Certified operation and service personnel	No. of operation and service personnel certified with relevant education and/or courses
Indicator	Certification level	Is it secured that responsibilities are aligned with certification levels?
Indicator	Training of personnel	Have relevant personnel been provided with suitable training towards managing the tasks responsible for during an extraordinary event?
Indicator	Maintenance functions	Competent and well-trained staff is ensured in all cases?
Indicator	Switch to generator power	Is it ensured that key personnel know how to switch to generator power and know the fuel requirements for the generators?
Issue	Emergency response organization mobilization	Mobilization/scrambling of the emergency response organization.
Indicator	Mobilization checklist	Do the municipality have a mobilization checklist to follow?

Type	Issue name	Issue description
Indicator	Up-to-date contact information	Is the contact information on people and entities that may need to be contacted when a incident occur regularly reviewed and updated (both internal and external personnel)?
Issue	Notification of response resources	Notification of required internal and external response resources according to action plan.
Indicator	Organization's resources	Is the mobilization of the organization's resources based on severity of incident and stated in the action plans?
Indicator	Responsible for delegation of response activities	Is the person responsible for delegate response activities during extraordinary events known to the staff?
Indicator	Notification routines	Are notification routines regarding who, when and how to notify, stated in the action plan?
Indicator	Responsibility awareness	Is the municipality aware of how the responsibility is divided between the cooperative actors in case of an extraordinary event?
Issue	External alert/communication	Alerting, informing and communicating with relevant external stake-holders, e.g. head office, authorities, etc.
Indicator	Communication with cooperating actors	Have the municipality routines for communication with cooperating actors in case of an extraordinary event?
Issue	Adapt (stop/reduce) operation	Adaptation of the operation according to the event e.g. reduces, minimize or stop operations.
Indicator	Valve adjustments	Do the municipality provide the possibility to adjust/stop the operation by the use of valves and pumps?
Indicator	Criticality awareness	Is the municipality aware of the most critical areas (e.g. Not covered by ring mains)?
Indicator	Emergency water	Do the municipality provide the possibility to supply emergency water to exposed consumers?
Issue	Start combat/handling of threat/event	Combat of threat/event with required available resources.
Indicator	24-hour-a-day, seven-day a week rota	Are there on-duty personnel that is always available?
Indicator	Standard operation procedures (SOP)	Are SOPs in place to ensure rapid reaction and appropriate response to smaller leaks?
Indicator	Incident protocols	Are standard responses and corrective actions developed to deal with larger breaks?
Indicator	Crisis management team	Do the municipality has a crisis management team made up of all critical functions as documented in the incident protocols?

Type	Issue name	Issue description
Indicator	Availability of external resources	Do the municipality provide the possibility to call for external resources 24-hour-a-day, seven-day a week?
Issue	Communication (status update)	Communicating the status of the situation during the initial response as relevant (internally and externally).
Indicator	Immediate response communication checklist	Do the municipality has a immediate response communication checklist to follow, which include guiding principles?
Indicator	Most efficient communication strategy	Is the most efficient communication strategy is assessed (e.g. E-mails, in-person meetings, internal social media meetings, phone calls, etc.)?
Indicator	Consumer communication	Do the municipality provide the possibility to notify the public through efficient channels if water outage/unfit for drinking?
Issue	Media handling	Use of dedicated resources for media handling during initial response.
Indicator	Press officer/media handling responsible	Are guidelines regarding how to handle the media during initial response stated (e.g. in a media handling strategy)?
Indicator	Media agreement	Have the municipality established agreements with local media channels to provide the public with secure and updated information if water outage/unfit for drinking?
Indicator	Media handling strategy during initial response	Are guidelines regarding how to handle the media during initial response stated (e.g. a media handling strategy in the incident protocols)?
Indicator	Press release	Is a basic press release that can be quickly adapted during a crisis, established?
Issue	Smartness opportunity in the respond/recover phase	Are there any smart features ("smartness") included in the critical infrastructure(s), which makes it easier to respond to or recover from an event? Can it help in response/recovery?
Indicator	Increased leak detection abilities	Has the smart features increased the municipality's leak detection abilities?
	Phase IV - Respond/recover	
Issue	Resourcefulness/emergency response resources (internal)	Internal emergency response resources and response/ mobilization time. Equipment (fixed/mobile, automatic/manual, etc.), personnel, organization, etc.
Indicator	Initiate response plan	Average time needed to initiate response plan
Indicator	Inform personnel	Average time needed to inform relevant personnel

Type	Issue name	Issue description
Indicator	Assessing appropriate response resources	Average time between discovering the event to adequate use of response resources are assessed
Indicator	Reaction time during day	Average reaction time from receiving the notification, to on-duty personnel has assessed leakage severity
Indicator	Reaction time during night	Average reaction time from receiving the notification, to on-duty personnel has assessed leakage severity
Indicator	Are the responses/remedial actions effective? (feed flow)	Response time to restore feed flow*
Indicator	Are the responses/remedial actions effective? (damaged equipment)	Response time to restore damaged equipment*
Issue	Resource allocation and staffing (including buffer capacity)	Sufficient number of persons attending to critical functions, including back-up personnel in case of additional needs, unavailability of personnel or exchange of personnel. Duty schemes enabling adequate mobilization to provide timely response are needed.
Indicator	Vacation routines	Is vacation routines regarding competent personnel available at all time established and implemented?
Indicator	Appropriate rota system	Is an appropriate rota system implemented to ensure sufficient amount of back-up personnel?
Issue	Emergency response resources (external)	External emergency response resources and response/ mobilization time. Equipment, personnel, organization, agreements/contracts, etc.
Indicator	Inform cooperating actors	Average time needed to inform cooperating actors
Indicator	Mobilization time (external)	Average time needed for external response resources to be present at the site of leakage
Issue	Communication between actors	Response is often dependent on information from other actors. It is essential that the (local) information and communication systems are available throughout the duration of the situation until control has been regained. The information itself needs to be understandable for all actors involved (including use of common language).
Indicator	Communication procedures	Has the municipality developed communication procedures to follow during response?
Indicator	Emergency communication channels	Are emergency communication channels established?*

Type	Issue name	Issue description
Issue	Robustness of responsible function	Endurance of critical functions to complete the response. This includes personnel in charge of critical tasks as well as the upholding of critical infrastructure systems (e.g. main safety functions).
Indicator	Robust response	Is the number of available competent personnel considered sufficient to provide a robust response (based on tests, trainings, real incidents, etc.)?
Indicator	Emergency water (not dependent on the distribution network)	For how long can the cans, tanks, bottles available provide the city with water
Issue	Action plan - response (availability, familiarity, use)	Availability, familiarity with, and use of action plans for response actions.
Indicator	Action plan - response	Do the action plan includes measures and strategies on how to secure a robust response?
Issue	Training (table-top, simulator, drills, etc)	Training on how to deal with potential scenarios is essential in order to know what to do, not only with respect to identical or similar scenarios as trained on, but also with respect to response to other (unexpected) scenarios. This includes the use of simulators, table-top exercises, emergency preparedness drills, etc.
Indicator	Emergency training of personnel	No. of personnel provided with yearly emergency training
Indicator	Training consistency	Is the training consistent with existing regulations, standards, codes of practice and requirements of regulatory authorities?
Indicator	Communication training	No. of personnel provided with emergency communication training
Indicator	Incident management training	Have relevant personnel been through the incident management training?
Issue	Joint exercises	Resilient response and recovery through joint exercises with external actors.
Indicator	Carried out cooperative exercise	Has the municipality carried out a cooperative exercise with external actors within own area?*
Indicator	Frequency of joint exercises	Frequency of joint exercises
Issue	Combat threat/event	Combat threat/event until the situation is fully under control. This may require exchange of exhausted response personnel.
Indicator	Combat procedures	Do the combat procedures stated in the emergency preparedness plan include responding guidelines?
Indicator	Combat personnel	Are suitable work shifts established to prevent exhausted response personnel?

Type	Issue name	Issue description
Issue	Communication (status update)	Communicate the status of the situation during response and recovery as relevant (internally and externally).
Indicator	Secondary response communication checklist	Do the municipality have a secondary response communication checklist to follow after immediate response?
Issue	Media handling	Use dedicated resources for media handling during response and recovery.
Indicator	Media handling strategy during response and recovery	Are guidelines regarding how to handle the media during response and recovery stated in the incident protocols?
Issue	Secure area	Secure the area and limit access to relevant response and investigation personnel (including securing any evidence).
Indicator	Secure area - procedures	Do the municipality have procedures to follow on how to secure the area?
Indicator	Average time needed to secure the area	Average time needed to secure the area
Issue	Repair damages (unplanned maintenance)	Repair any damages to the critical infrastructure.
Indicator	Repair strategy	Is a repair strategy in place covering prioritized order of repair?
Indicator	Repair strategy efficiency	Has the repair strategy been tested towards the considered threat?
Issue	Risk assess and clarify re-start/continuing operation	Make risk assessment and clarifications (including approvals) before re-start/ continuing of operation.
Indicator	Quality control measures	Are there procedures for quality control before restarting operation?
Indicator	Checklist	Is the staff required to work through a post-restart checklist?
	Phase V - Adapt/learn	
Issue	Debriefing	Provide a debriefing of the event and the response operation to personnel directly involved.
Indicator	Timing of debriefing	Is the debriefing conducted within a week after the incident?
Indicator	Crew coordination	Is debriefing of crew coordination conducted?
Indicator	Determining the cause	Is an analysis of the possible causes performed?
Indicator	Performance assessment	Has a performance assessment of response and recovery been conducted?*
Issue	Media handling	Provide information to the media about what happened, the response operation, investigations, follow-up of involved persons, etc.
Indicator	Media handling strategy after an incident	Are guidelines regarding how to handle the media after an incident stated in the incident protocols?

Type	Issue name	Issue description
Indicator	Review of media strategy	Are there routines established for reviewing and updating the media handling strategy after an incident
Issue	Event investigation and reporting including recommendations for adaptation/improvement	Investigation of event, including underlying causes, and recommendation for adaptation/improvement of operations (physical, technical, operational, organizational, etc.).
Indicator	System for determining which incidents should be investigated	Do the municipality provide a system for determining which incidents that should be investigated?
Indicator	Event investigation technique	Has the municipality established a process for event/incident investigation that ensures that the underlying as well as immediate causes of events/incidents are understood, taking full account of human and organizational factors?
Indicator	Prevent recurrence	Has the municipality established a process for ensuring that the findings of investigation and analysis are acted upon in a timely fashion and suitable interventions put in place to prevent recurrence of the incident or similar incidents?
Indicator	Employee involvement	Is the municipality encouraging employee involvement during event investigation?
Indicator	Updating of emergency preparedness plans/incident protocol	Are there routines for emergency preparedness plan/incident protocol updating after an incident?
Issue	Presentation/communication of event investigation	Presentation and communication of the results of the investigation internally and externally (notifications, reports, presentations, press conferences, etc.).
Indicator	Disseminating information	Has the municipality established a routine for dissemination of information on incidents/events causation and suitable interventions/modifications to all relevant parties (both internal and external), as quickly as possible?
Indicator	Communication channel	Is the most suitable communication channel established for all relevant parties (e.g. meetings, e-mails, phone calls, etc.)?
Issue	Implementation and follow-up of recommendations for adaptation/improvement	Implement and follow-up the recommended adaptations/ resilience improvements.
Indicator	Consider recommendations	Do the municipality has routines to consider recommended changes to prevent similar events from happening again?
Indicator	Intervention plan	Are intervention plans developed on the basis of the incident investigation?

Type	Issue name	Issue description
Indicator	Monitoring of progress	Are the municipality monitoring progress and following up recommendations arising from incident investigation?
Indicator	Follow up employees	Are employees regularly followed up in their work to check if new procedures are followed?
Indicator	Evaluating the success	Has the municipality established a routine for evaluating the success of interventions and modifications?
Issue	Emergency response operation reporting including lessons learned	Reporting of the response operation and any lessons learned for future emergency response and resilience improvements.
Indicator	Incident reporting format	Has an effective incident reporting format been developed?
Indicator	Record and report outcomes	Are outcomes of the event investigations recorded and reported?
Indicator	Assessing emergency plans and routines	How well did the last exercise fulfill the goals?*
Indicator	Documentation of resources	Has the municipality established routines to evaluate if the resources available were sufficient to handle the event?
Indicator	Sufficient competence	Has the municipality established routines to evaluate if the available competence was sufficient to handle the incident/event?
Issue	Implementation and follow-up of lessons learned	Implementation and follow-up of the lessons learned from the emergency response operation (resources, capabilities, etc.).
Indicator	Update training and exercise plans	Are training and exercise plans updated according to the lessons learned, having in mind suitable competence?
Indicator	Update documentation of resources	Are the resources available updated according to the resource evaluation?
Indicator	Budget allocation	Do the municipality provide the possibility to allocate the budget?
Indicator	Update maintenance schedule	Is the maintenance schedule revised after an incident?
Indicator	Update communication checklists	Is the communication plan/checklist regularly reviewed, including details of communication channels, contact lists, guidelines, etc.?
Issue	Presentation/communication of emergency response operation	Presentation and communication of the lessons learned from the emergency response operation internally and externally.
Indicator	Communication of emergency response	Are appropriate communication channels determined, based on the content and format of information?

Type	Issue name	Issue description
Indicator	Speed of communication	The speed with which the information can be shared with all relevant parties
Indicator	Evaluation of information	Is an evaluation of the nature of the information that is to be shared (i.e. details of lessons learned) performed prior to communication?
Issue	Feedback and learning from successful operations	Providing feedback and learning from successful operations in addition to event investigations, which focus on improving unsuccessful operations.
Indicator	Yearly report	Is the municipality conducting a yearly summarizing report, addressing both successes and failures compared to goals stated in the action plan?
Indicator	Feedback to personnel	The organization arrange meet ups for communication and positive feedback to personnel
Issue	System/archive to store knowledge	System/archive to store and retrieve knowledge/experience/ lessons learned from events and response operations.
Indicator	Capture information	Do the municipality have a system to capture the information in a format that is readily searchable and retrievable to allow ease of access?

5.3.4 Threat: Hacking of ICT systems

A hacking attack towards the drinking water supply in Stavanger has never occurred (at least what is known or discovered). However, the awareness related to ICT security is increasing due to the enhanced use and dependency of ICT based systems. Without proper cyber security in place, anyone with malicious intent could access the network and contaminate or cease the treatment and distribution of water. As for leakages, the possible consequences related to a hacking attack are varying in severity, dependent on the hackers approach (phishing, virus, Trojans, etc.), professionalism and intentions.

Due to the increased "smartness" and automation of the water supply, it has become more vulnerable and exposed towards hackers with bad intentions. To assess the resilience of the system will provide useful information regarding the current robustness of the security measures and available resources to cope with such surprises. In the following, a list with suggested issues (obtained from the generic issues provided by SINTEF and stated in appendix 5) and corresponding indicators, relevant for a hacker attack, will be given. The indicator marked with an * is found in Bodsberg et al. (2017). A discussion regarding the choice of issues and indicator will be presented in the next chapter.

Table 5.2: Relevant issues and corresponding indicators are identified for each of the five resilience phases. The threat considered is a hacker attack towards the operational control systems.

Type	Name	Description
	Phase I - Understand risks	
Issue	Information and knowledge about risk	Risk understanding is enhanced by basic knowledge of the concept of risk, and by specific knowledge about the risk on the particular plant, installation, etc. described in various risk analyses. A certain level of basic knowledge about risk is required in order to utilize the risk analyses information and/or to perform risk analyses
Indicator	Organizational culture awareness	Is there a focus on general awareness regarding the organizational culture among employees? (e.g. courses, surveys, meetings, etc.)
Indicator	Risk culture	Frequency of internal organizational control on risk culture
Indicator	Risk awareness	Do the organization provide a mandatory e-learning courses to raise risk awareness?
Indicator	Security policy	Is a clear security policy in place to help employees clearly understand their duties and responsibilities in terms of cyber security and what their roles and responsibilities are in case of an attack?
Indicator	Recruitment method	Are recruitment methods adapted to include risk management capabilities?
Issue	Knowledge about context	Knowledge about e.g. the specific threats/hazards and situational factors.
Indicator	ICT threats	Is information about relevant ICT threats communicated to personnel (e.g. through e-learning courses, information e-mails, etc.)?
Indicator	Understanding modern cyber attack strategy	Has the organization established a information security management system?
Indicator	Risk attitude	Is a survey conducted in order to map the overall risk attitude towards ICT security?
Indicator	Requirements for ICT security	It is specified what requirements for ICT security are to be taken into account when acquiring and developing ICT systems?
Indicator	Clear procedures	Has the organization established clear procedures related to upgrading and maintaining the services and systems?
Indicator	Testing regime	Is there a regime for testing of new software and new systems, as well as upgrading of existing systems?

Type	Issue name	Issue description
Indicator	Potential impacts	Has the organization conducted an evaluation of identified potential impacts of major operational disruptions on the infrastructure?
Indicator	Value of information	Is an criticality assessment related to the value of information been performed?
Indicator	Human factor	Is the human factor adequately accounted by the organization? (important for the accuracy of risk assessment and for the effectiveness of prevention and emergency management)
Indicator	Monitoring of global and local situation	Is the organization monitoring the global and local situation?
Issue	Knowledge about CI dependencies	Knowledge about dependencies between own CI and other CIs, including unexpected or non-intuitive dependencies.
Indicator	Dependency awareness	Is a systematic process for identifying critical dependencies conducted?
Indicator	Dependency characterization	Is the type of dependency (physical, cyber, geographic, logical) between own CI and other CIs characterized in order to consider relevant elements?
Indicator	Limited analysis	Is a limited analysis of the CI dependencies conducted based on open source information?
Issue	Event reports	Information about real incidents and accidents gives knowledge about what have happened in the past, which also provides insight in what may go wrong in the future.
Indicator	Reporting routines	Are comprehensive reporting routines established throughout the organization?
Indicator	Report follow-up	Has the organization established routines for follow-up and analyzing event reports?
Indicator	Efficacy of reporting	Is the efficacy of reporting monitored?
Issue	Failure data gathering	Failure data provides information on the status of the critical infrastructure systems and potential causes of events.
Indicator	Routines for data gathering	Are there established thorough routines for data gathering?
Indicator	Database	A common format for information database (making it easy to transfer data) is established?
Indicator	Follow-up failures	Do the organization has routines to follow-up on failure frequencies?

Type	Issue name	Issue description
Issue	Information about quality of barriers	Information about the quality of barriers, e.g. based on test results or real demand, gives knowledge about how well the safe-guards / defenses are protecting against accidental events. It provides insight in the technical systems that prevent the development of an accidental event.
Indicator	Assessment of current system	Is an assessment of the current system been performed?
Indicator	Current system	How many breaches have occurred?
Indicator	Hygienic barriers	Are hygienic barriers in place to detect deviation in water quality?
Indicator	Redundant treatment paths	Redundant treatment paths?
Indicator	"Custom made" operational control systems	Are the operational control systems "custom made" in order to fit the need and requirements to the organization?
Indicator	Routines to identify deficiencies	Do the organization has routines to identify deficiencies in the operational control systems?*
Indicator	System testing	Is a methodology for system testing under various stress-load scenarios and recovery conditions established?
Indicator	Quality of firewall	Frequency of firewall revision
Indicator	Quality of spam filter	Is the spam filter tested towards known spamming techniques?
Indicator	Malware protection	Is a business grade or enterprise variety malware protection installed? (Basic computer security programs designed for home computers should not be used)
Indicator	Encryption	Are data encryption technologies enabled on the organizations computers?
Indicator	ISO/IEC 27001 certification	Is the organization ISO/IEC 27001 certified?
Issue	Risk/safety/resilience performance requested by senior management	When risk/safety/resilience performance is requested by senior management it signals the importance of risk/safety/resilience in general and the specific issues that are addressed in particular. It enhances the awareness of the importance of risk/safety/ resilience in the organization.
Indicator	Cyber security is a part of the risk management strategy	Is a sound and robust technology risk management framework established?
Indicator	Effective internal controls	Are regular internal controls and risk management practices implemented (to achieve security, reliability, resiliency and recoverability (in accordance with the regulations))?

