Alliance for IoT
and Edge Computing
Innovation

White Paper IoT and Crisis Preparedness

Release 1.0

AIOTI FG Buildings and Communities

June 2023

Executive Summary

The main objective of this vision paper is to identify the steps to be followed to develop societal resilience towards short-term and long-term risks. The purpose is to showcase the best practices and insights needed to (1) SENSE, (2) RESPOND, (3) DEFEND, and (4) RECOVER within the IoT domain by involving all key stakeholders of this value chain.

According to the World Health Organization[1], the emergency cycle is divided into four different phases: (1) Prevent; (2) Prepare; (3) Respond, and (4) Recover.

Hence, this whitepaper aims to cover the four phases of emergency management as an integrated overview of four different fields of threats:

1. Pandemics and other Health-related threats,

2. Natural Disasters,

3. Cyber Attacks, and

4. Attacks on Public Spaces.

[1] https://www.euro.who.int/en/health-topics/health-emergencies/pages/about-health-emergencies-in-the-european-region/emergency-cycle

Table of Contents

Table of Figures

List of Tables

1. Introduction

According to several scientific reports[2], hurricanes, cyclones, earthquakes, mudslides, floods, wildfires, volcanic eruptions and weather events like extreme droughts and monsoons are increasing worldwide due to climate change. In 2020, according to NOAA[3], all months except December were the warmest ever recorded. Moreover, the 2020 Annual Climate Report[4] states that combined land and ocean temperature has increased at an average rate of 0.08°C per decade since 1880. Lastly, many reports have shown that these climate changes have led to the appearance of Natural Disasters.

On the other hand, ecosystems and societies have also struggled with adverse events from non-natural causes, such as terrorist attacks and worldwide pandemics. Terrorism can take several forms (including technology, biological agents, or other methods)[5] to coerce societies and governments, and it can happen anytime. When faced with a worldwide pandemic, communities and ecosystems face an invisible threat capable of spreading across international borders. From natural to non-natural causes, disasters harm public safety and must be addressed as an integrated and complete scenario.

Resilience is the capacity of social, economic and environmental systems to cope with a hazardous event or trend or disturbance, responding or reorganising in ways that maintain their essential function, identity and structure while also maintaining the capacity for adaptation, learning and transformation (IPCC, 20141).[6] Resilience also refers to 'the degree to which the system minimises the level of service failure magnitude and duration over its design life when subject to exceptional conditions' (Butler et al., 2014, p. 3). Resilience becomes relevant when the probability of avoiding failure decreases due to shocks or stresses (Figure 1.)

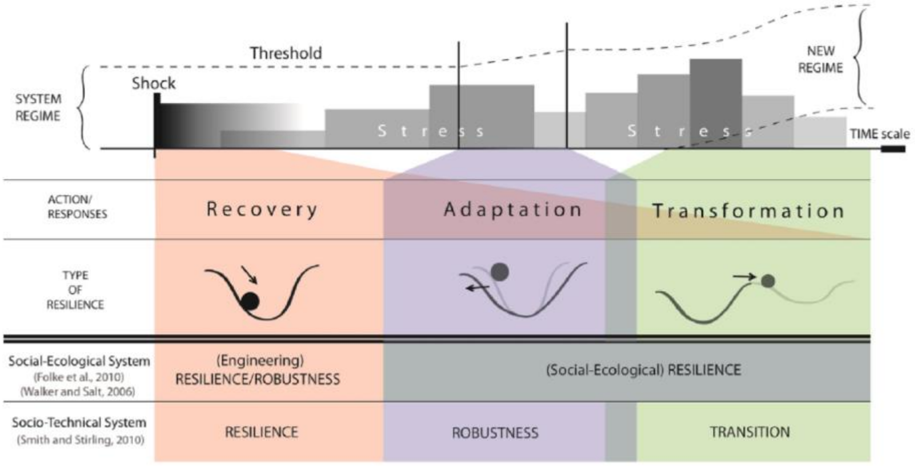

Threshold
Shock
SYSTEM REGIME
NEW REGIME
Stress
Stress
TIME scale
ACTION/ RESPONSES
Recovery
Adaptation
Transformation
TYPE OF RESILIENCE
Social-Ecological System (Folke et al., 2010) (Walker and Salt, 2006)
(Engineering) RESILIENCE/ROBUSTNESS
(Social-Ecological) RESILIENCE
Socio-Technical System (Smith and Stirling, 2010)
RESILIENCE
ROBUSTNESS
TRANSITION

Figure 1: Three system states of resilience for the short-, medium and long-term perspectives (Chelleri et al., 2015)

[2] https://sciencing.com/negative-effects-natural-disasters-8292806.html

[3] https://www.climate.gov/news-features/understanding-climate/climate-change-global-temperature

[4] https://www.ncdc.noaa.gov/sotc/global/202013

[5] https://www.readynh.gov/disasters/terrorism.htm

[6] https://archive.ipcc.ch/pdf/assessment-report/ar5/wg2/WGIIAR5-AnnexII_FINAL.pdf

Planning for recovery requires replacing and repairing affected infrastructure and investing in the capacity to reduce risk, and therefore begins before the occurrence of a disaster (UNDP/BCPR, 2011). Planning for recovery means creating conditions that allow an appropriate, effective and quick response to a disaster or disruption threat. Policies must be based on understanding the risks and vulnerabilities, capacity, exposure of people and assets, the environment and the characteristics of the disaster.

This approach can help prevent and mitigate the risk and prepare and respond effectively (UNISDR, 2015). Planning to reduce disaster risk is essential to enhance resilience in all aspects of the system since it increases the capacity of the system to absorb shocks and prevent or reduce losses (UNISDR, 2015; Chelleri et al., 2015). Effective recovery planning requires preparation for not only risks but also the anticipation of the consequences. Capacities must be in place to effectively respond to recovery, rehabilitation and reconstruction after a disaster. Good planning may provide an opportunity to rebuild the physical, social, economic or environmental system to prepare it for future shocks better.

This strategy, called 'Build Back Better', is an ideal reconstruction and recovery process that delivers resilient, sustainable, and efficient recovery solutions to disaster-affected communities. The 'Build Back Better' (BBB) concept motivates communities to become stronger and more resilient after a disaster (Mannakkara et al., 2008). BBB was defined as a way to utilise the reconstruction process to improve a community's physical, social, environmental, and economic conditions to create a more resilient community, where resilience is defined as "the capacity to recover or 'bounce back' after an event" (Twigg, 2007). The approach includes focusing on clean energy, such as investing in renewable energy sources like wind and solar power and transitioning away from fossil fuels but also includes investments in transportation infrastructure, such as electric vehicle charging stations, and improvements to public transportation systems. In addition, the BBB approach includes investments in education and job training programs, focusing on creating opportunities for underserved communities and helping people transition to new industries.

Overall, the Build Back Better approach is about creating a more equitable, sustainable, and prosperous future by investing in the areas that will help us overcome the present challenges and build a better tomorrow. Therefore, the concept of BBB proposes a broad, holistic approach to post-disaster reconstruction to address the wide range of prevalent issues, including those mentioned above and ensure that affected communities are regenerated in a resilient manner for the future. It has been adopted by several countries, including the United States, Canada, and Japan, to address the challenges presented by the COVID-19 pandemic and to create a more resilient and sustainable future. Investing in infrastructure, education, healthcare, and other areas will help create a more equitable and sustainable society. Its goal is to recover from the pandemic and build a more resilient and prosperous future.

2. An Era of Pandemics

'It's an era of pandemics we are entering. If you look at what has been happening over the past few years, I mean from HIV to Ebola to MERS to SARS, these were all epidemics which could be contained, but we should not think it is all over when we've overcome Covid-19. The risk is still there. The EU must prepare for an era of Pandemics'

President von der Leyen, European Commission

Digital health technologies hold the potential to bring about major improvements in the efficiency of health systems, both in terms of care provision and the administration of the system as a whole. For many years, there have been efforts across European health systems to facilitate and promote their use. However, realising the potential of digital tools in health care has proved to be a long, arduous and complex endeavour with mixed results.

The unique challenges generated by COVID-19 have nevertheless created different needs and pushed a new momentum for digital health technologies adoption, resulting in their use accelerating during the pandemic. Digital health tools have become integral to pandemic responses across the region in supporting communication and monitoring, the continued provision of health services, and transitions from pandemic-related restrictions.

Our society needs to leverage the momentum and consolidate evidence from digital health during the pandemic to provide an evidence base for making the best use of digital health tools in the medium and longer term.

2.1 Overview of the Current State of Play

Before the COVID-19 pandemic, Europe had a wide discrepancy regarding policy and strategy development towards digital health by area and country. According to the 2015 World Health Organization (WHO) global survey on eHealth, 70% of reporting countries in the WHO Europe region had an eHealth policy or strategy in place. Still, only 27% had one for telehealth[7], with a greater propensity in the northern EU countries compared to the Central and Southern countries.

According to the WHO (EU), 43% of reporting countries had policies or legislation defining medical jurisdiction, liability or reimbursement of eHealth services. 53% had no legislation allowing individuals to access their electronic health records, and only 13% had policies on regulating the use of big data in the health sector. In addition, only 11 reporting countries had a national authority responsible for managing this.

The pandemic prompted a rapid uptake and concrete implementation of digital health tools. Despite this, various countries were positioned differently at the pandemic's start. Northern EU countries were relatively well set, with digital health already integrated into their health systems. Other countries were advanced in some ways but not in others, e.g. having a well-developed technical infrastructure but relatively restrictive regulations. In contrast, others had not yet integrated digital health tools into their wider health systems. This limitation caused countries to start from different points when the pandemic struck.

[7] N. Fahy, G.A. Williams, COVID-19Health System, Response Monitor Network; "Use of Digital Health Tools in Europe, before, during and after COVID-19", WHO Regional Office for Europe, 2021.

Figure 2: ***Covid-19 cases in the world. (9.04.2020) Source: Center for Systems Science and Engineering (CSSE) at JHU***

Overall, there are four main areas (Table 1) where digital health tools are being used in response to COVID-19: first, communication and information; second, monitoring and surveillance; third, supporting provision of health services; and fourth, vaccination, immunity and pharmacovigilance.

Table 1: Digital health tools implementation for addressing COVID-19's spread

Areas	Main actions
Communication and Information	- Communicating information on COVID-19 with the public
	- Combating misinformation on COVID-19
Monitoring and Surveillance	- Adapting existing tools to support monitoring surveillance and contact tracing
	- Using mobility data to model diffusion of COVID-19
	- Using genomic data to detect and track new variants
	- Public databases and social media data to support monitoring and surveillance
	- Using mobile apps to support contact tracing
	- Mobile and web-based apps to support symptom tracking and self-diagnosis
	- Using mobile apps to support or enforce self-isolation and quarantine
Supporting Provision of Health Services	- Using remote consultations to support the provision of essential care
	- Using digital tools to manage hospital capacity
	- Using AI to identify infections and potential treatments
Vaccination, Immunity and Pharmacovigilance	- Identifying individuals eligible for vaccination
	- Combating vaccine hesitancy
	- Monitoring of adverse reactions
	- Using immunity certificates to support the reopening of economies

On top of this, on 31 March 2021, the Commission launched an online public consultation on the Health Emergency Preparedness and Response Authority (HERA)[8]. Part of the EU's answer to the COVID-19 pandemic and a strong European Health Union, HERA aims to improve Europe's capacity and readiness to respond to cross-border health threats and emergencies.

HERA is part of the European Health Union, as announced by President von der Leyen in her September 2020 State of the Union address. It will provide a dedicated structure to support the development, manufacturing and deployment of medical countermeasures during a health crisis of natural or deliberate origin. HERA could use foresight, surveillance and market intelligence to plan and coordinate medical countermeasures. The exact remit of HERA will be set out in a legislative proposal later this year. The Commission will consider the feedback received before finalising the legislative proposal.

