H2020 Project: Smart Resilience Indicators for Smart Critical Infrastructure
D2.1 - Understanding “smart” technologies and their role in ensuring resilience of infrastructures

Coordinator: Aleksandar Jovanovic EU-VRi
Project Manager: Bastien Caillard EU-VRi
European Virtual Institute for Integrated Risk Management
Haus der Wirtschaft, Willi-Bleicher-Straße 19, 70174 Stuttgart
Contact: smartResilience-CORE@eu-vri.eu
Understanding “smart” technologies and their role in ensuring resilience of infrastructures

File name / Release: D2.1_v54bc31102017
Pages: 67
Status: Final
No. of annexes: 2
Dissemination level: PU

SmartResilience: Smart Resilience Indicators for Smart Critical Infrastructures
Grant Agreement No.: 700621
Project No.: 12135

WP title: WP2: Challenges and interdependencies of Smart Critical Infrastructures (SCIs)
Deliverable No.: 2.1

Date:
Due date: October 31, 2017
Submission date: October 31, 2017

Keywords:
Smart system, Smart critical infrastructure, resilience, challenges, Internet of Things, Smart maturity model, Emerging risk management framework

Reviewed by:
L. Bodsberg
P. Auerkari

Approved by Coordinator:
A. Jovanovic

Stuttgart, October 2017
## Release History

<table>
<thead>
<tr>
<th>Release No.</th>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>March 14, 2017</td>
<td>The first draft of the report sent to the task partners with the literature review of the characteristics and challenges of Smart systems</td>
</tr>
<tr>
<td>2</td>
<td>September 14, 2017</td>
<td>Second draft of the report sent to the project case study partners for validation</td>
</tr>
<tr>
<td>3</td>
<td>October 20, 2017</td>
<td>Third draft of the report set for review</td>
</tr>
<tr>
<td>4</td>
<td>October 25, 2017</td>
<td>Fourth draft shared with co-authors for feedback</td>
</tr>
<tr>
<td>5</td>
<td>October 30, 2017</td>
<td>Sent to European commission</td>
</tr>
</tbody>
</table>
Modern critical infrastructures are becoming increasingly smarter (e.g. the smart cities). Making the infrastructures smarter usually means making them smarter in the normal operation and use: more adaptive, more intelligent etc. But, will these smart critical infrastructures (SCIs) behave smartly and be smartly resilient also when exposed to extreme threats, such as extreme weather disasters or terrorist attacks? If making existing infrastructure smarter is achieved by making it more complex, would it also make it more vulnerable? Would this affect resilience of an SCI as its ability to anticipate, prepare for, adapt and withstand, respond to, and recover? What are the resilience indicators (RIs) which one has to look at?

These are the main questions tackled by SmartResilience project.

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

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

The basic idea of this task is that the modern critical infrastructures (CI) are becoming increasingly smarter (e.g. the smart cities, smart energy supply). In short-term, making the infrastructures smarter usually means making them smart in the normal operation and use: more adaptive, more intelligent etc. systems. This way, the infrastructures powered by the smart systems can learn smartly and react smartly. However, in long-term this increased smartness makes these infrastructures also more complex and more vulnerable to the unknown and emerging risks. With the smartness CIs enabled by the increased use of information technology (IT) may become part of networks where nodes represent different smart CIs and the links mimic the physical and relational connections among them. In such a networked system, the disruption in IT of one smart CI can potentially disrupt the functionality of other CIs. Furthermore, IT in itself is a CI. Then, the question arises, what if IT itself fails? The aspect of smartness has been studied extensively in smart city research, but also needs to be explored for CIs and specifically, what it means for smart CIs in this project.

Hence, it is at first important to clearly state what is meant by “smart” for a CI. The questions posed in the grant agreement (GA) to address this concern are:

1. What makes the selected Smart Critical Infrastructure “smart” and how do we assess the level of its “smartness”?
2. What are the challenges originating from the application of new technologies when enhancing the “smartness” of the selected Critical Infrastructures?

To address these questions, at first, the literature review was conducted, then literature review findings by the case study partners were followed.

The research on the first question provides an understanding of what are the characteristics of a “smart system”. Further, it helped derive a definition of smart CIs in the project. Next, types of technologies and specific smart technologies are identified for each of the project CI. As a basis for the above work, a smart maturity model is defined. Basis the smart technologies used in the project SCIs, their level of smartness has been identified. This model will be further used in WP5 and the level of smartness of CIs will be further refined. The research on the second question presents the current and emerging challenges related to the use of smart and new technologies in CIs.

The main result suggests that the smart systems used in the CIs have three key characteristics:

1. Integrated and interconnected
2. Intelligent
3. Autonomous

The respective current challenges posed by the use of these smart and new technologies are:

1. Vulnerability due to interconnectedness
2. Vulnerability due to centralization
3. Compromise of individual privacy
4. Governance relate challenges
5. Inconsistent adoption
6. Increased automation

Besides these current challenges, emerging challenges related to these technologies also are identified.

As an extra mile, these findings were then assessed by the case study partners. In the end, we propose that the Emerging Risk Management Framework from CEN Workshop Agreement (CWA) 16649, can be extended to manage these new smart technology related risks.
The report starts introducing the task, followed by a review chapter of smarter systems characteristics, and continues with a chapter on current and emerging challenges of related to new technologies in the SCIs. The subsequent chapter focuses on assessing the results from the literature in the project case studies. Chapter 6 deals with the SmartResilience approach to emerging risks of new smart technologies. Finally, Chapter 7 presents the main conclusions of this report. Lastly, the respective annexes on the glossary of the report and review process are included in the annex section.

This task provides essential inputs to other tasks and WPs of the SmartResilience project. The challenges related with smart and new technologies are relevant to task 2.2 and for WP 3 in defining the methodology for the project. Similarly, the smart system characteristics and challenges are of significance in the development of issues and indicators in WP4. The maturity model to assess the maturity levels of smart CIs provides the basis for work in WP5. The recommendations provided for the extension of the ERMF CWA 16649 standard will lay the foundation for the work on standardization in WP6.
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release History</td>
<td>i</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>iii</td>
</tr>
<tr>
<td>List of Figures</td>
<td>vii</td>
</tr>
<tr>
<td>List of Tables</td>
<td>viii</td>
</tr>
<tr>
<td>List of Acronyms</td>
<td>ix</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>11</td>
</tr>
<tr>
<td>1.1 Background- needs and requirements</td>
<td>11</td>
</tr>
<tr>
<td>1.1.1 Call text, task description, objectives and work in GA</td>
<td>11</td>
</tr>
<tr>
<td>1.1.2 Organization of work</td>
<td>12</td>
</tr>
<tr>
<td>1.1.3 Relation to other parts of the project</td>
<td>12</td>
</tr>
<tr>
<td>1.1.4 Report Structure</td>
<td>13</td>
</tr>
<tr>
<td>2 Characteristics of smart systems</td>
<td>14</td>
</tr>
<tr>
<td>2.1 Review of Literature for “smarter” systems characteristics of SCIs</td>
<td>14</td>
</tr>
<tr>
<td>2.1.1 Smart systems are integrative and interconnected</td>
<td>15</td>
</tr>
<tr>
<td>2.1.2 Smart systems are intelligent</td>
<td>15</td>
</tr>
<tr>
<td>2.1.3 Smart systems are autonomous</td>
<td>16</td>
</tr>
<tr>
<td>2.2 What is a smart critical infrastructure in SmartResilience project?</td>
<td>16</td>
</tr>
<tr>
<td>2.3 Types of smart and new technologies</td>
<td>16</td>
</tr>
<tr>
<td>2.4 Specific smart and new technologies</td>
<td>19</td>
</tr>
<tr>
<td>3 Smart systems maturity model for critical infrastructure</td>
<td>26</td>
</tr>
<tr>
<td>3.1 Example of Smart maturity model for Airports</td>
<td>28</td>
</tr>
<tr>
<td>3.2 Application of the proposed maturity model</td>
<td>28</td>
</tr>
<tr>
<td>4 Current and emerging challenges of new smart technologies on SCIs</td>
<td>30</td>
</tr>
<tr>
<td>4.1 Literature review of current challenges</td>
<td>30</td>
</tr>
<tr>
<td>4.1.1 Vulnerability due to interconnectedness</td>
<td>30</td>
</tr>
<tr>
<td>4.1.2 Vulnerability due to centralization</td>
<td>31</td>
</tr>
<tr>
<td>4.1.3 Compromise of individual privacy</td>
<td>31</td>
</tr>
<tr>
<td>4.1.4 Governance related challenges</td>
<td>32</td>
</tr>
<tr>
<td>4.1.5 Inconsistent Adoption</td>
<td>32</td>
</tr>
<tr>
<td>4.1.6 Increased automation</td>
<td>33</td>
</tr>
<tr>
<td>4.2 Emerging challenges related to the new technologies and smartness</td>
<td>33</td>
</tr>
<tr>
<td>5 Smart technologies and related challenges for SmartResilience case studies</td>
<td>35</td>
</tr>
<tr>
<td>5.1 ALPHA (“Financial System”) - City of Edinburgh</td>
<td>35</td>
</tr>
</tbody>
</table>
5.2 BRAVO (“The smart city”) – The future oriented and sustainable community
5.3 CHARLIE (“Healthcare”) – The Austrian health care system
5.4 DELTA (“Airport”) – Transportation infrastructure of Budapest airport
5.5 ECHO (Refinery) - NIS oil refinery-industrial plant in Serbia
5.6 FOXTROT (Water) - Drinking water supply in Sweden
5.7 GOLF (“Transport”) - Smart public transportation system (Cork City Council)
5.8 HOTEL (“Energy” – Energy supply infrastructure in Helsinki
5.9 Summary

6 Recommendations: SmartResilience approach to management of the emerging risks related to new smart technologies (CWA 16649)
6.1 Overview of Emerging Risk Management Framework (CWA 16649)
6.2 Possible extension towards resilience

7 Conclusions

References

ANNEXES
List of Figures

Figure 1: Relation of T2.1 to the other WPs and tasks in the project .......... 13
Figure 2: Characteristics of smart systems and underlying smart technologies 15
Figure 3: Example of the smartness maturity model applied to the DELTA case [42] ........................................................................................................ 28
Figure 4: Centralization of information processing in smart systems (adapted from [49]) ........................................................................ 31
Figure 5: Challenges related to increasing smartness of SCI, adapted from [61] 32
Figure 6: Emerging Risk Management Framework ..................................... 49
Figure 7: Extension of ERMF towards resilience SCIs ................................. 51
List of Tables

Table 1: Smart critical infrastructure in comparison with conventional infrastructures [75] ................................................................. 11
Table 2: Technologies in smart systems adapted from EPoSS SRA [86] ........... 17
Table 3: Specific smart technologies relevant for SmartResilience case studies (based on literature review) ..................................................... 19
Table 4: Maturity levels of smart critical infrastructures ........................................ 27
Table 5: Application of the proposed maturity model to the SmartResilience case studies ........................................................................ 28
Table 6: Identified challenges based on IRGC Factors (slightly adjusted from [18]) .......................................................... 33
Table 7: Smart technologies and related challenges for ALPHA case .............. 35
Table 8: Smart technologies and related challenges for BRAVO case ............. 39
Table 9: Smart technologies and related challenges for CHARLIE case .......... 40
Table 10: Smart technologies and related challenges for DELTA case .......... 41
Table 11: Smart technologies and related challenges for ECHO case study ...... 42
Table 12: Smart technologies and related challenges for FOXTROT case study. 43
Table 13: Smart technologies and related challenges for GOLF case study ...... 44
Table 14: Smart technologies and related challenges for HOTEL case study ...... 46
Table 15: Smart technologies for resilience and protection of the SCIs (not in the order of priority) .............................................................. 47
### List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>AR</td>
<td>Augmented Reality</td>
</tr>
<tr>
<td>ASD-B</td>
<td>Automatic Dependent Surveillance – Broadcast</td>
</tr>
<tr>
<td>ASM</td>
<td>Abnormal Situation Management</td>
</tr>
<tr>
<td>BIPV</td>
<td>Building-Integrated Photovoltaics</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-Circuit Television Camera</td>
</tr>
<tr>
<td>CEN</td>
<td>European Committee for Standardization</td>
</tr>
<tr>
<td>CI</td>
<td>Critical Infrastructure</td>
</tr>
<tr>
<td>CMMS</td>
<td>Computerized Maintenance Management Software</td>
</tr>
<tr>
<td>CRISP</td>
<td>Evaluation and Certification Schemes for Security Products</td>
</tr>
<tr>
<td>CWA</td>
<td>CEN Workshop Agreement</td>
</tr>
<tr>
<td>DCS</td>
<td>Distributed Control System</td>
</tr>
<tr>
<td>ECMWF</td>
<td>European Centre for Medium-Range Weather Forecasts</td>
</tr>
<tr>
<td>EMS</td>
<td>Energy Management System</td>
</tr>
<tr>
<td>EPoSS</td>
<td>European Technology Platform on Smart Systems Integration</td>
</tr>
<tr>
<td>ER</td>
<td>Emerging Risk</td>
</tr>
<tr>
<td>ERP</td>
<td>Enterprise Resource Planning</td>
</tr>
<tr>
<td>ERMF</td>
<td>Emerging Risk Management Framework</td>
</tr>
<tr>
<td>ESB</td>
<td>Electricity Supply Board</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>F2F</td>
<td>Face to Face</td>
</tr>
<tr>
<td>FEWS</td>
<td>Flood Early Warning System</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GA</td>
<td>Grant Agreement</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>GIS</td>
<td>Geographical Information System</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications</td>
</tr>
<tr>
<td>HMI</td>
<td>Human Machine Interface</td>
</tr>
<tr>
<td>HR</td>
<td>Human Resources</td>
</tr>
<tr>
<td>IAP</td>
<td>Intelligent Alarm Processor</td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control System</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IPT</td>
<td>Integrated Project Team</td>
</tr>
<tr>
<td>IRGC</td>
<td>International Risk Governance Council</td>
</tr>
<tr>
<td>ISCM</td>
<td>Integrated Substation Condition Monitoring</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITS</td>
<td>Intelligent Transport System</td>
</tr>
<tr>
<td>LIDAR</td>
<td>Light Detection and Ranging</td>
</tr>
<tr>
<td>LIMS</td>
<td>Laboratory Information Management System</td>
</tr>
<tr>
<td>MCDM</td>
<td>Multi-Criteria Decision Making</td>
</tr>
<tr>
<td>MEMS</td>
<td>Micro-Electro-Mechanical Systems</td>
</tr>
<tr>
<td>MES</td>
<td>Manufacturing Execution System</td>
</tr>
<tr>
<td>MNBS</td>
<td>Micro-Nano-Bio Systems</td>
</tr>
<tr>
<td>MOEMS</td>
<td>Micro-Opto-Electro-Mechanical Systems</td>
</tr>
<tr>
<td>MtM</td>
<td>More than Moore</td>
</tr>
<tr>
<td>NFC</td>
<td>Near field communication</td>
</tr>
<tr>
<td>NIS</td>
<td>Petroleum Industry of Serbia</td>
</tr>
<tr>
<td>OM</td>
<td>Outage Management</td>
</tr>
<tr>
<td>OPW</td>
<td>Office of Public Works</td>
</tr>
<tr>
<td>PDM</td>
<td>Probability Distributed Models</td>
</tr>
<tr>
<td>QR</td>
<td>Quick Response</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio-Frequency Identification</td>
</tr>
<tr>
<td>RPS</td>
<td>RPS Group Plc</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SCI</td>
<td>Smart Critical Infrastructure</td>
</tr>
<tr>
<td>SHEM</td>
<td>Streamflow Hydrology Estimate using Machine Learning</td>
</tr>
<tr>
<td>SMR</td>
<td>Smart Mature Resilience (SMR)</td>
</tr>
<tr>
<td>SRA</td>
<td>Strategic Research Agenda</td>
</tr>
<tr>
<td>USDHS</td>
<td>US Department of Homeland Security</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Background - needs and requirements

1.1.1 Call text, task description, objectives and work in GA

The overall goal of the SmartResilience project is to assess the resilience of smart critical infrastructures (SCIs). To do so, an important step is to understand “what it means to be “smart” for a critical infrastructure?” In the Grant Agreement (GA), task 2.1 is assigned to address this query [75].