Type	Issue name	Issue description
Indicator	Security awareness foundation	Do the organization have a strong security awareness foundation that are able to provide adequate cyber resilience?
Indicator	Evaluate threat trajectories	Do the senior management team regularly evaluating threat trajectories from a position of risk profiling and business acceptability?
Issue	Communication risk/resilience at all levels in the organization	To obtain widespread risk awareness in the organization it is important that information about risk and resilience are properly communicated at all levels in the organization. This can be obtained through various channels, e.g. meetings, safety alerts, bulletins, etc.
Indicator	Communication of risk and resilience	Are the risk/resilience communicated at all levels in the organization through suitable communication channels?
Indicator	Adequate updating of personnel	Is the organization regularly evaluating the employees' need for information?
Issue	Smartness opportunity in the understand risks phase	Are there any smart features ("smartness") included in the critical infrastructure(s), which makes it easier to understand risks, e.g. through the functioning of these smart features?
Indicator	Increased access to information	Easy access to relevant data?
	Phase II - Anticipate/prepare	
Issue	Risk/hazard identification	Systematic risk/hazard identification is a prerequisite in order to anticipate what may go wrong. It expands on the repertoire of incidents/accidents that have been experienced.
Indicator	Risk- and vulnerability analysis	Is a risk- and vulnerability analysis used for planning and decision-making in order to reduce vulnerability or to increase emergency capacity?*
Indicator	ICT adapted risk- and vulnerability analysis	A ICT adapted risk- and vulnerability analysis is used for planning and decision-making in order to reduce vulnerability or to increase emergency capacity related to ICT security?
Indicator	Cooperation with experts	Is the risk- and vulnerability analysis performed in cooperation with relevant experts?
Indicator	Hazard identification	Is a systematic approach for hazards identification utilized (e.g. brainstorming, checklists, hazard database, experience from the past)?
Indicator	Vulnerability assessment	Is a vulnerability assessment performed in order to develop programs and strategies for managing the impact of disasters as effectively and efficiently as possible?

Type	Issue name	Issue description
Indicator	Decisions of agents involved	Do the organization consider explicitly integration of the decisions of the relevant agents involved (e.g. policy makers, corporations, operators, and lay people)?
Issue	Learning form own events and experiences	The most obvious source of information on what may go wrong (and how to treat such situations) is the experience from incidents and accidents in own organization. It is a particular obligation to any organization to avoid the reoccurrence of events. Learning from success stories, e.g. "what went right", should also be included.
Indicator	Incident analysis	Are routines regarding incident analysis conducted after incidents or accidents?
Indicator	Dissemination of lessons learnt	The organization secures dissemination of lessons learnt throughout the organization?
Indicator	Use of theoretic models	Is a verified model used that described the steps that a company needs to take in order to learn from incidents?
Indicator	Yearly reports	Is the organization conducting yearly incident/accident reports in order to see development over time?
Issue	Learning from other`s events and experiences	The manifestation of potential events in real occurrences constitutes only a small percentage of the potential events. Therefore, it is important to learn as much as possible also from other's incidents and accidents. Today's accessibility of information makes organizational borders no excuse for learning from outside own organization. Learning from success stories, e.g. "what went right", should also be included.
Indicator	Sharing information and knowledge	Do the organization actively search for information from available sources?
Indicator	Exchange of data	Encourage exchange of data across water utilities?
Indicator	Cooperative forum	Do the organization convenes a cooperative forum for internal and external actors in order to share experiences?*
Issue	Status on risk, events, quality of barriers, etc.	The status on risk, events, quality of barriers, etc. compared to thresholds, provides information on where to focus attention.
Indicator	Regular meetings	Are regular status meetings organized for relevant personnel?
Indicator	Constant monitoring of barriers	Is barrier monitoring established to ensure that plans are being followed and to confirm that risk controls/barriers are effective?

Type	Issue name	Issue description
Indicator	Quality of service (QoS)	Measurement of overall performance (considering error rates, bit rate, throughput, transmission delay, availability, jitter, etc.)
Issue	Trends in risk, events, quality of barriers, etc.	Increase in reported events or negative development in the quality of barriers are clear indications of the need to take action to remedy the situation.
Indicator	Investigate unknown traffic	Is the organization investigating unknown traffic and traffic patterns?
Indicator	Unplanned interruptions	How many unplanned shutdowns have occurred in the past year?
Issue	Increased preparedness under certain situations/conditions	Increasing preparedness based on predefined signals/warnings/ gauges/measurements etc. of threats, situational factors, etc.
Indicator	Coordinated preparedness plan	Is a coordinated preparedness plan established between the relevant actors? (which is initiated under extraordinary events)
Issue	Emerging risks	Vigilance with respect to identifying emerging risks early, using risk radars, etc.
Indicator	Analyzing event reports	Are event reports and failure data analyzed when abnormalities are detected?
Indicator	Monitor devices with access to data	Is the organization monitoring/logging the employers use on the organization's devices with Internet access (pc, iPad, etc.)?
Issue	Early warning systems	Early warnings / weak signals provide information about potentially deteriorating safety before this is manifested in trends. It provides an opportunity to be proactive and take action at an early stage.
Indicator	Traffic against not open gates	Is the organization constantly monitoring traffic against not open gates?
Indicator	Spam mail frequency	Frequency of spam mails not detected by the spam filter
Issue	Information on continuously updated threat assessments	Actively seeking information on threat assessments ("threat levels") by e.g. authorities
Indicator	Cooperation with supplier	Are regular meetings with supplier(s) of the telecommunication system provided?
Indicator	Frequency of threat assessment updates	Frequency of threat assessment updates
Indicator	Coordination of threat level	Is the threat assessment coordinated according to a level of threat set by the authorities?
Indicator	Bulletins	Are bulletins of weekly/monthly/yearly summaries of new vulnerabilities established?
Issue	Alert systems	Utilization of fixed technical alert systems, identifying threats and/or increased level of threat.

Type	Issue name	Issue description
Indicator	Cyber alert system	Is a cyber alert system implemented for detecting and rectifying operational anomalies in essential equipment and systems?
Indicator	Water quality alert system	Is an alert system implemented for notifying deviations from predefined water quality?
Issue	Changes (technical, organizational, external)	Any changes, whether they are deliberate or not, may cause unintentional effects on safety and security. Close attention should be paid to changes with respect to potential negative effects.
Indicator	Loss of personnel (organizational)	When personnel quits, are there procedures to follow in order to assess loss of competence and replacement?
Indicator	Consequence assessment (organizational, technical, external)	Are the consequences of potential changes always assessed and evaluated?
Indicator	Testing before implementing (technical)	Potential changes are always thoroughly tested?
Indicator	"Fall back" solution (technical)	Do the organization provide a "fall back" solution?
Issue	Audits	Regular searching for problems/weaknesses/failures through audits (internal and/or external).
Indicator	Information security audit	Is an audit on the level of information security in the organization performed? (assessing integrity, confidentiality and availability)
Indicator	Frequency of audits	Frequency of security audits
Indicator	Cooperation with ICT experts	Are audits performed in cooperation with ICT experts through the whole process (planning and preparation, establish audit objectives, performing the review, etc.)?
Indicator	Audit report	Is an audit report prepared at the completion of each audit?
Issue	Robustness (functions/systems)	Resilience through robust design, e.g. large safety margins.
Indicator	Sufficient capacity	Is sufficient capacity on hardware and network provided?
Indicator	Segmentation of networks	Has the organization implemented zoning of communication network, separated process supervision system from administrator systems and Internet as much as possible?
Indicator	Data storage	Is the data storage system decentralized?
Indicator	Back-up copies of data	Frequency of backup
Indicator	Storage of back-up data	Are copies of important data kept at a different physical location or back it up over the Internet to a remote server, or both?

Type	Issue name	Issue description
Issue	Redundancy (functions/systems)	Resilience through redundant functions and/or systems.
Indicator	Redundant telecom lines	Are redundant telecom lines in place to secure communication?
Indicator	No. of telecom suppliers	No. of telecom suppliers
Issue	Back-up/alternative (functions/systems)	Internal back-up systems or alternatives.
Indicator	Back-up system	Is a internal back-up network/system available at the facility, plant, etc. if the communication between home-based computers and the facility breaks down?
Indicator	Emergency generator unit	For how long can the emergency generator unit provide the facility, plant, etc. with enough electricity to sustain production?
Indicator	Alternative water supply	Is an alternative water supply provided?
Indicator	Emergency water (not depending on the distribution network)	Is an emergency water solution provided (e.g. tanks, bottles, etc.)?
Issue	Security plans	Preparing for resilience through security plans.
Indicator	Prevention	Solutions, policies and procedures are identified to reduce the risk of attacks?
Indicator	Resolution	Have plans and procedures considering the resources that will be used to remedy a threat, been developed?
Indicator	Restitution	Are the organization prepared to address the repercussions of a security threat with their employees and costumers to ensure that any loss of trust or business is minimal and short-lived?
Issue	Emergency preparedness plans (and crisis organization)	Preparing for resilience through emergency preparedness plans, including pre-planned crisis organizations.
Indicator	Emergency preparedness plan/Incident procedures	Do the organization have an emergency plan for extraordinary events? (An emergency plan indicates that there is procedures and processes to follow in case of extraordinary events)*
Indicator	Cooperation in planning	Is the emergency preparedness plan executed in cooperation with relevant actors?
Indicator	Capacities within the emergency organization	Do the organization have an overview of capacities within the emergency organizations? *
Indicator	Communication plan	Is a communication plan prepared?

Type	Issue name	Issue description
Indicator	Test the plans	Are the plans tested regularly to ensure all systems across the enterprise are included, and personnel and contact details are still valid?
Issue	Business continuity plans	Preparing for resilience through continuity plans.
Indicator	Continuity planning	Are there routines and continuity plans as a means to uphold the most safety-critical activities of the organization?*
Indicator	Business continuity testing	Is business continuity testing of potential issues conducted?
Issue	Training plans (table-top, simulator, drills, etc.)	Training plans on how to deal with potential scenarios is essential in order to know what to do, not only with respect to identical or similar scenarios as trained on, but also with respect to response to other (unexpected) scenarios. This includes the use of simulators, table-top exercises, emergency preparedness drills, etc.
Indicator	Cyber security training	Are plans for cyber security training of employees developed?
Indicator	Training and exercise plan	Are training and exercise plans, considering emergency preparedness drills, developed and adjusted according to level of threat?
Indicator	Communication training plan	Is a training plan provided related to communication procedures during an extraordinary event?
Issue	Joint exercises plans	Preparing for resilient emergency response through plans for joint exercises with external actors.
Indicator	Coordinated training and exercise	Are training and exercising plans coordinated with relevant external actors?
Issue	Adaptability/renewal of training (timely revisions)	The repertoire of training scenarios should be reviewed and adapted regularly based on experience from own and other's accidents, and the training material updated accordingly. The training should cover a sufficiently broad specter of scenarios.
Indicator	Renewal of training scenarios	Are the training plans adapted regularly in order to fit modern cyber attack strategies?
Indicator	Specter of scenarios	Are there routines to develop new training scenarios on the basis of tests, audits, monitoring and authority recommendations?
Indicator	Frequency of renewal	Frequency of training plan reviews
Issue	Cooperation agreements (external resources)	Pre-planned agreements of use of external resources in crisis situations.

Type	Issue name	Issue description
Indicator	Pre-planned agreements	Has the organization established pre-planned agreements with relevant external actors in crisis situations?
Indicator	Routines for communication with cooperating actors	Have the organization routines for communication with cooperating actors (security firms, suppliers, etc.) in case of an extraordinary event?
Issue	Physical entrance control	Physical barriers and other systems to prevent unauthorized entrance of areas, buildings, rooms, etc.
Indicator	Surveillance of facility, plant, etc.	Are cameras in place outside and inside the facility, plant, etc.?
Indicator	Access	Are personal access secured by cards and personal code?
Indicator	Limited access to critical/restricted areas	Are access to security restricted areas controlled in order to ensure that no unauthorized persons and vehicles enter these areas?*
Indicator	Burglar alarm	Is a burglar alarm in active use?
Indicator	Security guards present	Are security guards present at the facilities, plant, etc.?
Issue	Cyber entrance control	Barriers and systems to prevent unauthorized access to IT systems.
Indicator	Personal password	Are personal passwords mandatory?
Indicator	Password strength	Are there requirements to password strength?
Indicator	Frequency of password renewal	Frequency of password renewal
Indicator	Multi-factor authentication	Multi-factor authentication when accessing the IT systems?
Indicator	Previous employees	Are there established procedures for removing access from previous employees?
Indicator	Categorization of users	Is it secured that only personnel needing access have access?
Indicator	Limited access to critical functions	Are critical functions protected against unauthorized personnel?
Issue	Planned maintenance	Planned maintenance of critical systems and equipment to ensure adequate functioning.
Indicator	Routines for maintenance	Do the organization have routines for when and how the operational control system may be taken down for system maintenance and upgrading?*
Issue	Smartness vulnerability in the anticipate/prepare phase	Are there any smart features ("smartness") included in the critical infrastructure(s), which makes it more difficult to anticipate what may happen and/or prepare for it, e.g. if failures occur in these smart features?
Indicator	Manual operation testing	Frequency of testing of manual operation

Type	Issue name	Issue description
	Phase III - Absorb/withstand	
Issue	Passive safety systems	Passive physical safety systems designed into the critical infrastructure to prevent (access of) threats or any escalation of an event.
Indicator	Water flow	Are pumps needed to "push" the water through the treatment process?
Indicator	Manual operation	Is it possible to treat and deliver water without the use of ICT systems?
Issue	Active safety systems	Automatic and/or manual safety systems to detect/prevent/ withstand an event.
Indicator	Detectors	Are detectors present to detect abnormalities in the water quality?
Indicator	Follow-up routines	Are routines established to follow-up suspicious activities (high outgoing traffic, strange looking files, etc.)?
Indicator	Firewall	Is the firewall always switched on?
Indicator	Software	Is the software continuously updated?
Indicator	Anti-malware solution	Are anti-malware solutions installed and regularly updated?
Indicator	Sensor network	Is the critical infrastructure a part of the national sensor network - Varslinssystem for digital infrastruktur (VDI)?
Issue	Notification/alarm	Notification of an event, e.g. by releasing an alarm, as soon as possible to the responsible unit, e.g. a control center.
Indicator	Alerting and notification software	Are activity logs accompanied by alerting and notification software and options that can be configured to alert/notify responsible personnel?
Indicator	Intrusion detection system (IDS)	Are IDS used to supplement the firewalling systems and access control systems by providing intrusion notification?
Indicator	Alarms for water quality deviation	Are alarms going of when deviations in water quality are detected and responsible personnel are notified?
Indicator	Alarms for failure in equipment	Are real time alarms created in the operational control system when any equipment fail in distributed or pump station?
Issue	Confirmation of threat/event	Confirming that the threat/event is real, and what kind of threat/ event it is.
Indicator	Signs	Are personnel trained to know what signs to take seriously (e.g. through e-learning courses, lectures, etc.)?
Indicator	Alerts	Are defense systems with notification mechanisms installed?

Type	Issue name	Issue description
Issue	Action plan - reaction (availability, familiarity, use)	Availability, familiarity with, and use of pre-planned action plans for immediate reaction to an event.
Indicator	Action plan - reaction	Are measures and strategies on how to secure a robust reaction included in the action plan?
Indicator	Tailored action plan	Has the organization constructed an action plan tailored for the relevant threat?
Indicator	Available action plan	Is the action plan available for relevant personnel?
Indicator	Familiarity	Are personnel familiar with where to find the action plan?
Issue	Competent personnel	Competent/experienced personnel are required to obtain a resilient reaction to withstand an (expected or unexpected) event.
Indicator	Certified operators	No. of operators certified with relevant education and/or courses?
Indicator	Certification level	Is it secured that responsibilities are aligned with certification levels?
Indicator	ICT competence	No. of personnel with a formal ICT education
Indicator	Monitoring competence	Is an overview of competence gained, lost and needed through obtain e.g. trough monitoring of personnel starting and leaving?
Indicator	Training of personnel	Have relevant personnel been provided with suitable training towards managing the tasks responsible for during an extraordinary event?
Indicator	Switch to alternative water supply	Is it ensured that key personnel know how to switch to alternative water supply?
Indicator	Switch to generator power	Is it ensured that key personnel know how to switch to generator power and know the fuel requirements for the generators?
Indicator	Cooperation with other actors	Is cooperation established with other actors (e.g. other municipalities, similar organizations, etc.) for competence exchange?
Indicator	Competence of suppliers	Is the choice of suppliers based on a competence assessment?
Indicator	Gaining competence	How often do representatives for the drinking water organization meet with relevant external experts?
Issue	Emergency response organization mobilization	Mobilization/scrambling of the emergency response organization.
Indicator	Mobilization checklist	Do the organization have an mobilization checklist to follow?

Type	Issue name	Issue description
Indicator	Up-to-date contact information	Is the contact information on people and entities that may need to be contacted when a incident occur regularly reviewed and updated (both internal and external personnel)?
Issue	Notification of response resources	Notification of required internal and external response resources according to action plan.
Indicator	Organization's resources	Is the mobilization of the organization's resources based on severity of incident and stated in the action plans?
Indicator	Responsible for delegation of response activities	Is the person responsible for delegate response activities during extraordinary events known to the staff?
Indicator	Notification routines	Are notification routines regarding who, when and how to notify, stated in the action plan?
Indicator	Responsibility awareness	Is the organization aware of how the responsibility is divided between the cooperative actors in case of an extraordinary event?
Issue	External alert/communication	Alerting, informing and communicating with relevant external stake-holders, e.g. head office, authorities, etc.
Indicator	Communication with cooperating actors	Have the organization routines for communication with cooperating actors in case of an extraordinary event?
Issue	Adapt (stop/reduce) operation	Adaptation of the operation according to the event e.g. reduces, minimize or stop operations.
Indicator	Supply water manually	Are there available procedures on how and when to start manual operation and supply?
Indicator	Alternative water source	Are there available procedures on how and when to use the alternative water source?
Issue	Start combat/handling of threat/event	Combat of threat/event with required available resources.
Indicator	CERT/CSIRT function	Is a CERT/CSIRT function available?
Indicator	Incident response unit/crisis management team	Do the organization has access to a dedicated team trained to deal with attacks are accessible internally or externally when needed?
Indicator	24-hour-a-day, seven-day a week rota	Are there on-duty personnel that are always available?
Indicator	Emergency preparedness plan	Are combat procedures stated in the emergency preparedness plans?
Indicator	Availability of external resources	Do the organization provide the possibility to call for external resources 24-hour-a-day, seven-day a week?

Type	Issue name	Issue description
Issue	Communication (status update)	Communicating the status of the situation during the initial response as relevant (internally and externally).
Indicator	Immediate response communication checklist	Do the organization has a immediate response communication checklist to follow, which include guiding principles?
Indicator	Most efficient communication strategy	Is the most efficient communication strategy is assessed (e.g. E-mails, in-person meetings, internal social media meetings, phone calls, etc.)?
Indicator	Signatory of communication	Is the signatory of communication sent internally and externally established?
Indicator	Consumer communication	Do the organization provides the possibility to notify the public through efficient channels if water outage/unfit for drinking?
Issue	Authority contact/liaison	Establishing contact/liaison with authorities and communicate regularly during initial response.
Indicator	Authority communication routines during initial response	Are authority communication routines and guidelines established in the communication plan?
Issue	Media handling	Use of dedicated resources for media handling during initial response.
Indicator	Press officer/media handling responsible	Is a press officer or other media handling personnel appointed during the initial response?
Indicator	Media handling strategy during initial response	Are guidelines regarding how to handle the media during initial response stated (e.g. in a media handling strategy)?
Indicator	Media agreement	Have the organization established agreements with local media channels to provide the public with secure and updated information if water outage/unfit for drinking?
Indicator	Previous events	Are previous similar events (local or global) taken into consideration when developing the best media handling strategy?
Indicator	Press release	Is a basic press release that can be quickly adapted during a crisis, established?
Issue	External decision support (at various levels)	A situation may require the support from outside own organization. Thus, the necessary external support, including accompanying ICT systems, must be available when required.