Coordinate EU-wide risk assessments for emerging or unknown cross-border health threats based on the available epidemic intelligence knowledge at the relevant EU bodies, including the ECDC and the Union Civil Protection Knowledge Network, to identify medical countermeasures. Further, cooperation will be sought with the World Health Organization (WHO).

2.2 Research Challenges and Objectives

Due to COVID-19's spread, the European healthcare systems' capacity has been put under unprecedented pressure. The crisis highlighted the strengths and weaknesses of dealing with an event of these proportions. This pandemic has made explicit that we should take the opportunity to implement an ambitious reform agenda for European health systems through the direct involvement of all stakeholders and policymakers at the regional, national and EU levels.

In particular, the following challenges should be considered as the key ones to be addressed:

- New investment in the healthcare and societal sector. In particular, the pandemic has made clear how local primary services have suffered a reduction of investments over the last decades, limiting the territory's capacity to address the challenges coming from COVID-19 adequately. Additionally, the crisis has clarified the consequences of confusing short-term cost savings with efficiency gains through improved care delivery design. For example, the reduction of the workforce and implicit attrition in service delivery have left some countries ill-equipped to deal with the spike in demand for healthcare.
- Developing an integrated budget framework for health investments to limit and address the fragmentation of the EU's health systems.
- Improved investments in the EU's health data infrastructure and digital health. Despite the pandemic manifesting the potentiality of digital solutions to free up resources and make health systems more resilient, the deployment of digital health tools and infrastructure is still fragmented across the EU. On top of this, the ability to rapidly access real-time and comparable data on how patients and populations are affected by the disease and the effectiveness of different public health measures and treatments is crucial for high-quality analysis and support to the decision-making process. Additionally, in this scenario, it became relevant to invest in the improvement of the EU standardisation process of health data quality, collection and interoperability and to improve and accelerate the creation of a European Health Data Space with a clear governance framework for access to data including for secondary use for research.

According to the above-reported main points, this chapter aims to shed light on scenarios and best practices implemented by the AIOTI members and the need to implement a value-based approach to drive innovation and the EC and European countries' policy-making process.

[8] Health Emergency Preparedness and Response Authority (HERA)https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1522

2.3 Vision Ideal Scenarios Innovation and Technology

Overall, the COVID-19 pandemic has demonstrated the importance of innovation and technology in responding to public health emergencies. IoT solutions can help mitigate the impact of pandemics by improving public health surveillance, enhancing healthcare delivery, and supporting remote work and education, with some scenarios detailed below.

- **Telemedicine and remote health monitoring**: One of the biggest challenges of pandemics is the rapid spread of the disease, which can quickly overwhelm healthcare systems. Telemedicine and remote health monitoring technologies can help mitigate this by enabling doctors and nurses to remotely monitor patients' health, reducing the need for in-person visits and freeing up hospital beds for more severe cases.

- **Contact tracing** is a critical tool for controlling the spread of infectious diseases. IoT technologies, such as wearables and location-tracking devices, can help automate and improve the accuracy of contact tracing efforts, making it easier to identify and isolate potential sources of infection.

- **Smart buildings and infrastructure** technologies can help reduce the risk of transmission by automatically adjusting ventilation systems, monitoring air quality, and controlling access to public spaces. IoT-enabled infrastructure can also improve the efficiency and safety of transportation systems, reducing the risk of transmission for essential workers who need to travel.

- **Remote education and e-learning**: Pandemics can disrupt traditional education systems, but e-learning and remote education technologies can help ensure continuity of education. IoT-enabled platforms can facilitate remote learning, allowing students to access digital resources, collaborate with peers and teachers, and engage in virtual classrooms.

- **Data analytics and forecasting** based on the large amounts of data collected from IoT systems on the spread of infectious diseases, which can be analysed and used to develop predictive models and forecasts. These capabilities can help governments and healthcare systems better prepare for future outbreaks, allocate resources more effectively, and develop targeted interventions.

2.3.1 Adaptation of Smartphones within Europe

In 2020, 81% of people aged 16-74 in the EU used a smartphone for private purposes in the three months before the survey. However, 18% responded that when using or installing an app on the smartphone, they never restricted or refused access to personal data such as their location or contacts. In 6% of the cases, they did not know if it was possible to restrict or refuse access to their data when using or installing an app. The share of people who never restricted or refused such access was highest among the youngest (20% for 16-24 years old) and lowest among the eldest (14% for 65-74 years old).[9]

[9] https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20210506-2

2.3.2 Contact Tracing Apps during the Pandemic

Coronavirus contact-tracing apps were meant to play a significant role in how some countries dealt with the spread of the disease. However, so far, they have had a limited impact. Many IT companies have released tracking applications based on Bluetooth low-energy technology[10]. These programs, however, have several limits; first of all, they must be downloaded by a large percentage of users to be fully useful. Furthermore, they must be made functional: Bluetooth connection must always be on, and the device needs to be connected to the Internet at least once a day to transmit keys to the central server, which can constitute a problem for people over 65 who have poor access to and understanding these procedures. On top of this, there are fundamental issues in centralised or decentralised systems, the influence of powerful Tech firms such as Google and Apple, and privacy and confidentiality concerns/issues; there has also been a behavioural challenge that not much emphasis has been put on.

2.4 Risk Analysis

A risk analysis systematically evaluates the risks and threats associated with implementing and using technology, such as software applications, hardware devices, and network infrastructure. Its main goal is to identify and assess the likelihood and impact of various risks, such as security breaches, system failures, and compliance violations, and develop strategies to mitigate or manage them. A thorough risk analysis typically involves several steps, including asset identification (hardware, software and network components that need to be evaluated), threat identification (such as cyberattacks, data breaches or natural disasters), risk assessment, mitigation and monitoring strategies.

Risk assessment aims at evaluating the likelihood and impact of the identified threats and determining the level of risk associated with each one. Risk mitigation develops and implements strategies to mitigate or manage the identified risks, such as security controls, backup and recovery procedures, or disaster response plans. Finally, risk monitoring and review handle the continuous monitoring of the technology environment for new risks and update the risk management strategies as required.

A technological risk analysis is an essential component of any comprehensive risk management plan, as it helps organisations identify and manage potential risks to their technology assets and ensure the continued availability, integrity, and confidentiality of those assets.

[10] Zastrow M. Coronavirus contact-tracing apps: can they slow the spread of COVID-19? Nature 2020; 10.1038/d41586-020-01514-2.

Table 2: Risk Analysis

Risk Category	Potential Risks	Mitigation Strategies
Privacy and Security	Breach of sensitive data such as health records	Use of encryption and secure protocols for data transmission and storage, implementation of access controls and user authentication
	Unauthorised access to IoT devices and networks	Implementation of strong password policies, regular software updates and patch management, regular security assessments and testing
	Malware and ransomware attacks on IoT devices and networks	Use of security software and firewalls, regular backup and recovery procedures, incident response and disaster recovery plans
Technical	Hardware and software failures	Regular maintenance and monitoring, use of redundant systems and failover mechanisms
	Integration challenges with legacy systems and infrastructure	Use of standard protocols and APIs for interoperability, implementation of testing and validation procedures
	Connectivity issues and network congestion	Use of load balancing and traffic management techniques, implementation of Quality of Service (QoS) policies, use of edge computing and distributed architectures
Ethical	Bias and discrimination in data collection and analysis	Regular review and monitoring of data models and algorithms, implementation of fairness and transparency principles
	Inequitable access to IoT technologies and resources	Promotion of universal access and inclusion, implementation of community engagement and participation strategies
	Misuse of data for surveillance or control purposes	Implementation of clear and transparent data governance policies, adherence to ethical principles and human rights frameworks

2.5 Behavioural and Cultural Challenges

The Behavioural and Cultural Challenges faced by Europe in an era of pandemics can be quite complex and varied, such as:

- **Non-Compliance with Guidelines** may be due to a lack of understanding or trust in the guidelines or cultural or social factors that make it difficult for people to comply.

- **Stigma and Discrimination** against certain groups, such as people of specific nationalities or ethnicities, frontline workers, or people who have contracted the disease, can lead to social isolation and exclusion and make it difficult to contain the spread of the disease.

- **Misinformation and Rumours** can be a significant challenge during a pandemic, leading to confusion and mistrust of public health authorities, making it more difficult to control the disease's spread, and leading to non-compliance with guidelines.

- **Lack of Preparedness** and response planning may be due to a lack of funding or resources or due to cultural attitudes that downplay the severity of the threat.

- **Socioeconomic Factors** can often make the impact of a pandemic felt more severely by certain socioeconomic groups, such as those with lower incomes, in precarious employment, or living in crowded conditions, which can lead to more significant inequalities in health outcomes and exacerbate existing social and economic disparities.

Research indicates why key healthcare stakeholders need to be faster to adopt health IT and leverage opportunities afforded by digital transformation (DT). In particular, the following must be considered for this chapter's purposes.

1) The adoption of health IT is usually resisted by powerful actors in healthcare delivery[11]

2) The resistance stems from various factors such as professional norms [physicians regard tasks aside from patient treatment as administrative nuisances][12]

3) Adverse influence [powerful, tech-averse physicians affect other's use of health IT][13]

4) Threats to professional autonomy (physicians aim to maintain the status and refuse new technology)[14], and

5) Privacy concerns [due to hacked medical devices[15] and absent and opaque app privacy policies[16]].

[11] Bhattacherjee, Anol, and Neset Hikmet. 2007. Physicians' resistance toward healthcare information technology: a theoretical model and empirical test. European Journal of Information Systems 16 (6): 725–737.

[12] Fichman, Robert G., Rajiv Kohli, and Ranjani Krishnan. 2011. Editorial overview—the role of information systems in healthcare: current research and future trends. Information Systems Research 22 (3): 419–428.

[13] Venkatesh, Viswanath, Xiaojun Zhang, and Tracy A. Sykes. 2011. ''Doctors do too little technology'': A longitudinal field study of an electronic healthcare system implementation. Information Systems Research 22 (3): 523–546.

[14] Walter, Zhiping, and Melissa Succi Lopez. 2008. Physician acceptance of information technologies: Role of perceived threat to professional autonomy. Decision Support Systems 46 (1): 206–215.

[15] Meskó, Bertalan, Zsófia Drobni, Éva Bényei, Bence Gergely, and Zsuzsanna Gy}orffy. 2017. Digital health is a cultural transformation of traditional healthcare. Health 3 (38).

[16] Sunyaev, Ali, Tobias Dehling, Patrick L. Taylor, and Kenneth D. Mandl. 2015. Availability and quality of mobile health app privacy policies. Journal of the American Medical Informatics Association 22 (e1): e28–e33.

Additional barriers for organisations to adopt healthcare IT solutions include initial and ongoing costs. Shifting towards the organisational level, the providers need more incentives to implement health IT systems or share their data due to competitive concerns[17]. Such proprietary strategising, however, not only impedes the digital transformation of healthcare means that healthcare providers cannot leverage the total patient data available across systems[18].

Response to public health emergencies requires a change in regular behavioural patterns; therefore, coordination and understanding of communities within different cultures is a prerequisite. Understanding the information ecosystem and communicating with communities will help create sustainable behavioural change since epidemics centre around human behaviour.

2.6 Overview of Data Analysis and Value-Based Healthcare

The global Internet of Things (IoT) in the healthcare market size is expected to experience significant growth by reaching USD 446.52 billion by 2028[19]. This is attributed to the rising focus on active patient-centric care and patient engagement, the rise in high-speed technologies for IoT connectivity, and the rising need for implementing cost-control actions within the healthcare sector. On top of this, the increasing awareness regarding fitness and health is leading to the demand for self-health management techniques, which has surged the demand for several medical wearable devices globally as people can easily access and monitor their health anytime. Moreover, several manufacturers are focusing on introducing advanced monitoring devices to cater to the growing consumer demand. Additionally, the COVID-19 pandemic has caused a change in providers' willingness to implement IoT solutions, which helped diagnose the virus using IoT.