Accordingly, the call text requires addressing “A better understanding of the critical infrastructure architecture is necessary for defining measures to achieve a better resilience against threat in an integrated manner including natural and human threats” [75]. Further, it is also stated that the “impacts and potential challenges of new technologies has to be integrated into case studies” [75].

Correspondingly, the main objective as of task 2.1 as per the task description in GA is to gain a better understanding of the nature of “smarter” technologies and their current and future emerging challenges when being applied in the context of critical infrastructures[75]. Also, the task aims to identify and analyze general (not hazard specific) challenges originating from the enhancement of critical infrastructures by new technologies with the goal to make them “smarter” [75].

Consequently, T2.1 provides answers to the questions [75]:

- What makes the selected Smart Critical Infrastructure “smart” and how do we assess the level of its “smartness”?
- What are the challenges originating from the application of new technologies when enhancing the “smartness” of the selected Critical Infrastructures?

The outcome is expected to inform on criteria for evaluating the “smartness” of a critical infrastructure by adjusting maturity models initially developed and applied within the scope of smart city research [75].

These requirements are addressed in the GA in chapter 1.1.3 i.e. “the modern critical infrastructures (CI) are becoming increasingly smarter (e.g. the smart cities, smart energy supply). Making these CIs smarter usually means making them smarter in normal operations and use: more adaptive more intelligent” [75]. In addition, these infrastructures differ from the conventional infrastructures as presented in the Table 1.

<table>
<thead>
<tr>
<th>Infrastructure characteristics</th>
<th>Conventional CI</th>
<th>Smart CI (SCIs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stakeholder involvement</td>
<td>Stakeholders are often engaged with the aim to create local support for the project, but without active involvement in the project design and operation</td>
<td>Stakeholders are often required to support the project and may have an active and ongoing role in the project design and operation</td>
</tr>
<tr>
<td>Engineering approach</td>
<td>Solutions enable standardization and replication which can significantly reduce project costs and delivery times</td>
<td>SCI solutions require a custom-made, location-specific design and do not lend themselves to standardization and replication</td>
</tr>
</tbody>
</table>
Further, the GA emphasizes that the use of new and smart technologies brings about new and emerging challenges.

The work in this task builds on the research presented in GA. To achieve the objectives of the task, a comprehensive literature review was conducted. The results of Task 2.1 provide a better understanding of the critical infrastructure architecture by identifying the characteristics of the smart systems used in the critical infrastructures, and the challenges that arise due to the use of such systems [75]. Also, this task defines a smart maturity model. Furthermore, these smart technologies and respective current and emerging challenges are validated by all the eight case studies in the project. This provides recommendations for extension of the resilience approach to manage emerging risks related to new smart technologies used by the SCIs.

### 1.1.2 Organization of work

The task objectives, as stated before, were implemented in following main steps. At first, a literature review was conducted to:

- Identify the characteristics of smart systems
- Define the conceptual terms i.e. smart systems, smart critical infrastructures,
- Identify specific smart technologies used in the CIs from different literature sources
- Define the smart maturity model for the project
- Identify the challenges of new smart technologies

In the second step, the identified specific smart technologies and challenges were checked and validated by the case study partners. Lastly, extension of the resilience related approach is analyzed to manage emerging risks related to new smart technologies used by the SCIs.

### 1.1.3 Relation to other parts of the project

The use of smart technologies in the CIs is one of the basic premises of the SmartResilience project. The relation of this task with other WPs and respective tasks is depicted in Figure 1. The findings of this report are significant to other tasks of the project in many ways. The results of the report are relevant to the task 2.2 considering the challenges posed by the use of smart and new technologies in the smart CIs. And they are relevant to the task 3.2 in defining the methodology for the project. Similarly, the smart system characteristics and challenges informed the development of issues and indicators in WP4. The maturity model to assess the maturity levels of smart CIs provides the basis for work in WP5. The recommendations provided for the extension of the EMRF CWA 16649 standard [18] will inform the work on standardization in WP6.

<table>
<thead>
<tr>
<th>Infrastructure characteristics</th>
<th>Conventional CI</th>
<th>Smart CI (SCIs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environmental footprint</td>
<td>Often increased environmental footprint due to material and energy intensive processes (manufacturing, distribution, operation)</td>
<td>Often reduced environmental footprint due to the solutions being nature-based and self-regenerating</td>
</tr>
<tr>
<td>Susceptibility to external factors</td>
<td>CI is susceptible to power loss, mechanical failure of industrial equipment and price volatility</td>
<td>SCIs are susceptible to extreme weather conditions, seasonal changes in temperature or rainfall and disease and similar</td>
</tr>
<tr>
<td>Monitoring and control</td>
<td>CI have decentralized operations. These systems have conventional monitoring and control of the operations.</td>
<td>SCIs are living and complex systems that can be monitored and effectively managed by a deep understanding of the key control variables</td>
</tr>
</tbody>
</table>
**1.1.4 Report Structure**

The report starts with the introduction of the task in chapter 1, followed by a chapter 2 on the review of the characteristics of smart systems, types of smart and new technologies and specific technologies. Then chapter 3 provides the smart systems maturity model and chapter 4, the current and emerging challenges of related with the use of these technologies in the SCIs. Subsequently, in chapter 5, assessment of the currently used smart technologies and related current and emerging challenges are presented. The next chapter 6, is about the SmartResilience approach to emerging risks of new smart technologies and followed by the chapter 7 on conclusions from this report. Lastly, the relevant annexes are included in the annex section.
2 Characteristics of smart systems

2.1 Review of Literature for “smarter” systems characteristics of SCIs

Most of the research on smart systems is focused on smart cities and on the factors that contribute to their smartness. Smart cities are composed of critical infrastructures, such as smart airports, smart manufacturing, smart healthcare system, smart water supply systems, etc. These cities are also referred to as CI of CIs. Recently, the focus has been shifting from city to critical infrastructures [86] [23] [24] [28], and is considered useful in this task. For example, the strategic agenda of the European Technology Platform on Smart Systems Integration (EPoSS) provides the definition of smart systems which is seen directly applicable to the project. The smart systems according to EPoSS are defined as “self-sufficient intelligent technical systems or subsystems with advanced functionality, enabled by underlying micro-, nano- and bio-systems and other components. They are able to sense, diagnose, describe, qualify and manage a given situation, their operation being further enhanced by their ability to mutually address, identify and work in consort with each other. They are highly reliable, often miniaturized, networked, predictive and energy autonomous” [86]. However no clear characteristics of the “smart systems” are defined in the current research.

The literature review revealed that the smart systems are primarily characterized by the scientific community into three key characteristics:

1. Integrated and interconnected [12] [33] [86] [35] [4]
2. Intelligent [12] [86] [32]
3. Autonomous [86]
2.1.1 **Smart systems are integrative and interconnected**

The smart systems are integrative and interconnected [12] [33] [86] [35] [4]. This means that within and outside the cities, the smart technologies integrate and interconnect all the CIs including transport systems such as airports and seaports, communications systems, roads, bridges, tunnels, rails, subways, essential services such as water, power and even major buildings [33].

This integration helps in monitoring the conditions of CIs and leveraging the collective intelligence of related CIs. In CIs operating assets/services i.e. people, plant, equipment, knowledge, models, databases, etc. are self-aware (via sensors) of their state. When integrated with field devices, actuators and operating equipment, they show intelligent processing capability. Every system is able to recognize its condition and publish that information and all other interoperating devices can take immediate and appropriate action [16]. This way the collective intelligence of the CIs is leveraged.

Further, combining ICT, web technology, sensors, monitoring systems, automated controls, modeling and other decision-support applications with other organizational, design and planning efforts helps to dematerialize and speed up bureaucratic processes and also to identify new, innovative solutions to managing complexity [12]. The development of digitalization, hard- and software, communication technology and common standards makes it possible to collect, store, analyze and distribute vast amounts of data and information. Essentially, this means that not only the individual processes in the CIs can be observed, monitored and controlled in isolation, but also due to the integrated systems their interaction and the effects of the changes in one infrastructure on another can be visualized [16].

2.1.2 **Smart systems are intelligent**

The smart systems are also referred with adjectives such as intelligent or digital [12] [86] [32]. Intelligence here means the inclusion of complex analytics, optimization, and visualization, modelling, in the operational business processes to make better operational decisions [34] [12]. They maximize performance, cost effectiveness, and profit by planning, continuously monitoring status and impacts of responses and applying learning to determine and implement appropriate action for planned and unplanned situations. Actions and decisions are adaptive, predictive and proactive [16].
The use of ICT and web 2.0 technology in the infrastructures are central factors for ensuring that it operates intelligently [12] [5]. ICT infrastructure includes wireless infrastructure (fiber optic channels, Wi-Fi networks, wireless hotspots, kiosks), and service-oriented information systems [12].

At a next level of advancement, the smart systems are considered artificially intelligent, meaning that they make machines to do things that would require intelligence comparable to human [7] e.g. in the use of sensors that help in reducing operator distraction and error [86], optimization of vehicle control, navigation and logistics [86]. Also, a smart system can autonomously or through networking safeguard and optimize every aspect of the critical chain [87]. It is also able to sense, diagnose, describe, qualify and manage a given situation [87] and makes the system more adaptive in a change scenario.

In addition, some authors suggest that smart systems use “smart computing technologies to make the critical infrastructure components and services of a city—which include city administration, education, healthcare, public safety, real estate, transportation, and utilities—more intelligent, interconnected, and efficient” [85]. Smart computing refers to a “new generation of integrated hardware, software, and network technologies that provide IT systems with real-time awareness of the real world and advanced analytics to help people make more intelligent decisions about alternative actions and that will optimize business processes and business balance sheet results” [85].

2.1.3 Smart systems are autonomous

Smart systems are autonomous systems that employ modern software engineering technology such as continuous deployment, data-driven engineering, continuous feedback on their own behavior, shared learning of more and less effective behaviors as well as continuous evolution of functionality and performance [8]. By means of these technologies and operations, they become aware of their own capabilities and limitations, leading to long-term autonomy requiring minimal or no human operator intervention [54]. Some examples of such a system are robotic platforms and networked systems that combine computing, sensing, communication, and actuation [54]. In the large complex systems such a critical infrastructures, autonomous characteristic is becoming a precondition for optimally managing the behavior of a large number of components [63]. For example, new smart grids require precisely autonomous operations to manage hundreds or even thousands of small energy producers as well as regulate innumerable battery storage devices and energy consumers (e.g. cold storage facilities) in order to use them as buffers [63].

2.2 What is a smart critical infrastructure in SmartResilience project?

Based on the literature research about the characteristics of smart systems, the definition of smart critical infrastructure is derived. In SmartResilience project, Smart Critical Infrastructure is a critical infrastructure [27], which is efficient and able to maximize the service it provides by the use of intelligent systems, such as IoT, artificial intelligence, sensors, actuators and smart computing within an integrative and interconnected network [12] [86] [32]. SCIs are also self-sufficient adaptive intelligent technical systems with advanced functionality, enabled by underlying micro-nano-systems and other components [73]. Thereby, these SCIs shall help deliver improved participative governance and a vision for sustainable and resilient future [5].

2.3 Types of smart and new technologies

The strategic research agenda (SRA) by EPoSS [25] provides a comprehensive overview of the current and future prospects of underlying smart technologies used in Europe within various sectors such as energy, aerospace, health, transport, etc. It recognizes the link between the smart systems and their application in different sectors. The underlying technologies in SRA are taken as a base for developing the link between the smartness characteristics and technologies applicable to the CIs in SmartResilience project.

An adapted list of characteristics and type of (underlying) smart and new technologies is presented in Table 2. Incorporation of these type of technologies into the modern critical infrastructure makes them smarter in normal operation and use: more adaptive and more intelligent [25] [73].
Table 2: Technologies in smart systems adapted from EPoSS SRA [86]

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Type of smart technology</th>
<th>Brief description</th>
<th>Smartness characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Artificial intelligence</td>
<td>The goal of artificial intelligence as a science is to make machines do things that would require intelligence if done by human [7] e. g. reduced operator distraction and error [86], or optimization of vehicle control, navigation and logistics [86]. It can also autonomously or through networking, safeguard and optimize every aspect of the critical chain [87], and it is able to sense, diagnose, describe, qualify and manage a given situation [87]. Artificial intelligence is not one technology but rather a group of related technologies – including natural language processing (improving interactions between computers and human or “natural” languages); machine learning (computer programs that can “learn” when exposed to new data) and expert systems (software programmed to provide advice) – that help machines sense, comprehend and act in ways similar to the human brain.</td>
<td>Intelligent</td>
</tr>
<tr>
<td>2.</td>
<td>Integrated systems</td>
<td>Smart systems integrate all the systems into one and centralize the operations. These systems help in efficient monitoring and control of the operations.</td>
<td>Integrative and Interconnected</td>
</tr>
<tr>
<td>3.</td>
<td>Big/Open data producing</td>
<td>Smart systems are informed by the effective use of data assets to secure better outcomes. They invest in system-wide data (big and open) capture, integration and analytics capabilities. Open data supports their commitments to transparency and innovation [67].</td>
<td>Integrative and Interconnected; Intelligent</td>
</tr>
<tr>
<td>5.</td>
<td>Semiconductors &amp; More than Moore (MtM) technologies</td>
<td>More than Moore (MtM) technologies add functions to normal semiconductor chips. These advances can allow chips, for example, to communicate through wireless connection or work directly with magnetics and fluids</td>
<td>Intelligent</td>
</tr>
<tr>
<td>6.</td>
<td>Micro-sensors, micro-actuators</td>
<td>Micro-sensors gather data and micro-actuators and convert energy into motion [86]. They are enabled by Micro-Electro-Mechanical Systems (MEMS)¹, Micro-Opto-Electro-Mechanical Systems (MOEMS)², and Microfluidics ³</td>
<td>Intelligent; Autonomous</td>
</tr>
</tbody>
</table>

¹ MEMS (Micro-Electro-Mechanical Systems) expand silicon technology by incorporating sensors and mechanical movement [50]. The term MEMS has come to describe any tiny machine, but the more precise definition is that a MEMS is a device that combines sensing, actuating and computing [2]. MEMS are also referred to as micro-machines or micro systems technology (MST) in Europe. MEMS devices generally range in size from 20 micrometers to a millimeter (i.e. 0.02 to 1.0 mm). MEMS fabrication allows micro-sensors, which gather data, and micro-actuators, which convert energy into motion, to integrate on the same substrate [27].

² MOEMS enhance the MEMS concept to include light sources and optical components [50]. Their small size, low cost, low power consumption, mechanical durability, high accuracy, high switching make them a perfect solution to the problems of the control and switching of optical signals in telephone networks [38].