Type	Issue name	Issue description
Indicator	Security firms	Do the organization have an agreement with a security firm providing decision support during extraordinary event?
Indicator	Available telecom suppliers	Are the telecom suppliers available on a 24-hours basis?
Issue	Coordination between actors (at various levels), internal	Coordination within each emergency response team, coordination of all resources/teams at the scene of the event (or nearby), local coordination of the entire emergency response operation from a central emergency response center, etc. Sharing of information.
Indicator	Clearly defined responsibilities	Are the responsibilities to each response team/each member in between a response team clearly defined?
Indicator	Internal coordination	Are procedures regarding internal coordination during an incident established?
Issue	Coordination between actors (at various levels), external	External coordination with area, regional or wider resources, including headquarters, authorities, etc. Sharing of information.
Indicator	External coordination	Are procedures regarding external coordination during an incident established?
	Phase IV - Respond/recover	
Issue	Resourcefulness/emergency response resources (internal)	Internal emergency response resources and response/ mobilization time. Equipment (fixed/mobile, automatic/manual, etc.), personnel, organization, etc.
Indicator	Requirements awareness	Do the organization provide an overview of the material and personnel resources most critical to manage an extraordinary event?
Indicator	Assessing appropriate response resources	Average time between discovering the event to adequate use of response resources are assessed
Indicator	Initiate response plan	Average time needed to initiate response plan
Indicator	Inform personnel	Average time needed to inform relevant personnel
Indicator	Reaction time during night	Reaction time from receiving the notification to on-duty personnel is present at the facility
Indicator	Are the responses/remedial actions effective? (feed flow)	Response time to restore feed flow*
Indicator	Are the responses/remedial actions effective? (damaged equipment)	Response time to restore damaged equipment*

Type	Issue name	Issue description
Indicator	Performance assessment	Has a performance assessment of response and recovery been conducted?*
Issue	Resource allocation and staffing (including buffer capacity)	Sufficient number of persons attending to critical functions, including back-up personnel in case of additional needs, unavailability of personnel or exchange of personnel. Duty schemes enabling adequate mobilization to provide timely response are needed.
Indicator	Vacation routines	Is vacation routines regarding competent personnel available at all time established and implemented?
Indicator	Appropriate rota system	Is an appropriate rota system implemented to ensure sufficient amount of back-up personnel?
Issue	Emergency response resources (external)	External emergency response resources and response/ mobilization time. Equipment, personnel, organization, agreements/contracts, etc.
Indicator	Inform cooperating actors	Average time needed to inform cooperating actors
Indicator	Mobilization time	Average time needed for external response resources to be present at the facility, plant, etc. after received alarm
Issue	Communication between actors	Response is often dependent on information from other actors. It is essential that the (local) information and communication systems are available throughout the duration of the situation until control has been regained. The information itself needs to be understandable for all actors involved (including use of common language).
Indicator	Establish communication with telecom supplier	Is communication with telecom supplier established immediately after incident detection? The communicating parts should provide more or less the same high degree of competence concerning the threat
Indicator	Emergency communication channels	Are emergency communication channels established?*
Indicator	Communication procedures	Has the organization developed communication procedures to follow during response?
Indicator	Redundant communication alternatives	Are redundant communication alternatives available to secure the communication systems throughout the duration of the situation?

Type	Issue name	Issue description
Issue	Robustness of responsible function	Endurance of critical functions to complete the response. This includes personnel in charge of critical tasks as well as the upholding of critical infrastructure systems (e.g. main safety functions).
Indicator	Robust response	Is the number of available competent personnel considered sufficient to provide a robust response (based on tests, trainings, real incidents, etc.)?
Indicator	Duration of manual operation	For how long can the water be supplied by manual operation?
Indicator	Alternative water supply sustainability	For how long can the alternative water source sustain the water supply?
Indicator	Emergency water (not dependent on the distribution network)	For how long can the cans, tanks, bottles available sustain the city with water?
Issue	Organizational robustness (back-up functions)	Even if single persons are unavailable for some reason the critical functions should be ensured through pre-planned back- up, e.g. by deputies given the same training as the main responsible persons.
Indicator	Deputies	Are deputies given the same training as the main responsible persons?
Indicator	Access solutions	Are temporary access solutions to the most critical functions provided to specific personnel if the administrator is away from work over a longer period of time?
Issue	Action plan - response (availability, familiarity, use)	Availability, familiarity with, and use of action plans for response actions.
Indicator	Action plan - response	Do the action plan includes measures and strategies on how to secure a robust response?
Issue	Training (table-top, simulator, drills, etc.)	Training on how to deal with potential scenarios is essential in order to know what to do, not only with respect to identical or similar scenarios as trained on, but also with respect to response to other (unexpected) scenarios. This includes the use of simulators, table-top exercises, emergency preparedness drills, etc.
Indicator	Emergency training of personnel	No. of personnel provided with yearly emergency training
Indicator	Security awareness training	No. of personnel provided with regular security awareness training
Indicator	Communication training	No. of personnel provided with emergency communication training
Indicator	Incident management training	Have relevant personnel been through the incident management training?

Type	Issue name	Issue description
Indicator	Training consistency	Is the training consistent with existing regulations, standards, codes of practice and requirements of regulatory authorities?
Issue	Joint exercises	Resilient response and recovery through joint exercises with external actors.
Indicator	Frequency of joint exercises	Frequency of joint exercises
Issue	Combat threat/event	Combat threat/event until the situation is fully under control. This may require exchange of exhausted response personnel.
Indicator	Combat procedures	Do the combat procedures stated in the emergency preparedness plan include responding guidelines?
Indicator	Combat personnel	Are suitable work shifts established to prevent exhausted response personnel?
Issue	Communication (status update)	Communicate the status of the situation during response and recovery as relevant (internally and externally).
Indicator	Secondary response communication checklist	Do the organization have a secondary response communication checklist to follow after immediate response?
Issue	Authority contact/liaison	Establish contact/liaison with authorities and communicate regularly during response and recovery.
Indicator	Authority communication routines during response and recovering	Are authority communication routines and guidelines established in the communication plan?
Issue	Media handling	Use dedicated resources for media handling during response and recovery.
Indicator	Media handling strategy during response and recovery	Are guidelines regarding how to handle the media during response and recovery stated in a media handling strategy?
Issue	Repair damages (unplanned maintenance)	Repair any damages to the critical infrastructure.
Indicator	Repair strategy	Is a repair strategy in place covering prioritized order of repair?
Indicator	Repair strategy efficiency	Has the repair strategy been tested towards the considered threat?
Issue	Risk assess and clarify re-start/continuing operation	Make risk assessment and clarifications (including approvals) before re-start/ continuing of operation.
Indicator	Quality control measures	Are there procedures for quality control before restarting operation?
Indicator	Checklist	Is the staff required to work through a post-restart checklist?

Type	Issue name	Issue description
	Phase V - Adapt/learn	
Issue	Debriefing	Provide a debriefing of the event and the response operation to personnel directly involved.
Indicator	Timing of debriefing	Is the debriefing conducted within a week after the incident?
Indicator	Crew coordination	Is debriefing of crew coordination conducted?
Indicator	Determining the cause	Is an analysis of the possible causes performed?
Issue	Media handling	Provide information to the media about what happened, the response operation, investigations, follow-up of involved persons, etc.
Indicator	Media handling strategy after an incident	Are guidelines regarding how to handle the media after an incident stated in a media handling strategy?
Indicator	Review of media strategy	Are there routines established for reviewing and updating the media handling strategy after an incident?
Issue	Event investigation and reporting including recommendations for adaptation/improvement	Investigation of event, including underlying causes, and recommendation for adaptation/improvement of operations (physical, technical, operational, organizational, etc.).
Indicator	Event analysis	Has the organization established a process for event/incident investigation that ensures that the underlying as well as immediate causes of events/incidents are understood, taking full account of human and organizational factors?
Indicator	Prevent recurrence	Has the organization established a process for ensuring that the findings of investigation and analysis are acted upon in a timely fashion and suitable interventions put in place to prevent recurrence of the incident or similar incidents?
Indicator	Security assessment	Is an evaluation of current security measures and barriers carried out after an incident?
Indicator	Employee involvement	Is the organization encouraging employee involvement during event investigation?
Indicator	Recommendations	Do the organization provide the possibility to obtain improvement recommendations from experts (internally or externally)?
Indicator	Updating of risk- and vulnerability analysis	The risk- and vulnerability analysis is updated after an incident
Indicator	Updating of emergency preparedness plans/incident protocol	Are there routines for emergency preparedness plan/incident protocol updating after an incident?

Type	Issue name	Issue description
Issue	Presentation/communication of event investigation	Presentation and communication of the results of the investigation internally and externally (notifications, reports, presentations, press conferences, etc.).
Indicator	Disseminating information	Has the organization established a routine for dissemination of information on incidents/events causation and suitable interventions/modifications to all relevant parties (both internal and external), as quickly as possible?
Indicator	Communication channel	Is the most suitable communication channel established for all relevant parties (e.g. meetings, e-mails, phone calls, etc.)?
Issue	Implementation and follow-up of recommendations for adaptation/improvement	Implement and follow-up the recommended adaptations/ resilience improvements.
Indicator	Communication of identified improvements	Are identified improvements communicated to decision makers?
Indicator	Consider recommendations	Do the organization have routines to consider recommended changes to prevent similar events from happening again?
Indicator	Monitoring of progress	Are the organization monitoring progress and following up recommendations arising from incident investigation?
Indicator	Follow up employees	Are employees regularly followed up in their work to check if new procedures are followed?
Indicator	Evaluating the success	Has the organization established a routine for evaluating the success of interventions and modifications?
Issue	Emergency response operation reporting including lessons learned	Reporting of the response operation and any lessons learned for future emergency response and resilience improvements.
Indicator	Incident reporting format	Has an effective incident reporting format been developed?
Indicator	Record and report outcomes	Are outcomes of the event investigations recorded and reported?
Indicator	Assessing emergency plans and routines	How well did the last exercise fulfill the goals?*
Indicator	Documentation of resources	Has the organization established routines to evaluate if the resources available were sufficient to handle the event?
Indicator	Sufficient competence	Has the organization established routines to evaluate if the available competence was sufficient to handle the incident/event?

Type	Issue name	Issue description
Issue	Implementation and follow-up of lessons learned	Implementation and follow-up of the lessons learned from the emergency response operation (resources, capabilities, etc.).
Indicator	Update training and exercise plans	Are training and exercise plans updated according to the lessons learned, having in mind suitable competence?
Indicator	Update documentation of resources	Are the resources available updated according to the resource evaluation?
Indicator	Update communication checklists	Is the communication plan/checklist regularly reviewed, including details of communication channels, contact lists, guidelines, etc.?
Issue	Presentation/communication of emergency response operation	Presentation and communication of the lessons learned from the emergency response operation internally and externally.
Indicator	Communication of emergency response	Are appropriate communication channels determined, based on the content and format of information?
Indicator	Speed of communication	The speed with which the information can be shared with all relevant parties
Indicator	Evaluation of information	Is an evaluation of the nature of the information that is to be shared (i.e. details of lessons learned) performed prior to communication?
Issue	Feedback and learning from successful operations	Providing feedback and learning from successful operations in addition to event investigations, which focus on improving unsuccessful operations.
Indicator	Yearly report	Is the organization conducting a yearly summarizing report, addressing both successes and failures compared to goals stated in the action plan?
Indicator	Feedback to personnel	Do the organization arrange meet ups for communication and positive feedback to personnel?
Issue	System/archive to store knowledge	System/archive to store and retrieve knowledge/experience/ lessons learned from events and response operations.
Indicator	Capture information	Do the organization have a system to capture the information in a format that is readily searchable and retrievable to allow ease of access?

6 Discussion

There is an increasing realization that building resilience is an important component of enhancing the sustainability of many systems, also in the water industry (Diao et al., 2016). The method presented in the previous sections is, as mentioned, developed by SINTEF. The case study and the methodology will be the basis for the following discussion. It should be mentioned that the issues and indicators do not represent a final resilience assessment for the chosen threats (due to limited access to the companies, the information was only gathered through four interviews and literature reviews), but suggestions of issues and corresponding indicators found relevant (the generic issues in appendix 5 is used as basis). Some of the indicators are generic (as for the issues) and can be representable for both threats, while some indicators are threat-specific. Also, the indicators "real values" (ref. chapter 3) will not be established, as best and worst values should be decided by the organizations themselves (e.g. what is good or bad considering response time is not known by the author of this thesis). However, most of the desired answers on the yes/no questions are obvious. The threats considered above will be separately deliberated with respect to the suggested issues and indicators. In addition, some method pros and cons will be discussed.

6.1 Water pipe leakage

In the following, the issues and indicators considered relevant for a leakage will be discussed. Not all of the issues/indicators suggested in table 5.1 will be included, as some of them are obvious. The discussion will be divided in accordance with the resilience phases.

Leakages varies in severity from small leakages that is very hard to detect, to complete pipe ruptures causing flooding on the surface. This means that not all indicators will be relevant for the whole range. E.g. leakage listening is not relevant for complete pipe ruptures as these will be visible on the surface, or media handling is not relevant for small underground leakages. However, in order to stay resilient towards any kind of water leakage, the whole range from small leaks to flooding events needs to be considered. As water leakages on the distribution system only accounts for the municipality of Stavanger, IVAR will not be taken into consideration in the following.

6.1.1 Understanding risk

In this phase, nine issues were identified as relevant for the water supply in Stavanger considering the mentioned threat. Parts of the distribution network are considered especially vulnerable towards water leakage, as the case study revealed. These parts are important to be aware of as it provides insight in how the system may fail, and the potential consequences. Thus, the degree of system knowledge could be measured by thoroughly addressing the external operational conditions throughout the municipality, as soil characteristics (type of soil, movement, acidity, etc.) and traffic loading, and assessing the overall condition of the distribution network, including its design. Also, the chosen method for leakage control should be questioned according to its effectiveness. Is the chosen method considered the most effective or is it compromised?

Risk understanding is enhanced by basic knowledge of the concept of risk, and by specific knowledge about the risk related to the particular system/network. Thus, the vulnerabilities and critical areas of the distribution network should be communicated to relevant personnel in order to raise awareness of the potential consequences and increase the knowledge about which aspects of the system that contribute the most to the risk. Also, by addressing the number of vulnerable consumers on the basis of consumers not covered by ring mains or living in areas of bad corrosion protected water pipes, a more complete picture of the risks and associated consequences are provided.

The potential socioeconomic impacts of disruptions in the water supply are included as an indicator relevant for the knowledge about context due to many reasons. It provides community overviews (e.g. of vulnerability), it enables vulnerability comparisons between other communities, and the possibility to track potentially progress in risk reduction or recovery is obtained. This is an important indicator due to the society's dependency towards a predictable and secure drinking water supply. However, this is only relevant for larger water leaks. Furthermore, the municipality should understand the geographic context and local circumstances affecting the water distribution system and which could cause leakages of different severity. Even though the probability for an earthquake happening in the municipality of Stavanger is considered very low, it should be assessed when evaluating resilience.

Information about real events and incidents provides the municipality with knowledge and insight in what may go wrong in the future, hence understanding the risk. An event/incident reporting system is a key element in any system for learning lessons. If incidents are not reported, lessons cannot be learned. This is why good and effective reporting routines and appropriate leak reporting systems that encourage reporting are so important. The format and content of the information captured by the reporting system is also important. To enable effective follow-up and analysis of the incident data, causal information needs to be captured. Thus, the efficacy of reporting should be monitored and reviewed regularly. The same counts for failure data gathering, where technical failures are considered. As small leak events could indicate vulnerable pipes and areas on the distribution network, technical failures in pumps, valves, etc. are providing valuable information about their operating state.

The quality of barriers and their support functions are important to assess for proper risk understanding as it provides information about the technical systems that prevent the development of an accidental event. The water balance is indicating the water losses (amount of water put into distribution is compared with the sum of the components of water consumed or used), which also provides information regarding the system integrity. Standard methods have been developed to estimate the different components of the water balance (see Van Zyl, 2014, pp. 47-48), and should be calculated and analyzed on an annual basis. The municipality should operate and maintain the system in such a way that water losses are minimized. Even though the expanded treatment facility at Langevatn provides efficient treatment towards corrosive water, the pipes constituting the distribution network should be of good quality and corrosion protected in order to provide a secure and reliable water supply and reduce the number and severity of leakages. In addition, regular pipe inspections should be performed. Consumer complaints are normally due to the esthetic water quality or due to lack of pressure from the tap. Thus, consumer complaints should be taken seriously as lack of

pressure could indicate a leak on the distribution system. Further, for the water supply to be resilient towards water leakages, it should be tested under various stress-load scenarios and recovery conditions. Water meters, pumps and valves are barrier support functions. The quality of these should be taken care of through preventive maintenance plans.

The involvement of senior management is important for staff motivation, engagement and initiative. The senior management should regularly perform internal controls as established in the regulations (Drikkevannsforskriften), to achieve security, reliability, resiliency and recoverability. Further, the senior management should evaluate threat trajectories based on the event reports and failure gatherings from a position of risk profiling and business acceptability. The senior management should also establish a leakage management strategy (passive control, regular survey (sounding, waste metering), and/or leakage monitoring in zones or sectors) tailored towards the drinking water supply in Stavanger, based on availability, capacities and resources, and economy.

6.1.2 Anticipate/prepare

In the second phase, nineteen issues were identified as relevant for water leakages on the distribution network. To be able to measure the municipality's ability to anticipate and prepare for the mentioned threat, relevant indicators for each of the considered issues were identified. Systematic risk/hazard identification is a prerequisite in order to anticipate what may go wrong. A risk- and vulnerability analysis should be conducted, as it is useful for planning and decision-making as probabilities and consequences related to the relevant threat is assessed. For the risk- and vulnerability analysis credibility, the analysis should be performed in cooperation with relevant experts and agents involved. In the risk- and vulnerability analysis conducted for the water supply in Stavanger, water leakages are considered high probability – low consequence kind of events, due to pipe dimension and the robust network design that makes it possible to isolate leaks and still deliver water.

The municipality's ability to learn from own and other's events and experiences are important to measure, as it is highly desirable to avoid the reoccurrence of undesirable events, as mentioned above. Thus, the municipality should keep records covering the exact position of the leak, cause and type of leak, repair carried out, pipe material and size, and whether pipe replacement was necessary. Also, verified theoretical models that describe the steps a company needs to take in order to learn from events and incidents are available, and should be used to secure an effective and consistent methodology for this purpose. For the lessons learned to stay "learnt" they should be disseminated throughout the organization. The possibility to learn from other's events and experiences should not be overlooked, and procedures for actively searching after relevant information from other sources should be established and maintained, e.g. by convene cooperative forums for internal and external actors in order to share experiences. This could contribute to the identification of new leakage scenarios not thought of by the municipality itself.

The status on risk, events and quality of barriers compared to threshold values, provides information on where to focus attention. By organizing regular status meetings, values obtained from e.g. failure data gathering and event reports could be discussed and compared to relevant thresholds, and further displaying the standing condition of the

distribution network. As the municipality of Stavanger focused upon pipe renewal in order to reduce the number of leakages caused by bad quality pipes, this is included as an indicator when assessing the resilience towards water leakage. The goal was a replacement rate of 1 percent per year, thus it is naturally to compare the yearly replacement rate obtained to this value when performing the resilience calculations. The indicator Infrastructure Leakage Index (ILI) is used to quantify improvements in loss management and benchmark the municipality against others. ILI is calculated by the ratio between the current annual real losses (CARL) and the unavoidable annual real losses (UARL) (for calculations see Van Zyl, 2014, pp. 50), and is assessing the real (physical) water loss form the supply network of water distribution systems. Furthermore, the overall functionality of the distribution network in Stavanger is yearly provided with a quality index and compared to other municipalities, functioning as a yearly status update.