Despite this potentially growing role of AHA-IoT services in the healthcare market, a systemic dimension of innovation still needs to be reached. A value-driven innovation can support decision-makers choices and promote innovation sustainability.

We are increasingly experimenting, both at local and global dimensions, that EVIDENCE of the AHA-IoT services value is needed to help decision-makers adopt innovation to support social and healthcare services sustainability. Limited available resources, the increasing number of older people and the level of demand for chronic diseases management services push decision-makers to choose between the resources they would need to fund all potentially useful interventions (e.g., social or healthcare programmes) and those that are actually in their budgets. It is a fact that, in limited resource settings, the available budget must be allocated as efficiently as possible, and decision-makers are called to make comparisons across alternative uses of the same amount of resources. The achievement of this objective and evaluation of the services' effectiveness level can be supported by a structured process to generate objective EVIDENCE of services' costs-effectiveness.

It is also essential to consider that the healthcare sector's IoT market is highly fragmented. A comprehensive picture of the AHA-IoT services' value and sustainability is needed at the EU level to promote the quality and equity of AHA services around Europe and strengthen the European Digital Market. That is why a shared EVIDENCE generation process is perceived as a critical objective to be pursued, leading to replication and scaling up processes of innovative services.

[17] Ozdemir, Zafer, Jack Barron, and Subhajyoti Bandyopadhyay. 2011. An analysis of the adoption of digital health records under switching costs. Information Systems Research 22 (3): 491–503.

[18] Romanow, Darryl, Sunyoung Cho, and Detmar Straub. 2012. Editor's comments: riding the wave: past trends and future directions for health IT research. MIS Quarterly iii-x.

[19] Internet of Things (IoT) in Healthcare Market Size, Share and COVID-19 Impact Analysis, By Component (Devices, Software, and Services), By Application (Telemedicine, Patient Monitoring, Operations and Workflow Management, Remote Scanning, Sample Management, and Others), By End-User (Laboratory Research, Hospitals, Clinics, and Others), and Regional Forecast, 2021-2028

2.7 Scenarios and Best Cases

The outbreak of COVID-19 has shown that healthcare resources must be prioritised to tackle the pandemic properly and continue carrying out the most urgent interventions from common pathologies. In this line, new medical services should be developed to optimise scarce healthcare resources. Patients' remote assistance and remote monitoring are two services that can be implemented with that objective. In this regard, the AIOTI members represent many different IoT/ICT services.

In particular, this paragraph provides possible IoT and edge computing business-driven scenarios, examples and use cases that can be applied to address the IoT and edge computing high-level challenges and objectives in the health domain; a snapshot of the most relevant is reported here.

TRIALOG (Personalised Decision support system + IAMHappy Smart Health IoT-based Recommender System [well-being recommendation system]).

Use Case: Personalised Health Knowledge Graph

Trialog's current health applications do not adequately consider contextual and personalised knowledge about patients. To design "Personalised Coach for Healthcare" applications to manage chronic diseases, there is a need to create a Personalised Healthcare Knowledge Graph (PHKG) that takes into consideration a patient's health condition (personalised knowledge) and enriches that with contextualised knowledge from environmental sensors and Web of Data (e.g., symptoms and treatments for diseases). To develop PHKG, aggregating knowledge from various heterogeneous sources such as the Internet of Things (IoT) devices, clinical notes, and Electronic Medical Records (EMRs) is necessary. This paper explains the challenges of collecting, managing, analysing, and integrating patients' health data from various sources to synthesise and deduce meaningful information embodying the vision of the Data, Information, Knowledge, and Wisdom (DIKW) pyramid. Furthermore, it promotes a solution that combines: 1) IoT data analytics and 2) explicit knowledge, illustrated using three chronic disease use cases on users – asthma, obesity, and Parkinson's[20] - for more accurate diagnostics, preventive health and better doctor assistance. The stakeholders were patients and doctors (paediatric specialists in both the pulmonary and sleep departments), the main facilitators encountered in the service's implementation. In contrast, the main barriers to the service's implementation were data accessibility and interlinking datasets from heterogeneous sources.

Use Case: IAMHappy

Smart Health IoT-based Recommender System. Healthy lifestyles, fitness, and diet habits have become central applications in our daily lives. Positive psychology, such as well-being and happiness, is the ultimate dream of everyday people's feelings (even without awareness). Wearable devices are being increasingly employed to support well-being and fitness. Those devices produce physiological signals that machines analyse to understand emotions and physical states. The Internet of Things (IoT) technology connects (wearable) devices to the Internet to easily access and process data, even using Web technologies (aka Web of Things).

We design IAMHAPPY, an innovative IoT-based well-being recommendation system, to encourage everyday people's happiness. The system helps people deal with day-to-day discomforts (e.g., minor symptoms such as headache and fever) by using home remedies and related alternative medicines (e.g., naturopathy, aromatherapy), activities to reduce stress, among others.

A web-based knowledge repository for emotion was developed to focus on happiness and well-being by helping analyse data produced by IoT devices to understand users' emotions and health. The semantics-based knowledge repository is integrated with a rule-based engine to suggest recommendations to achieve happiness in the quotidian. The naturopathy application scenario supports recommendation system[21] on users for preventive health and improved well-being. The stakeholders involved were users willing to boost their immune systems during the COVID-19 pandemic; the main barriers encountered in the service's implementation have been accessibility to data, interlinking datasets from heterogeneous sources, and retrieving and citing scientific knowledge from unstructured knowledge (scientific publications, websites, books, among others) to prove facts.

[20]Personalized Health Knowledge Graph [Gyrard et al. 2018] https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=1005andcontext=aii_fac_pubImpact

[21] IAMHAPPY: Towards an IoT knowledge-based cross-domain well-being recommendation system for everyday happiness [Gyrard et al. 2021 Elsevier Smart Health Journal] https://corescholar.libraries.wright.edu/cgi/viewcontent.cgi?article=2541andcontext=knoesisImpact

Bi-rex: Big Data Innovation and Research Excellence | HomeEmo - Home dialysis
Partners: MISTER Smart Innovation, Tecnoideal, MEDICA SpA | Experience's duration: 2019-2022 |Experience's funding source/s – procurer: Emilia-Romagna Region local funding through "LR 14/2014" – 2019 Call

Home dialysis, and therefore relocated from hospital centres, is for all companies in the Healthcare sector an essential line of research. Its advantages are many:

- Greater comfort for patients: they are often older people who suffer from home/hospital travel.
- According to many studies, home dialysis, possibly being carried out over a long time, has greater effectiveness.
- Being more effective, patients treated with home dialysis need less medication.
- The healthcare company saves both the costs of transporting the patient and the number of drugs administered to him.

Nowadays, technical difficulties remain, thus strongly limiting the spread of this kind of method. They can be summarised in three categories:

1. Disinfection management. Traditional hospital machines have internal hydraulic circuits that must be disinfected after each treatment to avoid bacterial proliferation, which is dangerous for the patient. The cleaning and disinfection operation is difficult to manage at home, both for problems related to the supply of disinfectants and the operation itself.
2. Patient safety. As no nursing specialised staff is present, the machine must be able to identify more potentially critical situations than the hospital ones, directly analysing fluids (blood and dialysate) with in-line sensors.
3. Treatment control. The caregiver cannot properly conduct treatment verification and machine supervision at home. To avoid that, specialised personnel have to move periodically to check the machine; it is necessary not only to have a direct remote connection with it, independent of the patient's home, but also that the machine can report in advance any technical or clinical criticalities self-learning thanks to its integrated sensors.

HomeEmo intends to solve the mentioned problems. Regarding the problem of disinfection, it is intended to radically change course developing the components and sensors necessary to carry out home dialysis with a new generation of disposable hydraulic circuits; regarding *patient safety*, we will develop a series of optical sensors based on spectrometric analysis, able to monitor different parameters of both blood and dialysate. In particular: haematocrit, saturation, and pH in the blood; haemoglobin (for identifying any haemolysis) and urea in the dialysate. Finally, to remote control the machine, we will develop a Machine Learning technology that, working on the large amount of data acquired, can provide accurate evaluations of therapies progress according to the treatment parameters.

This functionality will be beneficial to manage the Post Marketing Clinical Follow Up, i.e. monitoring and evaluation activities of medical devices' clinical performance that will become fundamental with the adoption of the new European regulation MDR 2017/745 in force since the end of May 2020.

- Outcomes of the experience: The optical sensors developed within the project will be applied in the home dialysis machine and also on many other devices already produced by Tecnoideal for the Medica group. The ability to obtain clinically relevant information from the large amount of data saved by a machine can also be used on different devices already produced by Tecnoideal, i.e., those that treat chronic patients, for whom it is important to analyse the progress of treatments over time. Finally, the home dialysis machine would constitute a unique device on the market. Tecnoideal and the Medica group also intend to enhance this new asset through an industrial partnership to perform the necessary clinical validations preparatory to marketing.

- Experience's implemented exploitation and eventual next steps: With the new sensors on board, it is expected to gain significant market share for devices for CRRT and Apheresis, for which it is expected to double the current turnover, of c.ca 3 M€, within a couple of years.

The introduction of the urea sensor and the dual hematocrit sensor on chronic dialysis machines should allow the Devices of the Medical Group to enter a market otherwise saturated and well-manned by multinationals. With the unique characteristics mentioned above, it is expected to produce a thousand machines annually within three years. As mentioned, the home dialysis machine will need a short clinical verification before the market accepts it. It will take about two years after the project's end to start selling the first machines.

INFN Laboratory for Technology Transfer (National Institute of Nuclear Physics-Bologna)

1. **A secure cloud-edges computing architecture for metagenomics analysis**

Partners: INFN, CNR, Genova University | Experience's duration: 2 years| Experience's funding source/s – procurer: Local funding

2. **Smart city Active ageing**

Partners: INFN TTLab. Unibo DEI, BiRex Pilot Plant |Experience's duration: 1 year | Experience's funding source/s – procurer: Local funding

3. **Healthcare: Smart and remote control**

Partners: INFN TTLab. Unibo DEI, BiRex Pilot Plant |Experience's duration: 1 year | Experience's funding source/s – procurer: Local funding

1. A secure cloud-edge computing architecture for metagenomics analysis

Portable sequencing machines, such as the Oxford Nanopore MinION, are making genome sequencing ubiquitous. Consequently, metagenomic studies are becoming increasingly popular, yielding important insights into microbial communities covering diverse environments, from terrestrial to aquatic ecosystems. Furthermore, the adoption of low-power IoT computing devices represents a feasible way of distributing and managing those machines on the field. However, a key issue is represented by the huge amount of data produced during operations, whose management is challenging considering the resources required for efficient data transfer and processing.

This experience proposes a novel architecture combining Edge and Cloud computing paradigms to address such challenges. The focus of the experience is the Edge layer, responsible for the dynamic management of the full analysis pipeline of IoT devices producing large datasets like the MinION ones while adopting proper security mechanisms that handle the authentication of on-field devices and the confidentiality of the transmitted data. The key aspect is that the Edge computing environment allows splitting the analysis workflow between the data source and the Cloud infrastructure. Once the sequencing information is pre-processed at the edge of the infrastructure, a Cloud-based IoT platform, such as the one provided by Thingsboard, can collate data, trigger alarms or identify and maintain set points through machine learning techniques.

In this experience, the team designed the general Edge-Cloud architecture and a prototype implementation integrated with the INFN Cloud infrastructure, specifically focusing on access security. Specifically, we carried out some preliminary experiments that confirm that the approach is promising both from the performance and the security point of view.

A key result is that the proposed architecture has broad relevance because it represents a composable, open-source and reusable solution addressing the problem of managing networks of IoT devices through custom-built services producing large datasets in different operative conditions and for heterogeneous sets of use cases.