³ Microfluidics expands MEMS to the control and analysis of fluids [50]. MEMS has many applications in microfluidics with many of the key building blocks such as flow channels, pumps and valves fabricated using mature micromachining techniques. Chemical analysis, drug delivery, biological sensing, environmental monitoring and many other applications typically incorporate MEMS microfluidic devices. It should be noted that in MEMS fluidic devices the type of flow (laminar or turbulent), effect of bubbles, capillary forces, fluidic resistance and capacitance all have an effect on their final design [38].
<table>
<thead>
<tr>
<th>Nr.</th>
<th>Type of smart technology</th>
<th>Brief description</th>
<th>Smartness characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Combinational sensing</td>
<td>Human skin is a good example of combinational sensing, as it combines sensitivities to heat and pressure (touch). Combinational sensing provides similar, engineered, solutions in two ways: (1) combining discrete sensors or (2) using one sensor structure to measure several things.</td>
<td>Integrative &amp; interconnected; Intelligent</td>
</tr>
<tr>
<td>8.</td>
<td>Multifunctional materials</td>
<td>Multifunctional materials can combine structure with a further function or functions.</td>
<td>Intelligent</td>
</tr>
<tr>
<td>9.</td>
<td>Energy management &amp; scavenging</td>
<td>Energy management &amp; Scavenging technologies allow smart systems to make the most efficient use of resources and to gain their operating power from their surroundings.</td>
<td>Integrative &amp; interconnected; Intelligent</td>
</tr>
<tr>
<td>10.</td>
<td>Opto/organic/bio data processing</td>
<td>Memory and data processing in electronic computers is now routine. But new ways of data processing, using processes which “bio-mimic” the brain are also emerging.</td>
<td>Intelligent</td>
</tr>
<tr>
<td>11.</td>
<td>Machine cognition &amp; Human Machine Interfaces (HMIs)</td>
<td>As systems increase in complexity, human limits may constrain their use. Advances in HMIs will relieve this situation, and devices that better “understand” the user will provide major advantages in ease and accuracy of operation.</td>
<td>Integrative &amp; interconnected; Intelligent</td>
</tr>
</tbody>
</table>
### 2.4 Specific smart and new technologies

Based on the literature review, Table 3 provides a list of specific smart technologies under each type of technology identified in Chapter 2.3 that could be relevant for each one of the case studies in the SmartResilience project.

<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>ALFA</th>
<th>BRAVO</th>
<th>CHARLIE</th>
<th>DELTA</th>
<th>ECHO</th>
<th>FOXTROT</th>
<th>GOLF</th>
<th>HOTEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artificial intelligence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Virtual agents⁴ [13]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Identity analytics⁵ [13]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Recommendation systems⁶ [13]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Chatbots ⁷ [60]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Robo-advisors⁸, [60] [13] [41]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Machine learning, Cognitive computing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Smart wallets⁹</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Insurance underwriting AI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Supportive devices (e.g. assistive robots) [24]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Chatbot technology with artificial intelligence [78]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Machine-learning techniques [11] [62]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Prognostic algorithms to estimate useful lifetime of a battery pack or unit [62]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Building automation systems [1]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• AI driven optimal power flow [69]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Process visualization and simulation [16]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Machine learning [15]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Advanced algorithms [12] [15]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Predictive control models [13] [16]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• AI – Driven Emergency Response System [14] [57]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• AI system to optimize generation of power, heat and cooling adapted to market and weather forecasting [77]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

⁴ Computer-generated, animated characters serving as online customer service representatives.
⁵ Solutions combining big data and advanced analytics to help manage user access and certification.
⁶ Algorithms helping match users and providers of goods and services.
⁷ Chatbots are used by banks to improve customer experience. These software programs use messaging as an interface through which companies can help their customers answer questions, find information and offer personalization.
⁸ In wealth management space, Robo-advisors provide substantive advice and recommendations based on a person’s portfolio, risk tolerance and previous actions.
⁹ Smart wallets monitor and learn users’ habits and needs and alert and coach users, when appropriate, to show restraint and to alter their personal finance spending and saving behaviors.
### SmartResilience: Indicators for Smart Critical Infrastructures

#### Table: Type of smart technology

<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>ALFA</th>
<th>BRAVO</th>
<th>CHARLIE</th>
<th>DELTA</th>
<th>ECHO</th>
<th>FOXTROT</th>
<th>GOLF</th>
<th>HOTEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>systems [66]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Block chain(^{10})</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Electronic payment systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Grid edge technologies (^{16}) [89]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Rooftop solar tiles and building integrated photovoltaics (BIPV) [89]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Smart substation automation system (^{17}) [69]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Integrated Substation Condition Monitoring (ISCM) (^{18}) [69]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Health &amp; information systems [24]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Crisis control center</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Automated fire safety system [42]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Energy harvesting system (^{13}) [90]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SCADA systems for baggage handling [23]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• RFID enabled(^{20}) [58]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Virtual service providers(^{21}) [30]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• On-line integrated production optimization (^{22}) [91]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Supply chain management solution (software) [16]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Smart energy management software(^{23}) [16]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SCADA system(^{24}) [64]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Water treatment systems(^{25}) [64]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Immobilized Micro-organism Treatment System(^{26}) [64]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Membrane bioreactor system(^{27}) [64]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Water distribution control systems [64]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Flood forecasting system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Monitoring of rotating assets e.g. in turbines (^{28}) [72]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Smart Energy Buildings to improve efficiency and reduce costs (^{71})</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Smart Meters [9]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Meter Failure Monitor(^{29}) [47]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

\(^{11}\) Machine-learning techniques to model the behavior of individual devices and battery storage units by reviewing data from smart meters and sensors.

\(^{12}\) Advanced algorithms analyze data such as economic conditions and weather patterns to forecast demand.

\(^{13}\) Model predictive control is an advanced multivariable control technique based on nonlinear programming that has been implemented in refineries and petrochemicals manufacturing.

\(^{14}\) An Artificial Intelligence algorithm monitor all the incoming customer communication via Twitter, Facebook, online chats and identify whether they relate to some critical emergency (like fire, faulty equipment, crime). Once identified as an emergency case, the system figures out which department and location (e.g. safety department) are best equipped to handle the situation and automatically push the customer complaint to mobile phones of all the relevant stakeholders. By getting the first-hand information directly from the customer and facilitating quick communication, response to the emergency becomes effective.

\(^{15}\) Can act as a proxy streamflow data when a stream gauge fails. In addition, due to the machine learning capabilities, it can even make estimates of stream levels where there is no actual stream gauge present. It could be useful for predictive stream flow in areas vulnerable to flooding events.

\(^{16}\) Block-chains are shared, tamperproof, peer-to-peer digital ledgers that enable a single, global version of transaction truth.

\(^{17}\) Using grid edge technologies and services, customers will produce, consume, store, and sell electricity.

\(^{18}\) The automated substation for Smart Grids must integrate all aspects of intelligence, from protection, automation and remote control to operational safety and advanced data collection.

\(^{19}\) ISCM is a modular system for monitoring all relevant substation components, from the transformer and switchgear to the overhead line and cable. Based on known, proven tele-control units and substation automation devices, ISCM provides a comprehensive solution perfectly suited to substation environments. It integrates seamlessly into the communication infrastructure so that monitoring information from the station and the control center is displayed.

\(^{20}\) Energy harvesting system by using piezoelectric materials, which can generate electric power subject to traffic loads, thunder vibrations.

\(^{21}\) RFID (radio-frequency identification) enabled smart airport – providing access to real-time location information of all objects and individuals.

---
## Type of smart technology

<table>
<thead>
<tr>
<th>ALFA</th>
<th>BRAVO</th>
<th>CHARLIE</th>
<th>DELTA</th>
<th>ECHO</th>
<th>FOXTROT</th>
<th>GOLF</th>
<th>HOTEL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Energy Management System (EMS) [69].</td>
<td>• Remote control and automation systems [89]</td>
<td>• CCTV (video surveillance) with recognition/authentication capabilities [24]</td>
<td>• Enhanced CCTV camera</td>
<td>• Risk based inspection software</td>
<td>• Smart Waste-Water Management system [31] [77]</td>
<td>• Cyber Security within Integrated Project Team [28]</td>
<td>• Smart Grid [32] [74]</td>
</tr>
<tr>
<td>• Voltage Stability Analysis application</td>
<td>• Optimization and aggregation platforms, smart appliances and devices, IoT [89]</td>
<td>• IoT Gateways which further analyze data collected by</td>
<td>• Digital boarding [23]</td>
<td>• Computerized Maintenance Management Software (CMMS)</td>
<td>• Smart Grid for Water [37]</td>
<td>• Smart Micro-grid [33] [74]</td>
<td></td>
</tr>
<tr>
<td>• Advanced distribution</td>
<td></td>
<td>• Hold baggage system [23]</td>
<td>• Biometric access control systems</td>
<td>• Distributed control system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Departure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

21 Virtual service providers (integrated value proposition for different customer segments throughout the airport, airport city, or airport city cluster)

22 It can be done by integrating MES, ERP, and a LIMS, flowsheet optimization, planning, and scheduling

23 Water distribution control systems seek to reduce power consumption and regulate the pressure distribution within each section of the water supply network to achieve a reliable water supply with fewer leaks

24 Supervisory control and data acquisition systems (SCADA) analyze real-time conditions, providing data for fast adjustments

25 Water treatment systems can be used to supply high-quality tap water by eliminating problems such as turbidity, bacteria, and salinity.

26 Immobilized Microorganism Treatment System is a processing system to remove some substances (e.g. nitrogen and phosphorous) that cannot be removed by simple processes. It is used in cases when action is required to prevent eutrophication of public waterways, or when the treated water is to be reutilized.

27 Membrane bioreactor system is used to remove suspended solids called “activated sludge,” which multiply by a biological reaction. It also can remove bacteria and other larger microbes to produce high-quality treated water.

28 Monitoring of rotors and bearings provides information about structural conditions and aging of infrastructure/equipment. This is an essential part of predictive maintenance.

29 Meter Failure Monitor is a technology to monitor where the power is out in its territory. By sending messages to the meters to see if they responded, the utility is able to locate where to send crews in the field or verify if power has been active. This avoids callback system, which requires staff to make phone calls to customers in order to determine whether the electricity is back on.

31 Smart Waste-Water Management System can be used reporting, monitoring and control of individual municipalities and on-ground workers through innovative web applications. Also can enable the cities to monitor waste transportation, provide MIS reports for waste collection and transportation and notify ULBs about vehicle breakdown and maintenance thereby ensuring a higher level of transparency in municipal administration.

32 The Smart Grid is expected to control the demand side as well as the generation side, so that the overall power system can be more efficiently and rationally operated.

33 Micro-grids controlled in this way have the features of connecting and adjusting to the main grid intelligently, showing and using the input and output status of batteries, and controlling power smoothly in an emergency (including isolating the micro-grid from the main grid if needed)
### Type of smart technology

<table>
<thead>
<tr>
<th>ALFA</th>
<th>BRAVO</th>
<th>CHARLIE</th>
<th>DELTA</th>
<th>ECHO</th>
<th>FOXTROT</th>
<th>GOLF</th>
<th>HOTEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>management systems integrates Distribution SCADA, Outage Management (OM), and Advanced Fault and Network Analysis on a software platform[^30] [69]. • General Packet Radio Service (GPRS)/Global System for Mobile Communications (GSM) modem, fiber optic devices and send them to a data center or the cloud [24] • Alarm and emergency communication applications for mobile devices [24] • Closed circuit security system [24] • Smart firewalls [24] control system [23] • Smart Facility management system [23] • Automated Passenger Information System [42] • Lock doors of Automated Border Gates [42] • Near field communication (NFC) [23] • Automatic Dependent Surveillance – Broadcast (ADS-B) system to transmit their positions based on on-board navigational instruments and global position system (GPS) technology [23] (DCS) • Assets condition based monitoring [11]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[^30]: Distribution SCADA, Outage Management, and Advanced Fault and Network Analysis integrated enables the user to monitor, control and optimize the secure operation of the network and efficiently manage day-to-day maintenance efforts while guiding operators during critical periods.
<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>ALFA</th>
<th>BRAVO</th>
<th>CHARLIE</th>
<th>DELTA</th>
<th>ECHO</th>
<th>FOXTROT</th>
<th>GOLF</th>
<th>HOTEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miniaturized: Micro-Nano-Bio Systems (MNBS)</td>
<td>-</td>
<td>-</td>
<td>Miniature camera for surveillance with nano-materials</td>
<td>-</td>
<td>Micro-bots 37 that remove disease-causing bacteria from water [84]</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>MEMS, MOEMS, Microfluidics</td>
<td>-</td>
<td>-</td>
<td>MEMS sensor for runway temperature monitoring that measures and</td>
<td>-</td>
<td>Microfluidics used for flow sensors, flow channels, valves,</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

34 Communication analytics data can be used to analyze the communication before, during and after an event.
35 Big Data for Dynamic Energy Management in Smart Grids is used to optimize the operation of Smart Grids.
36 Using intelligent sensors and information from employee and passenger reports about service and equipment. For example, an automated wheel-measuring machine built into the track at the tram depot detects the condition of a tram’s wheel when it rolls over it.
37 A micro-robot is a miniaturized, sophisticated machine designed to perform a specific task or tasks repeatedly and with precision.
<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>ALFA</th>
<th>BRAVO</th>
<th>CHARLIE</th>
<th>DELTA</th>
<th>ECHO</th>
<th>FOXTROT</th>
<th>GOLF</th>
<th>HOTEL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Micro-sensors, micro-actuators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Smart grids**, **Micro grids**, **Smart metering**, **Intelligent control system**
- Wireless multi-sensor networks ready for independent operation (e.g., by energy harvesting and/or low power sensors, especially chemical sensors)
- Intelligent Alarm Processors (IAPs) 38

- **Identification systems items such as tags, bracelets, labels and smart badges (e.g. ultrasound-enabled)** [24]
- **Biometric scanners** [24]
- **RFID systems with location services (software components) to assess and monitor relative movement of assets/patients/staff etc.** [24]
- **Barcode or Quick Response (QR) code reading**
- **Pattern or face recognition sensors combined with IoT**
- **Fire & smoke detectors** [42]
- **Automated Border Gate Kiosk** [42]
- **Proxy and biometric readers** [42]
- **Built-in hardware security features and access routines (bio-authentication features)**
- **Wireless multi-sensor networks, ready for independent operation (e.g., by energy harvesting and/or low power sensors, especially chemical sensors)** [25]
- **Wireless vibration sensors on essential pumps to monitor asset health** [22] [11]
- **Wireless networks and remote sensors** 39 [15].
- **Ultra-low power/cost sensors** 40 [81]
- **RFID tags** 41 [81]
- **Water sensors. e.g., for leakage status, rainfall and water level.** [65]
- **Ultrasonic sensors (water level)** 42 [65]
- **Smart Water Sensors to monitor water quality in rivers, lakes and the sea** [69]
- **Biosensors to detect water contamination** [55]
- **Bacteria-filled sensor for water monitoring** 43 [71]
- **Water level sensors**
- **Float level sensors. e.g., magnetic float sensors, air bubblers**
- **Radar level** 44 [65]
- **Aerial sensors** 45 e.g. drop disposable micro sensors
- **Visual sensing e.g. image based automated monitoring of flood formation**
- **Ultrasonic and infrared sensors based on ultrasonic range finding with remote temperature sensing**
- **Occupancy sensor to save energy in commercial buildings** [50]

---

38 Intelligent Alarm Processors (IAPs) reduce the critical time needed to analyze faults in the grid and take corrective action, as well as the risk of incorrect analysis.

39 Wireless networks and remote sensors that can collect and transmit data from a variety of measuring points are becoming increasingly common in the oilfield

40 Ultra-low power/cost sensors allow for data collection on different devices across the manufacturing supply chain

41 Radio-frequency identification (RFID) tags, that allow for tracking of manufacturing components across the supply chain
<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>ALFA</th>
<th>BRAVO</th>
<th>CHARLIE</th>
<th>DELTA</th>
<th>ECHO</th>
<th>FOXTROT</th>
<th>GOLF</th>
<th>HOTEL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>encryption, protection from unauthorized access, remote updates and patches, etc.) [25]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Combinational sensing</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>“Contactless” traveler clearance system (self-process through the border without the need to physically use a passport (contactless), entirely relying on facial recognition [72]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Machine cognition &amp; Human Machine Interfaces</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Augmented Vision Video panorama Human-Machine Interface for Remote Airport Tower Operation [65]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

42 When the water level decreases in the tank, the ultrasonic sensor detects this decrease and sends the reading to Arduino. Arduino alarm the user that there is a decrease in the tank.