The trends in risk, events and quality of barriers can be measured by monitoring the frequency of water meter failures, of pumping failures, of valve failures and of bursts, showing negative development and provides indications on the need to take action to remedy the situation. As the daily water distribution in Stavanger is dependent on the pumps, valves and water meters to function optimally, the data provided from the monitoring of these devises should be the main source of information used to establish trends and hence support decisions. Yearly reports should also be considered when evaluating trends in risks, etc. but as these are not provided on a daily basis the actions needed to counteract negative developments should mainly be based on continuously monitoring of equipment integrity.

Continuous monitoring will also provide information regarding possible leakages on the distribution network. E.g. sudden pressure changes could indicate leaks, as leakage has been found to be very sensitive to system pressure. Further, by monitoring the water consumption, e.g. by the use of water meters, deviation from normal consumption will be revealed and should be investigated. Temperature should also be monitored as temperature changes could cause soil movement that again could cause a pipeline to break. Also, the flow rate should be monitored, as a large drop in flow rate indicates leaks.

Regular searching for problems, failures and weaknesses through internal and/or external audits are recommended. A water audit quantifies the total water losses and leakage in a network. The water audit has two components: 1) system appraisal, and 2) water balance calculation (as introduced above). The purpose of the appraisal is to regularly review (Farley, 2001):

- Regional characteristics (e.g. influencing factors, components of water loss)
- Current practice and methodologies
- Level of technology
- Staff skills and capabilities
- The municipality's data and methodology for the water balance calculations.

An audit report should be prepared at the completion of each audit. It should include a description of findings, including recommended improvements or remedial measures, together with timelines.

Robust design is a prerequisite for a resilient water distribution system. Thus, each component in the pipe network should be designed to function correctly under the local conditions. Pipe diameters should be selected on the basis of desired flow rate, pressure requirements, and trade-off between capital and operational costs. E.g. consider a case where the designer of the distribution network can choose between a smaller and larger pipe diameter for the system. The smaller diameter pipe will be less costly to construct, but due to greater friction losses more energy will be required to pump the water (meaning higher operational cost). Conversely, the larger pipe diameter will be more expensive to construct, but the operating costs will be lower due to less energy required. Furthermore, the system should be capable of handling diurnal peak demand during peak demand periods and the future demands should also be accounted for. Also, by dividing the distribution network into several zones, will help the engineers to understand and operate the system in smaller areas, and allows better leakage management and control to take place. Water meters linked to a central control station via telemetry so that the flow data are continuously recorded provide this. By analyzing these data, particularly of flow rates during night, it could be determined whether consumption in any zone has progressively and consistently increased, which could indicate a burst or undetected leak. The "zoning" makes it easier to locate the position of the leak.

The system redundancy could be provided through e.g. the use of ring mains/looped pipe network, emergency connection points, and isolation valves. Ring mains have the advantage that each point in the network can be served through multiple routes, and thus, supply water to most consumers even when pipes are isolated for maintenance work. Isolation valves should be placed in such a way that they allow for the isolation of sections of the system with minimum impact on the rest of the network. Also, to secure a reliable telecommunication system, redundant telecom lines with different suppliers should be in place. Further, backup systems like emergency water, which supply is not dependent on the distribution network (water bottles, tanks, etc.), and emergency generator unit to secure electricity should be available.

Emergency preparedness plans are important in the planning for resilience. Emergency preparedness plans indicates that there is procedures and processes to follow in case of extraordinary events. This do not account for small leakages, which detection and repair happens on a weekly basis. However, if a complete pipe burst occurs on a vulnerable point of the distribution network, e.g. on the single pipeline providing Åmøy with water (see appendix 4), this would cause temporary water outage for the people living there. Procedures on how to handle such incidents should be stated in the emergency preparedness plan. Also, relevant cooperating actors, like asphalters and road workers, should take part in the planning of extraordinary events, as these services are necessary for an efficient response. A communication plan should also be prepared. Training and exercise plans on how to deal with potential scenarios should be complementary to the emergency preparedness- and communication plans.

Maintenance actions can be classified into proactive/planned and reactive maintenance. As unexpected failures are bound to occur even in the best-maintained systems, it will never be possible to only do proactive maintenance. However, it is important to do proactive maintenance to such an extent that unplanned failures are kept to a minimum

and resources can be used in the most effective manner to ensure the integrity of the system.

6.2.3 Absorb/withstand

In the absorb/withstand phase, thirteen relevant issues were identified from the table in appendix 5. The event has now occurred, and the municipality's ability to provide a resilient reaction to absorb and withstand the event is supposed to me measured. Active safety systems should be in place to detect, prevent and withstand a water leakage. Constant monitoring of the distribution network would help to detect too high/low pressures, flow rate deviations and abnormal water consumption. By installing water meters at strategic places on the distribution network (zoning) also the leak location will be easier to identify. Telemetry systems that raise alarms for such conditions mentioned above should be installed to secure a rapid notification to responsible personnel.

The possibility to confirm that the leak is real, and its severity, should be obtained by the use of a software that arrange logged data into a form where it can be used for analyzing and interpretations. In addition to manual nightly leakage listening that could be more effective to identify smaller leaks, as these will not always provide visible deviations in pressure and flow. In a telemetered system, night flow data can be received and analyzed regularly. This enables changes in the night flow to be quickly identified, and hence reducing the awareness time. When compared with previous readings, it enables the "leakage control team" to prioritize inspections. Such logger software typically contains an "error table" which identifies the zones where night flows deviate from a pre-set alarm level. The error table could be scanned on a daily basis to identify unreported burst or, in response to poor pressure complaints, to confirm a reported burst.

Competent and experienced personnel are a prerequisite for obtaining a resilient reaction to withstand an event, thus it is important to be aware of the competence available and the competence missing throughout the department, e.g. by monitoring new personnel and personnel leaving. Design, installation and management of water distribution systems can involve a range of personnel, all of whom must be competent to undertake both required and assigned tasks. This involves training sessions, relevant education, certification and registration. Certification could include a series of levels through which personnel can progress and should preferably include considerations of both experience and training. Responsibilities should be aligned with certification levels (World Health Organization, 2014).

When the leak is detected and confirmed, a notification of required internal and external response resources should be issued according to the action plan. The action plan should be tailored for the municipality in Stavanger, with measures and strategies on how to secure a robust reaction. The mobilization of the resources should be based on the leakage severity and urgency. However, the possibility of a full emergency response should be available if necessary, thus proper notification routines regarding who, when and how to notify is important for the sake of an effective response. In addition to available personnel, both internally and externally, on a 24-hour-a-day, seven-day a week basis. Thus a proper rota system should be established. Also, clear responsibility division between cooperating actors is important to be aware of. Standard operating

procedures (SOP) should be in place to ensure rapid reaction and appropriate response to smaller leaks, while emergency preparedness plans and incident protocols are necessary to deal with larger breaks.

The most effective communication strategy should be established in order to provide regularly status updates during the initial response. Well-planned and well-executed communication, fully integrated into every step of a crisis and emergency response, can reduce the potential consequences of an event. The pre-prepared communication plan should include guidelines and/or checklists regarding communication at the beginning of an event. Routines regarding notification of consumers should also be in place if the leak is of such dimensions that the consumers are affected. If the leakage does affect the consumers, the media should also be contacted and handled. A media handling strategy should have been prepared, in addition to a basic press release that is easy to adapt according to situation and severity. Agreements with local media channels should also be established to provide the public with secure and updated information if water outage.

6.1.4 Respond/recover

In the fourth phase, respond/recover, fourteen issues were found to be relevant for a resilient response to, and recovery from, a leakage of various sizes and severities.

The internal emergency response resources and response mobilization time should be assessed and evaluated. Average time needed to initiate response plan, inform relevant personnel, repair damaged equipment and restore feed flow should be estimated on the basis of previous leak events and training and exercise sessions. Furthermore, the time needed to inform external resources and the time needed by the external emergency response resources to mobilize, are also important measures to include when the overall mobilization time is to be assessed. To secure a robust response, all critical functions should be covered, also during vacation seasons. Thus, vacation routines regarding competent personnel available at all time should be established and implemented.

The communication provided during an event is crucial for effective response activities. Response is often dependent on information from the different actors, thus it is essential that the information and communication systems are available throughout the duration of the situation until control has been regained. The most effective emergency communication channels should be in place and known to the relevant parties of the response team (both internal and external), in addition to the communication procedures to follow during the event. Communication and messages should be adjusted according to the level of response needed.

Training on how to deal with potential scenarios is essential in order to know what to do, not only with respect to identical or similar scenarios, but also with respect to response to other (unexpected) scenarios. Training and exercise sessions should be executed both internally and through joint exercises with external actors. As already mentioned, leakages on the distribution network are considered high probability, low consequences kinds of events. Last year, almost two leaks were detected every week (99 in total). The leaks were detected and repaired without any severe consequences for the consumers. Pipe bursts that causes large leaks and water outage on the other hand are rare types of leakage events that requires more comprehensive trainings and robust

responsible functions. An overview of number of personnel provided with yearly emergency training should be kept. The training should be consistent with existing regulations, standards and codes of practice and requirements of regulatory authorities, to secure a solid and relevant training and exercise content. Also, joint exercises should be carried out with relevant cooperating actors on a yearly basis. The ability to sustain the critical function of the infrastructure (i.e. supply of hygienically reassuring drinking water) should also be assessed and included in the training plans. This could be provided by addressing for how long the emergency drinking water (not dependent on the distribution network) could provide the city, district, area, zone, etc. with water, and the number of personnel needed and available to distribute it.

If the leak is of a more severe character, the leak location should be secured against traffic and people until the damage is repaired and normal operation is regained. The municipality should have procedures to follow for this purpose.

New technology enable rapid and accurate leak detection, but investing in rapid detection is futile unless repairs can be performed quickly. The time and complexity for repairs varies widely, from one employee needed to tightening a loose screw/nut to large crews and excavators spending days repairing deeply buried mains. Thus, a repair strategy should be established covering prioritized order of factors to repair when a leak is detected to provide efficient recovery of feed flow. Before re-starting the operation after a repair, a quality control should be conducted (e.g. by a second opinion, tests, etc.). This could encourage the personnel to be more accurate in the first place, as routine repairs might be executed "carelessly". Also, a post-restart checklist should be a requirement to follow before re-starting normal feed flow.

6.1.5 Adapt/learn

In the last and fifth phase, adapt/learn, ten issues were considered relevant for the water supply in Stavanager. The municipality's ability to learn from a leakage scenario is to be assessed and measured. A debriefing of the event and the response operation should be provided to the personnel directly involved. Through a debriefing process the crew coordination is evaluated in accordance to their performance. For the debriefing to be as efficient and valuable as possible it is recommended to conduct the debriefing within a week after the incident. However, it is not necessary to include the smallest leaks as these are considered routine procedures. Extraordinary events with a more severe outcome, on the other hand, should be evaluated and assessed with the response and performance in mind. The same accounts for the media handling during this phase. Only leaks with severe consequences require post-event media handling.

A system for determining which incidents that should be investigated should be in place, i.e. being able to identify those incidents where the circumstances will give rise to new lessons. If big investigations were initiated for even the smallest leaks, this would be a waste of resources. A proper investigation technique should be established, and include methods for the investigation of underlying as well as immediate causes. Appropriate investigation techniques should also ensure that all relevant people are involved in the investigation, so that important information is not missed. In addition, appropriate "ownership" of the investigation is important; it needs to be owned by people within the organization who holds the power to make sure that the findings are acted upon within

a reasonable timeframe, and that appropriate changes and interventions are carried out to prevent recurrence of the incident.

It is essential that the findings from the incident investigation are communicated to relevant internal personnel and external actors. Further, an effective system for acting on the findings should be established. The municipality should have routines to consider recommended changes and develop appropriate intervention plans accordingly (including timescales for implementation of any interventions or modifications and designated responsibilities for implementing corrective actions). The new procedures, modifications and/or interventions should be monitored, considering their effectiveness and success. It should regularly be evaluated whether the identified interventions have had the anticipated impact in terms of preventing the recurrence of similar incidents.

The emergency preparedness plans should be assessed, e.g. by considering how well the last emergency preparedness exercise fulfilled the goals. Routines for resource and competence evaluation should be in place in order to update the resources and competence available if necessary. Also, the training and exercise plans should be updated according to the lessons learned.

The dissemination of lessons learned from an emergency response operation is crucial. In an effective system for learning lessons, the information that is communicated should include details of the underlying and immediate causes of the event so that the opportunity for learning is not limited (Keeley, Gadd & Fullam, 2006). The speed with which the information can be shared with all relevant parties, and the quality of the information, is relevant for the effectiveness of the process.

A system or archive to store and retrieve knowledge, experiences and lessons learned from events and response operations should be available. To capture the information in a format that is readily searchable and retrievable to allow ease of access enables lessons learned to stay learnt.

6.2 Hacking of the water supply

In the following, the issues and indicators considered relevant for a hacker attack will be discussed. Not all of the issues/indicators suggested in table 5.2 will be included, as some of them are obvious. The discussion will be divided in accordance with the resilience phases. For this threat, both the municipality of Stavanger and IVAR are represented. As some of the indicators discussed above also counts for the coming discussion, these will not be included twice.

The severity of a hacker attack is dependent on the level of security, and the hacker's intentions and skills. Sometimes a hack attempt is obvious. More often, attacks are harder to recognize. Most hacks follow warnings that were overlooked: emailed tip-offs, both internal and external, about a potential security risk that was never read, phone calls that were ignored. The same cyber attack can mean different levels of severity for different businesses. It all boils down to the organization or company's security and awareness to early warnings. It takes companies an average of 229 days to discover a malicious attack (Palmer, 2016).

6.2.1 Understanding risk

In the first phase, nine relevant issues were identified. It is important to understand risk from an ICT security perspective in order to respond to factors that may lead to a failure in the confidentiality, integrity or availability of the system. ICT security risk is the harm to a process, or the related information, resulting from some purposeful or accidental event that negatively impacts the process or the related information (Elky, 2006). In general, the knowledge about ICT security risks related to the water supply in Stavanger needs to be increased, as admitted by both the municipality and IVAR, This could be provided by mandatory e-learning courses to raise risk awareness. A clear security policy should be in place and communicated to personnel. This should include duties and responsibilities in terms of cyber security, and how to obtain a conscious security behavior. A study performed by Kruger, Drevin & Steyn (2010) showed that the use of e-learning courses and vocabulary tests to assess a security awareness level are beneficial. A significant relationship between knowledge of concepts (vocabulary) and behavior was observed.

As the modern cyber attack is constantly developing, knowledge about context is crucial for the organizations to address. The organization should identify potential impacts of major operational disruptions in the water supply, and evaluate the ICT security accordingly. A criticality assessment needs to be performed to address the value of information the organizations possess. Requirements for ICT security should be addressed when acquiring and developing ICT systems. Further, clear procedures related to maintenance and upgrading of the services and systems should be in place. However, a system is never stronger than its weakest link, thus the human factor should be assessed. According to IBM (2014) over 95 percent of all incidents recognize “human error” as a contributing factor. The most commonly reported form of human errors include poor patch management, system misconfiguration, use of default user names and passwords or easy-to-guess passwords, lost mobile devices or laptops, and disclosure of regulated information through use of an incorrect email address. This illustrates the importance of addressing the risk attitude of employees. Taking adequate account of the human factor is essential both for the accuracy of risk assessment and for the effectiveness of prevention and emergency management. Further, monitoring of both the local and global situation regarding the development of cyber attacks towards other water works and distribution could contribute to a better understanding of the context.

Event reporting should be a requirement considering the potential severe consequences of a hacker attack. Every threat alert and security incident could provide the organizations with the opportunity to acquire valuable information on the adversary and use it to proactively hunt for advanced persistent threats that may have evaded the organizations defenses. As for the threat discussed above, reporting routines should be established and encouraged. The efficacy of reporting should be monitored and analyzed. This also accounts for the failure gathering, as mentioned above.

Information about quality of barriers should be regularly obtained and evaluated. As hackers continuously develop their methods and unpredictability also the security systems should regularly be assessed. The operational control systems should be “custom made” in order to fit the needs and requirements. To many water works today

are using a “off the shelf” systems (e.g. MS Windows). The quality of the firewall should be regularly revised and the spam filter should be tested towards known spamming techniques. Further, a business grade or enterprise variety malware protection should be installed (basic computer security programs designed for home computers should not be used), and data encryption technologies enabled on the organizations computers.

To obtain widespread risk awareness throughout the organizations, it is important that information about risk and resilience are properly communicated. This could be obtained through various channels. Due to the rapid changes in the IT operating and security environment, the employees’ need for information should be regularly evaluated. Also, the importance of senior management involvement should be included., as discussed above.

6.2.2 Anticipate/prepare

In the anticipate/prepare phase twenty-six issues were found to be relevant for a hacker attack towards the water supply in Stavanger. The identified indicators will measure the ability to the municipality and IVAR to anticipate and prepare for such a threat. Risk/hazard identification should be prepared by, amongst other, the use of risk- and vulnerability analysis. An ICT adapted risk- and vulnerability analysis is recommended, however as this is not a common procedure in the water industry, a conventional risk- and vulnerability analysis is also included as an indicator. They could perhaps be weighted differently in the calculations in order to emphasize the importance of a new and adapted approach.

Status on risk, events and quality of barriers should be assessed through regular meetings organized for relevant personnel. In addition to constant monitoring of barriers to ensure that risk controls/barriers are effective. The Quality of services (QoS) is a measure of the overall performance of service. To quantitatively measure the QoS, several related aspects of the network service are considered, e.g. error rates, bit rate, throughput, transmission delay, availability, etc. Further, the trends in risk, event and quality of barriers should be analyzed to counteract potential negative developments. Unknown traffic and traffic patterns towards their network should be investigated, and the number of unplanned interruptions due to disturbance in the barrier efficiency should be assessed.

The comprehensive information technology development and online connectivity has changed the way businesses and organizations operate. Due to the increased global interconnectedness and explosive use of social media and mobile devices, the risk of cyber attacks and data breaches have increased exponentially (Carpenter, 2014). This was recognized by both the municipality and by IVAR. Even though the probability of such an event was considered very low, the potential consequences could be severe. In addition to e criticality assessment of the information the organizations possess, they should stay precautious and vigilant by analyzing event reports and monitor the employers’ use of the organization’s devices with Internet access.

Early warnings provide information about potentially deteriorating safety before this is manifested in trends. It provides an opportunity to be proactive and take action at an early stage. This could be provided by constant monitoring of traffic against not open gates, and keeping an overview of the spam mail frequency, i.e. spam mails not detected

by the spam filter. Traffic against not open gates should optimally be monitored and evaluated by the organization itself, as the supplier of the systems most likely have many companies, businesses and organizations to keep an eye on. Spam mails not detected by the spam filter should be reported, and not just deleted.

Audits should be performed on a regular basis in order to identify problems, weaknesses and/or failures. The primary functions of an ICT audit are to evaluate the systems that are in place to guard the organization's information, ensuring data integrity, confidentiality and availability. Audits should assess the risk to the organization's valuable asset (its information) and establish methods of minimizing those risks. The audit should be performed in cooperation with external ICT experts, and a report is to be prepared in the end of each audit.

Robustness and redundancy of the operational control systems to IVAR and the municipality could be measured by addressing factors that should be present to secure a robust and redundant system. Networks should be segmented a much as possible to prevent unauthorized access to the most critical functions, both internally and externally. By frequently taking backups of the data and information in a completely separate system, necessary information will not be lost if a hacker attack should happen. With the data in tact the recovery phase will become easier. The copies of important data should be kept at a different physical location or a remote server (or both). Data backup and recovery should be an integral part of the business continuity plan. The redundancy could be secured by the use of redundant telecom lines provided by two different telecom suppliers. Further, a backup network should be available at the facility if the remote communication is attacked. An alternative water supply should be in place for emergency situations.