2. Smart City Active ageing

This experience produced a full data collection workflow from a laser sensor connected to a mobile application, working as an edge device, which transmits the data to a Cloud platform for analysing and processing data.

The app was developed to receive data from electronic boards controlling IoT sensors via the Bluetooth Low Energy protocol, sending it to an IoT Cloud endpoint of the INFN Cloud infrastructure based on the Thingsboard solution via the MQTT(S) communication protocol. Several functions are implemented in this application, such as BLE device scanning, secure connections, multiple authentication methods, and data transfer via MQTT.

The IoT Cloud endpoint is fully customisable for multiple use cases, connecting to other services of the INFN Cloud infrastructure, such as solutions for stream processing based on Kafka, Big Data analytics processing based on Spark, and visualisation and selection based on Grafana and Elasticsearch.

3. Healthcare: Smart and remote control

This experience analysed Edge controlled/assisted systems with Multi-access Edge Computing based approach O-RAN (Transforming the Radio Access Networks Industry Towards Open, Intelligent, Virtualized and Fully Interoperable RAN).

The main outcome of the experience is an intelligent edge-pervasive service through which users can get real-time, personalised assistance and experiences. The service fills the need for automatic real-time optimisation of heterogeneous resources and fast configurations, optimally selecting network functions and AI techniques.

Regarding the exploitation and further development, processing a large amount of data can benefit from using MEC (multi-access edge computing) instead of uploading data to the cloud, which could cause additional round-trip delays. Low latency is a key requirement in this experience.

The proposed use cases consisted of implementing these three services in a controlled but real pilot to validate the obtained improvements and measure the better use of healthcare resources. The two services, patient remote assistance and remote monitoring, enable remote homecare and monitoring channels to communicate between patients and doctors. Remote monitoring and assistance services allow data collection from connected medical devices at home (scale, tensiometer pulse oximeter, thermometer, activity wristband, among others), register the data in a Health Platform, and the doctors consult the patient's information and contact them if necessary.

3. Natural Disasters

Disasters are a mixture of threats, threat factors and inadequate capability or risk-reduction measures. Disasters, primarily caused by natural hazards, are not the greatest threat to humankind. A hazard becomes a disaster when it coincides with a vulnerable situation when societies or communities cannot cope with their resources and capacities. A hazard is a physical event, phenomenon or human activity that can cause loss of life or injury, damage to property, social and economic disruption or degradation of the environment. Hazards have various origins: natural (geological, hydro, meteorological, and biological) or human (environmental or technological) actions. Risk is the probability of adverse effects or predicted losses (deaths, accidents, properties, livelihoods, disrupted economic activity or damaged environment) arising from interactions between natural or manufactured hazards and vulnerable populations. Climate change will create new hazards, such as the melting of glaciers, sea level rise, and extreme weather in proportions never seen before. A natural disaster is a natural event that overwhelms local resources and threatens the community's function and safety. Disasters are hard to plan and anticipate since they are innately different from common emergencies.[22]

Figure 3: ***Floods reported in Europe***

The United Nations defines a disaster as "the occurrence of sudden or major misfortune which disrupts the basic fabric and normal functioning of the society or community".

[22] Study and Exposure to Natural's Disaster for World Cities (IJSRD, 11.2021). Retrieved on 30 November 2021 from: IJSRD - International Journal for Scientific Research and Development | Vol. 8, Issue 11, 2021 | ISSN (online): 2321-0613

Disaster Management and IoT

The first 72 hours of a disaster's aftermath are crucial. Disaster management is coping with natural and human-caused disasters and preventing them. It involves preparation, response and recovery to minimise the impact of disasters. IoT helps to improve response, minimises risks, and can transform disaster management from a reactive approach to a proactive one thanks to the data generated by these devices. IoT enables our prediction and early warning systems to improve our response and preparedness systems. According to the Global Disaster Preparedness Center[23], emergency management has four phases: Mitigation, Preparedness, Response, and Recovery. In summary, the four stages with the combinatorial value in which IoT devices (can) play a crucial role:

Mitigation: Minimising the effects of disaster, such as implementing building zoning and codes, public education and vulnerability analyses. IoT devices and sensors can collect near-real-time data on barometric readings, water levels, and volcanic activity to detect cloudbursts, earthquakes, volcanic activities, tornadoes, and wildfires and send early warnings. Critical infrastructure can be protected through predictive maintenance. Sensors to monitor pollutants and contaminants, including radioactive situations, enable hazard mitigation.

Preparedness: Preparing response, including emergency exercises, early warning systems, training and preparedness plans. Real-time data from sensors, cameras and other connected devices can be embedded into infrastructure, allowing city managers to prioritise repairs and employ preventive maintenance. Connected devices deployed in bridges, roads, and buildings and other infrastructure can also provide alerts and enhance communications. IoT devices can monitor the strategic reserves of water, food, clothing, medical equipment and other vital supplies to ensure acceptable levels.

Response: Minimise hazards created by disasters, such as emergency relief and search and rescue. IoT can facilitate response planning and actions through sensors to monitor key personnel's movement, sensors, and smart clothing. First responders can also be equipped with audio and video sensors supported by autonomous drones and vehicles, allowing dangerous situations to be monitored and assessed from a safe distance. In the meantime, IoT can help people know where to find a safe location or life-saving supplies. Connected digital signs, such as bus stops on roadways, can also spread critical information quickly. Battery-powered IoT devices can enable limited communications services such as emergency micro-messaging.

Recovery: Return the community to normal through medical care, temporary housing, restoration of communication, and disbursement of assistance in cash or kind. IoT devices can help rescue and search operations and monitor post-disaster conditions, with vital infrastructure and continuous flow of information and disseminate information to the public. At the same time, normal communications are still being repaired.

Disaster management can be described as coordinating and managing resources and responsibilities to deal with all humanitarian aspects of emergencies, particularly preparedness, response and recovery to mitigate the impact of disasters. A disaster is an event or series of events resulting in casualties and destruction or loss of property, facilities, climate, critical services or livelihoods on such a scale beyond the usual capacity of the community concerned. Such disasters include floods, hurricanes, earthquakes and volcanic eruptions, which can have immediate effects on human health, as well as secondary impacts causing more death and destruction from floods causing landslides, earthquakes resulting in explosions, tsunamis causing severe flooding and typhoons sinking ferries. Such emergencies involve technology or manufacturing, typically involving hazardous material, which occurs where these materials are made, used or transported.

3.1 Overview of the current State of Play

[23] Global Disaster Preparedness Center. Home - PrepareCenter

Nowadays, critical assets face numerous threats that can compromise their safety and lead to unforeseen disasters with significant impacts. The proactive management of natural disasters and extreme climatic conditions are considered to be the resilience of critical infrastructure and societal functions[24]. Europe is highly and particularly vulnerable to natural disasters due to its geographical location, climate, and topography, whose current state of play can be described as follows:

- **Increasing frequency and intensity** of natural disasters such as floods, wildfires, droughts, and storms are becoming more frequent and intense in Europe due to climate change, resulting in an increased risk of loss of life, property damage, and economic losses. This increase amplifies the risk for critical assets, which is also evident by recent projections that the extreme flooding events in Europe are expected to increase substantially by 2050[25], with a major impact on deteriorating structures.

- **Ageing infrastructure** that has exceeded its design lifespan and faces major deterioration issues[26]. The outdated design of these critical assets constructed in a different era indicates that infrastructure is not expected to withstand natural disasters and extreme environmental conditions.

- **Varied impact** across Europe, with some regions being more vulnerable than others. For example, Southern Europe is more vulnerable to wildfires, while Northern Europe is more vulnerable to flooding. Cascading effects and systemic risks can trigger even minor incidents, causing significant disruption to other assets and human and financial losses.

- **Improved disaster management**: European countries have significantly improved their capabilities in recent years, enhancing early warning systems, developing disaster risk reduction plans, and improving emergency response and recovery.

- **Cooperation and solidarity**: EU has established a framework for cooperation and solidarity among member states to manage natural disasters better. The Civil Protection Mechanism allows member states to request and provide assistance during emergencies, such as natural disasters.

- **Continued challenges** still need to be addressed, despite the improvements in disaster management. Some examples are the improvement of the resilience of critical infrastructure, addressing socioeconomic inequalities that contribute to vulnerability, and developing effective long-term strategies for climate adaptation.

Even though many devices exist to monitor hazard evolution and impact on critical assets, the capability to connect the majority of sensors and actuators to provide a large-scale assessment based on the computation of data at every level and asset has not been satisfactorily exploited.

[24] Koursari, E., Wallace, S., Valyrakis M., and Michalis P. (2019). The need for real time and robust sensing of infrastructure risk due to extreme hydrologic events. 2019 UK/China Emerging Technologies (UCET), Glasgow, United Kingdom, 2019, 1–3. doi: 10.1109/UCET.2019.8881865

[25] Jongman, B.; Hochrainer-Stigler, S.; Feyen, L.; Aerts, J.C.J.H.; Mechler, R.; Botzen, W.J.W.; Bouwer, L.M.; Pflug, G.; Rojas, R.; Ward, P.J. (2014). Increasing stress on disaster risk finance due to large floods. Nat. Clim. Chang., 4, 264–268.

[26] Michalis, P., Sentenac, P. (2021) Subsurface condition assessment of critical dam infrastructure with non-invasive geophysical sensing. Environ Earth Sci 80, 556 (2021). https://doi.org/10.1007/s12665-021-09841-x

3.2 Research Challenges and Objectives

The sudden nature of many natural hazards indicates that, in most cases, they can proactively compromise the ability to respond to such threats with disastrous consequences. Reliable methods to evaluate natural hazards and deteriorating factors are important for the efficient and proactive management of critical assets[27]. Despite the recent advances in developing and applying IoT systems, critical infrastructure is still considered to be managed traditionally. For example, this process involves on-site engineers making decisions based on their skills and experience, mostly using paper-based analytics. At the same time, the existing sensing devices do not exploit the interoperability aspects to deliver better services that optimise the operation and maintenance of critical systems. The European Union (EU) has identified research challenges and objectives for natural hazards to improve its disaster risk management and resilience:

- Improve the EU's understanding of natural hazards, including their frequency, intensity, and impact, as well as their interactions with human and built environments.
- The EU aims to improve its early warning systems to provide accurate and timely information to decision-makers and the public to reduce the risk of disasters.
- Develop better risk assessment and mapping tools to identify and prioritise areas most vulnerable to natural hazards.
- The EU aims to improve its disaster response and recovery capabilities by enhancing stakeholder communication, coordination, and cooperation.
- Develop effective strategies to adapt to the impacts of climate change, which are expected to exacerbate the frequency and intensity of natural hazards.
- The EU aims to promote the development of innovative technologies and solutions that can improve disaster risk management and resilience, such as remote sensing, artificial intelligence, and blockchain.
- Finally, socioeconomic factors contributing to vulnerability to natural hazards, such as poverty, inequality, and inadequate infrastructure, are targets to address.

One of the main challenges is that there are still several uncertainties about the real-time evolution of natural and climatic hazards. This challenge is because most IoT applications provide limited and scarce information, mainly focused on assessing the safety of single assets. The numerous existing sensing solutions also do not have interoperability characteristics. Therefore asset owners do not take full advantage of existing technological developments with advanced prediction capabilities and the potential to incorporate all critical information into one management platform. The latter is expected to enhance decision-making in the different disaster management phases, considering the dynamics derived from the infrastructure system perspective.