43 The sensor is filled with bacteria that produce a small measurable current as they feed and grow. When disturbed by incoming toxins and pollutants, the electric current drops, alerting researchers to the presence of unwanted contaminants.

44 Radar level is mainly put into use for detection of level in continuous level measurement applications.

45 Aerial sensor is a device used to detect and track airborne or atmospheric vehicles.
Smart systems maturity model for critical infrastructure

The concept of smart maturity model is not a new and exclusive concept developed for SmartResilience project. The maturity levels provide a rigorous benchmark rating method that enables the comparison between one’s organization capability and its competitors. This maturity model has been extensively researched and developed for use in the smart cities field [17] [67] [38] [6]. For example, the Scottish government has developed a smart cities maturity model [67], which can be used to assess the smartness level of the city [67]. Also, the International Organization for Standardization (ISO) have developing standards on smart community infrastructures, such as ISO/DIS 37153 on maturity model for assessment and improvement (currently under development) [93] and ISO/DIS 37154 on best practice guidelines for transportation [94]. In addition, SAE International provides and defines levels of driving automation, from no automation to full automation [97].

The incorporation of smart systems, such as smart devices, into the critical infrastructure functioning makes it a new technology to increase the artificial intelligence, making them more autonomous, improving its performance, and increasing its functionality [86]. This incorporation also involves the integration of systems and use of big and open data.

The new smart technologies are used to different extent in modern critical infrastructures, and these maturity levels can be further adapted to derive the level of smartness of the critical infrastructure case studies used in the SmartResilience project. The Smart Mature Resilience (SMR) project funded by the EU’s Horizon 2020 focused suggested five maturity stages to improve the resilience of European regions against natural and man-made hazards [92]. Based on this idea, a maturity model is proposed to assess the maturity levels of smart infrastructures in terms of their three primary characteristics, identified in Chapter 2: i) integrative and interconnected [12] [33] [86] [35] [4], ii) intelligent [12] [86] [32], and iii) autonomous [8] [54]. The maturity levels of a smart infrastructure are presented in Table 4, adapted from the smart cities [67] and smart grids [38] maturity models, as well as from SAE International levels of driving automation [97].
### Table 4: Maturity levels of smart critical infrastructures

<table>
<thead>
<tr>
<th>Characteristics for smartness</th>
<th>Level 0: Non-Existent</th>
<th>Level 1: Reactive</th>
<th>Level 2: Informed</th>
<th>Level 3: Managed</th>
<th>Level 4: Automated / Predictive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrative and Interconnected</td>
<td>The CI has no connectivity, and therefore is isolated from other CIs.</td>
<td>ICT architectures are used to integrate and interconnect specific operating assets/services within a CI.</td>
<td>The operating assets/services of a CI are integrated and interconnected through ICT architectures.</td>
<td>Some CIs are integrated and interconnected through ICT architectures.</td>
<td>CIs are completely integrated and interconnected, and therefore decision makers can optimize operations within the whole network of CIs.</td>
</tr>
<tr>
<td>Intelligent</td>
<td>The CI has no intelligence, and therefore has just analog processes in place.</td>
<td>The CI’s intelligence is based on simple data collection for specific purposes.</td>
<td>The CI is continuously monitored with intelligent information to support operational decisions.</td>
<td>The CI is intelligent to some extent, as it uses the collected information to automatically improve its operational performance.</td>
<td>The CI is fully intelligent, using data analytics for automated predictive and preventative operational decisions, and real-time response capabilities for non-predictable events.</td>
</tr>
<tr>
<td>Autonomous</td>
<td>The CI has no autonomy, and therefore has just manual processes in place.</td>
<td>The CI’s autonomy is based on simple control system, which includes sensing and/or actuation.</td>
<td>The whole CI is autonomous, but not 100% reliable. Thus, some human intervention is required, while it is learning from the surrounding environment.</td>
<td>The CI is autonomous and completely reliable in specific situations, while in others still requires human intervention.</td>
<td>CIs have full autonomy requiring minimal or no human intervention.</td>
</tr>
</tbody>
</table>
3.1 Example of Smart maturity model for Airports

This section provides an application of the smartness maturity model to an airport (see Figure 3). This example was prepared in collaboration with partners from the DELTA (“Airport”) case study, which looks into the transportation infrastructure of Budapest airport. According to the information provided by this partner, the Budapest airport can be classified as a smart infrastructure of level 2. The Budapest airport integrates sensors for signal acquisition, elements transmitting information to the ‘Command and Control’ unit that takes decisions and provide instructions based on available information, components transmitting decisions and instructions, as well as actuators that perform or trigger the required actions.

![Figure 3: Example of the smartness maturity model applied to the DELTA case [42].](image)

3.2 Application of the proposed maturity model

Based on the specific smart and new technologies checked and validated for the SmartResilience cases from Table 7 to Table 14, this section assesses the smartness level of the cases in the project.

<table>
<thead>
<tr>
<th>No</th>
<th>Cases</th>
<th>Level</th>
<th>Description from the cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>ALPHA</td>
<td>Level 3: Managed</td>
<td>“Complement live customer service agents by answering simple, easily addressed queries, with some cognitive systems learning over time”. This shows an autonomy level 3. “Virtual agents (e.g. Luvo) are used in banking and complement service agents by answering simple, easily-addressed queries. Some cognitive systems learn over time”, which demonstrates an intelligence level 3.</td>
</tr>
<tr>
<td>2.</td>
<td>BRAVO</td>
<td>Level 2: Informed</td>
<td>“Smart substation automation system is partly used”, which shows an autonomy level 2. “Smart metering are used in some regions in Heidelberg, full rollout initiated”, which shows an intelligence level 2.</td>
</tr>
<tr>
<td>No</td>
<td>Cases</td>
<td>Level</td>
<td>Description from the cases</td>
</tr>
<tr>
<td>----</td>
<td>-------</td>
<td>-----------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>3</td>
<td>CHARLIE</td>
<td>Level 3: Managed</td>
<td>“Databases are used that integrate data from many different sources in the healthcare system, including all relevant inpatient and outpatient care settings”. “Public Transport data is used to assess accessibility of medical services”. These examples show an integration and interconnectedness level 3.</td>
</tr>
<tr>
<td>4</td>
<td>DELTA</td>
<td>Level 2: Informed</td>
<td>“The center plays the role of background supervisor and game master for the drill.” “RFID tags will be used to track actors” “CCTV camera footage will be software processed to track actors.” These examples demonstrate an intelligence level 2.</td>
</tr>
<tr>
<td>5</td>
<td>ECHO</td>
<td>Level 2: Informed</td>
<td>“CMMS is used to plan, conduct and analyze maintenance processes.” This shows an intelligence level 2. “Distributed controlled systems are used to control of operative production processes”. This shows an autonomy level 2.</td>
</tr>
<tr>
<td>6</td>
<td>FOXTROT</td>
<td>Level 3: Managed</td>
<td>“The smart grid for water is used to measure use of water and also predict future demands” This exemplifies an intelligence level 3. “Big data from public health web services is used to get early warning if the water treatment or the distribution network has been contaminated” This demonstrates an integration and interconnectedness level 3.</td>
</tr>
<tr>
<td>7</td>
<td>GOLF</td>
<td>Level 3: Managed</td>
<td>“FEWS provide an open data-handling platform for managing hydrological forecasting processes and warning systems. Flow into Carrigadrohid is predicted by FEWS from a hierarchy of rainfall sources. Every forecast uses: observed data where it is available (from the start of the simulation up to time now); Met Eireann’s Harmonie data for the first 4 hours into the future”. “RPS utilizes the previously developed MIKE21 storm surge model to generate storm surge forecasts from October to April for various locations around the Irish coast. RPS have automated the process whereby Met data pertaining to wind and atmospheric pressure is downloaded daily from the Met Eireann FTP (File Transfer Protocol) site and used to inform the storm surge forecasting model. The model is run daily from October to April and once post processing is completed the forecast data is uploaded to a designated secure website which is only accessed by OPW and other restricted organizations. The OPW then make a decision based on the predicted tidal levels on whether to issue a flood warning”. These examples display an intelligence level 3.</td>
</tr>
<tr>
<td>8</td>
<td>HOTEL</td>
<td>Level 2: Informed</td>
<td>“Analytics is used optimize generation of power, heating and cooling, adapting to market and weather forecasting”. “Smart grid is used to measure demand in power, heating and cooling systems and to predict future demand (combined with weather forecasting). These examples show an intelligence level 2.</td>
</tr>
</tbody>
</table>
4 Current and emerging challenges of new smart technologies on SCIs

4.1 Literature review of current challenges

With the increasing introduction of smart new technologies into the market, ("emerging") risks also increase [18] [23] [26] [28] [49] [61] [82]. A review of the literature including scientific literature and projects related to resilience of the CIs was conducted to understand the challenges related to new and smart technologies on the resilience of the CIs. These challenges are summarized in this chapter. These are broadly:

1. Vulnerability due to interconnectedness [23] [82]
2. Vulnerability due to centralization [49] [82]
3. Individual Privacy [26]
4. Governance related challenges [61]
5. Inconsistent Adoption [28] [82]
6. Increased Automation [82]

4.1.1 Vulnerability due to interconnectedness

Some of the characteristics of the smart systems pose challenges for the resilience of the CIs. One such character is interconnectedness of the system. According to the USDHS, the integrated cyber-physical infrastructure in cities create environmental and economic efficiency while improving the overall quality of life [82]. For example, interconnected transport systems are assisted with the smart devices through smart communication systems or through wired and wireless connections. This interconnectedness on one side removes the barriers between the cyber and physical infrastructures, and on the other hand, expands the potential attack surface [82]. For example, in case of civil aviation, "Cyber security is an issue because many civil aviation organizations rely on electronic systems for critical parts of their operations, and for many organizations their electronic systems have safety-critical functions" [23]. If these systems are face a cyber-attack due to their interconnectedness, the safety critical functions of civil aviation can be potentially impacted.

The risks related to the interconnectedness constantly change as new threats and vulnerabilities surface along with ever-changing technology implementations [23]. Hacking of connected objects is a common example. With the Internet of Things, all kinds of machines become connected to the Internet and the role of humans diminishes, even to the point they are removed from the equation. This will generate huge increases in productivity. The dark side is that these connected objects are vulnerable to hacking. For many objects connected with internet, the risks associated with becoming hacked are limited. However, as the objects within the smart CIs become connected, their risk surface to threat such as hacking increases tremendously. Cybercriminals spy on the security gaps in IT of smart CI to manipulate them. Hacking the control system of planes, energy plants, self-driving cars, surveillance cameras and many other connected machines can disrupt vital systems. This may have impact far beyond the type of hacking resulting in embarrassing privacy leaks, as real threat to life. Hence, the adoption and increased reliance on smart technologies such as IoT may be done for example for surveillance and safety purpose, but in parallel may create or increase challenges for the smart CIs’ resilience by making them more vulnerable [82].

In addition, to the physical incidents creating physical consequences, exploited cyber vulnerabilities can result in physical consequences as well [82]. Moreover, potential consequences for the new smart technologies are still unknown [82]. This introduces uncertainty in terms of the potential impact. Furthermore, ambiguity increases with the increase in smartness, meaning that one does not know which
vulnerable system will be attacked and how. In such CIs, cyber security has a major stake in providing safety [23]. The challenge becomes bigger as the safety does not integrate security, and especially cyber security is not well integrated in organizations [23].

4.1.2 Vulnerability due to centralization
Marchese and Linkov [49] argue that the smart systems have a “pyramid-like structure with centralized information processing” to ensure performance efficiency and fast operations, as can be seen in Figure 4.

![Centralization of information processing in smart systems](image)

Data is aggregated within a central operating node (e.g. a sensor network reporting the events in an industrial plant) which then signal the operators for action, thereby increasing the dependency on one node. The centralization of data may have a larger impact of an event compared to a system, which is designed for resilience with layers of “redundancy and modularity” [49]. Coupled with the inherent level of automation and controllability of systems makes vulnerabilities particularly dangerous if a malicious actor can exploit them [82], meaning that if the attack is targeted at those central and autonomous nodes, it may lead to the complete inoperability of critical functions [49].

4.1.3 Compromise of individual privacy
Furthermore, according to the EU CRISP (Evaluation and Certification Schemes for Security Products) project, social aspect such as the rights and freedoms of the individuals may be compromised to ensure the safety and security goals by means of smart systems [26]. For example, increased collection of video surveillance cameras nowadays detects and recognizes individuals, relate the images to other databases and uniquely identifies a person. These systems are in extensive use in most public areas in EU countries, public means of transport, CIs, hospitals, private houses, and aerial vehicles such as drones. The collection and processing of all this data has significant impact on the privacy and personal data protection. Such surveillance can erode social freedoms and public goods such as privacy, to ensure precautionary or mitigation measures of an unknown event to avoid damage to people, public goods and service, etc. [26].
4.1.4 Governance related challenges

Governance related challenges are associated with implementation the rules, processes, practices, norms and actions. The smart systems are complex in nature, while a user such as a policy maker or CI operator seeks simplicity of information in the decision making process. This leads to a gap in understanding a complex system, thereby creating a hurdle in decision-making.

Moreover, on one side the use of smart systems suggests enhancing the participation of the stakeholders and on the other side, different governance related challenges arise such as compliance issues, complexity in understanding the system, uncertainty and ambiguity [61], see Figure 5.

The fast pace of research and development in smart and new technologies provides very miniscule amount of time for the policy area to develop. Even the standardization field is crippled to deal with this fast-paced development. The direct implication of this is that there are not many laws and standards that these new technologies need to comply with. Also these smart systems can be easily tampered to deceive the law makers.

In addition, the information availability about these complex systems is limited, leading to increase in the possibly of unknown and uncertain situations.

Furthermore, governance related challenges could stem from lack of cross-sectoral cooperation. Cross-sectoral cooperation is the basis for a smart integrated system and as highlighted in previous research, smart CIs are interdependent on each other [12] [33] [86] [35] [4]. Lack of cross-sector cooperation rejects the purpose of these systems leading to large scale CIs operating in silos. Similar is the case with lack of inter-departmental cooperation within a large CI. Furthermore, the lack of vision for IT teams within the CIs could lead to secluded approaches to managing cyber-risks while it should be a crosscutting theme across all operating functions in a smart CI.

4.1.5 Inconsistent Adoption

Evolution of smart CIs occurs at different rates due to factors such as resource availability, needs and preference of users (e.g. utility operators’ use of smart technologies), or scale and accessibility (e.g. size of the airport, transport systems, water distribution system, etc.) [82]. The inconsistency in the use of new and
smart technologies within the SCIs pose new security challenge (e.g. cyber security) for its operators, industry and other stakeholders. Further, merging the new technologies in the old legacy systems, unknown aspects or blind-spots may remain where older legacy systems are dominant making it difficult for the new technologies to report the operational status, problems or efficiency opportunities [82]. In a transportation system for instance, the legacy systems may have security controls typically focused on the simple necessity of reducing the risk of physical product tampering or theft. However, the security and threat environment within intelligent transport system (ITS) is beginning to shift towards connected transportation systems as they become increasingly interconnected to the wider world [28]. Further, as ITS systems become universal, they will involve a significant number of devices and components over a large area, all requiring regular maintenance and upgrades. The cities with budget constraints may not have the staff or resources to cope up with the maintenance activities to ensure a secured ITS [28].

4.1.6 Increased automation
With the increased automation in the cyber-physical infrastructures, the control of the systems shifts from people to algorithms-based systems. On one side, this transition introduces a “level of security and resilience into the system by mitigation any potential human errors” [82], on the other hand, it potentially presents new safety, security and resilience related challenges, such as

- “Increasing the number of system access points and, therefore, potential attack vectors” for example, in a transportation systems, “automation that comes with autonomous vehicles that requires the use of a wide variety of sensors, including light detection and ranging (LIDAR), GPS, radar, and video cameras, all of which add potential vulnerabilities and attack vectors to autonomous vehicles” [82].
- Weakening of human skills [82];
- “Loss of visibility into all parts of a system” [82];
- “Cascading failures; necessary changes in emergency response plans (e.g., humans will not be present in areas of the system they once were)” [82];
- “Unanticipated permutations of automated functioning” [82]; or
- “Unintentional elimination of manual overrides” [82].