A comprehensive cyber-security plan should be prepared. A cyber security plan needs to focus on three key areas (Staysafeonline, n.d.):

- Prevention: Solutions, policies and procedures need to be identified and communicated to reduce the risk of attacks
- Resolution: Procedures needs to be in place to determine the resources necessary to remedy a threat
- Restitution: The organization need to be prepared to address the repercussions of a security threat with their employees and costumers to ensure that any loss of trust is minimal and short lived.

Both IVAR and the municipality should have prepared emergency preparedness plans for follow-up and response to errors and problems, as well as continuity plans as a means to uphold the most safety-critical activities of the organizations. Strong business continuity planning is a vital platform in order to ensure that prevention measures are in place and for providing an action plan if a problem occurs. Business continuity plans should include cyber attack scenarios of different severity in order to be prepared to fend off a sophisticated attack. Defined triggers need to be in place so it is clear when a breach has occurred, in addition to control mechanisms, such as procedures to close down systems and communication plans. Regular business continuity testing of potential issues ensures that the plan can be modified if necessary, and that relevant personnel is aware of what could happen and how to respond (Zurich municipal, 2014).

Even the best security technology in the world is insufficient if employees do not understand their roles and responsibilities in safeguarding sensitive data and protecting the organization's resources. Hence, practices and policies should be in place, which promote security and trainings of employees. Training of employees is a critical element of security considering both the prevention of a hacker attack and responding to it, hence reducing the vulnerability related to human factors. Training and exercise plans should be developed on the basis of the risk- and vulnerability analysis and the emergency preparedness and business continuity plans. Also, joint exercise plans should be conducted in cooperation with relevant external actors.

The repertoire of training scenarios should be reviewed and adapted regularly, considering the nature of hacking. Modern cyber attack strategies are constantly developing, thus renewal of training scenarios is essential for both IVAR and the municipality of Stavanger to stay "up to date". Routines should be established for the development of training scenarios on the basis of tests, audits, monitoring and authority recommendations.

Entrance control, both physical and cyber, is crucial for the prevention of unauthorized access to the treatment facility, the offices, and the operational control systems. The physical entrance could be ensured by the use of cameras for surveillance, and cards and personal codes to secure personal access. A burglar alarm should be installed, and security guards should be present. The operational control systems could only be accessed by the use of personal passwords. There should be established requirements and recommendations related to the strength of the password, and frequency of renewal. A multi-factor authentication should be utilized. Also, access should be removed from previous employees. Further, critical functions and components of the water supply should be available to a limited number of personnel.

Both IVAR and the municipality of Stavanger are more or less dependent on their operational control systems for optimal operation and water distribution, making them vulnerable towards disruptions. The treatment process is controlled and monitored by the use of such systems, thus testing of manual operation should be conducted regularly, also over longer periods of time, in order to prepare for an extraordinary event where the operational control system is affected and/or out of service.

6.2.3 Absorb/withstand

In the third phase, absorb/withstand, seventeen relevant issues were identified. A hacker attack has now occurred, and IVARs and the municipality's ability to absorb and withstand the attack, is to be measured. There are many ways a hacker attack can affect the organization, and the impacts varies depending on the nature and severity of the attack. Results of cyber attack towards the water supply may include denial of service, disruption of business functions, or the ultimate destruction of data and systems.

The impact and possible consequences towards a safe and reliable water supply depends on what degree of access the hackers have obtained. It is also reasonable to assume that, even though the hacker could have had access to the systems for a long period of time, when the hacker actually starts "doing something", e.g. adding huge

amounts of chlorine[3], controlling the valves, etc., this would be quickly discovered. The active and passive safety systems should prevent the hackers from accessing the most critical components in the first place, i.e. detecting the attack at an early stage. There should be established routines regarding follow up of suspicious activities (high outgoing traffic, strange looking files, etc.), the firewall should always be switched on and the software and anti-malware solutions should be continuously updated. The Norwegian National Security Authority (NSM) is organizing a national sensor network online. The sensor network is supposed to uncover hacking attempts against critical infrastructures. This sensor network is an annunciator system for digital infrastructures. It is voluntarily, but recommended to be a part of. Further, if the hackers have gained access to the most critical parts of the operational control system, which e.g. controls the treatment process, the water treatment and supply should be possible to carry out without the use of the operational control system (manually controlling the valves, chlorine pumps, etc.).

When un-normal activities are detected, a notification or alarm should be released as soon as possible to the responsible. Activity logs should be accompanied by alerting and notification software and options that can be configured to alert/notify responsible personnel. An intrusion detection system (IDS) should be used to supplement the firewalling systems and access control systems by providing intrusion notifications. IDS is a device or software application that monitors a network or systems for malicious activity. Alarms for water quality deviation should not be a part of the operational control system network, but connected to a separate modem. This would secure that potential contaminations are detected before distributing the water to the consumers. When a cyber attack/threat is detected, the employees should know where to go for information. Thus, a well-prepared, tailored action plan should be in place.

As for the leakage scenario presented above, the relevant competence available throughout the organizations should be assessed in order to provide a resilient reaction to withstand an event. In addition to certified operators, the ICT competence is important to include when measuring the ability to withstand a hacker attack, e.g. represented by the number of personnel with higher ICT education. Also, by regularly meet ups with external experts on the field, competence could be gained and disseminated.

The severity of the attack should be assessed and categorized by gathering relevant facts and information in a methodically manner. This would determine the nature of the incident and the proper technical response. IVARs and the municipality's ability to combat a hacker attack could be measured by assessing the availability of personnel, both internally and externally. Also, a Computer Emergency Response Team (CERT) function should be available. A CERT function is an expert group that handles computer security incidents (NSM, n.d.). In addition to a CERT function, IVAR and the municipality should have access to a dedicated incident response unit/crisis management team trained to deal with extraordinary events. As a computer security incident ultimately is a business problem, not just a technical problem, an effective response is therefore

[3] As stated by one of the interviewees; the only contamination a hacker attack could cause is to add high amount of chlorine. He did not consider this harmful to the consumers as when the consumers smelled the chlorine, they would not drink the water.

interdisciplinary. Following a breach, the IT systems should be secured in order to contain the breach and ensure it is not on going. This could mean that IVAR and/or the municipality have to isolate or suspend a compromised section of its network temporarily or possibly even the entire network.

Both IVAR and the municipality should have an immediate response communication checklist to follow, which include guiding principles. To communicate frequently is important during a hacker attack in order to prevent nervous and upset personnel. Thus, the most efficient communication strategy should be assessed. If the consumers are affected by the attack, e.g. outage of water, the possibility to notify the public should be present. The authorities should be contacted, and kept updated during the whole responding process. Also, the media should be included during the initial response to prevent false rumors and panic among the citizens. Hence companies may benefit substantially from a sustained communications response to a significant computer security incident.

6.2.4 Respond/recover

In the fourth phase, respond/recover, fifteen issues were found to be relevant for a resilient response to, and recovery from, a hacker attack towards the water supply in Stavanger. Active response is the execution of the incident response plan to restore systems, minimize consequences, and reduce future risk. Hence, this should be obtained by the use of the identified indicators.

The internal emergency response resources necessary, and required mobilization time, should be assessed when measuring a resilient response. As no hacker attack have ever happened towards the water supply in Stavanger (as they know of), the time needed to inform personnel, initiate response plan, reaction time during night, and time to restore damaged equipment, should be based on executed training and exercise sessions. This underscores the importance of constantly updating the training scenarios in accordance with the development in new hacking techniques and the corresponding consequences. Also the external emergency response resources should be evaluated on the basis of response time.

Due to the potential severe consequences of a hacker attack towards the water supply in Stavanger, the allocation of resources is considered especially important. Both IVAR and the municipality should have access to competent personnel whenever needed. Hence, an appropriate rota system that ensure sufficient amount of back-up personnel and suitable vacation routines should be implemented.

As response is often dependent on information from other actors, maybe especially considering a hacker attack, communication between actors should be established immediately. The telecom supplier is essential to include in the communication plans. Further, emergency communication channels should be in place and available during the whole phase.

The robustness of the responsible functions is important to measure, as this provides insight in the ability to uphold the critical infrastructure systems, i.e. deliver safe an reliable water. A robust response requires a sufficient number of competent personnel, internally and externally. Thus, the number of competent personnel should regularly be

assessed and evaluated on the basis of test, trainings, real incidents, etc. This includes the CERT function and the incident response unit, in addition to operators and engineers. If single persons are unavailable for some reason the critical functions should be ensured through pre-planned back up. This could be obtained by providing the same training to deputies as for the main responsible person, and ensure temporary access solutions to the most critical function to specific personnel if the administrator is not present. Also, the ability to uphold the water supply by manual operation and the sustainability of the alternative water supply and the emergency water should be evaluated.

As previously mentioned, there has never been a hacker attack towards the water supply in Stavanger (at least not that is known of). This means that the training on how to deal with potential scenarios is essential and should be conducted regularly. The training should include emergency training, security awareness training, communication training and incident management training. As the consequences related to a hacker attack is ranging, the scenarios included in the training sessions requires participation of all relevant cooperating actors and personnel. Also, the training should be consistent with existing regulations, standards and requirements of regulatory authorities. There should be kept an overview of the number of personnel conducted the relevant training sessions.

The combat should uphold until the situation is fully under control. This may require exchange of exhausted response personnel. Again, dependent on the consequences and severity of the attack. The combat procedures should include responding guidelines to ensure that plans are being followed even under stressful situations. Suitable work shifts should be established to ensure that the response could maintain the intensity throughout the phase. As for the same reasons mentioned above, the media should also be included during the response and recovery.

Once malicious codes and other unauthorized network activities have been eradicated, the response team should turn to recovery. To simply restore a device to service in its pre-incident condition is insufficient (Christian & Lilley, n.d.). A compromised device may have been compromised through a specific vulnerability that now is known to the company. Thus, it is essential to patch that device and other appropriate network assets and taking other necessary steps to harden them against future attacks. Liability risks from unknown tools and exploits are significant, but the risks related to known vulnerabilities and exploits – particularly those that have been used against the organizations successfully in the past – are yet more substantial. Hence, a risk assessment and clarification (including approvals) before re-starting normal operation should be conducted.

6.2.5 Adapt/learn

In the last and fifth phase, adapt/learn, ten issues were identified as relevant for a resilient learning. As already mentioned do computer security incidents expose technical vulnerabilities of company systems. The organizations can address those vulnerabilities and thereby prevent their systems from being exploited in the same manner in the future.

As the issues and corresponding indicators identified are more or less the same as for the previous threat, this phase will not be discussed in detail. However, an overall presentation of learning from a hacker attack will be provided.

Active responses put organizations and companies incident response and emergency preparedness plans to the test. Weaknesses or inadequacies in the incident response should be identified, analyzed and addressed. A comprehensive investigation may be necessary in the event of significant breakdowns, while a single meeting may be sufficient to cover any lessons learned from a number of different computer security incidents. Crew coordination should be assessed, and performance should be rated. Further, the plans and protocols should be updated accordingly. Process flaws should be identified, and recommendations for adaptation and improvements should be considered. Lessons learned should be incorporated and communicated throughout the organizations, and followed up. The competence and resources should be assessed and evaluated, and training and exercise plans updated according to the lessons learned and competence/resource assessments. Further, a system should be available that store and retrieve knowledge and experiences from events and response operations.

6.3 Method pros and cons

The main objective of WP 3 of the SmartResilience project, where SINTEF is the lead partner, is to develop a methodology for assessing resilience of SCIs based on resilience indicators (as presented in the introduction of this thesis). The call text explicitly asks for an "indicator-based approach assessing the level of resilience using a scale approach applicable across critical infrastructures" (Øien et al., 2017b, pp. iii). The resilience attributes being measured are corresponding to the project's definition of resilience (see page 27), and consist of the five phases of the resilience cycle. The resilience curve, presented in fig. 6.1 below, describes the SCI functionality (e.g. deliver and supply hygienically reassuring water) as a function of time, before, during and after an adverse event, and is treated as a conceptual model (i.e. the method do not consider the exact shape, size or area of the curve directly). It is an "indirect measurement using issues (what) and indicators (how) within each of the five resilience phases" (Øien et al., 2017b, pp. iii). This provides the basis for a resilience assessment of specific threats, specific SCIs or an entire area/city at a certain point in time. According to Øien et al. (2017b), the method can be used to:

- Provide an overview of strengths and weaknesses with respect to resilience
- Identify gaps
- Point at improvement needs
- Trending; follow up own development over time
- Compare with others (benchmarking)

The resilience assessment method developed by SINTEF seems to be a great point of departure for assessing resilience for smart critical infrastructures, however some problematic aspects with the model are present, and will be discussed in the following.

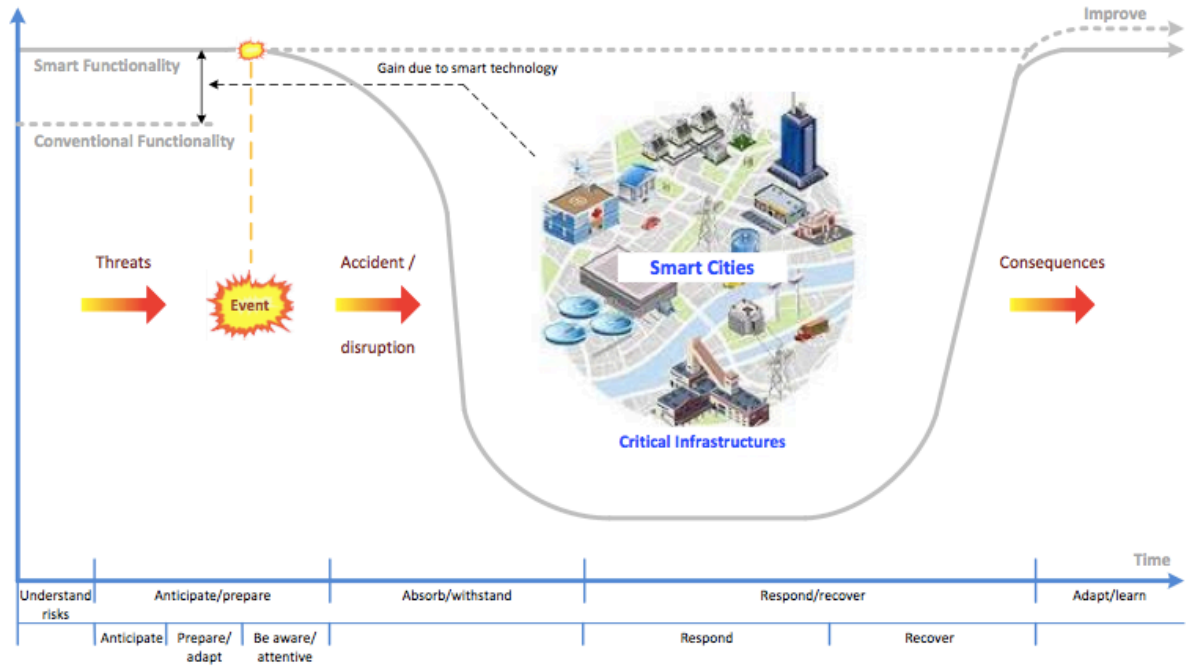

Figure 6.1: The five resilience phases – the resilience attributes – corresponding to the Smart Resilience project definition of resilience (Øien et al., 2017b).

6.3.1 Model evaluation

In theory, if the methodology is applied correctly it will provide an overview of strengths, and weaknesses/gaps in the various phases of the resilience cycle. If gaps are identified, the assessment and resilience indicators will provide added value for the organization. The assessment method is made very flexible, and it is possible to adjust the model to suit every CI in whatever area by using scenario specific issues and indicators. The model could be used both as an internal assessment, requiring end users contribution in selection of issues and indicators and best/worst values, and as an external assessment, using external assessors where the issues, indicators and range of values are predefined. The rationale behind the model development is also easy to understand. Thus, due to its alleged flexibility, transparency and applicability (identification of gaps, improvement areas, trending and benchmarking), the model seems both useful and necessary. However, there are some drawbacks.

The SmartResilience methodology is based on indicators. The indicators show "how" an issue can be measured, and several indicators may be needed to represent one issue. The generic candidate issues were provided both by collecting existing issues from the risk, security, safety, crisis management, business continuity and similar domains, and by capturing typical topics discussed in resilience literature. The indicators will typically be described as a ratio, a number, as questions, a score on some scale, or similar. Two different approaches are used for obtaining the indicators. The first is the use of conventional indicators in a top-down manner, and the other is a bottom-up use of indicators from big data or open data sources. The first approach is supposed to identify most of the relevant issues and corresponding (conventional) indicators. Meaning that the indicators from big data or open data sources will be additional and especially useful for capturing smart technology issues that supplements the conventional indicators.

The process of choosing and identifying relevant issues and corresponding indicators was both comprehensive and time consuming. The quality of some of the indicators was compromised in some cases were the issue was considered important, but suitable indicators were missing due to lack of data and/or hard to identify from the author's point of view/knowledge/expertise. Thus, to obtain valid indicators of high quality was challenging. Underlying causes and contributing factors could be of such a nature that it is difficult to obtain quantitative measures that are individually valid and collectively have adequate coverage. One issue needs to be measured by one or more indicators. The number of indicators needed, depends on how well the indicator(s) cover all aspects of the issue. I.e. some issues could be measured with just one indicator, while other issues could be measured with an undetermined amount of indicators. This seems a little un-consistent and vague, and issues only measured by one single indicator become very vulnerable with respect to that indicator. However, if that indicator is suitable and cover all important aspects of the issue, it would not be expedient to obtain indicators "just to obtain indicators" if nothing new is added/measured. But, if indicators are left out due to lack of data, the issue is compromised and the results will not be representable. However, this is a matter of resources to be spent of the resilience assessment (this is where Big Data provides an advantage compared to the conventional indicators). Also, the method seems easy to manipulate by intentionally exclude issues and indicators where the real value is known to be low. Or, if it is known that an indicator will obtain a low score, additional and more arbitrary indicators where the score is known to be good, could be added to the assessment (without really measuring something new) in order to raise the overall score obtained for that issue. However, this is outside the scope of the methodology itself.

By using equal weights throughout the calculations, the results remain transparent and simple. However, this will not provide a realistic representation, as some indicators/issues/threats will be of greater concern and importance to a critical infrastructure than others. But, as stated by Øien et al. (2017b, pp. 42): "…the method development is an evolutionary process. It still remains to be seen to what degree we can "manage" without the use of (non-equal) weights. One option is to start with equal weights, and based on experience and empirical data introduce weights as part of tuning and optimizing the method/model". All models are simplifications of the real world, and it will always be a balance between having a model that is simple and transparent on one hand, and being sufficiently realistic on the other. However, it seems like when using equal weights, too much is hidden within the final RIL value.

Some indicator requirements are stated by Øien et al. (2017). High validity and high reliability are scientific requirements. These are in addition to several non-scientific requirements to indicators. The non-scientific requirements stated in the SmartResilience project are given in appendix 1. Evaluation of indicators should ideally be made on the basis of both scientific and non-scientific requirements. This could be unwieldy and confusing to relate to, hence, making the process of identifying indicators even more comprehensive.

As already mentioned, the methodology could be applied both for internal and external resilience assessments. The methodology described in this thesis is aiming for internal assessment, meaning that domain experts/end users are needed in order to define

issues and indicators important for their critical infrastructure, in addition to determination of the range of values (best and worst values) for each indicator. They are in a way "configuring" the resilience model (Øien et al., 2017b). This configuring is said to be a one-time effort prior to using the model for calculating the RILs. However, considering the developing nature of the threats that are expected to cause most harm (e.g. terror attack, hacking, extreme weather events), the issues and indicators must be evaluated in accordance to their relevance on a regular basis. In the external assessment, issues, indicators and the range of values (best and worst values) are predefined, meaning that the "configuring" is a part of the method development (Øien et al., 2017b). The assessment, i.e. assigning values to the indicators and performing the calculations, are performed by external assessors. The internal assessment is more extensive and requires more resources, whereas the external approach is more simplified and requires fewer resources. Thus, at first sight it could be tempting to invest in an external assessment from an economic and timesaving point of view. On the other hand, the issues and indicators may be better adapted to suit each specific user when performing an internal assessment. If the compromise by executing an external assessment is a less representable resilience picture, there would be no point in performing the assessment in the first place.