[27] Pytharouli, S.; Michalis, P.; Raftopoulos, S. (2019). From Theory to Field Evidence: Observations on the Evolution of the Settlements of an Earthfill Dam, over Long Time Scales. Infrastructures, 4, 65. https://doi.org/10.3390/infrastructures4040065

3.3 Vision Ideal Scenarios Innovation and Tech

Earthquakes, storms, heat waves and floods have been leading causes of death from natural disasters during the past year, affecting all regions worldwide. The most recent figures show that natural disasters caused losses of $131.7 billion in 2018[28] and affected millions worldwide. While Mother Nature is unpredictable, several technologies promise to help with forecasting and prevention and allow responders to act sooner rather than later:

1. The development of smart and resilient infrastructure can help to minimise the impact of natural hazards by incorporating advanced monitoring systems, remote sensing, and other technologies that can detect and respond to hazards in real-time.

2. Next generation forecasting and early warning systems can help to predict and prevent the impact of natural hazards, which can be achieved by integrating data from multiple sources, including remote sensing, social media, and citizen science.

3. Using data analytics and modelling can help improve risk assessment and mapping, allowing decision-makers to understand the impact of natural hazards and develop effective disaster management strategies.

4. The development of climate-resilient agriculture can help address the impact of natural hazards on food security through precision agriculture technologies, such as sensors, drones, and artificial intelligence.

5. Innovative risk financing solutions can help mitigate natural hazards' economic impact, achieved through insurance products, catastrophe bonds, and other financial instruments that can provide rapid and flexible funding in the event of a disaster.

6. Developing citizen engagement and social innovation can help build community resilience through social media, crowdsourcing, and other technologies that facilitate communication, collaboration, and community-driven solutions.

Overall, these ideal scenarios for innovation and technology can help to address the challenges of natural hazards in Europe by enhancing disaster risk management and resilience and promoting sustainable and climate-resilient development. With technological advancements such as Artificial Intelligence and Machine Learning making it easier for scientists to process and interpret a large amount of data, weather prediction and its impact on populations can now be better addressed. Different technological solutions may apply when analysing each natural disaster as a single one.

- **Landslides and Earthquakes:** Predictive solutions for earthquakes now use artificial intelligence and machine learning, technologies capable of processing and interpreting large data. A recent solution developed by experts at Cornell University[29] can better forecast so-called "slow-slip earthquakes," a type of tectonic motion of much lower intensity that can last hours or days. While prediction is a tricky word for those studying seismology, advancements in artificial intelligence may help scientists find patterns otherwise impossible to track.

[28] https://www.usnews.com/news/best-countries/slideshows/technology-can-save-the-world-from-natural-disasters

[29] https://arxiv.org/abs/1909.06787

- **Storms:** Weather prediction currently does not rely on new technology -- if anything, it uses rather old technology, such as radars that were first used in World War II. Despite the rather conservative methods of collecting data, innovation may improve forecasting. Advances in artificial intelligence promise to allow for a larger quantity of weather data to be analysed faster, more accurately and in greater detail, making weather predicting outcomes more accurate. At the same time, only sophisticated algorithms such as efficient and intelligent signal and image processing, quality control mechanisms, pattern recognition, data fusion (combining diverse streams of observations), data assimilation, or mapping will soon be able to handle in-depth analyses of data from multiple domains, such as geophysics, the atmosphere, the ocean, and the biosphere.

- **Extreme Temperatures:** Forecasting models use complex algorithms to assess upcoming heat waves' onset, duration and demise. According to a study conducted in India[30], predicting heat waves is becoming increasingly important worldwide, as their frequency is growing and the losses they bring are overarching. Heat waves cause the loss of human lives but also cause health issues, increase economic spending, and affect agricultural production, energy and infrastructure.

- **Floods:** Floods caused by natural causes, such as increased rainfall or storms, can also be predicted with sophisticated technological models. Artificial intelligence can help technologists better interpret a growing amount of data and create forecasting models that automatically alert authorities.

- **Epidemics:** Several methods are currently used to forecast the spread of particular emerging epidemics. Forecasting models can identify hot spots of emerging diseases and predict trends regarding where the problem will most likely expand.

3.4 Risk Analysis

A business impact analysis (BIA) determines the potential impacts of interrupting time-sensitive or critical business processes. There are numerous hazards; depending on their timing, magnitude and location, many possible scenarios could unfold for each hazard. Therefore, BIA is presented as a qualitative or quantitative approach to determine the nature and extent of disaster risk by analysing potential hazards and evaluating existing conditions of exposure and vulnerability that together could harm people, property, services, livelihoods and the environment on which they depend.

There are many "assets" at risk from hazards. Hazard scenarios that cause significant injuries should be highlighted to ensure appropriate emergency plans are in place. The potential for environmental impact and an incident's impact on customer relationships, community, and other stakeholders should also be considered.

As the risk assessment is conducted, the focus is on weaknesses that make an asset more susceptible to damage from a hazard. Vulnerabilities include deficiencies in building construction, process systems, security, protection systems and loss prevention programs. They contribute to the severity of damage when an incident occurs.

For example, a building without a fire sprinkler system could burn to the ground, while a properly designed, installed and maintained fire sprinkler system would suffer minor fire damage. Finally, the impacts of hazards can be reduced by investing in mitigation. Creating a mitigation strategy should be a high priority if there is a potential for significant impacts.

3.5 Behavioural and Cultural Challenges

[30] https://www.nature.com/articles/s41598-019-45430-6

Climate change and environmental degradation contribute to the frequency and intensity of natural hazards, posing new challenges for disaster risk management and resilience. Addressing these issues requires collective action and behavioural change at the societal level. Many European individuals and communities lack awareness of the risks and impacts of natural hazards. They are not adequately prepared to respond to disasters, leading to a lack of readiness, inadequate response, and increased vulnerability.

Effective risk communication is crucial to help individuals and communities understand the risks associated with natural hazards and to encourage appropriate behaviours. However, risk perception can be influenced by factors such as culture, beliefs, and values, making it difficult to communicate risk effectively.

Social inequalities and vulnerabilities, such as poverty, lack of access to healthcare, and inadequate infrastructure, can exacerbate the impact of natural hazards on certain populations, particularly those already marginalised or disadvantaged. Furthermore, trust in authorities and institutions is important for effective disaster risk management, as it can affect the willingness of individuals and communities to follow guidelines and take action. However, trust can be eroded by past experiences, political factors, and misinformation.

In response to the UN Environment Programme (UNEP), the Adaptation Gap Report 2021 urgently outlines the need to step up efforts to adapt to climate change. It is encouraging to see the rise of stakeholder engagement during the COVID-19 pandemic in the development and adaptation plans/measures, which is critical for the change required to tackle climate risks and increase resilience effectively. Nevertheless, whereas Technology Transfer is being mentioned in the report, the emphasis on Behavioural Change has not, although the latest is crucial and central to adaptation.

3.6 Overview of Data Analysis

An overview analysis of data and IoT solutions can play a crucial role in helping Europe tackle the challenges of natural hazards:

1. The use of data analytics and modelling can help decision-makers better understand the risks and impact of natural hazards, allowing for more informed and effective decision-making, which can include risk assessment, early warning systems, and disaster response planning.

2. Real-time monitoring and response IoT solutions, such as sensors and remote sensing technologies, can provide real-time data on natural hazards, allowing for quick and effective responses. These include monitoring floods, landslides, and earthquakes and tracking the movement of natural hazards such as hurricanes.

3. IoT solutions can help to improve communication and coordination among different stakeholders involved in disaster response, including emergency responders, government agencies, and citizens. This solution can include using social media and other communication technologies to disseminate information and coordinate response efforts.

4. Infrastructure can become more resilient with IoT to withstand the impact of natural hazards better by including sensors to monitor the structural integrity of buildings, bridges, and other infrastructure and using advanced materials and construction techniques.

5. Data and IoT solutions can also help Europe adapt to the impacts of climate change, which are likely to increase the frequency and severity of natural hazards, via monitoring changes in weather patterns and sea levels, as well as developing new technologies to mitigate the impact of climate change.

Overall, data and IoT solutions can help Europe to build resilience to natural hazards by improving decision-making, response, and communication, as well as developing resilient infrastructure and adapting to the impacts of climate change. However, it is important to note that effectively using these solutions requires addressing the behavioural and cultural challenges that can affect their adoption and implementation.

3.7 Scenarios and Best Cases

Cross-domain Emergency Managing and Planning about Hazard Crisis data integration using ontologies

Partners: Manas Gaur, Saeedeh Shekarpour, Amelie Gyrard, Amit Sheth. empathi: An ontology for Emergency Managing and Planning about Hazard Crisis. International Conference on Semantic Computing Conference (ICSC) 2019.

In the domain of emergency management during hazard crises, having sufficient situational awareness information is critical. It requires capturing and integrating information from sources such as satellite images, local sensors and social media content generated by local people. A bold obstacle to capturing, representing and integrating such heterogeneous and diverse information is the lack of a formal ontology which properly conceptualises this domain and aggregates and unifies datasets. Thus, in this paper, we introduce the empathy ontology, which conceptualises the core concepts concerning the domain of emergency management and planning of hazard crises. Although empathy has a coarse-grained view, it considers the concepts and relations essential in this domain.

SPADE: multi-purpoSe Physical-cyber Agri-forest Drones Ecosystem for governance and environmental observation

Partners: Trialog, AnySolution. More information: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/org-details/999999999/project/101060778/program/43108390/details

The strategic objective of SPADE is to develop an Intelligent Ecosystem to address the multiple purposes concept in the light of deploying UAVs to promote sustainable digital services for the benefit of a large scope of various end users in the sectors of agriculture, forestry, and livestock, including individual UAV usability, UAV type applicability (e.g., swarm, collaborative, autonomous, tethered), UAV governance models availability and trustworthiness. Multi-purposes will be further determined in the sensing dataspace reusability based on trained AI/ML models. These will enable sustainability and resilience of the overall life cycle of developing, setting up, offering, providing, testing, validating, and refining, as well as enhancing digital transformations and 'innovation building' services in Forestry, Cropping and Livestock Farming. Pilot prototypes will contribute towards greater challenges such as deforestation, precision cropping and animal welfare. First, SPADE will create a digital platform that can realise the potential benefits of using drones. This platform is making drone operations better accessible and controllable and providing a service channel for value-added services enabled by drones. Second, SPADE demonstrates three innovative use cases of drones using the digital platform. While demonstrating the use cases, the benefits coming from the use of drones are analysed and quantified on a detailed stakeholder-level basis. The project use cases will demonstrate the new business opportunities, and the demonstrations/pilots will also serve as an analysis platform to investigate the regulatory framework at an international and national level.

SEP: Smart Event Processor - a framework that combines real-time data from different sources, correlating them and concluding on the existence of an event (alarm), activating a rapid response from the reaction mechanisms.

Partners: Ubiwhere

Cities need strong and resilient critical infrastructure to adapt to natural and human-made catastrophes, as these are dynamic and evolving realities that require systematic monitoring. Municipalities have many sensors capable of signalling the existence of an irregularity: air quality stations, CCTV cameras, and fire-fighting systems, among others. However, without interoperability between these systems and the emergency systems, the necessary responses will not be activated to inform about the urgency of moving firefighting teams to put out the fire and paramedics to rescue the victims and take them to the hospital. The Smart Event Processor provides a rule-based alarms' layer to monitor data from IoT systems in a city ecosystem. It allows the combination of data in a given event to activate the response mechanisms in an agile and reliable way. It is of key value in scenarios where the provision of rapid response is fundamental, particularly in Security and Civil Protection.

The Smart Event Processor is deployed on the network edge close to where the raw data is generated. This component processes large amounts of raw data, generating complex events and transferring them to a third-party control application running in the cloud. The amount of data transferred to the cloud/core of the network is highly reduced, improving the real-time processing performance of the whole system.