4.2 Emerging challenges related to the new technologies and smartness
Besides the current challenges present in chapter 4.1, the CWA 16649 standard – Managing emerging technology related-risks identifies challenges (basis the International Risk Governance Council – IRGC factors, see Table 6) related to the implementation of new technologies [18]. These are also relevant for the technology empowered with smart devices and systems since they can possibly bring new and unknown risks to the critical infrastructures. Hence, the related emerging risks (ERs) related to smartness are extremely important for the smart CIs. These challenges are supplemented with others found in literature [98].

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Challenge</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Scientific unknowns</td>
<td>Dealing with emerging risks requires dealing with scientific unknowns. These unknowns, can be tractable or intractable, and contribute to risks by being, e.g. unanticipated, unnoticed, and over- or underestimated.</td>
</tr>
<tr>
<td>2</td>
<td>Loss of safety margins</td>
<td>The level of connectivity in many social and technical systems is greater than in the past and the interconnections are increasing. The pace at which these systems operate is becoming faster and many are operating under higher levels of stress. This can lead to tight-coupling of components within systems and to loss of safety margins - a loss of slack or buffering capacity that leaves systems more vulnerable to disruption and thus increases the likelihood that new risks will emerge.</td>
</tr>
<tr>
<td>Nr.</td>
<td>Challenge</td>
<td>Description</td>
</tr>
<tr>
<td>-----</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>3</td>
<td>Positive feedback</td>
<td>Systems exhibiting positive feedback react by amplifying a change or perturbation that affects them. Positive feedback tends to be destabilizing and can amplify the likelihood or consequences of an emerging risk.</td>
</tr>
<tr>
<td>4</td>
<td>Varying susceptibilities to risk</td>
<td>The consequences of an emerging risk may be different from one context (situation/system/population) to another. Geography, genetics, experience and wealth are just some of the possible contextual differences that create varying susceptibilities to risk.</td>
</tr>
<tr>
<td>5</td>
<td>Conflicts about interests, values and science</td>
<td>Public debates about emerging risks seldom witness a clear separation between science, values, and interests. The conflicts that result have the potential to contribute to fertile ground for risk emergence or amplification. For e.g. emerging risks may be amplified when efforts to assess them and take early management measures encounter opposition on the grounds of contested science or incompatible values.</td>
</tr>
<tr>
<td>6</td>
<td>Social dynamics</td>
<td>Social change can lead to potential harm, or it can attenuate it. It is therefore important for risk managers to identify, analyze and understand changing social dynamics.</td>
</tr>
<tr>
<td>7</td>
<td>Technological advances</td>
<td>Risk may emerge when technological change is not accompanied by appropriate prior scientific investigations or post-release surveillance of the resulting public health, economic, ecological and societal impacts. Risks are further exacerbated when economic, policy or regulatory frameworks (institutions, structures and processes) are insufficient, yet technological innovation may be unduly retarded if such frameworks are overly stringent.</td>
</tr>
<tr>
<td>8</td>
<td>Temporal complications</td>
<td>A risk may emerge or be amplified if its time course makes detection difficult (e.g., the adverse effects of the risk only become evident after a long period of time) or if the time course does not align with the time horizons of concern to analysts, managers and policymakers.</td>
</tr>
<tr>
<td>9</td>
<td>Communication and information asymmetries</td>
<td>Risks may be complicated or amplified by untimely, incomplete, misleading or absent communication. Effective communication that is open and frank can help to build trust. In many cases, such communication can attenuate, or lead to better anticipation and management of, emerging risks. Information asymmetries fall under the umbrella of communication related challenges and occur when some stakeholders hold key information about a risk that is not available to others. These asymmetries may be created intentionally or accidentally. In some cases, the maintenance of asymmetries can reduce risk, but in others, it can be the source of risk or the amplification of risk by creating mistrust and fostering non-cooperative behaviors.</td>
</tr>
<tr>
<td>10</td>
<td>Perverse incentives</td>
<td>Perverse incentives are those that induce counterproductive or undesirable behaviors, which lead to negative, unintended consequences. Such incentives may lead to the emergence of risks, either by fostering overly risk-prone behaviors or by discouraging risk prevention efforts.</td>
</tr>
<tr>
<td>11</td>
<td>Malicious motives and acts</td>
<td>Malicious motives give rise to emerging risks and therefore practitioners need to consider intentional as well as unintentional causes of risk. Malicious motives and acts are not new, but in a globalized world with highly interconnected infrastructures (e.g., trade agreements and information and communication systems) they can have much broader-reaching effects than in the past.</td>
</tr>
<tr>
<td>12</td>
<td>Safety of employees data at work</td>
<td>The safety and security of the employee data may be threatened in a company without even their knowledge. Cyber-crime can be manipulate the employees’ data from the outside due to a lack of data security. This can have an effect on their security functions and making the employees vulnerable to unknown risks.</td>
</tr>
</tbody>
</table>
5 Smart technologies and related challenges for SmartResilience case studies

The specific technologies identified in chapter 2.4, as well as the current and emerging challenges (see Chapter 4) related with the use of these technologies are checked by all case study partners. Table 7 to Table 14 lists the type of technologies employed, respective specific technologies used making the CIS’s smart, how they are used. In addition, these tables also specific resilience related challenges arising due to the use of the technologies in smart CIs.

5.1 ALPHA ("Financial System") - City of Edinburgh

The smart technologies and related challenges for the ALPHA case study, which portraits the case of a smart financial system critical infrastructure for the City of Edinburgh, are presented in Table 7.

<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>No.</th>
<th>Specific Smart technologies (from literature sources) also used in case study</th>
<th>If yes, how is it used?</th>
<th>Specific challenge related to the use of smart technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Artificial Intelligence</td>
<td>1</td>
<td>Virtual agents 46</td>
<td>● Complement live customer service agents by answering simple, easily addressed queries, with some cognitive systems learning over time.</td>
<td>● Vulnerabilities related to interconnectedness and diverting to another platform, ● Centralization due to systems integration</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Identity analytics 47</td>
<td>● Identity verification and access ● Customer behavior analysis and personalization ● Fraud detection ● Process efficiencies</td>
<td>● Vulnerabilities related to interconnectedness, centralization, ● Privacy, data governance and data security; ● There may also be inconsistencies and compliance issues due to a lack of regulatory frameworks around new technologies.</td>
</tr>
</tbody>
</table>

46 Computer-generated, animated characters serving as online customer service representatives.
47 Solutions combining big data and advanced analytics to help manage user access and certification
<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>No.</th>
<th>Specific Smart technologies (from literature sources) also used in case study</th>
<th>If yes, how is it used?</th>
<th>Specific challenge related to the use of smart technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommendation systems</td>
<td>3</td>
<td>• Customer behavior analysis and personalization • Process efficiencies</td>
<td></td>
<td>• Vulnerabilities related to centralization,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Privacy, data governance and data security;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• There may also be inconsistencies and compliance issues due to a lack of regulatory frameworks around new technologies.</td>
</tr>
<tr>
<td>Chatbot</td>
<td>4</td>
<td>• Virtual agents (e.g., Luvo) are used in banking and complement live customer service agents by answering simple, easily-addressed queries. Some cognitive systems learn over time.</td>
<td></td>
<td>• Vulnerabilities related to interconnectedness and diverting to another platform, interconnectedness and centralization due to systems integration;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• There may also be inconsistencies and compliance issues due to a lack of regulatory frameworks around new technologies.</td>
</tr>
<tr>
<td>Robo-advisors</td>
<td>5</td>
<td>• Online advice sites as replacement for F2F advice as low-cost, transparent option - for many financial entities this is under consideration • Personalized communications and advice • Algorithm-based wealth management • Compliance purposes</td>
<td></td>
<td>• Challenges are still being assessed, as this is a developing area in the financial sector.</td>
</tr>
</tbody>
</table>

48 Algorithms helping match users and providers of goods and services
49 Chatbots are used by banks to improve customer experience. These software programs use messaging as an interface through which companies can help their customers answer questions, find information and offer personalization.
50 In wealth management space, Robo-advisors provide substantive advice and recommendations based on a person’s portfolio, risk tolerance and previous actions.
<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>No.</th>
<th>Specific Smart technologies (from literature sources) also used in case study</th>
<th>If yes, how is it used?</th>
<th>Specific challenge related to the use of smart technologies</th>
</tr>
</thead>
</table>
| 6 Machine learning, Cognitive computing | 6 | • Customer modelling  
• Predictive analytics  
• Personalized customer interactions and solutions  
• Portfolio balancing to maximize profit  
• Compliance purposes | • Vulnerabilities related to interconnectedness, centralization  
• Privacy, data governance and data security  
• There may also be inconsistencies and compliance issues due to a lack of regulatory frameworks around new technologies. |
| 7 Smart wallets | 7 | • Payment methods via smart device-based payments, either at point of sale, using a QR code, an app or notification via another device (e.g., a laptop) | • Vulnerabilities related to interconnectedness, centralization,  
• Individual privacy, data governance and data security  
• There may also be inconsistencies and compliance issues due to a lack of regulatory frameworks around new technologies. |
| 8 Insurance underwriting AI systems | 8 | • Claims process  
• Fraud prevention  
• Process efficiency  
• Pattern identification  
• Profiling | • Vulnerabilities related to interconnectedness, centralization, integration,  
• Individual privacy, data governance and data security  
• There may also be inconsistencies and compliance issues due to a lack of regulatory frameworks around new technologies. |
| 9 Block chain | 9 | • Process efficiencies  
• Payment  
• Clearing  
• Settlement | • Vulnerabilities related to interconnectedness, centralization, integration of systems,  
• Individual privacy, data governance and data security  
• There may also be inconsistencies and compliance issues due to a lack of regulatory frameworks around new technologies  
• There are also vulnerabilities around business continuity. |
| 2. Integrated systems  
1 Electronic payment systems | 1 | • Transfer funds between individuals and entities | • Vulnerabilities related to interconnectedness, centralization  
• Data governance and security; there may also be issues of privacy |

51 Smart wallets monitor and learn users’ habits and needs and alert and coach users, when appropriate, to show restraint and to alter their personal finance spending and saving behaviors

52 Blockchain are shared, tamperproof, peer-to-peer digital ledgers that enable a single, global version of transaction truth.
<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>No.</th>
<th>Specific Smart technologies (from literature sources) also used in case study</th>
<th>If yes, how is it used?</th>
<th>Specific challenge related to the use of smart technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>Cloud solutions</td>
<td>Data storage, Business processes, Software testing</td>
<td>Vulnerabilities related to interconnectedness, Privacy, data governance and data security; There may also be risks due to a lack of transparency around accountability and host nations’ regulatory frameworks, particularly for core services.</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Data management and new generation analytics improve fraud detection and criminal activity</td>
<td>Fraud detection / prevention e.g., money laundering, Greater response capability / efficiency, Pattern identification, Risk simulations</td>
<td>Vulnerabilities related to interconnectedness, Centralization, privacy, data governance and data security; There may also be inconsistencies and compliance issues due to a lack of integrated regulatory frameworks and emerging challenges around new technologies, Loss of direct control over IT.</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Trading algorithms manage volumes of real-time data</td>
<td>Automated trading systems direct client access to the market</td>
<td>Vulnerabilities related to interconnectedness, Centralization, data governance and security; There may also be inconsistencies and compliance issues due to a lack of regulatory frameworks around new technologies. There is also a lack of suitable, robust risk management, control frameworks and scenario planning / stress testing for specific risks, specifically intraday market risks.</td>
</tr>
</tbody>
</table>

3. Big/Open Data producing technologies
5.2 **BRAVO (“The smart city”) – The future oriented and sustainable community**

The smart technologies and related challenges for the BRAVO case study, which portrays the case of a smart city critical infrastructure oriented for the future of sustainable community, are presented in Table 8.

<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>No.</th>
<th>Specific Smart technologies (from literature sources) also used in case study</th>
<th>How is it used?</th>
<th>Specific challenge related to the use of smart technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Integrated systems</td>
<td>1</td>
<td>Rooftop solar tiles and building integrated PV (BIPV)</td>
<td>Customer use/personal use</td>
<td>Inconsistency of power generation</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Smart substation automation system 53</td>
<td>Partly used</td>
<td>Vulnerability due to interconnectedness</td>
</tr>
<tr>
<td>2. ICT &amp; smart computing solutions</td>
<td>1</td>
<td>Optimization and aggregation platforms, smart appliances and devices, IoT</td>
<td>Smart Lighting in the Bahnstadt neighborhood</td>
<td>Vulnerability due to interconnectedness</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>GPRS-/GSM modem, fiber optic</td>
<td>Used throughout city</td>
<td>Inconsistent adoption</td>
</tr>
<tr>
<td>3. Micro-sensors, micro-actuators</td>
<td>1</td>
<td>Smart metering 54</td>
<td>Used in some regions in Heidelberg, full rollout initiated</td>
<td>Vulnerability due to interconnectedness</td>
</tr>
</tbody>
</table>

---

53 The automated substation for Smart Grids must integrate all aspects of intelligence, from protection, automation and remote control to operational safety and advanced data collection.

54 Intelligent control of power consumption using smart metering
5.3 CHARLIE ("Healthcare") – The Austrian health care system

The smart technologies and related challenges for the CHARLIE case study, which portrays the case of a healthcare critical infrastructure in Austria, are presented in Table 9.

### Table 9: Smart technologies and related challenges for CHARLIE case

<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>No.</th>
<th>Specific Smart technologies (from literature sources) also used in case study</th>
<th>If yes, how is it used?</th>
<th>Specific challenge related to the use of smart technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Artificial Intelligence</td>
<td>1</td>
<td>Data mining and network-based knowledge discovery</td>
<td>Used to derive resilience-related indicators for healthcare infrastructure based on large-scale datasets</td>
<td>Particularly relevant are vulnerabilities due to inconsistent adoption, increased automation. Relevant challenges also include interconnectedness, centralization, and governance related challenges</td>
</tr>
<tr>
<td>2. Integrated systems</td>
<td>1</td>
<td>Health &amp; information systems</td>
<td>Databases are used that integrate data from many different sources in the healthcare system, including all relevant inpatient and outpatient care settings</td>
<td>Particularly relevant are vulnerabilities due to inconsistent adoption, increased automation. Relevant challenges also include interconnectedness, centralization, and governance related challenges</td>
</tr>
<tr>
<td>3. Big/Open Data producing technologies</td>
<td>1</td>
<td>Medical claim data</td>
<td>Used in monitoring the flow of patients through the healthcare system with particular emphasis on care processes for emergency care</td>
<td>Particularly relevant are vulnerabilities due to interconnectedness, inconsistent adoption, increased automation. Relevant challenges also include centralization, and governance related challenges</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Public transport data</td>
<td>Used to assess accessibility of medical services.</td>
<td>Particularly relevant are vulnerabilities due to interconnectedness, inconsistent adoption, increased automation. Relevant challenges also include centralization, and governance related challenges</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Electronic medical records</td>
<td>Used in monitoring the flow of patients through the healthcare system with particular emphasis on care processes for emergency care</td>
<td>Particularly relevant are vulnerabilities due to interconnectedness, inconsistent adoption, increased automation. Relevant challenges also include centralization, and governance related challenges.</td>
</tr>
</tbody>
</table>
5.4 DELTA (“Airport”) – Transportation infrastructure of Budapest airport

The smart technologies and related challenges for the DELTA case study, which portraits the case of an airport critical infrastructure in Budapest, are presented in Table 10.