The methodology is said to be suitable for benchmarking by comparing results with others. However, as the relevance and quality of issues and corresponding indicators are based on local circumstances and available data sources, the RILs obtained are not necessarily comparable. It could be argued that, due to the use of equal weights, the RIL is independent of the number of issues, indicators, threats, etc. included, since it is calculated as a weighted average. But, as discussed above, this is 1) not realistic and 2) easy to manipulate. Benchmarking seems easier and more comparable with the external assessment, because the same issues and indicators are used.

The completeness of the selected issues and indicators is important to address as this relates to the quality of the process of identifying and selecting issues and indicators. Øien et al. (2017b) suggest, as a rule of thumb, that a minimum of seven to eight issues per phase should be identified and selected to provide a sufficiently complete resilience picture. Assuming that not all phases are at the minimum number of issues, there should be about 40-50 issues for one specific threat for one critical infrastructure. This means that, using the municipality of Stavanger as an example, if the resilience levels should be assessed for each threat towards the drinking water supply considered in the risk- and vulnerability analysis, a total of 880-1100 issues needs to be identified. Furthermore, a full scope assessment for a city covers all the relevant critical infrastructures, all relevant threats for each critical infrastructure, all five phases of the resilience cycle, all relevant issues for each phase and all indicators for measuring the issues. Thus, thinking about all the different end-users, multi-agency cooperation and coordination required, different organizational goals, professional cultures, lines of accountability, etc., in addition to the matter of costs, this seems like an insuperable and overwhelming task. It could be argued that the number of issues will be reduced when using generic issues, but they still have to be included in the calculations, thus the number of calculations will be the same. However, the method could also be used to assess the resilience for only one critical infrastructure and a chosen number of threats, e.g. by choosing threats on the basis of probability/consequence criteria. In general, as some threats are more common than other (ref. the two threats discussed above), disasters related to such

threats do not longer, or rarely, occur in modern societies that used to be commonplace. As discussed above, it do not seem efficient or necessary to apply such a comprehensive methodology for threats that occurs regularly, where the causal factors are well understood, and where routines and procedures are established and thoroughly evaluated on the basis of yearly reports. For threats like terror attacks, hacking attempts, extreme weather events, cascading effects, etc., where little or no previous experiences exists, the uncertainties are deep and the potential consequences are devastating, the methodology could contribute to a better risk understanding, enhance awareness and increase the feeling of being prepared.

The methodology used when assessing resilience should provide the possibility to test the system, critical infrastructure, etc. towards different loads and stresses, ranging from high to low probabilities and consequences (Diao et al., 2016). Thus, the methodology suggested by SINTEF should be able to test the SCI's ability to deal with crisis, typically very severe scenarios (worst case). In the SmartResilience methodology, the scenario for a specific SCI is given by the threat. The methodology is used to assess the resilience level, given this specific threat. However, the resilience level obtained is a relative measure, without any "acceptance level" that indicates "sufficient ability of the SCI to deal with a specific crisis" (Øien et al., 2017b, pp. 42). Thus, stress testing of the SCIs may be more appropriately carried out using direct measures and predictions, as illustrated in figure 6.2 below. In the direct measurements or predictions, focusing directly on the parameters of the resilience curve, attributes such as rapidity and robustness may be used. The figure shows the resilience curve before, during and after an event/incident. The robustness represents the ability to minimize the loss in functionality. The rapidity represents the time needed to recover from the event and regain the functionality. These measures could be used for stress testing. This is said to be further developed in a later stage of the SmartResilience project.

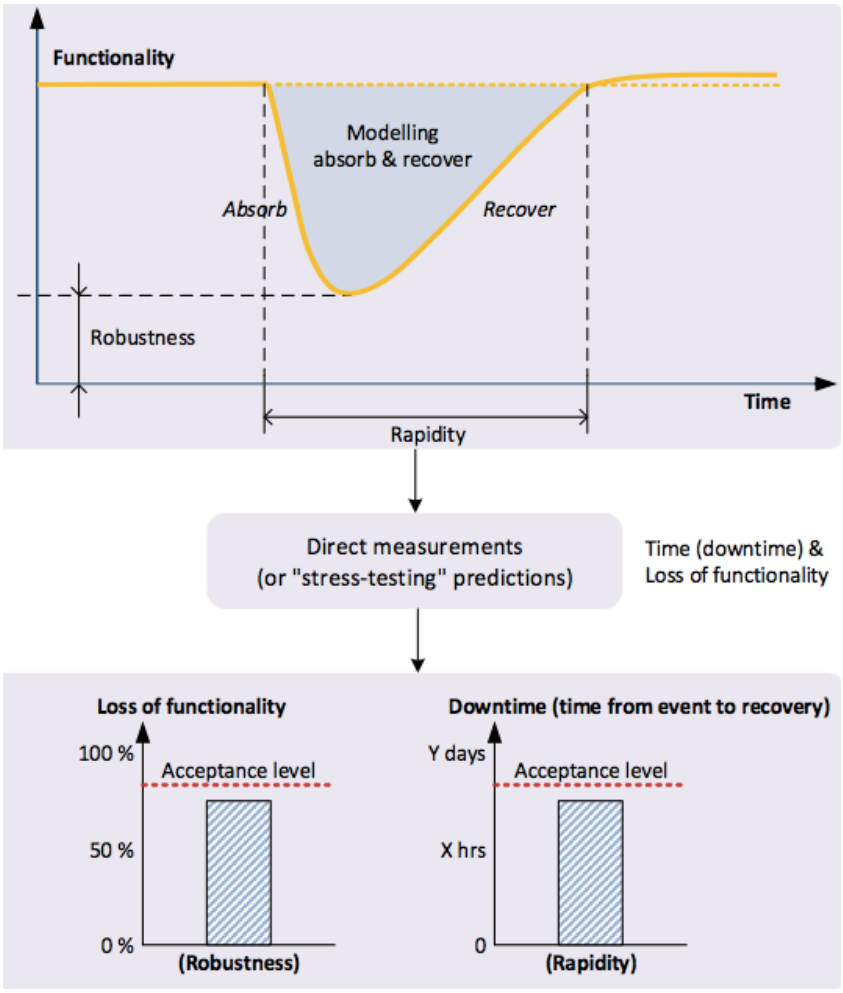

Figure 6.2: Stress testing by direct measurements/predictions are focusing directly on parameters of the resilience curve, attributes such as robustness and rapidity may be used (Øien et al., 2017b).

6.3.2 Summary

Overall, the method developed by SINTEF and discussed above seems du be a useful contribution to an increased focus on the resilience of critical infrastructures and the extensive use of "smart" technology. It is important to raise awareness regarding the vulnerabilities related to the use of such technology, and by addressing the concept of resilience is a good way to start. As new types of threats are developing, the conventional risk- and vulnerability analysis are coming to short. Risk analysis is built on the premise that hazards are identifiable (Labaka, Hernantes & Sarriegi, 2015). However, nowadays, it is almost impossible to forecast when a crisis would occur and how it would evolve. In this context, resilience has become an essential concept in the field of critical infrastructure protection.

As identified during the interviews with both IVAR and the municipality of Stavanger, the term "resilience" was not a known term to them. Assuming this is representative for a wide range of CIs, the concept of resilience needs to be disseminated throughout the industries responsible for CIs. By increasing system resilience, the vulnerabilities will decrease. This illustrates the importance of implementing a resilience assessment to address new and emerging threats. However, in general, there seems to be some

barriers towards enhancing resilience. Various inhibitors are found in different areas and are due to, among other, individual defense mechanisms (like denial and downgrading of threat importance), organizational beliefs and rationalizations (like "disasters do not happen to us" and "we can deal with these events"), and cost of preparations (Boin & McConnel, 2007). These are barriers important to overcome if an efficient resilience assessment is to be performed.

To summarize the discussion presented above: Yes, the model is easy to manipulate and the process of identifying issues and indicators are comprehensive and time consuming. However, if the methodology is applied correctly, and as it is meant to, it will represent a great tool for addressing the resilience towards specific threats, identify gaps and point out improvement needs. But, a lot of resources are necessary in order to include the necessary level of detail and quality. Data needs to be obtained in order to measure important indicators, meaning that new routines and procedures need to be implemented in order to collect these data (e.g. reporting routines). It is comparable to the restoration of an old house. You would, most likely, not paint on top of rotten walls, but change the wall panel before painting it. Thus, if the resilience assessment should be implemented, it should not be compromised or degraded to a halfway assessment. However, the matter of costs is of course a problem. The conversion of "paper plans" into organizational readiness can be both expensive and time consuming. Investing resources to plan for crisis and extreme events that may never occur is not easy to sell.

7 Conclusions

Modern society relies on the effective functioning of critical infrastructure networks to provide public services and enhance quality of life. This constantly growing dependence is accompanied by an increased sense of vulnerability to new and emerging threats such as terror attacks, hacking attempts and climate change. Thus, the question is being raised – how can modern societies prepare for a breakdown in CIs? In this context, critical infrastructure is thought of as networks for the generation and supply of energy sources, food supplies and public order (e.g. transportation, public health, information and telecommunications, water, banking and finance, etc.). The criticality related to a breakdown in one or more CIs is dependent on locations, systems and cultures, however, the potential to cause very serious problems are widely recognized.

As mentioned above has resilience become an essential concept in the field of critical infrastructure protection. Resilience are going beyond the traditional risk management methods by not only defining policies for facing expected events, but also by taking unexpected events into account. Both risk management and resilience must be combined to adequately cope with crisis, as the latter builds on the first. Although there are several definitions regarding the concept of resilience in the literature, as listed in a previous chapter, the methodology developed by SINTEF is based on the following definition:

"Resilience of an infrastructure is the ability to anticipate possible adverse scenarios/events (including the new/emerging ones) representing threats and leading to possible disruptions in operation/functionality of the infrastructure, prepare for them, withstand/absorb their impacts, recover from disruptions caused by them and adapt to the changing conditions."

This definition of resilience addresses the aspects important before, during and after an incident, and is hence representable for a holistic resilience framework. The methodology presented above is supposed to support decision makers in diagnosing and improving the critical infrastructure resilience level. This is a good intention, and also very much needed throughout the network of CIs, thinking about the new and future threats. However, there are some well-defined barriers present against new concepts like resilience. The various inhibitors are found in the areas of organizational preparedness, governance and society. This was also experienced during the interviews in the work for this thesis. It seems like people's responses to potential future threats typically encompass a range of dysfunctions (e.g. downgrading threat importance, denial, impotence, etc.). It has proven incredibly hard to break through these mental barriers. Also, when challenged by critical events elsewhere, it seems like organizations have a tendency towards rationalizing, meaning that they interpret the potential threats in a "this do not happen to me" manner. A third barrier is related to the costs of preparation. As discussed above, the methodology will require a lot of resources if its full potential is to be utilized. Promoting resilient systems requires, first, investments in time and resources to prepare plans that may never need to be activated. Secondly, it requires cooperating with multiple external stakeholders, who have their own priorities, mandates, information capacities, decision making cycles, etc., and third, simulations, exercises and training. This is not an impossible mission, however, it takes valuable time

and money that could be used to increase efficiency and services of the critical infrastructure instead.

As discussed above, promoting resilience strategies in preparation for critical infrastructure breakdowns is not an easy job. It competes against other vulnerabilities and priorities related to day-to-day operation and longer term goals. Conditions for enhanced resilience capacities seem to most likely emerge on the crest of catastrophes (Boin & McConnel, 2007). However, disasters and crisis do not guarantee change and learning. But it is when normal operations are unintentionally interrupted that established policies, procedures, cultures and legitimacies change course. The question is, do we afford to wait that long?

So, assuming a future with "smarter" water supply (more adaptive and more intelligent), the main risk aspects are related to the use and dependency of the operational control system and a reliable communication between critical components of the system (e.g. pumps, valves, water meters, alarms, etc.). Also, a conservative attitude towards new concepts and terms need to be mentioned when addressing risk aspects related to a more intelligent water supply, due to reasons mentioned above. The capacity to handle deviations and breakdowns are represented by the redundancy, alternative and emergency water, and the opportunity and capability to deliver water manually. In addition to organizational preparedness related to personnel and resources. The issues and indicators presented in table 5.1 and 5.2 are identified to be important and relevant when assessing the resilience of the water supply in Stavanger towards water leakages and hacking attempts. However, the methodology was found to be too comprehensive for high probability, low consequences types of threats as no "added value" were identified (compared to current practices). But for threats were current practices such as risk management, emergency preparedness and response, business continuity, etc. comes to short; the resilience assessment could be able to provide a more complete overview. The methodology developed by SINTEF provides a tool for systematizing issues in accordance with five resilience phases. This makes it possible to identify gaps and need for improvement. However, before the excitement takes overhand, expectations should be tempered. Preventing all extreme threats from materializing is not possible. Every conceivable "worst case" that may unfold cannot be identified. Terrorists and hackers can become inventive beyond our imaginations. Prevention requires that one knows the source and dynamics of threats, but the literature shows that this is impossible (Boin & McConnel, 2007). With this said, a resilience assessment is still important as it, most likely, will limit the potential consequences associated with rare threats.

References:

Alessandri, A., & Filippini, R. (2012, September). Evaluation of resilience of interconnected systems based on stability analysis. In *International Workshop on Critical Information Infrastructures Security* (pp. 180-190). Springer Berlin Heidelberg.

Alexander, D. E. (2013). Resilience and disaster risk reduction: an etymological journey. *Natural Hazards and Earth System Sciences*, *13*(11), 2707-2716.

Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of risk research*, *12*(1), 1-11.

bedreVANN.no. Om bedreVANN. Accessed 5 may 2017 via < http://bedrevann.no/>

bedreVANN. (2015). *Tilstandsvurdering av kommunale vann- og avløpstjenester. Resulteter 2015.* Accessed 5 may 2017 via < http://bedrevann.no/pdf/bedreVANN2015.pdf>

Bodsberg, L., Øien, K., Grøtan, T. O., Øren, A., Hoem, Å., Jovanovic, A., +++++. (2017). *Supervised RIs: Defining resilience indicators based on risk assessment frameworks.* Draft, unpublished. SINTEF.

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience.*Journal of Contingencies and Crisis Management*, *15*(1), 50-59.

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., ... & von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake spectra*, *19*(4), 733-752.

Buhr, K., Karlsson, A., Sanne, J. M., Albrecht, N., Santamaría, N. A., Antonsen, S., ... & Csapó, G. (2016). End users' challenges, needs and requirements for assessing resilience.

Carpener, G. (2014). *Ahead of the curve: Understanding emerging risks.* Marsh & McLennan Companies. Accessed 3 June 2017 at https://www.mmc.com/content/dam/mmc-web/Files/AheadoftheCurve-UnderstandingEmergingRisks.pdf

Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile Networks and Applications*, *19*(2), 171-209.

Christian, M.A. & Lilley, S. (n.d.). Preparing For and Responding To a Computer Security Incident: Making the First 72 Hours Count. Accessed 5 June 2017 at < https://iapp.org/media/pdf/resource_center/Mayer-Brown_Cyber-Sec.pdf>

Clarke, J., Coaffee, J., Rowlands, R., Finger, J., & Hasenstein & Siebold, U. (2016). Resilience Evaluation and SOTA Summary Report.

Diao, K., Sweetapple, C., Farmani, R., Fu, G., Ward, S., & Butler, D. (2016). Global resilience analysis of water distribution systems. *Water Research*, *106*, 383-393.

Divall, G. (2016, 30. November). Smart Cities & Critical Infrastrucutre Cyber Attack Vulnerabilities. Accessed 10 March 2017 at < https://www.brighttalk.com/webcast/14737/230379/smart-cities-critical-infrastructure-cyber-attack-vulnerabilities>

Drikkevannsforskriften. Forskrift 22 desember 2016 nr 1868 om vannforsyning og drikkevann.

EPD Guidance Document. (2007). *Water leak detection and repair program.* Georgia: Georgia Environmental Protection Division (EPD). Accessed 23 May 2017 at < https://epd.georgia.gov/sites/epd.georgia.gov/files/related_files/site_page/Leak_Detection_and_Repair.pdf>

EU Commission. (2008). COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Off. J. Eur. Union FEBBRARO Angela SACCO Nicola*.

Farley, M. (2001). Leakage management and control. *A best practice training manual*.

Fisher, R. E., Bassett, G. W., Buehring, W. A., Collins, M. J., Dickinson, D. C., Eaton, L. K., ... & Millier, D. J. (2010). *Constructing a resilience index for the enhanced critical infrastructure protection program* (No. ANL/DIS--10-9). Argonne National Lab.(ANL), Argonne, IL (United States). Decision and Information Sciences.

Elky, S. (2006). An Introduction to Information Security Risk Management.*SANS Institute*.

Eusgeld, I., Nan, C., & Dietz, S. (2011). "System-of-systems" approach for interdependent critical infrastructures. *Reliability Engineering & System Safety*,*96*(6), 679-686.

Fekete, A., Hufschmidt, G., & Kruse, S. (2014). Benefits and challenges of resilience and vulnerability for disaster risk management. *International journal of disaster risk science*, *5*(1), 3-20.

Ganin, A. A., Massaro, E., Gutfraind, A., Steen, N., Keisler, J. M., Kott, A., ... & Linkov, I. (2016). Operational resilience: concepts, design and analysis.*Scientific reports*, *6*.

Gheorghe, A. V., & Schlapfer, M. (2006, October). Ubiquity of digitalization and risks of interdependent critical infrastructures. In *Systems, Man and Cybernetics, 2006. SMC'06. IEEE International Conference on* (Vol. 1, pp. 580-584). IEEE.

Guthrie, P., & Konaris, T. (2012). Infrastructure and resilience. *Foresight, Government Office for Science, Commissioned Review*.

Haimes, Y. Y. (2009). On the definition of resilience in systems. *Risk Analysis*,*29*(4), 498-501.

Hollnagel, E. (2015). RAG – Resilience Analysis Grid. Accessed 5 March 2017 at http://erikhollnagel.com/onewebmedia/RAG%20Outline%20V2.pdf

Hollnagel, E. (2011). Prologue: the scope of resilience engineering. *Resilience engineering in practice: A guidebook*.

Hollnagel, E. (2011). RAG-The resilience analysis grid. *Resilience engineering in practice: a guidebook. Ashgate Publishing Limited, Farnham, Surrey*, 275-296.

Hollnagel, E., Woods, D. D., & Leveson, N. (2007). *Resilience engineering: Concepts and precepts*. Ashgate Publishing, Ltd..

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. *Reliability Engineering & System Safety*, *145*, 47-61.

IBM. (2014). IBM Security Services 2014. Cyber Security Intelligence Index. Accessed 3 June 2017 at < https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf>

ITU (International Telecommunication Union), 2017. *ICT for smart water management.* Accessed 30 March 2017 at http://itunews.itu.int/en/570-ICT-for-smart-water-management.note.aspx

IVAR. (2016, 19 September). Utbygging Langevatn. Accessed 11 February 2017 at http://www.ivar.no/utbygging-langevatn/category747.html

Johnsen, S. O. & Røstum, J. (2015). *Eksempel på mal for risikovurdering knyttet til informasjonssikkerhet og driftskontrollsystem for vann og avløp.* SINTEF Teknologi og samfunn. Sikkerhet.

Jovanovic, A.S, Schmid, N. & Klimek, P. (2015). *Use of indicators for assessing resilience of critical infrastructures.* Draft

Jovanović, A., Klimek, P., Choudhary, A., Schmid, N., Linkov, I., Øien, K., ... & Molarius, R. (2016). Analysis of existing assessment resilience approaches, indicators and data sources.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk analysis*, *1*(1), 11-27.

Keeley, D., Gadd, S., & Fullam, B. (2006). Principles for learning lessons from incidents-a UK perspective. In *INSTITUTION OF CHEMICAL ENGINEERS SYMPOSIUM SERIES* (Vol. 151, p. 61). Institution of Chemical Engineers; 1999.

Kjellesvik, T. I. & Gjerstad, K. O. (2011). *Hovedplan drikkevann 2050.* Mariero, Stavanger: IVAR

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, *18*(5), 316-327.