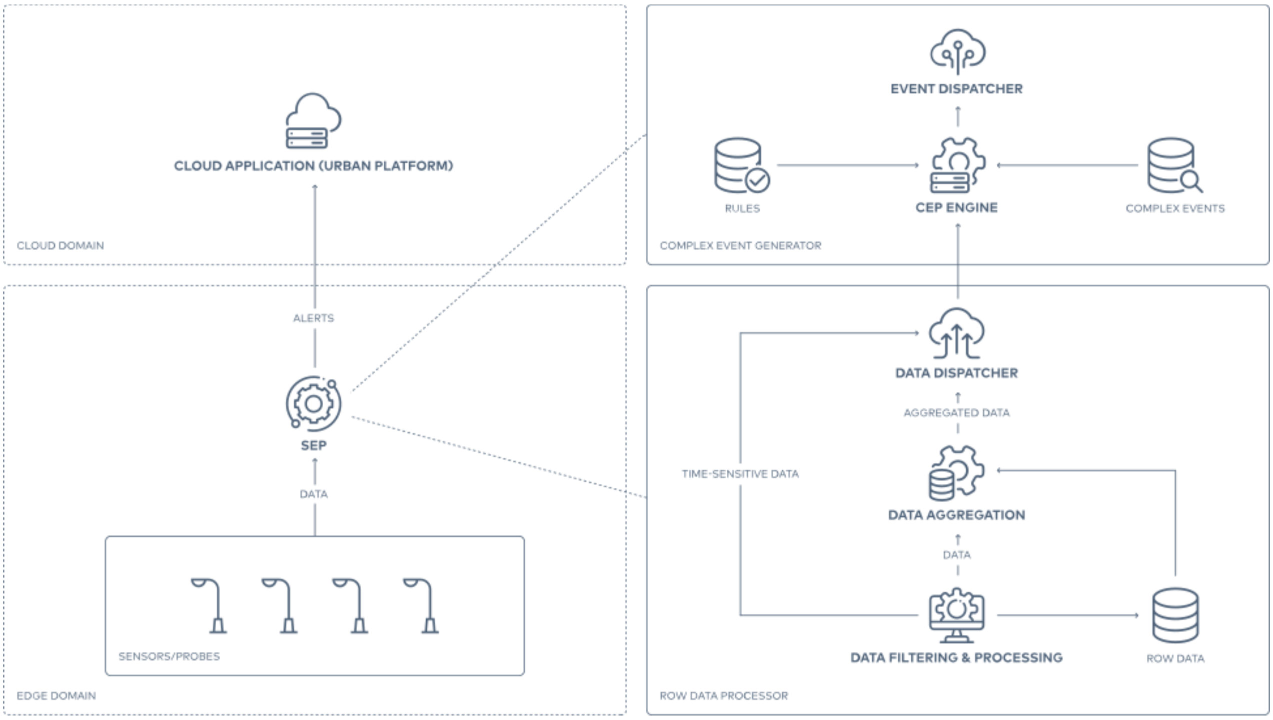


Figure 4: SEP: Smart Event Processor overview

Raw data processor

First, the sensing data provided by the sensing devices are pre-processed, filtered and stored in a database. Some types of data are time-sensitive, e.g. data from accelerometers capable of detecting earthquakes. Other data types that are more delay tolerant are processed by the data aggregation submodule and later dispatched when a configurable amount of data or elapsed time is reached.

Complex event generator

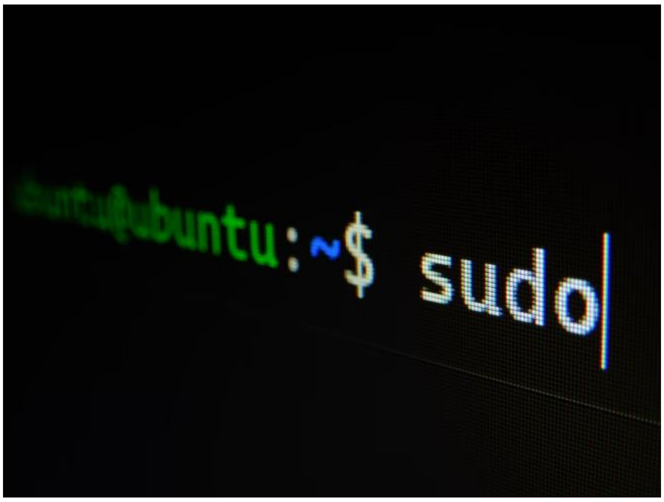
Is implemented based on a Complex Event Processing (CEP) rule engine. The data received from the raw data processor will be matched with rules in the rule database. If the matching is successful, complex events will be inferred and generated to send to the upper application. In some cases, the CEP engine also analyses previously generated complex events (history) to infer certain events more accurately.

4. Cybersecurity take on Crisis Management

Cybercriminals, who are becoming increasingly sophisticated, could take advantage of natural disasters such as hurricanes, wildfires and tornadoes to wreak havoc on critical infrastructures, experts say, including transportation, emergency response, water and sewer systems and hospitals.

4.1 Overview of the current State of Play

Natural disasters can strike anytime and often without warning. For small- and medium-sized businesses (SMBs), the aftermath of a natural disaster can be devastating regarding property damage and data loss. Most businesses face unique cybersecurity challenges when hit by natural disasters. With damaged or destroyed infrastructure, power outages, and limited resources, all businesses, especially SMBs, must be prepared to protect their data and systems from cyberattacks. By taking proactive measures to bolster their cybersecurity posture, these businesses try to ensure that they can weather the storm - literally and figuratively.



```
ubuntu@ubuntu:~$ sudo
```

Figure 5: *"sudo" stands for "superuser do", to execute commands with superuser privileges in Linux bash terminal (WSL).*

After a natural disaster strikes, organisations often scramble to restore critical business functions. This can leave them vulnerable to cyberattacks from opportunistic criminals who seek to take advantage of the chaos. Some of the most common cybersecurity threats businesses face in the aftermath of a natural disaster include:

Phishing attacks: Phishing attacks are one of the most common types of cyberattacks, and they can be particularly devastating in the wake of a natural disaster. With employees working remotely and using personal devices to access corporate data, companies must have stringent anti-phishing measures.

Ransomware attacks: Ransomware is malware that encrypts a victim's files and demands a ransom be paid for the files to be decrypted. Ransomware attacks can be particularly damaging to an organisation, as they may not have the resources or backup systems to recover from an attack.

Data breaches: In the aftermath of a natural disaster, many organisations experience severe breaches due to damaged or destroyed infrastructure, power outages, or employee errors. To protect against data breaches, implement comprehensive security solutions such as firewalls, intrusion detection/prevention systems, and data loss prevention solutions. Companies should also have strict policies and procedures for managing data backups and recovery.

4.2 Research Challenges and Objectives

There are several steps that a business can take to mitigate the cybersecurity threats they face in the aftermath of a natural disaster. These steps include:

1. A business continuity plan:

Creating a business continuity plan is a significant first step to protecting your company data. As seen before, comprehensive business continuity plans that include security solutions such as firewalls, intrusion detection/prevention systems, encryption and data loss prevention solutions are essential for protecting against data breaches. This plan should outline how the business will continue to operate in the event of a natural disaster. It should include information on backup locations for critical data, alternative means of communication, and steps for rebuilding the physical infrastructure.

Firewalls: A firewall is a software or hardware-based system that filters traffic between two or more networks. It can block incoming or outgoing traffic from unauthorised sources to unauthorised destinations. Firewalls can be either network-based or host-based. Network-based firewalls are typically used to protect an entire network, while host-based firewalls are installed on individual computers or servers.

Intrusion Detection/Prevention Systems: An intrusion detection system (IDS) monitors network traffic for signs of suspicious activity or attempts to access unauthorised resources. An intrusion prevention system (IPS) goes one step further by blocking traffic that meets certain criteria. IDS/IPS systems can be either network-based or host-based.

Encryption: Encryption is a process of transforming readable data into an unreadable format using a key. This prevents unauthorised individuals from accessing the data. Encryption can be used for both storage and communication purposes. When encrypting data at rest (i.e., stored on a server), it is important to use a strong encryption algorithm such as AES256. For data in transit (i.e., being sent over a network), SSL/TLS encryption should be used.

2. A robust backup solution:

A robust backup solution should be one of the most important components of a business continuity plan. A robust backup and recovery plan is crucial for recovering from a ransomware attack or other types of data loss. This solution should be able to quickly and easily restore the data if it is lost or corrupted. Cloud-based backup solutions are often more secure than on-premise solutions because they are housed off-site and away from potential threats.

3. Training:

For cybersecurity measures to be effective, educating employees on cybersecurity best practices is one of the most effective ways to prevent phishing attacks and other human error-based incidents. Employees should be trained on proper security protocols such as password management, handling sensitive information, and recognising phishing emails/websites.

4.3 Vision Ideal Scenarios Innovation and Tech

Several times, cybersecurity is applied to Critical Infrastructures such as energy. This technology addresses several solutions, such as platforms that allow the isolation of the network, public access to critical or industrial infrastructure, the isolation of communities of renewable energy, and island-to-island service recovery. This is commonly based on three methods: (1) validation of the feasibility of island operation, (2) protection and monitoring against the digital intrusion of the operation's IT systems electricity on an island, and (3) validation of the absence of computer risk allows reconnection to public networks in electrical and information security.

Secure communication channels are essential for coordinating response efforts and sharing critical information in a crisis. Innovation and technology can help to develop secure communication solutions, including encrypted messaging platforms and secure video conferencing tools. Effective cybersecurity in crisis management requires up-to-date information about the latest cyber threats and vulnerabilities. Innovation and technology can help to develop cyber threat intelligence platforms that provide real-time information about emerging threats and vulnerabilities, allowing organisations to take proactive measures to protect against cyber attacks.

In the event of a cyber-attack during a crisis, time is of the essence. Innovation and technology can help to develop incident response automation tools that allow organisations to detect and respond to cyber-attacks quickly, which includes automated threat detection and response systems that use machine learning and artificial intelligence to identify and respond to cyber threats.

Effective cybersecurity in crisis management requires a culture of cybersecurity awareness and training among all stakeholders. ICT can help to develop cybersecurity training and awareness programs that use gamification and other interactive techniques to engage and educate stakeholders about cyber risks and best practices. Finally, cyber insurance can help organisations to mitigate the financial impact of a cyber attack during a crisis. Innovation and technology can help develop new cyber insurance models that consider the unique risks and challenges associated with crisis management.

Innovation and technology can be crucial in enhancing cybersecurity in crisis management by providing secure communication channels, cyber threat intelligence, incident response automation, cybersecurity training and awareness, and cyber insurance solutions. However, it is essential to note that effective cybersecurity in crisis management requires a holistic approach considering the people, processes, and technology involved.

4.4 Risk Analysis

Cybersecurity risk assessments help organisations understand, control, and mitigate all forms of cyber risk. It is a critical component of risk management strategy and data protection efforts. As organisations rely more on information technology and information systems to do business, the digital risk threat landscape expands, exposing ecosystems to new critical vulnerabilities. Risk analysis for cybersecurity on crisis management has identified the following:

- Cybersecurity threats to crisis management can come from various sources, including cybercriminals, hacktivists, and nation-state actors. These threats can be ransomware attacks, denial-of-service attacks, data breaches or others.

- Cyber attackers can exploit vulnerabilities in crisis management systems and networks. These vulnerabilities can arise from outdated software, weak passwords, unpatched systems, or misconfigured settings.

- The consequences of a cybersecurity breach during a crisis can be severe, from disruption of critical infrastructure, loss of confidential data, and reputational damage, up to financial losses.

- The likelihood of a cybersecurity breach during a crisis depends on various factors, including the level of preparedness and security measures in place, the complexity of the crisis, and the sophistication of the attackers.

- The impact of a cybersecurity breach during a crisis can be significant. It can disrupt communication channels, compromise critical systems and infrastructure, and impede the response efforts of crisis management teams.