<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>No.</th>
<th>Specific Smart technologies (from literature sources) also used in case study</th>
<th>If yes, how is it used?</th>
<th>Specific challenge related to the use of smart technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Integrated systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Crisis control center</td>
<td>The center plays the role of background supervisor and game master for the drill.</td>
<td>Efficiency of communication, data acquisition and processing</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Automated fire safety system</td>
<td>The Cerberus system will be deactivated by a simulated cyberattack.</td>
<td>Increased vulnerability to cyberattacks.</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>RFID enabled 55</td>
<td>RFID tags will be used to track actors.</td>
<td>Range of detectors is low.</td>
</tr>
<tr>
<td>2. ICT &amp; smart computing solutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Enhanced CCTV camera</td>
<td>CCTV camera footage will be software processed to track actors.</td>
<td>Relatively low resolution of most cameras.</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Digital boarding</td>
<td>Only simulated to generate simulated passenger flow.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Departure control system</td>
<td>Only simulated to determine data indicator value.</td>
<td>No</td>
</tr>
<tr>
<td>3. Big/Open Data producing technologies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Cloud-based data and application services</td>
<td>Communication among actors will be recorded into a cloud and analyzed.</td>
<td>Number of messages, providing network uplink.</td>
</tr>
<tr>
<td>4. Micro-sensors, micro-actuators</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>BAR- or QR code reading</td>
<td>For tracking actors during the drill.</td>
<td>Damaged code or broken reader.</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Fire &amp; smoke detectors</td>
<td>Only simulated, to trigger evacuation events.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Proxy and biometric readers</td>
<td>See RFID</td>
<td></td>
</tr>
</tbody>
</table>

55 RFID (radio-frequency identification) enabled smart airport – providing access to real-time location information of all objects and individuals
5.5 **ECHO (Refinery) - NIS oil refinery-industrial plant in Serbia**

The smart technologies and related challenges for the ECHO case study, which portrays the case of a refinery critical infrastructure of the NIS oil refinery-industrial plant in Serbia, are presented in Table 11.

<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>No.</th>
<th>Specific Smart technologies (from literature sources) also used in case study</th>
<th>If yes, how is it used?</th>
<th>Specific challenge related to the use of smart technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Artificial Intelligence</td>
<td>1</td>
<td>Process visualization and simulation[^56]</td>
<td>• The intention is to procure equipment in order to train operators</td>
<td>• Conflicts about interests, values and science</td>
</tr>
<tr>
<td>2. Integrated systems</td>
<td>1</td>
<td>On-line integrated production optimization[^57]</td>
<td>• There are manufacturing executing systems (MES), enterprise resource planning (ERP) and laboratory information management system (LIMS) exist.</td>
<td>• Social dynamics</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Supply chain management solution (software)</td>
<td>• There is SAP software that is used for procurement activities</td>
<td>• Social dynamics</td>
</tr>
<tr>
<td>3. ICT &amp; smart computing solutions</td>
<td>1</td>
<td>Risk based inspection software</td>
<td>• This helps in developing inspection plans</td>
<td>• Loss of safety margins, Positive feedback</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>CMMS</td>
<td>• Plan, conduct and analyze maintenance processes</td>
<td>• Information asymmetries</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Distributed control system (DCS)</td>
<td>• Used for the control of operative production processes</td>
<td>• Loss of safety margins, Positive feedback</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Assets condition based monitoring</td>
<td>• For Vibro monitoring, rotationary equipment</td>
<td>• Information asymmetries, Communication</td>
</tr>
<tr>
<td>4. Big/Open Data producing technologies</td>
<td>1</td>
<td>Big data analytics for production analysis and early warning for fluidized catalytic cracking units and reformers</td>
<td>• Within DSC data generated and analyzed on basic level</td>
<td>• Positive feedback</td>
</tr>
<tr>
<td>5. MEMS, MOEMS, Microfluidics</td>
<td>1</td>
<td>Microfluidics used for flow sensors, flow channels, valves, pumps</td>
<td>• Microfluidics used for calculation of flows, and used as barrier fluid in pumps</td>
<td>• Conflicts about interests, values and science</td>
</tr>
</tbody>
</table>

[^56]: Use visualization and simulation to train operators and engineers to understand the place of models in production operations and to use the models when and where needed.

[^57]: It can be done by integrating manufacturing execution system (MES), ERP, and a LIMS, flowsheet optimization, planning, and scheduling.
5.6 **FOXTROT (Water) - Drinking water supply in Sweden**

The smart technologies and related challenges for the FOXTROT case study, which portrays the case of a drinking water supply infrastructure in Sweden, are presented in Table 12.

<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>No.</th>
<th>Specific Smart technologies (from literature sources) also used in case study</th>
<th>If yes, how is it used?</th>
<th>Specific challenge related to the use of smart technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Integrated systems</td>
<td>1</td>
<td>SCADA system(^{58})</td>
<td>• As a SCADA</td>
<td>• Vulnerability due to interconnectedness</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Water treatment systems(^{59})</td>
<td>• To treat the water</td>
<td>• Vulnerability due to interconnectedness</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Membrane bioreactor system(^{60})</td>
<td>• To treat the water</td>
<td>• Vulnerability due to interconnectedness</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Water distribution control systems</td>
<td>• To distribute the water</td>
<td>• Vulnerability due to interconnectedness</td>
</tr>
<tr>
<td>2. ICT &amp; smart computing solutions</td>
<td>1</td>
<td>Smart Grid for Water(^{61})</td>
<td>• Measure use of water and also predict future demands</td>
<td>• Individual Privacy</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Predicting soft sensors</td>
<td>• Used for calculate dosage of precipitation chemicals</td>
<td>• Vulnerability due to interconnectedness</td>
</tr>
<tr>
<td>3. Big/Open Data producing technologies</td>
<td>1</td>
<td>Big Data from public health web services (^{36})</td>
<td>• Get early warning if the water treatment or the distribution network has been contaminated</td>
<td>• Governance related challenges</td>
</tr>
<tr>
<td>4. Micro-sensors, micro-actuators</td>
<td>1</td>
<td>Water sensors, e.g., for leakage status, rainfall and water level.</td>
<td>• Estimate flow, rainfall and potential leakage in distribution network</td>
<td>• Vulnerability due to interconnectedness</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Ultrasonic sensors (water level) (^{62})</td>
<td>• Estimate flow, rainfall and potential leakage in distribution network</td>
<td>• Vulnerability due to interconnectedness</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Smart Water Sensors to monitor water quality in rivers, lakes and the sea</td>
<td>• Measure water quality in coming raw water to the treatment plant</td>
<td>• Vulnerability due to interconnectedness</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Biosensors to detect water contamination</td>
<td>• Detect contaminations in raw and processed water</td>
<td>• Vulnerability due to interconnectedness</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Flow cytometry</td>
<td>• Detect contaminations in raw and processed water</td>
<td>• Vulnerability due to interconnectedness</td>
</tr>
</tbody>
</table>

---

\(^{58}\) Supervisory control and data acquisition systems (SCADA) analyze real-time conditions, providing data for fast adjustments.

\(^{59}\) Water treatment systems can be used to supply high-quality tap water by eliminating problems such as turbidity, bacteria, and salinity.

\(^{60}\) Membrane bioreactor system is used to remove suspended solids called “activated sludge,” which multiply by a biological reaction. It also can remove bacteria and other larger microbes to produce high-quality treated water.

\(^{61}\) With the tools of the smart grid for water, utilities can better understand how, where and when water is used while at the same time optimizing their business operations.

\(^{62}\) When the water level decrease in the tank, ultrasonic sensor detects this decreasing and sends the reading to Arduino. Arduino alarms the user that there is a decreasing in the tank.
5.7 GOLF ("Transport") - Smart public transportation system (Cork City Council)

The smart technologies and related challenges for the GOLF case study, which portrays the case of a smart public transportation critical infrastructure for the Cork City Council, are presented in Table 13.

Table 13: Smart technologies and related challenges for GOLF case study

<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>No.</th>
<th>Specific Smart technologies (From literature sources) also used in case study</th>
<th>If yes, how is it used?</th>
<th>Specific challenge related to the use of smart technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Integrated systems</td>
<td>1</td>
<td>Flood forecasting system</td>
<td>• Flood early warning system (FEWS) provides an open data-handling platform for managing hydrological forecasting processes and warning systems. Flow into Carrigadrohid is predicted by FEWS from a hierarchy of rainfall sources. Every forecast uses: observed data where it is available (from the start of the simulation up to time now); Met Eireann’s Harmonie data for the first 4 hours into the future; • The European Centre for Medium-Range Weather Forecasts’ (ECMWF) deterministic forecast from 4 to 120 hours beyond that. Rainfall ensembles from ECMWF are also run for information. The merged rainfall series is fed to four probability-distributed models (PDMs) rainfall runoff models, which together predict flow into the reservoir. Ensemble forecasts will also be available to inform the decision making process. The Flood Authority maintains and operates the forecasting system. This involves several GPRS enabled fluvial and tidal sensors that monitor water levels and update central databases every 15 mins. This information is then linked with Hydrological rainfall models to determine recommended levels of water releases from the Iniscarra dam.</td>
<td>• Malicious motives and acts – Vandalism of sensors or alterations that give false readings may lead to undesirable outcomes. • Information asymmetries • Key stakeholders, such as the Electricity Supply Board (ESB), Office of Public Works (OPW), Met Eireann and Cork City Council need to share data so a full picture of the issue can be obtained.</td>
</tr>
<tr>
<td>2. ICT &amp; smart computing solutions</td>
<td>1</td>
<td>Cyber Security within IPT</td>
<td>• Firewalls and VPN’s are used to ensure that connectivity to key data sources is secure. 3rd party denial of service test are undertaken periodically to ensure security levels are high.</td>
<td>• Malicious motives and acts • Cyber threats can lead to denial of service of key infrastructure or</td>
</tr>
</tbody>
</table>
### Type of smart technology

<table>
<thead>
<tr>
<th>No.</th>
<th>Specific Smart technologies (From literature sources) also used in case study</th>
<th>If yes, how is it used?</th>
<th>Specific challenge related to the use of smart technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Big/Open Data producing technologies</td>
<td>Network of intelligent sensors⁶³</td>
<td>• The Office of Public Works has installed several GPRS enabled fluvial and tidal sensors that monitor water levels and update central databases every 15 mins. The amount of these will increase in the coming years⁶⁴</td>
</tr>
<tr>
<td>4.</td>
<td>Micro-sensors, micro-actuators</td>
<td>Water level sensors</td>
<td>Several GPRS enabled fluvial and tidal sensors that monitor water levels and update central databases every 15 mins ⁶⁵.</td>
</tr>
<tr>
<td>5.</td>
<td>Combinational sensing</td>
<td>Storm surge system</td>
<td>• RPS Group Plc (RPS) was commissioned by the Office of Public Works (OPW) to undertake a real-time storm-surge forecasting service for the Republic of Ireland. • RPS utilizes the previously developed MIKE21 storm surge model to generate storm surge forecasts from October to April for various locations around the Irish coast. RPS have automated the process whereby Met data pertaining to wind and atmospheric pressure is downloaded daily from the Met Eireann FTP (File Transfer Protocol) site and used to inform the storm surge forecasting model. The model is run daily from October to April and once post processing is completed the forecast data is uploaded to a designated secure website which is only accessed by OPW and other restricted organizations. The OPW then make a decision based on the predicted tidal levels on whether to issue a flood warning.</td>
</tr>
</tbody>
</table>

---

⁶³ Using intelligent sensors and information from employee and passenger reports about service and equipment. For example, an automated wheel-measuring machine built into the track at the tram depot detects the condition of a tram’s wheel when it rolls over it.

⁶⁴ [http://data.corkcity.ie/dataset/river-lee-levels](http://data.corkcity.ie/dataset/river-lee-levels)

5.8 **HOTEL (“Energy”) – Energy supply infrastructure in Helsinki**

The smart technologies and related challenges for the HOTEL case study, which portrays the case of an energy supply critical infrastructure in Helsinki, are presented in Table 14.

<table>
<thead>
<tr>
<th>Type of smart technology</th>
<th>No.</th>
<th>Specific Smart technologies (from literature sources) also used in case study</th>
<th>How is it used?</th>
<th>Specific challenge related to the use of smart technologies</th>
</tr>
</thead>
</table>
| 1. Integrated systems    | 1   | Analytics for optimizing generation of power, heating and cooling, adapting to market and weather forecasting | • For power, as input for trading and to predict customer demand and required supply  
• For heating and cooling, to predict demand and supply scheduling | • Uncertainties in forecasting, vulnerabilities related to interconnectedness |
|                         | 2   | Smart Meters                                                                      | • Metering with options at the customer, to support demand side flexibility | • Inconsistent adoption |
|                         | 3   | (Meter) Failure Monitor \(^{66}\)                                                  | • Monitoring at customer and in the network | • Accuracy of location |
|                         | 4   | Social media monitoring                                                           | • Monitoring public responses to indicated deviations | • Biased information, communication |
|                         | 5   | Weather monitoring and forecasting                                                | • Monitoring flooding hazard, input in forecasting demand for power, heating and cooling | • Uncertainties in forecasting |
| 2. ICT & smart computing solutions | 1   | Smart Grid \(^{67}\)                                                             | • Control of power supply with demand side flexibility | • Inconsistency Adoption |
|                         |     | CMMS                                                                              | • Plan and analyze maintenance | • Information asymmetry |
|                         |     | Condition based monitoring                                                        | • Monitoring of rotating assets, with integrated experience | • Information asymmetry |
| 3. Big/Open data producing technologies | 1   | Social media monitoring through platforms such as Facebook and Twitter           | • Monitoring public indicators and responses to deviations | • Biased information, communication |
| 4. Machine cognition & Human Machine Interfaces | 1   | Technologies for augmented/virtual reality                                       | • Planned to use for design and maintenance | • Performance of available technology  
• Inconsistent adoption |

5.9 **Summary**

The smart and new technologies checked and validated in Table 7 to Table 14 make these CIs in the project smart. Several of the technologies identified in the literature are also applied within the SCIs in the project.

---

\(^{66}\) Meter Failure Monitor is a technology to monitor where the power is out in its territory. By sending messages to the meters to see if they responded, the utility is able to locate where to send crews in the field or verify if power has been active. This avoid callback system, which required staff to make phone calls to customers in order to determine whether the electricity was back on.

\(^{67}\) The Smart Grid is expected to control the demand side as well as the generation side, so that the overall power system can be more efficiently and rationally operated.
These smart technologies form the basis for identifying the level of smartness of the SCIs based on the smart maturity model proposed in chapter 3.2. At the same time, these technologies also raise challenges for these SCIs.

In addition, an evaluation of these technologies from resilience perspective was conducted based on the resilience cycle [44]. Interestingly, some of these technologies are also resilience oriented and are presented in Table 15. The SCIs may use these technologies to identify resilience related issues in different phases of the resilience cycle [44] for their systems.