Labaka, L., Hernantes, J., & Sarriegi, J. M. (2015). A holistic framework for building critical infrastructure resilience. *Technological Forecasting and Social Change*, *103*, 21-33.

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., ... & Nyer, R. (2014). Changing the resilience paradigm. *Nature Climate Change*,*4*(6), 407-409.

Manyena, S. B. (2006). The concept of resilience revisited. *Disasters*, *30*(4), 434-450.

Mattilsynet (2006). *Økt sikkerhet og beredskap i vannforsyningen – veiledning.* Accessed 28 March 2017 at < https://www.mattilsynet.no/mat_og_vann/vann/vannforsyningssystem/veiledning_i_beredskapsplanlegging_for_vannverk.1894/binary/Veiledning%20i%20beredskapsplanlegging%20for%20vannverk>

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., & Barton, D. (2012). Big data. *The management revolution. Harvard Bus Rev*, *90*(10), 61-67.

Menoni, S., Molinari, D., Parker, D., Ballio, F., & Tapsell, S. (2012). Assessing multifaceted vulnerability and resilience in order to design risk-mitigation strategies. *Natural Hazards*, *64*(3), 2057-2082.
Norsk Standard (2001). *Informasjonteknologi. Administrasjon av informasjonsikkerhet (ISO/IEC 17799:2000)*. Oslo: Norges Standardiseringsforbund (NSF).

Nasjonal sikkerhetsmyndighet (NSM) (2015). *Helhetlig IKT-risikobilde 2015.* Accessed 28 March 2017 at < https://www.nsm.stat.no/globalassets/rapporter/nsm_helhetlig_ikt_risikobilde_2015_lr.pdf>

NOU 2015:13 (2015). *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden.* Oslo: Departementenes sikkerhets- og serviceorganisasjon. Informasjonsforvaltning.

NSM. (n.d). Norges nasjonale cybercenter – NorCERT. Accessed 5 June 2017 at < https://nsm.stat.no/norcert/>

O'Rourke, T. D. (2007). Critical infrastructure, interdependencies, and resilience. *BRIDGE-WASHINGTON-NATIONAL ACADEMY OF ENGINEERING-*, *37*(1), 22.

Palmer, M. (7 September, 2016). Cyber attack survival guide. *Financial times.* Accessed 2 June 2017 at < https://ig.ft.com/sites/special-reports/cyber-attacks/>

Park, J., Seager, T. P., Rao, P. S. C., Convertino, M., & Linkov, I. (2013). Integrating risk and resilience approaches to catastrophe management in engineering systems. *Risk Analysis*, *33*(3), 356-367.

Powel AS. (2017, 11 january). Redusert vanntap og riktige prioriteringer med Powel Water Ledningsfornyelse. Accessed 12 april 2017 at < https://www.powel.com/no/nyheter/redusert-vanntap-og-riktige-prioriteringer-med-powel-water-ledningsfornyelse/>

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, *21*(6), 11-25.

Steen, R., & Aven, T. (2011). A risk perspective suitable for resilience engineering. *Safety science*, *49*(2), 292-297.

Van Zyl, J. (2014). *Introduction to Operation and Maintenance of Water Distribution Systems.* Accessed 30 May 2017 at http://www.wrc.org.za/Knowledge%20Hub%20Documents/Research%20Reports/TT600-14.pdf

Vollmer, M., Walther, G., Jovanovic, A., Schmid, N., Øien, K., Grøtan, T. O., ... & Egloff, R. (2016). Initial Framework for Resilience Assessment.

SmartResilience. (2016). The project. Accessed 6 February 2017 at <http://www.smartresilience.eu-vri.eu/?q=The-project>.

SRA. (2015). Society of risk analysis, glossary of the specialty group on foundations of risk analysis. Accessed 24 February 2017 at <http://www.sra.org/news/sra-develops-glossary-risk- related-terms>

Stavanger kommune. (2010a, 6 July). Hovedplan for vannforsyning, vannmiljø og avløp, 2011-2022 – offentlig høring. Accessed 10 February 2017 at http://www.stavanger.kommune.no/no/Arkiv-horinger/Hovedplan-for-vannforsyning-vannmiljo-og-avlop/

Stavanger kommune. (2010b, April). Klima- og miljøplan 2010 – 2025). Accessed 14 February 2017 at <http://www.stavanger.kommune.no/Documents/Natur%20og%20milj%C3%B8/Aktuelt/Klima-ogmiljoplan2010-2025_190510_rev_zip.pdf>

Stavanger kommune. (2013). Helhetlig risiko- og sårbarhetsanalyse for Stavanger kommune 2013. Sammendragsrapport. Accessed 19 April 2017 at < http://www.stavanger.kommune.no/Global/KBU/Byplan/Helhetlig%20risiko-%20og%20s%C3%A5rbarhetsanalyse%20for%20Stavanger%20kommune%202013.pdf>

Stavanger kommune. (2015). Årsrapport 2015. Accessed 27 April 2017 at < http://arsrapport2015.stavanger.kommune.no/PDF/arsrapport2015/%C3%85rsrapport%202015%20%E2%80%A2%20Stavanger%20Kommune.pdf>

Stavanger kommune. (2016). Årsrapport 2016. Accessed 27 April 2017 at < http://arsrapport2016.stavanger.kommune.no/PDF/arsrapport2016/Aarsrapport_2016-Stavanger_kommune.pdf>

StaySafeOnline (n.d). Implement a cyber security plan. Accessed 4 June 2017 at < https://staysafeonline.org/business-safe-online/implement-a-cybersecurity-plan/>

Suter, M. (2011). Resilience and Risk Management in Critical Infrastructure Protection: Exploring the Relationship and Comparing its Use. *Zürich: Center for Security Studies (CSS), ETH Zürich*.

Vatn, J., Hokstad, P., & Utne, I. B. (2012). Defining concepts and categorizing interdependencies. In *Risk and Interdependencies in Critical Infrastructures*(pp. 13-22). Springer London.

Woods, D. D., & Hollnagel, E. (2006). Prologue: resilience engineering concepts. *Resilience engineering. Concepts and precepts*, 1-16.

World Health Organization. (2014). *Water safety in distribution systems*. World Health Organization.

Wreathall, J. (2011). Monitoring—a critical ability in resilience engineering.*Resilience engineering in practice. Aldershot: Ashgate*, 61-8.

Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety*, *152*, 137-150.

Zurich municipal (2014, 18 December). Understanding the impact of cyber and information risk. Accessed 4 June 2017 at http://newsandviews.zurich.co.uk/download/understanding-the-impact-of-cyber-and-information-risk/

Øien, K. (2001). Risk indicators as a tool for risk control. *Reliability Engineering & System Safety*, *74*(2), 129-145.

Øien, K., Massaiu, S., Tinmannsvik, R. K., & Størseth, F. (2010, June). Development of early warning indicators based on resilience engineering. In*Submitted to PSAM10, International Probabilistic Safety Assessment and Management Conference* (pp. 7-11).

Øien, K., Utne, I. B., & Herrera, I. A. (2011). Building safety indicators: Part 1–theoretical foundation. *Safety science*, *49*(2), 148-161.

Øien, K., Grøtan, T. O., Øren, A., Jovanovic, A., Choudhary, A., Tetlak, K. & Jelic, M. (2017a). *Assessing Infrastructure Resilience Levels.* Release No.:1

Øien, K., Grøtan, T. O., Øren, A., Jovanovic, A., Choudhary, A., Tetlak, K. & Jelic, M. (2017b). *Assessing Infrastructure Resilience Levels.* Release No.:3

Appendix 1 – Criteria for candidate indicators and issues

This appendix provides a set of guidelines for defining good issues and indicators. The guidelines are more or less literally as given in appendix A.2.1 in Bodsberg et al. (2017, pp. xvii).

- "Issue" is a very general term referring to anything that is important in order to be resilient against severe threats such as terror attacks, cyber threats and extreme weather. It is WHAT that is important, and it is allocated to one of the five phases in the resilience cycle. E.g., it can be "training" performed in the anticipate/prepare phase.
- "Indicator" is HOW to measure the issues. E.g., it can be "Average number of exercises completed by operating personnel each month".
- One issue needs to be measured with at least one indicator, ideally with more than one.
- Normally, one indicator should belong to just one issue, and not overlap.
- One issue should normally be allocated to one phase. E.g. for the issue "communication", it is not the same communication that is needed in the various phases, and it is also measured with different indicators. Thus, it should be considered to specify the issue to fit the specific phase, e.g. "communication of anticipated threats" in the anticipate/prepare phase, and "communication during response" in the respond/recover phase. If not, it is too easy to "tick off" many/all phases.
- The completeness of the selected issues and indicators is another aspect of the quality of the process of identifying and selecting issues and indicators. There is obviously a minimum amount of issues needed to give a complete picture of the resilience in each phase of the resilience cycle. It is up to the users to define a required number of issues (and indicators) to provide a sufficiently complete resilience picture; however, as a rule of thumb a minimum of seven to eight issues per phase should probably be identified and selected. Assuming that not all phases are at the minimum number of issues, we may have about 40-50 issues for one specific threat for one critical infrastructure. Much less than this indicates incompleteness.
- High validity and high reliability are scientific requirements; however, there are also several non-scientific ("usefulness") requirements to indicators. In the SmartResilience project, it is stated e.g. that the indicators should be:
    - Clear,
    - Realistic,
    - Measurable,
    - Tangible,
    - Standardized,
    - Harmonized and performing

Appendix 2 – Interview: Current practice

This appendix provides the interview questions used to map the current resilience status of the water supply in Stavanger. The questions are based on the interview protocol and the general questions found in Annex 3 in the report written by Buhr et al. (2016). The questions were adapted and modified in order better suit the water supply as the CI. Only the questions considered relevant was included. The interviewees answering these questions where the head of the water and wastewater department in Stavanger (Jarle Furre) and a drinking water manager from IVAR (Karl Olav Gjerstad). The answers obtained from this were used as input to the case study and the following analysis. The term "resilience" was not a term known by the interviewees, but an explanation was given. However, they could very much relate to the term "robust", meaning that even though all of the phases of resilience (in the SmartResilience definition) were not considered in their understanding of the word, they felt that the work they provide is based on robust and reliable procedures. Hence, the questions asked related to resilience and resilience assessment was answered according to their interpretation of the term; that resilience and robustness are more or less the same.

In the following, only the questions asked will be stated. The answers are summarized in chapter 4 of this thesis.

Interview questions:

Current work with resilience:

- Describe what role this organization has for the drinking water supply in Stavanger.
- What risks are considered particularly relevant for the drinking water supply (in Stavanger), and how does your organization work to understand these risks?
- Are there any changing conditions considered particularly relevant, and how are you working in order to anticipate, prepare for and adapt to these changing conditions?
- What (sudden) disruptions are particularly relevant for the drinking water supply, and how are you working in order to withstand, respond to and recover rapidly from these disruptions?
- Does your organization work with the concept of resilience in order to maintain a safe and reliable drinking water supply?
- Does your organization work with the concept of resilience towards the drinking water supply?
    - Yes:
        - How is resilience understood in relation to the water supply in Stavanger?

Current work with <u>assessing</u> resilience (including use of indicators and the organizations challenges, needs and requirements).

- Has the drinking water supply in Stavanger been assessed for its resilience?
    - Yes:

        - Can you provide examples of such assessments?
        - What kind of information was used for such assessment?
        - Has such assessments met current needs and requirements?
        - How can these assessments be improved?
        - Is assessing resilience a continuously running process?
- Has indicators been used for assessment of resilience of the drinking water supply in Stavanger?
    - Yes:
        - Can you provide examples of such indicators and how they have been used?
        - Have these indicators met needs and requirements?

Projected needs and requirements:

- Can you foresee a changed need to assess resilience for the drinking water supply in Stavanger compared to today?
- If the drinking water supply in Stavanger should become increasingly "smarter", would it introduce new forms of risks into the system?

Appendix 3 – Interview: Operational Control Systems and security practice.

This appendix provides the interview questions asked when mapping the overall security related to the operational control systems at IVAR and the municipality of Stavanger. The interviewees answering these questions where the operational control system responsible at IVAR (Kjetil Birkedal Pedersen) and the head of the water and wastewater department in Stavanger (Jarle Furre). The answers obtained from this were used as input to the case study and the following analysis. The author of this thesis is far from an expert on operational control systems and ICT security, hence the questions where elaborated and prepared together with a friend and expert on the field Ole Christian Olsen, working at Profitbase. The questions asked are adapted with respect to maintaining confidentiality, integrity and availability of the operational control systems.

Operational control systems:

- Is the operational control system custom-made in order to fit your needs and requirements?
- Access:
    - Default or private passwords?
    - 2-factor authentication?
    - Access from home?
    - Who is given access? Restrictions?
    - Is the access removed for former employees?
- Interconnection with other networks?
- Are there any measures made to improve/reduce the probability for – and the consequences for – unwanted incidents? E.g.:
    - Testing the system towards known attacks?
    - Technical measures/plans (boundary protection of facility, segmentation of network)?
    - Human factors – courses, emergency preparedness training, security awareness training?
    - Establish organizational operational routines (changing passwords regularly, log critical operations)?
    - Restrictions in what are possible to control from home?
- Is the operational control system available online?
- Are there routines related to revision of firewalls?
- Is critical information encrypted?
- Value assessment related to criticality of information?
- ISO 27001 certified?
- Reporting routines?
    - Do your organization report traffic against not open gates?
    - Do your organization report spam mails not detected by the spam filter?
    - Do your organization report interruptions? (E.g. interruptions in communication between the PC at home and the server at the facility)
    - Do your organization provide an overview of who is logging in and report what they are doing while logged in? (Unusual account activity)

- Are critical functions provided with extra security measures?
- Zoning of the communication network, separate the process control system from administration systems and Internet as much as possible?
- Is your organization using checklists to secure the operational control systems, e.g. the checklist provided in appendix 1 in Johnsen & Røstum (2015)?
- Is there performed risk and vulnerability analysis especially suited for ICT and operational control systems?

Appendix 4 – Water distribution network in Stavanger

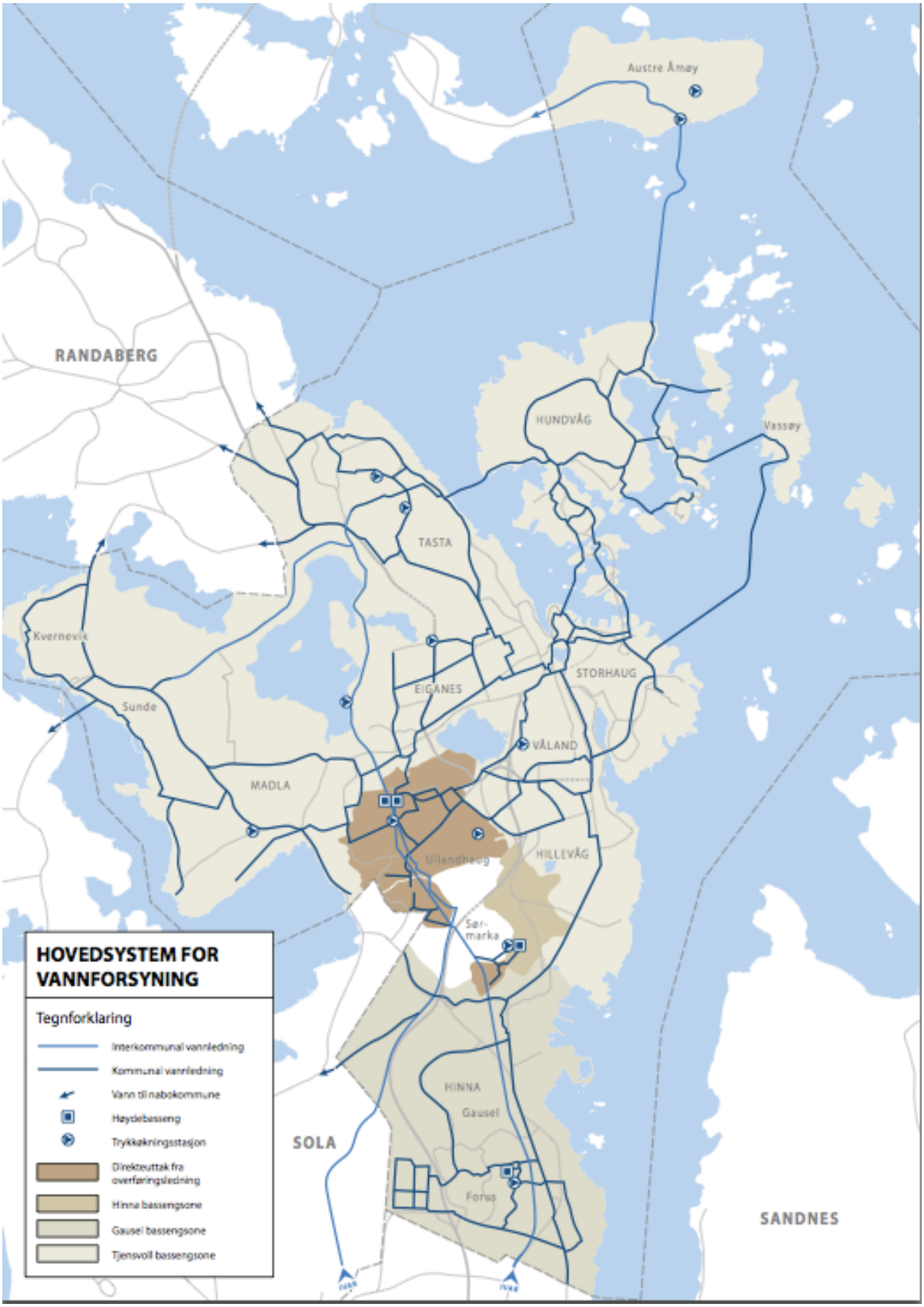

Figure A.4.1: Water distribution network in Stavanger, overview (Stavanger kommune, 2010a)

Appendix 5 – Generic candidate issues

Table A.5.1: Generic candidate issues. The green shaded rows are general issues, which are specified beneath (Øien et al., 2017b).

ID	Issue name	Issue description
I	Phase I - Understand risks	
	Risk understanding (general)	How we achieve knowledge and experience about risk/hazards
I.1	System knowledge	Knowledge about how the technical systems work and the interactions between systems, and knowledge about design assumptions and operational conditions. This knowledge provides insight in how systems may fail, and the potential consequences.
I.2	Information and knowledge about risk	Risk understanding is enhanced by basic knowledge of the concept of risk, and by specific knowledge about the risk on the particular plant, installation, etc. described in various risk analyses. A certain level of basic knowledge about risk is required in order to utilize the risk analyses information and/or to perform risk analyses.
I.3	Criteria for safe operation well defined and understood	In order to understand when support is needed it is necessary that the criteria for safe operation is well defined and understood.
I.4	Knowledge about context	Knowledge about e.g. the specific threats/hazards and situational factors.
I.5	Knowledge about CI dependencies	Knowledge about dependencies between own CI and other CIs, including unexpected or non-intuitive dependencies.
I.6	Event reports	Information about real incidents and accidents gives knowledge about what have happened in the past, which also provides insight in what may go wrong in the future.
I.7	Failure data gathering	Failure data provides information on the status of the critical infrastructure systems and potential causes of events.
I.8	Information about quality of barriers	Information about the quality of barriers, e.g. based on test results or real demand, gives knowledge about how well the safe-guards / defenses are protecting against accidental events. It provides insight in the technical systems that prevent the development of an accidental event.