Implementing cybersecurity measures to address the above risks is essential, including:

1. Regular risk assessments to identify vulnerabilities and threats.

2. Regular software updates and patches to address known vulnerabilities.

3. Strong password policies and two-factor authentication mechanisms.

4. Regular cybersecurity training and awareness programs for all stakeholders.

5. Incident response plans that outline steps to take in the event of a cybersecurity breach.

6. Regular testing and simulations of incidents to ensure the readiness of all stakeholders.

7. Regular backups and data recovery plan to ensure that critical data can be restored during a cyber attack.

By implementing these measures, organisations can improve their cybersecurity posture and reduce the risk of a cybersecurity breach during a crisis.

4.5 Behavioural and Cultural Challenges

It is important to develop a comprehensive cybersecurity culture across all stakeholders involved in crisis management, which includes awareness campaigns, regular training and education, and the development of a shared understanding of the importance of cybersecurity. Additionally, it may be necessary to implement governance frameworks that foster collaboration and communication between different teams and stakeholders. Finally, ensuring adequate resources are available to invest in cybersecurity measures, including personnel and funding, is important. Some behavioural and cultural challenges for cybersecurity in crisis management are present and need to be tackled:

Lack of awareness: Many stakeholders involved in crisis management may not be fully aware of the potential cyber threats and the importance of cybersecurity measures, which can lead to a lack of preparedness and a failure to implement necessary security measures.

Resistance to change: Crisis management teams may be resistant to change or reluctant to adopt new technologies or processes, which can impede the implementation of effective cybersecurity measures.

Complacency: In some cases, crisis management teams may become complacent about cybersecurity measures, assuming their current systems are secure enough, leading to a false sense of security and an increased risk of cyber attacks.

Siloed approach: Crisis management teams may operate in silos, with limited communication and collaboration between different teams and stakeholders. Implementing a coordinated and holistic approach to cybersecurity can make it challenging.

Limited resources: Crisis management teams may have limited resources both in terms of funding and personnel, making it difficult to invest in necessary cybersecurity measures and ensure sufficient cybersecurity experts on staff.

Cultural attitudes: Cultural attitudes towards cybersecurity may vary widely across different regions and countries. Some cultures may view cybersecurity as a lower priority than other issues, impacting the willingness to invest in cybersecurity measures.

By investing in cybersecurity measures, crisis management teams can better protect critical infrastructure and confidential data and ensure the continuity of operations during a crisis. Ultimately, it is essential to recognise that cybersecurity is a shared responsibility and requires a coordinated effort across all stakeholders involved in crisis management.

4.6 Overview of Data Analysis

Data analysis is critical to cybersecurity in crisis management, enabling stakeholders to make data-driven decisions and develop effective strategies to mitigate cyber risks. Data analysis for cybersecurity on crisis management involves collecting, processing, and analysing large amounts of data to identify and mitigate cyber risks, which should be collected from various sources, such as security logs, threat intelligence feeds, network traffic, and user behaviour data. Here are some concrete examples of data analysis processes used in cybersecurity:

- Intrusion detection systems (IDS) collect large amounts of network traffic data to identify and analyse potential attacks. Machine learning is used to train IDS to identify patterns of normal and abnormal behaviour and flag suspicious activity for further investigation.

- Vulnerability scanners collect data on the software and systems running on a network and compare them against known vulnerabilities. These vulnerabilities are then prioritised based on severity and potential impacts, allowing organisations to focus on the most critical issues.

- User behaviour analytics (UBA) uses data from network logs and other sources to identify user behaviour patterns that may indicate security risks. Clustering and anomaly detection can identify unusual user activity and flag potential threats.

- Threat intelligence feeds collected data on known threats and vulnerabilities from various sources. This data is then analysed to identify patterns and connections between threats, helping organisations better understand the threat landscape and develop more effective defence strategies.

- During a security incident, data analysis can identify the source of the attack quickly, determine the scope of the breach, and prioritise response efforts. Data visualisation tools such as dashboards and heatmaps can be used to communicate the incident's status and help teams coordinate their response efforts.

Data analysis involves several steps to achieve these different scenarios, including data collection, cleaning, pre-processing, analysis, and visualisation. During data cleaning, irrelevant or erroneous data is removed, and missing values are imputed. Data pre-processing involves transforming and normalising the data to ensure it is suitable for analysis.

Data analysis techniques, such as machine learning, statistical analysis, and data mining, can be used to identify patterns and anomalies in the data. These techniques can help to identify potential cyber threats and vulnerabilities, enabling crisis management teams to address them proactively.

Data visualisation tools, such as dashboards and graphs, can communicate the insights and findings from the data analysis to stakeholders, helping to understand cybersecurity better and inform decision-making processes.

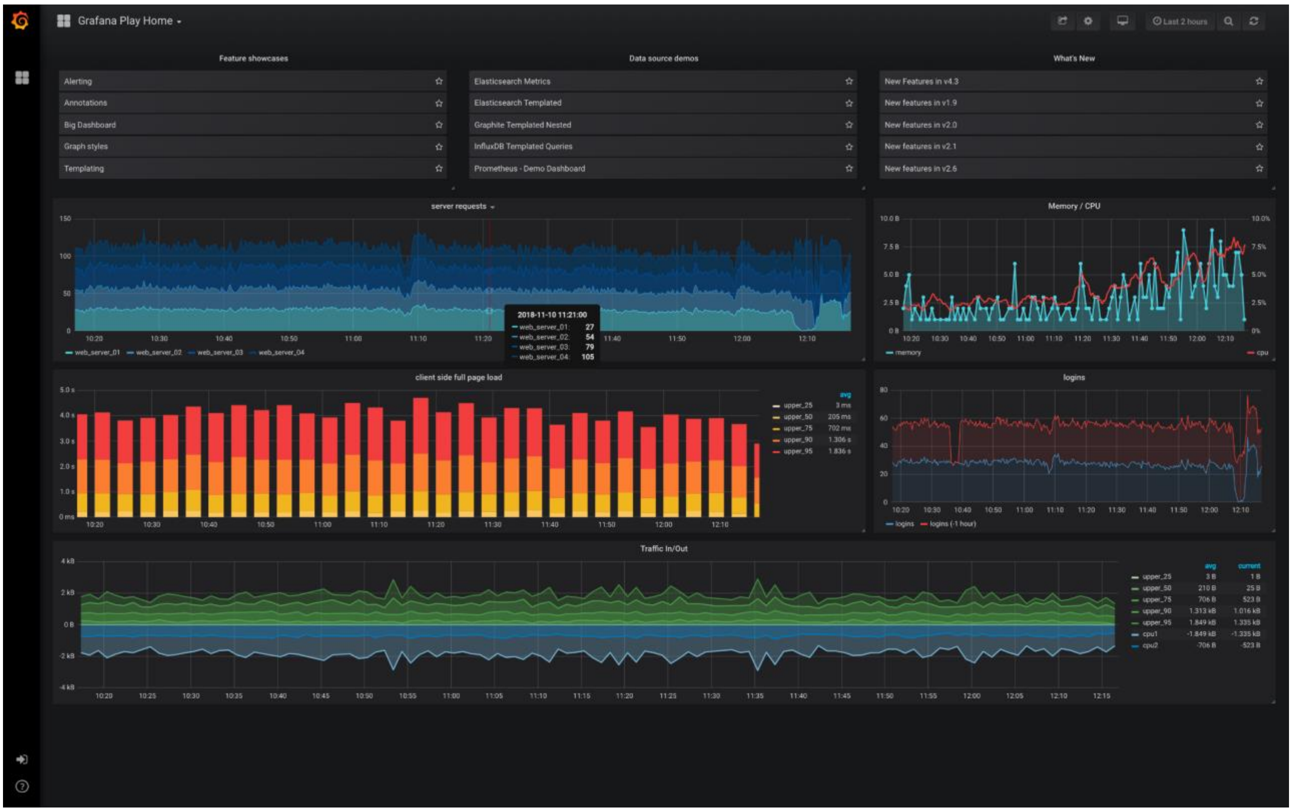


Figure 6: *Grafana, a multi-platform open-source analytics and interactive visualisation web application that provides charts, graphs, and alerts for the web when connected to supported data sources.*

Overall, data analysis is an essential tool for cybersecurity in crisis management and should be integrated into crisis management plans and strategies.

4.7 Scenarios and Best Cases

Cyber Crisis Management: A Decision-Support Framework for Disclosing Security Incident Information

Authors: O. Kulikova, R. Heil, J. van den Berg and W. Pieters, "Cyber Crisis Management: A Decision-Support Framework for Disclosing Security Incident Information," 2012 International Conference on Cyber Security, Alexandria, VA, USA, 2012, pp. 103-112, doi: 10.1109/CyberSecurity.2012.20.

The growing sophistication and frequency of cyber attacks force modern companies to be prepared beforehand for potential cybersecurity incidents and data leaks. A proper incident disclosure strategy can significantly improve the timeliness and effectiveness of incident response activities, reduce legal fines, and restore the confidence and trust of a company's key stakeholders. This scenario introduces four factors that shape organisational preferences regarding incident information disclosure. Together, they create challenges for a company when deciding whom, when, what, and how to share cyber security incident information. We propose a decision-support framework that provides step-by-step guidance for organisations to address these challenges and develop an appropriate incident disclosure strategy.

Crisis Management in a Federation – Cybernetic Lessons from a Pandemic

Author: Markus Schwaninger, University of St. Gallen, St. Gallen, Switzerland. Part of the Lecture Notes in Computer Science book series (LNCS,volume 13789). First Online: 10 February 2023. DOI: 10.1007/978-3-031-25312-6_75

This scenario aims to contribute to improving the management of pandemic crises. Its focus is on federal systems, which are particularly powerful in dealing with environmental complexity. We study crisis management in the Swiss Federation through five waves of the pandemic, spanning a year and a half. This research aims to learn how to deal with crises of the same type in the future. We apply the Viable System Model (VSM) as a framework for our inquiry, elaborating a diagnosis and a design for managing epidemic or pandemic crises. The VSM is a conceptual tool that is particularly strong for analysing federal systems. Hence substantial insights have surfaced to orientate future crisis management.

Cyber Crisis Management Roles – A Municipality Responsibility Case Study

Authors: Information Technology in Disaster Risk Reduction, 2020, Volume 575. ISBN : 978-3-030-48938-0. Grethe Østby, Basel Katt. DOI: 10.1007/978-3-030-48939-7_15

In this paper, the authors propose a role model that can be applied in societal cyber crisis management to build safety and standard procedures during cyber security crises. The authors define a societal cyber crisis as a cyber crisis which affects the society in which disaster is or might be the consequence. The process of creating our model started by analysing regulations and responsibilities in Norwegian municipalities, and we used steps of a design science research (DSR) research approach to create our suggested artefact. A combination of conventional crisis management and cyber crisis management is proposed to identify the interrelationships among diverse stakeholders when managing the preparation for and reaction to a cyber crisis incident. We present a cyber incident handling role model (CIHRM) usable for visualising cyber crises in diverse organisations. After our model has been reviewed by the cyber security research community, we plan to implement the model when analysing crisis management in various organisations to prepare for instructions, training and exercises at our training environment - The Norwegian Cyber Range.

5. Attacks on Public Spaces

5.1 Overview of the current State of Play

Public spaces such as commercial centres, recreational venues, open crowded gathering areas and events constitute "targets" for attacks (individuals or mass) that strongly impact the safety of citizens. In this context, a smart city uses digital technology not only to provide preparedness and early detection of threats to first responders and city authorities but also to connect, protect, and enhance the lives of citizens. The threat of attacks on public spaces in Europe has become a major concern in recent years, with numerous high-profile incidents occurring across the continent.

One example of this was the November 2015 Paris attacks, in which terrorists used encrypted messaging apps to communicate with each other and coordinate their actions. This scenario highlighted the need for law enforcement agencies to have the capability to monitor and decrypt such communications in order to prevent similar attacks in the future. Another example is the use of drones in attacks on public spaces, such as the attempted drone attack on Gatwick Airport in the UK in December 2018. This incident demonstrated the need for law enforcement agencies to have effective counter-drone technology to detect and disable rogue drones that threaten public safety.