Table 15: Smart technologies for resilience and protection of the SCIs (not in the order of priority)

<table>
<thead>
<tr>
<th>No.</th>
<th>Smart technologies</th>
<th>How does it improve resilience of SCIs?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Identity analytics: Smart recognition of individuals (terrorists &amp; criminals)</td>
<td>Improve the resilience in understanding risk phase [44]</td>
</tr>
<tr>
<td>2</td>
<td>Smart materials</td>
<td>Improve PPP/PPE and resilience in absorb/withstand phase [44]</td>
</tr>
<tr>
<td>3</td>
<td>Smart sensors (e.g. for chemicals, network of intelligent sensors, automatic sensors for unmanned operation, pattern or face recognition sensors combined with IoT)</td>
<td>Useful to understand emerging risks [44] [18] by providing signals for a potential disruption</td>
</tr>
<tr>
<td>4</td>
<td>Advanced analytics of Big-data (unstructured) from poor quality sources</td>
<td>Could provide useful information for faster analytical answers to first responders and enabling better decisions thereby improving the resilience in the response/recover phase</td>
</tr>
<tr>
<td>5</td>
<td>Software for integrated monitoring such as weather monitoring, social media monitoring, risk based inspections</td>
<td>Could provide useful information for improving the understanding of risks (especially emerging), anticipating/preparing for the eminent risk</td>
</tr>
<tr>
<td>6</td>
<td>Cyber Security solutions to ensure data protection such as Data management and new generation analytics improve detection of fraud and criminal activity</td>
<td>Improve the resilience in anticipate/prepare phase</td>
</tr>
<tr>
<td>7</td>
<td>Smart Surveillance through enhanced CCTV, RFID based technologies</td>
<td>Improve the resilience in understanding risk and anticipate/prepare phase [44]</td>
</tr>
</tbody>
</table>

The analysis of challenges on the use of smart technologies provided by our case study partners corroborate current and emerging challenges identified in the literature. In what concerns the current challenges, “vulnerability due to interconnectedness” is faced under the context of ALPHA, BRAVO, CHARLIE, and FOXTROT case studies; “vulnerability due to centralization” appears under the context of ALPHA and CHARLIE case studies; “compromise of individual privacy” is confirmed by ALPHA and FOXTROT; “governance related challenges” are faced under the context of ALPHA, CHARLIE, and FOXTROT; “inconsistent adoption” of smart technologies happen in BRAVO and CHARLIE cases; and “inconsistent automation” exist in the CHARLIE case.

With regard to the emergent challenges of smart technologies, the following 7 were checked and validated within the context of our case studies, namely: loss of safety margins, positive feedback, conflicts about interests, values, and science, social dynamics, technological advances, information asymmetries, and finally malicious motives and acts. Moreover, issues raised in the GOLF and HOTEL case studies about the information provided by stakeholders can fall into the communication and information asymmetries category of emergent challenges. Additionally, issues related with the accuracy of location, uncertainty in prediction, and optimization of local performance raised in the HOTEL case study can be categorized as challenges related with technical advances.
It is clear that the use of new and smart technologies also impose challenges to the resilience of the SCIs, especially, with the increasing and pervasive use of such technologies. For example, a report on smart transportation system reveals that globally the smart transportation market size is expected to grow from USD 72.05 Billion in 2016 to USD 220.76 Billion by 2021, at a Compound Annual Growth Rate (CAGR) of 25.1% during the period 2016–2021. Similar trends are also expected in other sectors [76]. Hence, it becomes critical to manage the challenges arising due to such technologies and ensure that the SCIs are resilient to any emerging risks. In order to do so, the SCIs need to advance from managing risks to a more proactive resilience oriented approach. The Emerging Risk Management Framework (CWA 16649) provides a basis for this approach.

6.1 Overview of Emerging Risk Management Framework (CWA 16649)

The Emerging Risk Management Framework (ERMF) provided under the CWA 16649 standard for managing emerging technology related risks is devoted to improving the ability of the EU industry, society and authorities to identify, monitor and manage emerging risks [18]. It was developed in the iNTeg-Risk project, and further adopted in the CEN (European Committee for Standardization) workshop agreement document [18]. It can be applied throughout the life of an infrastructure system, an organization and to a wide range of activities involving projects, products, services, assets etc. The core of this framework is its 10 procedures for managing emerging risks, which should help improving the communication and alignment of different stakeholders’ approaches. These 10 steps are illustrated in Figure 6 and is grouped into four broad areas i.e.

1. Emerging Risk Horizon Screening which includes the Step 1 Early warnings – notions [18]
2. Emerging Risk Pre-Assessment encompassing steps 2 to 4 [18]
3. Emerging Risk Assessment covering steps 5 to 8. This provides the foreground for deriving management decisions to treat risk in step 8 and ongoing monitoring, review and further improvements in Step 10 [18]
4. Communication and consultation i.e. Step 9 is manifested during the entire process [18].

It is a useful approach to understand the new smart technology related risks for the following reasons

- It can be used for different types of emerging risks as a generic framework and is not intended to force uniformity of emerging risk management.
- It suggests to consider the context of particular cases and its specific features
- Smart technology related risks are the emerging risks which have not been studied well so far and this framework aims at understanding managing these.
- ERMF provides decision support and guidance to implement risk management process at the levels of governance, policies, operations etc.

However, it needs to be aligned with the methodology, especially the resilience cycle proposed in SmartResilience project [44] [74]. It proposes that the resilience of an infrastructure as "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" [44]. Based on this definition, the resilience of the CI can be assessed in five phases, as shown in the resilience curve in Figure 7.
Phase I, understand risks, is applicable prior to an adverse event. It emphasizes the emerging risks (ERs) and includes their early identification and monitoring; e.g. what could the “adverse event” be? This is followed by phase II, anticipate/prepare, also applicable before the occurrence of an adverse event. It includes planning and proactive adaptation strategies, possibly also “smartness in preparation” [44]. Phase III, absorb/withstand, comes into action during the initial phase of the event and shall include the vulnerability analysis and the possible cascading or ripple effects; e.g. “how steep” is the absorption curve, and “how deep” down will it go? Phase IV, respond/recover, is related to getting the adverse event under control as soon as possible, influencing the “how long” will it last question. Further, it includes the post event recovery; e.g. “how steep up” is the recovery curve for normalization of the functionality? It is followed by phase V, adapt/learn, which encompasses all kinds of improvements made on the infrastructure and its environment; e.g. affecting “how well” the infrastructure is adapted after the event, and whether it is more resilient and “sustainable”. The activities in this phase also lead to preparation for the future events and hence, this resilience curve exhibits a reoccurring cycle [44].

Figure 6: Emerging Risk Management Framework

6.2 Possible extension towards resilience

The steps described the Emerging Risk Management Framework [18] can be extended towards the resilience cycle [44] considered in Smart resilience project as shown in Figure 7.

The step1 of the ERMF, early warnings – notions can be applied at the phase I - understand risk and phase II – anticipate/prepare of the resilience cycle. This can assist in detecting emerging risks as soon as possible and
in continuous monitoring of their evolution including the technical social and economic dimensions. It is done by actively searching, watching carefully, aggregating, classifying and monitoring emerging risks related to smart new technologies. This can enable the stakeholders to keep the maturation process of risk under control [18].

The step 2- context and concerns and identification of risk scenarios also help phase I - understand risk and phase II – anticipate/prepare of the resilience cycle by establishing the context and concerns of the case study from the stakeholders’ perspectives. In short, this step attempts to map the understanding of different stakeholders regarding new emerging risks related to the new technologies for e.g. as formulated in the end users need and challenges in SmartResilience task 1.3 [10]. Thus, this step of the EMRF focuses on defining the internal and external consideration that should be taken into account when managing the risk, and sets the scope and risk criteria for the remaining process [18]. It also suggests to focus on clarifying to the stakeholders about the initial framing of the issue and helping to define what conventions and conditions apply for e.g. regulation, directives, laws, etc.

The following step 3 to identify the emerging risk scenarios involves establishing cause and effect links and preparing a comprehensive list of risks and possible scenarios based on screened events [18]. Again, this step applies to the phase I understand risk and phase II – anticipate/prepare of the resilience cycle. In order to understand the emerging risks and resilience of new smart technologies it is imperative to develop and explore scenarios for emerging risks by expanding the scope of the assessment from risk to other kinds (e.g. - to go beyond the conventional risk assessment and integrate it with comprehensive technology assessment). This will lead to a realistic anticipation/preparation for emerging risk related to new smart technologies.

Further, the application of step 4 pre-assessment of selected scenarios (screening) produces a further refined picture of the previously identified risk scenarios [18], thereby improving the understanding of risk (phase I of the resilience cycle). It clarifies various perspectives on an emerging risk, defines the issues to be focused and forms the base criteria for how the risk should be managed and assessed. It also brings out the existing indicators, routines and conventions that can help in addressing the risk in a focused manner. In addition, it suggests measuring the potential impact of the threat on various dimensions such as technology/technical, human management, governance/communication and policies, and regulations/standardization [18]. Hence, this step also may help in estimating the absorbing capacity of the smart new technology to absorb the impact, thereby contributing to the phase III – absorb/withstand phase of the resilience cycle.

The next step of ERMF, i.e. step 5- emerging risk appraisal/ assessment/analysis focuses on arriving at a fully assessed set of risk scenarios with potential damages or adverse effects that are explored and quantified. This appraisal enables the stakeholders to gauge how the risk can be possibly reduced or contained, thereby contributing to assessing the absorbing capacity (i.e. phase III – absorb/withstand of the resilience cycle) of a smart technology in a critical infrastructure to absorb the shock in case of an event. Further, this step suggests to conduct a scientific risk assessment involving potential damages, assess ubiquitousness, persistence of damage, perceptions about the concerns, social responses to the risk, possibilities of mobilization/ conflicts, roles of institutions, governance structures, the analysis of the whole life cycle of the smart new technology and the cumulative risk assessment [18]. This will give the decision-makers the possibility to tackle the emerged risk related to smart new technologies, thereby contributing to the respond/recover phase of the resilience cycle.

The step 6 of the resilience cycle i.e. Emerging risk characterization contributes to three phases of the resilience cycle i.e. understand the risk (Phase I), anticipate/prepare (Phase II) for the emerging risk and respond/recover (Phase IV) from the threat scenarios. The characterization process allows the decision makers to distinguish between scientific facts from policy. It is crucial when large amount of risks and early warnings are to be dealt with, simultaneously. Some of the tools that can be used for characterization are multi-criteria decision making (MCDM), on scales such as simple, complex, uncertain or ambiguous, etc. [18].
Subsequent step 7 of the ERMF – Evaluation of emerging risks tolerability & acceptability, guides in reaching a consensus about the acceptability and tolerability of a risk. Tolerable risks will generally be associated to undertaking an activity – which is considered worthwhile for the value it provides. The main effort in this step of the process is usually focused on gathering and compiling the necessary knowledge, which, in the case of tolerability, must additionally support an initial understanding of required risk reduction and mitigation.
measures [18]. Hence, it relates to the phase III — absorb/withstand of the resilience cycle as it involves identifying vulnerabilities and possible effects such as threshold of resilience of a system which equates to tolerability in the ERMF [44].

Moreover, step 8 of the ERMF- Management & decision may correspond to the Phase IV- respond/recover and phase V- adapt/learn of the resilience cycle. This step focuses on clear information whether risk is acceptable/tolerable or not, if not what are the proposed measures to be undertaken in order for risk to become acceptable/tolerable. In case of the resilience cycle, this step would help in responding to the risk emerging from the use of new smart technology in SCIs. Furthermore, in adapt/learn phase of the resilience cycle by monitoring their effectiveness and reviewing decision, if necessary.

The step 9 of the ERMF, Emerging risk Communication and consultation is a continuous process throughout the framework and applies also throughout the resilience cycle. It ensures (through transparent risk framing, risk appraisal and risk management) definition and acceptance of the common position towards the emerging risks and trust in policies and measures proposed by the overall risk governance system. It suggests that a successful and effective communication is an increasingly important element of managing emerging risks related to new smart technologies. Especially, due to increased uncertainty, the emerging risk communication needs even more probabilistic thinking and this aspect can be improved for example by application of risk comparisons. Furthermore, the persuasion and efforts to align stakeholders’ stances and understanding better their behavioral patterns are often in the heart of the communication process. This needs to be a two way process.

Finally, step 10 of the ERMF, Emerging Risk monitoring, review and continuous improvement aids the control of the risk itself; control of changes to conditions affecting the risk; and control of appropriateness of the ERMF. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear. Consequently, monitoring, review and continuous improvement are of increased importance in particular for emerging risks. In this process the effective and continuous effort should be devoted to measuring the performance of risk management against indicators (which should be periodically reviewed for appropriateness). In addition, one should periodically review whether the risk management framework, policy and plan are still appropriate, given the possible change of external and internal context. It clearly corresponds to throughout the resilience cycle, especially, adapt/learn phase of the resilience cycle as it directly contributes to the learning and adapting process but also applies to other phases such as understand risk, anticipate/prepare, absorb/withstand, respond/recover and during the preceding and new resilience cycle.
Conclusions

The widespread use of smart technologies has attracted considerable attention amongst industry, academia, and government. In fact, prior work has documented the characteristics of “smart” systems, especially in the context of cities. The Scottish government, for example, reports that a smart city can enhance the city overall sustainably, well-being of their citizens, and economic development [67]. And these cities are composed of CIs making each a CI of CIs. Further, there is an increased use of smart and new technologies by these CIs to make them smart systems. According to the literature, smart systems comprise technologies that have advanced functionalities, and therefore are able to sense, diagnose, describe, qualify, and manage a given situation [86]. These systems have three key characteristics: i) integrative and interconnected, ii) intelligent, and iii) autonomous. Correspondingly, this task focused on addressing the question what makes the selected critical infrastructures “smart” and how do we assess their level of “smartness”.

In the SmartResilience project, smart CI is efficient and able to maximize the service it provides by the use of intelligent and autonomous systems within an integrative and interconnected network [12] [32][73] [86]. Thereby, these SCIs shall help deliver improved participative governance and a vision for a sustainable and resilient future [5]. The literature review also identified types of smart and new technologies that provide a link between smart systems’ characteristics and specific technologies applicable to the CIs in the SmartResilience project. Further, a five level maturity model to assess the maturity of smart CIs in terms of their three primary characteristics is proposed in Chapter 3. In addition, an example for a smart airport is illustrated.

Given the increasing use of smart and new technologies in smart CIs, there is a rise in challenges to the resilience of the SCIs. Consequently, this task also addresses the question - what are the challenges originating from the application of new technologies when enhancing the “smartness” of a selected Critical Infrastructure.

The literature review suggests that there are six main current challenges to the resilience of SCIs, namely:

- vulnerability due to interconnectedness;
- vulnerability due to centralization;
- compromise of individual privacy;
- governance related challenges;
- inconsistent adoption;
- inconsistent automation.

In addition, a list of emerging challenges is provided in chapter 4.2.

The use of smart and new technologies and corresponding challenges from the literature review were assessed by the CI case study partners in the SmartResilience project (see chapter 5). From that list, case study partners checked and validated the technologies employed in their CIs. Moreover, a list of smart technologies for resilience and protection of the SCIs was derived (see chapter 5.9), including: identity analytics, smart materials, smart sensors, advanced analytics of big-data, software for integrated monitoring, cyber security solutions, and smart surveillance. Further, these cases corroborate the challenges from the literature review. In particular, all the current challenges were covered within the context of the case studies, which implies that all the CIs in the project foresee similar challenges with the advanced use of smart and new technologies. Similarly, case study partners identified most of the emerging challenges as applicable for their respective CIs.

In order to manage the emerging risks related to the use of smart and new technologies, recommendations are provided in chapter 6. These recommendations are based on the extension of the ERMF CWA 16649
standard for the improvement of CIs resilience in managing smart and new technology related risks [18] [44] [74]. This EMRF is foreseen as instrumental to study a less explored area, such as resilience management of smart technology related emerging risks. It also provides decision support and guidance to implement a risk management process at the levels of governance, policies, and operations.