ID	Issue name	Issue description
I.9	Information about quality of barrier support functions	Information about the quality of barrier support functions, e.g. preventive maintenance, by-passing, etc. including human and organizational elements, gives knowledge about the operational readiness of the safe-guards / defenses. It provides insight in the operational support systems contributing to the readiness of the barriers.
I.10	Discussion of risk/safety/resilience issues in regular meetings	Exchange and spreading of information about on-going risk/ safety/resilience issues in regular meetings enhances risk/safety/ resilience awareness in the organization.
I.11	Risk/safety/resilience performance requested by senior management	When risk/safety/resilience performance is requested by senior management it signals the importance of risk/safety/resilience in general and the specific issues that are addressed in particular. It enhances the awareness of the importance of risk/safety/ resilience in the organization.
I.12	Communication risk/resilience at all levels in the organization	To obtain widespread risk awareness in the organization it is important that information about risk and resilience are properly communicated at all levels in the organization. This can be obtained through various channels, e.g. meetings, safety alerts, bulletins, etc.
	Smartness issues (general)	How smart features can create vulnerability or opportunity
I.13	Smartness vulnerability in the understand risks phase	Are there any smart features ("smartness") included in the critical infrastructure(s), which makes it more difficult to understand risks, e.g. through failures in these smart features?
I.14	Smartness opportunity in the understand risks phase	Are there any smart features ("smartness") included in the critical infrastructure(s), which makes it easier to understand risks, e.g. through the functioning of these smart features?
II	Phase !! - Anticipate/prepare	
	Anticipation (general)	What we can expect
II.1	Risk/hazard identification	Systematic risk/hazard identification is a prerequisite in order to anticipate what may go wrong. It expands on the repertoire of incidents/accidents that have been experienced.

ID	Issue name	Issue description
II.2	Learning form own events and experiences	The most obvious source of information on what may go wrong (and how to treat such situations) is the experience from incidents and accidents in own organization. It is a particular obligation to any organization to avoid the reoccurrence of events. Learning from success stories, e.g. "what went right", should also be included.
II.3	Learning from other`s events and experiences	The manifestation of potential events in real occurrences constitutes only a small percentage of the potential events. Therefore, it is important to learn as much as possible also from other's incidents and accidents. Today's accessibility of information makes organizational borders no excuse for learning from outside own organization. Learning from success stories, e.g. "what went right", should also be included.
	Attention/vigilance (general)	What we should look for
II.4	Operational disturbance	Any operational disturbance, in particular those leading to the actuation of control and/or safety systems, should be paid attention to since they may represent the initiation of accidental events.
II.5	Bypass of control and safety functions	If control and safety functions are bypassed, i.e. disabled, then these barriers provide false security. The safe-guards / defenses are made ineffective against accidental events through these by-passes, and it is important to have full knowledge and overview, and keep track of any by-passes in the barrier systems.
II.6	Activity level & simultaneous operations	The possibility that something goes wrong increases with the activity level in general and with simultaneous operations in particular. Unexpected interactions between activities can increase the accident risk. Thus, it is important to be particularly vigilant in periods with high activity / high number of simultaneous operations.
II.7	Status on risk, events, quality of barriers, etc.	The status on risk, events, quality of barriers, etc. compared to thresholds, provides information on where to focus attention.

ID	Issue name	Issue description
II.8	Trends in risk, events, quality of barriers, etc.	Increase in reported events or negative development in the quality of barriers are clear indications of the need to take action to remedy the situation.
II.9	Risk treatment (plans/systems)	Continuous follow-up of risk treatment identified, e.g. actions identified in risk register systems.
II.10	Increased preparedness under certain situations/conditions	Increasing preparedness based on predefined signals/warnings/ gauges/measurements etc. of threats, situational factors, etc.
II.11	Emerging risks	Vigilance with respect to identifying emerging risks early, using risk radars, etc.
II.12	Expecting the unexpected (look in the horizon)	Ability to foresee consequences, especially to "invent" unprecedented but meaningful/coherent outcomes/alternatives before "discovering" them.
II.13	Early warning systems	Early warnings / weak signals provide information about potentially deteriorating safety before this is manifested in trends. It provides an opportunity to be proactive and take action at an early stage.
II.14	Information on continuously updated threat assessments	Actively seeking information on threat assessments ("threat levels") by e.g. authorities
II.15	Alert systems	Utilization of fixed technical alert systems, identifying threats and/or increased level of threat.
II.16	Monitoring	Continuous monitoring of potential threats.
II.17	Changes (technical, organizational, external)	Any changes, whether they are deliberate or not, may cause unintentional effects on safety and security. Close attention should be paid to changes with respect to potential negative effects.
II.18	Audits	Regular searching for problems/weaknesses/failures through audits (internal and/or external).
II.19	Focus and resource spending on safety/resilience issues	Safety is often claimed to be first priority. This should also be reflected in the proportion of attention given to safety and resilience, e.g. in decision-making and spending of resources.
II.20	Budget for preparedness and response resources (increase/decrease)	Development (increase or decrease) in budgets/resources allocated for preparedness and response/recovery.
	Resilient design (general)	How to prepare a resilient design
II.21	Robustness (functions/systems)	Resilience through robust design, e.g. large safety margins.

ID	Issue name	Issue description
II.22	Redundancy (functions/systems)	Resilience through redundant functions and/or systems.
II.23	Diversity (functions/systems)	Resilience through less vulnerability by diverse functions and systems.
II.24	Back-up/alternative (functions/systems)	Internal back-up systems or alternatives.
II.25	Externalized redundancy	Redundancy through external resources.
	Resilient operation (general)	How to prepare a resilient operation
II.26	Resilience plans	Preparing for resilience through dedicated resilience plans.
II.27	Safety plans	Preparing for resilience through safety plans.
II.28	Security plans	Preparing for resilience through security plans.
II.29	Emergency preparedness plans (and crisis organization)	Preparing for resilience through emergency preparedness plans, including pre-planned crisis organizations.
II.30	Business continuity plans	Preparing for resilience through continuity plans.
II.31	Compliance with plans, procedures, rules	Compliance and ensuring of conditions for following predefined plans/procedures.
II.32	Training plans (table-top, simulator, drills, etc.)	Training plans on how to deal with potential scenarios is essential in order to know what to do, not only with respect to identical or similar scenarios as trained on, but also with respect to response to other (unexpected) scenarios. This includes the use of simulators, table-top exercises, emergency preparedness drills, etc.
II.33	Joint exercises plans	Preparing for resilient emergency response through plans for joint exercises with external actors.
II.34	Adaptability/renewal of training (timely revisions)	The repertoire of training scenarios should be reviewed and adapted regularly based on experience from own and other's accidents, and the training material updated accordingly. The training should cover a sufficiently broad specter of scenarios.
II.35	Experience in handling of expectations	The handling of exceptions provides hands-on experience in how to respond. Such exceptions may be experienced during commissioning and start-up of operations. Thus, it is valuable to have access to personnel with experience from commissioning and start-up, in addition to personnel experienced in the handling of exceptions during normal operation.
II.36	Cooperation agreements (external resources)	Pre-planned agreements of use of external resources in crisis situations.

ID	Issue name	Issue description
II.37	Knowledge about external support/resources)	Knowledge about possible external support/resources at various levels; local, regional, national, international.
II.38	Interoperability in communication (internal)	Compatibility of internal communication systems.
II.39	Interoperability in communication (external)	Compatibility with external communication systems.
II.40	Physical entrance control	Physical barriers and other systems to prevent unauthorized entrance of areas, buildings, rooms, etc.
II.41	Cyber entrance control	Barriers and systems to prevent unauthorized access to IT systems.
II.42	Planned maintenance	Planned maintenance of critical systems and equipment to ensure adequate functioning.
II.43	Financial resources/insurance	Necessary financial resources to maintain resilient operations and being financially prepared for major events/interruptions.
	Smartness issues (general)	How smart features can create vulnerability or opportunity
II.44	Smartness vulnerability in the anticipate/prepare phase	Are there any smart features ("smartness") included in the critical infrastructure(s), which makes it more difficult to anticipate what may happen and/or prepare for it, e.g. if failures occur in these smart features?
II.45	Smartness opportunity in the anticipate/prepare phase	Are there any smart features ("smartness") included in the critical infrastructure(s), which makes it easier to anticipate what may happen and/or prepare for it, e.g. through the functioning of these smart features?
III	Phase III - Absorb/withstand	
	Inherent absorption (general)	How the physical critical infrastructure is able to absorb an event
III.1	Passive safety systems	Passive physical safety systems designed into the critical infrastructure to prevent (access of) threats or any escalation of an event.
III.2	Absorption/damage limitation	Energy absorbed in order to limit damages, as part of a resilient design of the critical infrastructure.
	Resilient reaction (general)	How the critical infrastructure is able to provide a resilient reaction to withstand an event
III.3	Active safety systems	Automatic and/or manual safety systems to detect/prevent/ withstand an event.
III.4	Notification/alarm	Notification of an event, e.g. by releasing an alarm, as soon as possible to the responsible unit, e.g. a control center.

ID	Issue name	Issue description
III.5	Confirmation of threat/event	Confirming that the threat/event is real, and what kind of threat/ event it is.
III.6	Action plan - reaction (availability, familiarity, use)	Availability, familiarity with, and use of pre-planned action plans for immediate reaction to an event.
III.7	Competent personnel	Competent/experienced personnel are required to obtain a resilient reaction to withstand an (expected or unexpected) event.
III.8	Local knowledge	Personnel with detailed local knowledge on where to find what (e.g. buildings, systems, resources, etc.) is required to obtain a speedy resilient reaction.
III.9	Improvisation/adaptation (of reaction)	Ability to identify alternative paths of action, and discriminate between their respective consequences.
III.10	Flexibility of organizational structure (autonomy/regroup)	The organization handling disturbances, incidents and emergency situations should be clearly recognized by all personnel. The transformation from normal operation to an emergency situation and back to normal operation should be clearly defined and trained for. The organization also needs to be flexible and able to adapt to the development of the situation, including substitution of injured or otherwise inaccessible personnel.
III.11	Ability to make correct decisions	Authority, support and training in making critical decisions, including decisions with potentially large economic effects.
III.12	Internal alarm	Alerting personnel which may be in immediate danger.
III.13	Alternative mustering (escape way/evacuation)	Consider if alternative – other than predefined – escape directions and/or mustering locations needs to be chosen.
III.14	Internal announcement	Internal announcement over loudspeakers about the situation, and how personnel should act.
III.15	Emergency response organization mobilization	Mobilization/scrambling of the emergency response organization.
III.16	Alternative emergency response center consideration	Having and consider using (a predefined) alternative emergency response center in case the normal response center is or may be affected by the event.
III.17	Notification of response resources	Notification of required internal and external response resources according to action plan.

ID	Issue name	Issue description
III.18	Situational awareness (early sense making/avoid blind spots)	Being able to see the whole picture, to quest about and gather as much relevant information as possible.
III.19	Announcement of accident scene center (location)	Deciding on and announcing location of accident scene center.
III.20	Personnel tracking/overview	Providing overview of location and number of persons.
III.21	External alert/communication	Alerting, informing and communicating with relevant external stake-holders, e.g. head office, authorities, etc.
III.22	Adapt (stop/reduce) operation	Adaptation of the operation according to the event, e.g. reduce, minimize or stop operations.
III.23	Secure combat personnel	Deploying combat personnel (e.g. fire fighters, smoke divers, etc.) when considered safe.
III.24	Start combat/handling of threat/event	Combat of threat/event with required available resources.
III.25	Evacuation of non-essential personnel	Evacuation of non-essential personnel (i.e. personnel not part of emergency response) to a safe haven.
III.26	Status update	Obtaining regularly update of status of situation during the absorb phase (initial response).
III.27	Communication (status update)	Communicating the status of the situation during the initial response as relevant (internally and externally).
III.28	Authority contact/liaison	Establishing contact/liaison with authorities and communicate regularly during initial response.
III.29	Media handling	Use of dedicated resources for media handling during initial response.
	Decision support (general)	How we support decisions (remedy of goal-conflicts) in order to maintain critical functions
III.30	Decision support staffing (availability/knowledge)	Adequate decision support staffing, either locally or remotely, implies staffing being available when required with necessary knowledge, experience and authority to provide/suggest decisions/actions. This may also concern goal-conflicts.
III.31	Decision support ICT systems (and ICT personnel)	Decision support requires adequate (remote) ICT decision support systems in place. This also includes adequate support for the ICT systems themselves, i.e. availability of ICT personnel. It is crucial to avoid breakdown or malfunction of these systems during a critical situation.

ID	Issue name	Issue description
III.32	External decision support (at various levels)	A situation may require the support from outside own organization. Thus, the necessary external support, including accompanying ICT systems, must be available when required.
III.33	Understanding and willingness to use external support	Understanding that a complex situation can require external expertise to fully comprehend in order to take appropriate decisions, and willingness to receive support from outside.
III.34	Coordination between actors (at various levels), internal	Coordination within each emergency response team, coordination of all resources/teams at the scene of the event (or nearby), local coordination of the entire emergency response operation from a central emergency response center, etc. Sharing of information.
III.35	Coordination between actors (at various levels), external	External coordination with area, regional or wider resources, including headquarters, authorities, etc. Sharing of information.
	Redundancy for support (general)	How we compensate for degradation to uphold/maintain critical functions
III.36	Redundancy of decision support functions	Critical decision support functions, internal and external, should be redundant to ensure availability of support.
III.37	Redundancy in information processing	Critical information systems should be redundant to ensure information flow necessary for decision support.
	Smartness issues (general)	How smart features can create vulnerability or opportunity
III.38	Smartness vulnerability in the absorb/withstand phase	Are there any smart features ("smartness") included in the critical infrastructure(s), which makes it more difficult to absorb/ withstand an event?
III.39	Smartness opportunity in the absorb/withstand phase	Are there any smart features ("smartness") included in the critical infrastructure(s), which makes it easier to absorb/ withstand an event?
IV	Phase IV - Respond/recover	
	Response capacity and rapidity (general)	How we can ensure timely and sufficient response
IV.1	Resourcefulness/emergency response resources (internal)	Internal emergency response resources and response/ mobilization time. Equipment (fixed/mobile, automatic/manual, etc.), personnel, organization, etc.

ID	Issue name	Issue description
IV.2	Resource allocation and staffing (including buffer capacity)	Sufficient number of persons attending to critical functions, including back-up personnel in case of additional needs, unavailability of personnel or exchange of personnel. Duty schemes enabling adequate mobilization to provide timely response are needed.
IV.3	Emergency response resources (external)	External emergency response resources and response/ mobilization time. Equipment, personnel, organization, agreements/contracts, etc.
IV.4	Communication between actors	Response is often dependent on information from other actors. It is essential that the (local) information and communication systems are available throughout the duration of the situation until control has been regained. The information itself needs to be understandable for all actors involved (including use of common language).
IV.5	ICT systems (timely updating of information)	Timely response requires timely updating of necessary information about the situation and the need to communicate this between the involved actors.
	Resilient response and recovery (general)	How we can ensure completion of the response (without suffering damage)
IV.6	Robustness of responsible function	Endurance of critical functions to complete the response. This includes personnel in charge of critical tasks as well as the upholding of critical infrastructure systems (e.g. main safety functions).
IV.7	Organizational robustness (back-up functions)	Even if single persons are unavailable for some reason the critical functions should be ensured through pre-planned back- up, e.g. by deputies given the same training as the main responsible persons.
IV.8	Endurance of response	Having enough response resources, e.g. more shifts/teams/ resource pool, etc. to ensure completion of the response.
IV.9	Redundancy in skills; multiple skills	Redundancy in skills and multiple skills provide the organization with means to back-up critical functions. This goes beyond what is foreseen or pre-planned.
IV.10	Action plan - response (availability, familiarity, use)	Availability, familiarity with, and use of action plans for response actions.

ID	Issue name	Issue description
IV.11	Training (table-top, simulator, drills, etc)	Training on how to deal with potential scenarios is essential in order to know what to do, not only with respect to identical or similar scenarios as trained on, but also with respect to response to other (unexpected) scenarios. This includes the use of simulators, table-top exercises, emergency preparedness drills, etc.
IV.12	Joint exercises	Resilient response and recovery through joint exercises with external actors.
IV.13	Improvisation/adaptation (of response/recovery)	Ability to orchestrate new/novel actions by combining different resources in a new/novel manner, and the ability to (re-)use resources for other purposes than intended.
IV.14	Monitor effects and adapt (shit attention)	Monitoring the effect of chosen response strategies or actions, and ongoing adaptation (e.g. shift of attention) as required.
IV.15	Combat threat/event	Combat threat/event until the situation is fully under control. This may require exchange of exhausted response personnel.
IV.16	Search and rescue	Search for and rescue of missing personnel.
IV.17	Medical treatment	Medical treatment of injured personnel on scene.
IV.18	Medical evacuation	Evacuation of injured personnel for (further) medical treatment.
IV.19	General evacuation	General evacuation of the area, including emergency response resources.
IV.20	Status update	Obtain regularly update of status of situation during response and recovery.
IV.21	Communication (status update)	Communicate the status of the situation during response and recovery as relevant (internally and externally).
IV.22	Authority contact/liaison	Establish contact/liaison with authorities and communicate regularly during response and recovery.
IV.23	Media handling	Use dedicated resources for media handling during response and recovery.
IV.24	Secure area	Secure the area and limit access to relevant response and investigation personnel (including securing any evidence).
IV.25	Register involved personnel	Register all involved personnel; emergency response personnel, injured personnel and casualties.
IV.26	Repair damages (unplanned maintenance)	Repair any damages to the critical infrastructure.

ID	Issue name	Issue description
IV.27	Risk assess and clarify re-start/continuing operation	Make risk assessment and clarifications (including approvals) before re-start/ continuing of operation.
IV.28	Insurance claims	Make insurance claims to compensate for economic losses to regain financial strength.
	Smartness issues (general)	How smart features can create vulnerability or opportunity
IV.29	Smartness vulnerability in the respond/recover phase	Are there any smart features ("smartness") included in the critical infrastructure(s), which makes it more difficult to respond to or recover from an event? Can it hamper response/recovery?
IV.30	Smartness opportunity in the respond/recover phase	Are there any smart features ("smartness") included in the critical infrastructure(s), which makes it easier to respond to or recover from an event? Can it help in response/recovery?
V	Phase V - Adapt/learn	
	Learning/improvement (general)	How we learn and improve from the event and the response
V.1	Debriefing	Provide a debriefing of the event and the response operation to personnel directly involved.
V.2	Follow-up of injured personnel	Follow-up injured personnel, including long-term follow-up of mental stress and trauma.
V.3	Next-of-kin handling	Arrange for taking care of next-of-kin (travels, hotels, priests, shield from media, information, funerals, etc.)
V.4	Media handling	Provide information to the media about what happened, the response operation, investigations, follow-up of involved persons, etc.
V.5	Event investigation and reporting including recommendations for adaptation/improvement	Investigation of event, including underlying causes, and recommendation for adaptation/improvement of operations (physical, technical, operational, organizational, etc.).
V.6	Presentation/communication of event investigation	Presentation and communication of the results of the investigation internally and externally (notifications, reports, presentations, press conferences, etc.).
V.7	Implementation and follow-up of recommendations for adaptation/improvement	Implement and follow-up the recommended adaptations/ resilience improvements.

ID	Issue name	Issue description
V.8	Emergency response operation reporting including lessons learned	Reporting of the response operation and any lessons learned for future emergency response and resilience improvements.
V.9	Implementation and follow-up of lessons learned	Implementation and follow-up of the lessons learned from the emergency response operation (resources, capabilities, etc.).
V.10	Presentation/communication of emergency response operation	Presentation and communication of the lessons learned from the emergency response operation internally and externally.
V.11	Feedback and learning from successful operations	Providing feedback and learning from successful operations in addition to event investigations, which focus on improving unsuccessful operations.
V.12	Continuous resilience improvement (e.g. resilience level, robustness and rapidity)	Continuous focus on and improvement of those issues contributing least to resilience.
V.13	System/archive to store knowledge	System/archive to store and retrieve knowledge/experience/ lessons learned from events and response operations.
	Smartness issues (general)	How smart features can create vulnerability or opportunity
V.14	Smartness vulnerability in the adapt/learn phase	Are there any smart features ("smartness") included in the critical infrastructure(s), which makes it more difficult to adapt/learn from an event and/or the response?
V.15	Smartness opportunity in the adapt/learn phase	Are there any smart features ("smartness") included in the critical infrastructure(s), which makes it easier to adapt/learn from an event and/or the response? Can it provide additional information?