This task provides essential inputs to other tasks and WPs of the SmartResilience project. The challenges related with smart and new technologies are relevant for task 2.2. For task 3.2, the smart systems characteristics and challenges informed the development of methodology for CIs resilience assessment. Similarly, the smart system characteristics and challenges informed the development of issues and indicators in WP4. The maturity model to assess the maturity levels of smart CIs provides the basis for work in WP5. The recommendations provided for the extension of the ERMF CWA 16649 standard will inform the work on standardization in WP6.
References


[12] Chourabi, N et. al. (2012). Understanding Smart Cities-. An Integrative Framework. 45th Hawaii International Conference on System Sciences, Maui, HI, USA, pp. 2289-2297


[18] Deutsches Institut für Normung e.V.(2013), Managing emerging technology-related risk CWA 16649, Berlin


[80] Urban Tide(n.a), Overview of the Smart Cities Maturity Model, Scotland, Retrieved from https://static1.squarespace.com/static/5527ba84e4b0a3d0e89e14d/t/55aebbfc4b0f8960472ef49/1437515772651/UT_Smart_Model_FINAL.pdf


[86] Weiler et. al.(2013), Strategic Research Agenda of EpoSS, Strategic Research Agenda of EpoSS, Berlin


[93] ISO/PRF 37153 Smart community infrastructures -- Maturity model for assessment and improvement

[94] ISO 37154:2017 Smart community infrastructures -- Best practice guidelines for transportation


[96] IPIECA/API/IOGP (2015). Oil and gas industry guidance on voluntary sustainability reporting. IOGP Report 437


[99] Urban Tide (n.a), Overview of the Smart Cities Maturity Model, Scotland, Retrieved from [https://static1.squarespace.com/static/5527ba84e4b09a3d0e89e14d/t/55aebffce4b0f8960472e4f49/1437515772651/UT_Smart_Model_FINAL.pdf](https://static1.squarespace.com/static/5527ba84e4b09a3d0e89e14d/t/55aebffce4b0f8960472e4f49/1437515772651/UT_Smart_Model_FINAL.pdf) accessed on October 31, 2017

[100] SmartResilience (2017) D4.1 draft report on Supervised RIs: Defining resilience indicators based on risk assessment frameworks. EU project SmartResilience, Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany


[102] SmartResilience (2017) D1.4 Database specifications, template for resilience indicators and first version of the RIs database. EU project SmartResilience, Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany


### ANNEXES

<table>
<thead>
<tr>
<th>Annex 1</th>
<th>Glossary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annex 2</td>
<td>Response to internal review process</td>
</tr>
</tbody>
</table>
## Annex 1  Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emerging risk [95]</td>
<td>Emerging risk is understood as a risk not necessarily well known and spreading increasingly in its infrastructural context over time, leading to cascading and ripple effects. One example of such an emerging risk is a man-caused release of toxic aromatic liquids with cascading effects on several other critical infrastructures.</td>
</tr>
<tr>
<td>Stakeholder [96]</td>
<td>Stakeholder is any organization that has a stake, or interest, in the SCI in focus, either because they are affected by the SCI or because they affect it. End users are most likely found among stakeholders, but not all stakeholders will be end user.</td>
</tr>
<tr>
<td>Indicators [44]</td>
<td>In SmartResilience, it is the description of HOW to measure an issue. Any type/form of indicators are considered appropriate in the SmartResilience methodology, meaning that they can be yes/no questions, numbers, percentages, portions, or some other type. E.g., it can be &quot;percentage of personnel in a certain response team taken a certain course&quot;.</td>
</tr>
<tr>
<td>Smart systems [86]</td>
<td>Smart systems are self-sufficient intelligent technical systems or subsystems with advanced functionality, enabled by underlying micro nano and bio-systems and other components. They are able to sense, diagnose, describe, qualify and manage a given situation, their operation being further enhanced by their ability to mutually address, identify and work in consort with each other. They are highly reliable, often miniaturized, networked, predictive and energy autonomous.</td>
</tr>
<tr>
<td>Threats [106]</td>
<td>A threat is part of a threat scenario, i.e. part of the framework in which the case study is taking place. For example, the threat &quot;IEMI/HPMI&quot; is a threat for case study ALPHA, while &quot;flooding&quot; is a threat for case study HOTEL.</td>
</tr>
<tr>
<td>Challenges [106]</td>
<td>Once the threat is identified, a challenge arises as a difficulty, or “issue to be solved” in the process of dealing with threats. Examples for challenges are &quot;loss of safety margins&quot;, &quot;temporal complications&quot; or &quot;information asymmetries&quot;.</td>
</tr>
<tr>
<td>New risks [18]</td>
<td>New means that the risk did not previously exist and is caused by new processes, new technologies, new types of workplaces, or social or organizational change; or that a long-standing issue is newly considered as a risk due to a change in social or public perceptions; or that new scientific knowledge allow a long-standing issue to be identified as a risk.</td>
</tr>
<tr>
<td>End users [96]</td>
<td>End user targets to use the (smart) RIs and indicator-based assessment methodology developed by the SmartResilience project.</td>
</tr>
<tr>
<td>Issues [103]</td>
<td>Issue is a very general term referring to anything (factors, conditions, functions, actions, capacities, capabilities, etc.) that is important in order to be resilient against severe threats such as terror attacks, cyber threats and extreme weather. It is WHAT is important, and it is allocated to one of the five phases in the resilience cycle. E.g., it can be &quot;training&quot; performed in the anticipate/prepare phase.</td>
</tr>
<tr>
<td>Dimensions [103]</td>
<td>Possible structuring of issues and indicators according to dimensions. In SmartResilience, we use five dimensions: system/physical, information/data, organizational/business, societal/political, and cognitive/decision-making.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Levels [103]</td>
<td>Levels in a hierarchical model. Typically, the levels start from the smart city or smart critical infrastructure down to the indicators. A hierarchical model consists of a certain number of levels, sometimes also referred to as layers. In SmartResilience, we use a six levels model/structure.</td>
</tr>
<tr>
<td>Phases [103]</td>
<td>Phases in the resilience cycle. In SmartResilience we use five phases: Understand risks, anticipate/prepare, absorb/withstand, respond/recover, and adapt/learn.</td>
</tr>
<tr>
<td>Scenario [103]</td>
<td>In SmartResilience project, the term &quot;scenario&quot; is used for a specific selection of critical infrastructures and threats for a given area/city, i.e. the selected area, critical infrastructures and threats.</td>
</tr>
<tr>
<td>Dependency [103]</td>
<td>Dependency is a “linkage or connection between two infrastructures, by which the state of one infrastructure influences or is reliant upon the state of the other</td>
</tr>
<tr>
<td>Smartness [102]</td>
<td>Smartness of the CI is ability of to be integrative and interconnected, intelligent by the use of ICT, web technology, sensors and smart computing, smart governance oriented, inclusive of end-users, sustainable through future orientation and efficient and maximize service</td>
</tr>
<tr>
<td>Understand risk [103]</td>
<td>Understand Risk is the first phase in the resilience cycle in SmartResilience project. Includes and emphasizes understanding of (emerging) risks, and includes knowledge about the context, the systems, and previous events; &quot;What could ‘the event’ be’?</td>
</tr>
<tr>
<td>Anticipate/Prepare [103]</td>
<td>Anticipate/Prepare is the second phase of the resilience cycle in SmartResilience project and includes planning, proactive adaptation and vigilance/attention; “How to prepare for both expected and unexpected events”? “How to get early warnings”?</td>
</tr>
<tr>
<td>Absorb/Withstand [103]</td>
<td>Absorb/Withstand is the third phase of the resilience cycle in SmartResilience project and includes inherent absorption, resilient reaction, robustness and redundancy, and possible cascading/ripple effects; “How steep”? “How deep down”?</td>
</tr>
<tr>
<td>Respond/Recover [103]</td>
<td>Respond/Recover is the fourth phase of the resilience cycle in SmartResilience project and includes response and recovery capacity, ability and rapidity of the infrastructure and the surrounding environment; “How long”? “How steep up”?</td>
</tr>
<tr>
<td>Adapt/Learn [103]</td>
<td>Adapt/Learn is the fifth and last phase of the resilience cycle and SmartResilience project and includes learning and improvements made in/on the infrastructure and its environment; “How well”? “Sustainable”?</td>
</tr>
<tr>
<td>Inoperability [105]</td>
<td>Inoperability is the state suffered by individual sectors that result from a disruption in a different sector (or set of sectors).</td>
</tr>
<tr>
<td>Redundancy [100] [104]</td>
<td>If parts of the grid fail, alternatives have to be in place (“fall-back”) to assume the lost functionality. On the operator side, respective provisions can consist in e.g. stocking spare parts for the case of failing hardware as well as to foresee alternative routing for energy/data networks.</td>
</tr>
<tr>
<td>Artificial intelligence [86] [87]</td>
<td>The goal of artificial intelligence as a science is to make machines do things that would require intelligence if done by human e.g. reduced operator distraction and error, Optimization of vehicle control, navigation and logistics. Also, it can autonomously or through networking, safeguard and optimize every aspect of this critical chain, it is also able to sense, diagnose, describe, qualify and manage a given situation</td>
</tr>
<tr>
<td>Integration [18] [86] [87] [99]</td>
<td>Smart systems which brings together sensing, actuation and informatics/communications (ICT) consort with each other and enables communications within a connected world e.g. vehicle infrastructure interaction in automotive sector or collaborative service models as well as engagement with external stakeholders</td>
</tr>
<tr>
<td>Scientific unknowns [18]</td>
<td>Dealing with emerging risks requires dealing with scientific unknowns. These unknowns, can be tractable or intractable, and contribute to risks by being, e.g. unanticipated, unnoticed, and over- or underestimated.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Loss of safety margins due to interconnectedness [18]</td>
<td>The level of connectivity in many social and technical systems is greater than in the past and the interconnections are increasing. The pace at which these systems operate is becoming faster and many are operating under higher levels of stress. This can lead to tight-coupling of components within systems and to loss of safety margins - a loss of slack or buffering capacity that leaves systems more vulnerable to disruption and thus increases the likelihood that new risks will emerge.</td>
</tr>
<tr>
<td>Positive feedback [18]</td>
<td>Systems exhibiting positive feedback react by amplifying a change or perturbation that affects them. Positive feedback tends to be destabilizing and can amplify the likelihood or consequences of an emerging risk.</td>
</tr>
<tr>
<td>Varying susceptibilities to risk [18]</td>
<td>The consequences of an emerging risk may be different from one context (situation/system/population) to another. Geography, genetics, experience and wealth are just some of the possible contextual differences that create varying susceptibilities to risk.</td>
</tr>
<tr>
<td>Conflicts about interests, values, and science [18]</td>
<td>Public debates about emerging risks seldom witness a clear separation between science, values, and interests. The conflicts that result have the potential to contribute to fertile ground for risk emergence or amplification. For e.g. emerging risks may be amplified when efforts to assess them and take early management measures encounter opposition on the grounds of contested science or incompatible values.</td>
</tr>
<tr>
<td>Social dynamics [18]</td>
<td>Social change can lead to potential harm, or it can attenuate it. It is therefore important for risk managers to identify, analyze and understand changing social dynamics.</td>
</tr>
<tr>
<td>Technological advances [18]</td>
<td>Risk may emerge when technological change is not accompanied by appropriate prior scientific investigations or post-release surveillance of the resulting public health, economic, ecological and societal impacts. Risks are further exacerbated when economic, policy or regulatory frameworks (institutions, structures and processes) are insufficient, yet technological innovation may be unduly retarded if such frameworks are overly stringent.</td>
</tr>
<tr>
<td>Temporal complications [18]</td>
<td>A risk may emerge or be amplified if its time course makes detection difficult (e.g., the adverse effects of the risk only become evident after a long period of time) or if the time course does not align with the time horizons of concern to analysts, managers and policymakers.</td>
</tr>
<tr>
<td>Communication and information asymmetries [18]</td>
<td>Risks may be complicated or amplified by untimely, incomplete, misleading or absent communication. Effective communication that is open and frank can help to build trust. In many cases, such communication can attenuate, or lead to better anticipation and management of, emerging risks. Information asymmetries fall under the umbrella of communication related challenges and occur when some stakeholders hold key information about a risk that is not available to others. These asymmetries may be created intentionally or accidentally. In some cases, the maintenance of asymmetries can reduce risk, but in others, it can be the source of risk or the amplification of risk by creating mistrust and fostering non-cooperative behaviors.</td>
</tr>
<tr>
<td>Perverse incentives [18]</td>
<td>Perverse incentives are those that induce counterproductive or undesirable behaviors, which lead to negative, unintended consequences. Such incentives may lead to the emergence of risks, either by fostering overly risk-prone behaviors or by discouraging risk prevention efforts.</td>
</tr>
<tr>
<td>Malicious motives and acts [18]</td>
<td>Malicious motives give rise to emerging risks and therefore practitioners need to consider intentional as well as unintentional causes of risk. Malicious motives and acts are not new, but in a globalized world with highly interconnected infrastructures (e.g., trade agreements and information and communication systems) they can have much broader-reaching effects than in the past.</td>
</tr>
<tr>
<td>Safety of employees data at work [18]</td>
<td>The safety and security of the employee data may be threatened in a company without even their knowledge. Cyber-crime can be manipulate the employees’ data from the outside due to a lack of data security. This can have an effect on their security functions and making the employees vulnerable to unknown risks.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td>MEMS, MOEMS, Microfluidics [86]</td>
<td>MEMS (Micro- Electro- Mechanical Systems) expand silicon technology by incorporating sensors and mechanical movement. MOEMS (Micro- Opto- Electro- Mechanical Systems) enhance the MEMS concept to include light sources and optical components. Microfluidics expands MEMS to the control and analysis of fluids.</td>
</tr>
<tr>
<td>Semiconductors &amp; More-than-Moore (MtM) Technologies [86]</td>
<td>“More-than-Moore” technologies add functions to normal semiconductor chips. These advances can allow chips, for example, to communicate through wireless connection or work directly with magnetics and fluids.</td>
</tr>
<tr>
<td>Micro-sensors, micro-actuators [86]</td>
<td>Micro-sensors can, for e.g. miniaturize sensing to such an extent that body functions can be monitored internally without disturbance – the “Lab-in-a-pill”. Micro-actuators miniaturize movement and can for e.g. be applied to active noise cancellation, antenna steering and adaptive optics.</td>
</tr>
<tr>
<td>Combinational sensing [86]</td>
<td>Human skin is a good example of combinational sensing, as it combines sensitivities to heat and pressure (touch). Combinational sensing provides similar, engineered, solutions in two ways: (1) combining discrete sensors or (2) using one sensor structure to measure several things.</td>
</tr>
<tr>
<td>Multifunctional materials [86]</td>
<td>Multifunctional materials can combine structure with a further function or functions. For example threads which sense heat or moisture could be woven into diagnostic pads for healthcare.</td>
</tr>
<tr>
<td>Energy management &amp; scavenging [86]</td>
<td>Energy management &amp; Scavenging technologies allow smart systems to make the most efficient use of resources and to gain their operating power from their surroundings.</td>
</tr>
<tr>
<td>Opto/organic/bio data processing [86]</td>
<td>Memory and data processing in electronic computers is now routine. But new ways of data processing, using processes which “bio-mimic” the brain are also emerging.</td>
</tr>
<tr>
<td>Machine cognition &amp; Human Machine Interfaces [86]</td>
<td>As systems increase in complexity, human limits may constrain their use. Advances in Human machine Interfaces will relieve this situation, and devices that better “understand” the user will provide major advantages in ease and accuracy of operation.</td>
</tr>
<tr>
<td>Emerging Risk Management Framework [18]</td>
<td>The Emerging Risk Management Framework (EMRF) provided under the CWA 16649 standard for managing emerging technology related risks is devoted to improving the ability of the EU industry, society and authorities to identify, monitor and manage emerging risks.</td>
</tr>
<tr>
<td>Smart Critical Infrastructure</td>
<td>Smart Critical Infrastructure is a critical infrastructure which is efficient and able to maximize the service it provides by the use of intelligent systems such as Internet of Things, artificial intelligence, sensors, actuators and smart computing to within integrative and interconnected network. SCI are also self-sufficient adaptive intelligent technical systems with advanced functionality, enabled by underlying micro-nano-systems and other component. Thereby, these SCIs shall help deliver improved participative governance and a vision for sustainable &amp; resilient future.</td>
</tr>
<tr>
<td>Smart Maturity model</td>
<td>Smart maturity model is used to assess the maturity levels of smart infrastructures in terms of their three primary characteristics: i) integrative and interconnected, ii) intelligent, and iii) autonomous</td>
</tr>
</tbody>
</table>
Annex 2  Response to internal review process

The Content of this Annex has been submitted as part of the periodic review report to the PO/EU/ Reviewers.