Figure 7: High police presence in Lyon, France, during the 25th weekend of the yellow vests movement (2019)

First responders have learned many lessons from these attacks, including the need for better communication and coordination among different agencies involved in responding to such incidents. There is also a growing recognition of the importance of using technology, such as artificial intelligence and machine learning, to analyse large amounts of data and identify potential threats in real time. In response to these threats, many European countries have increased their investments in security technology and implemented new measures to protect public spaces.

For example, many cities have installed CCTV cameras and other surveillance systems to monitor public spaces and detect potential threats. Using advanced video analytics technology, CCTV can detect abandoned objects, track individuals, and identify potential threats, helping security personnel respond quickly and effectively to incidents. In addition, many public spaces now have enhanced security measures, such as metal detectors and bag checks, to deter potential attackers. In addition, many European cities have implemented mobile applications that allow members of the public to report suspicious behaviour or incidents in real time. These apps often include location-based reporting features, enabling users to pinpoint the exact location of the incident or threat.

Another area where ICT is being used to prevent attacks on public spaces is the development of early warning systems. These systems use a combination of sensors, cameras, and other data sources to detect potential threats, such as suspicious vehicles or individuals, and alert security personnel in real-time to respond and prevent potential attacks before they occur quickly. Finally, social media monitoring and analysis are also used to prevent public space attacks. Law enforcement agencies are increasingly using social media to monitor and identify potential threats and to track the activity of individuals who may pose a risk to public safety. This technology enables law enforcement agencies to detect potential threats and take action before an attack can occur.

Overall, while attacks on public spaces in Europe continue to pose a significant threat, advances in technology and increased investments in security measures are helping to improve the ability of first responders to prevent and respond to such incidents.

5.2 Research Challenges and Objectives

The generation, processing and sharing of large quantities of data in smart cities make urban systems and services potentially more responsive and able to act upon real-time data. Such data are extracted from CCTV camera systems, systems for crowd transitions and people density, systems for abnormal detection and situational awareness, and several sensors (sound, drones, fire/smoke, chemical precursors for explosives) that are part of an IoT network.

For such data that are continuously generated, strict latency-aware computational processing capabilities, as well as a homogeneous approach for data processing and generation of associated event information, are demanded. Also, novel Artificial Intelligence (AI) paradigms, Next Generation emergency call technologies (NG112), and new IoT applications, including Augmented Reality (AR), Virtual Reality (VR), Digital Twins (DT), virtual simulations, real-time searching engines, real-time sensing and measurements, and discovery services bring new challenges.

Expensive computing hardware with sufficient storage capacities can address the challenges of massive storage and scale computing. Cloud computing has already been used in previous years to eliminate the need for dedicated, expensive computing hardware. Cloud computing can be considered an efficient technology that enhances the Quality of Experience (QoE). Also, it provides on-demand storage and processing capabilities, mainly a cost-effective approach. The following table presents the advantages and limitations of cloud computing.

Overall, while cloud computing can provide significant benefits in terms of scalability, flexibility, and cost-effectiveness, which has made its adoption possible in several applications, it also has several limitations when it comes to preventing and responding to attacks on public spaces. As such, organisations must carefully consider these limitations when implementing cloud-based security solutions and ensure that appropriate measures are taken to mitigate these risks.

Table 3: Cloud computing advantages and limitations (prevention of public spaces attacks)

Advantages of cloud computing	Limitations of cloud computing
Scalability	Network latency causing delays
Flexibility	Data security breaches
Elasticity	Lack of reliable and secure network connectivity on public spaces
Multitenancy	Lack of skills and expert staff
Storage capacity	Computational time for data processing
Resource pooling	
Cost-effectiveness	

The recent edge computing technology is considered a flexible and viable solution that can overcome the limitations of cloud computing. Thus, edge computing can be used for real-time smart city environments enabling: i) context awareness, ii) geo-distributed capabilities, iii) low latency, iv) migration of computing resources from the remote cloud to the network edge, and v) data aggregation, analysis and management at the edge. According to those above, an IoT-based smart city that exploits connected smart sensors and IoT devices and adopts an edge computing scheme aligns with recent technology to improve citizens' safety and quality of life and provide them with security measures from first responders against several types of attacks.

Transforming a city into a smart city requires collaborative efforts between all stakeholders (e.g., government, industry, practitioners, residents and researchers) from many disciplines, such as computer science, survey/geoinformatics and civil engineering, systems engineering, electrical and computer engineering, among others. Bringing together stakeholders with different backgrounds to support smart city initiatives produces several challenges. Some of these challenges involve the differences in expert vocabulary, differences in disciplinary cultures, identification of available and appropriate resources, and integration of heterogeneous data and knowledge. A smart city mainly refers to six characteristics: 1) Smart economy, 2) Smart mobility, 3) Smart environment, 4) Smart people, 5) Smart living, and 6) Smart governance. However, other subcategories of those above include Smart health, Smart energy, Smart water and Smart waste, and Smart safety of public spaces, just to name a few. In such a context, a smart city should consider several objectives and research challenges:

1. Data from different IoT sources/devices should be available to be easily aggregated;
2. Data should be easily visualised and securely accessible, respecting privacy;
3. Detailed, measurable, real-time knowledge should be available at every level;
4. Analytics and decision-making systems should be used;
5. The city should incorporate state-of-the-art technologies for automation and further relevant extensibility;
6. The city should have a network of collaborative spaces;
7. Moreover, the decision-making processes should be much more open and inclusive.

One of the leading research challenges is developing reliable and effective IoT-based security systems that can detect potential threats and prevent attacks, which involves designing, improving and integrating sensors and other IoT devices that can accurately detect suspicious activity and provide real-time alerts to security personnel.

Secondly, another research objective is to improve the interoperability and compatibility of IoT devices and systems, which is critical in public spaces where different organisations or stakeholders may use multiple IoT devices and systems. Standardisation efforts are needed to ensure these systems can work seamlessly and effectively.

Thirdly, there is a need to develop advanced analytics and machine learning algorithms to process and analyse the large volumes of data generated by IoT devices, from the edge to the cloud, which involves developing algorithms that can detect patterns and anomalies in the data and provide actionable insights to security personnel.

Fourthly, another research objective is to ensure the security and privacy of the data generated by the devices, which involves integrating secure communication protocols, encryption techniques, and other security measures to protect sensitive data from cyber threats and unauthorised access.

Finally, there is a need to develop practical training and education programs for security personnel and other stakeholders to ensure they can effectively use and manage IoT-based security systems, which involves developing training programs that provide hands-on experience with IoT devices and systems and teach personnel how to respond to security threats in real-time.

Overall, preventing attacks on public spaces using IoT technologies is a complex and challenging area of research. However, with continued investment and innovation, it is possible to develop effective IoT-based security systems that can help prevent attacks and ensure the safety of public spaces.

5.3 Vision Ideal Scenarios Innovation and Technology

Innovation is crucial in achieving this vision of preventing attacks on public spaces using IoT technologies. It involves developing advanced and reliable systems that can accurately detect potential threats, provide real-time alerts, and prevent attacks before they occur. There are several areas where innovation is needed:

1. Development of advanced sensors and other IoT devices that can accurately detect suspicious activity in real-time, which must be designed to be highly sensitive and responsive to potential threats while also being robust and reliable enough to operate in a range of environments.

2. Another area of innovation is the development of machine learning algorithms and advanced analytics tools that can process and analyse large volumes of data generated by IoT devices to detect patterns and anomalies in the data and provide actionable insights to security personnel, enabling them to respond quickly and effectively to potential threats.

3. Furthermore, innovation is needed in communication protocols and encryption techniques to ensure that the data generated by IoT devices are secure and protected from cyber threats and unauthorised access, which involves developing new techniques and protocols that are robust and reliable enough to withstand potential attacks and provide secure communication channels for IoT devices.

4. Innovation is also needed in training and education to ensure security personnel and other stakeholders are adequately trained and prepared to respond to potential threats by developing comprehensive training programs that provide hands-on experience with IoT devices and systems and teach personnel how to respond to security threats in real time.

In summary, the vision and ideal scenarios for innovation and technology in preventing attacks on public spaces using IoT technologies involve developing advanced and reliable systems that can accurately detect potential threats, provide real-time alerts, and prevent attacks before they occur. This vision requires continued investment and innovation in sensor development, analytics, communication protocols, encryption, and training and education.

5.4 Risk Analysis

It is essential for identifying potential risks and threats associated with IoT-based security systems for public spaces, as described below:

- **Cybersecurity risks**: These threats include hacking, malware, and denial of service attacks, resulting in unauthorised access to sensitive data, system malfunction, and system shutdown. The risk level for this threat is high, as cyber-attacks are becoming increasingly sophisticated and common.

- **False alarms** can cause unnecessary panic and disruption and waste valuable time and resources. The risk level for this threat is moderate, as false alarms can be mitigated through advanced analytics and machine learning algorithms.

- **Technical failures** such as system malfunction or power outages can render IoT-based security systems ineffective. The risk level for this threat is moderate, as it can be mitigated through regular maintenance, system backups, and redundant systems.

- **Privacy concerns**: Using IoT-based security systems for public spaces raises concerns about privacy violations. The risk level for this threat is moderate, as it can be mitigated through GDPR-compliant and privacy-preserving technologies such as encryption and access controls.

- **Physical damage** to IoT devices due to vandalism, natural disasters, or accidents can render security systems ineffective. The risk level for this threat is low, as it can be mitigated through proper installation and maintenance.

- **False sense of security**: Using IoT-based security systems can create a false sense of security among the public, resulting in complacency and reduced vigilance. The risk level for this threat is low, as it can be mitigated through proper education and training of security personnel and the public.

In conclusion, IoT-based security systems for public spaces offer several benefits but pose risks and threats; therefore, detailed risk analysis and mitigation strategies are required to ensure the public's security and safety.

5.5 Behavioural and Cultural Challenges

Behavioural and cultural challenges are important factors that can impact the effectiveness of security measures against attacks on public spaces in Europe, including:

Cultural diversity: Europe is a diverse continent with different cultures, languages, and religions, making it challenging to develop security measures that are sensitive to the needs of different groups while still being effective.

Public perception of security measures, such as CCTV cameras, metal detectors, and bag searches, may be seen as intrusive or even oppressive by some public members, creating resistance and making it difficult to implement them effectively.

Fear and panic can be caused among the public by attacks on public spaces, making it difficult to respond effectively. For example, people may rush to exit a building or area, potentially causing further injuries or fatalities.

Lack of awareness and preparedness: Many people may not be aware of the risks associated with attacks on public spaces or know what to do in the event of an attack, making it difficult to implement effective prevention and response measures.

Limited resources: Local governments and law enforcement agencies may need more resources to prevent and respond to attacks on public spaces, making it challenging to implement adequate security measures and respond to incidents quickly and effectively.

Addressing these behavioural and cultural challenges requires a multi-faceted approach that involves educating the public about the risks associated with attacks on public spaces, developing culturally sensitive security measures, and engaging with local communities to build trust and cooperation.

5.6 Overview of Data Analysis

By collecting and analysing data from various sources, law enforcement agencies and security professionals can identify patterns and trends that may indicate a potential threat and take proactive measures to prevent an attack, thus playing an essential role in preventing and responding to attacks on public spaces in Europe. Some examples include:

1. Social media platforms can be valuable sources of information about potential threats to public spaces. Monitoring social media activity and analysing keywords and hashtags allow law enforcement agencies to identify potential threats and take proactive measures to prevent attacks.

2. CCTV cameras are widely used in public spaces in Europe, and video analytics can help to identify potential threats and suspicious activity. For example, facial recognition technology can identify individuals flagged as potential threats or previously involved in criminal activity.

3. Predictive analytics involves using machine learning algorithms to analyse data and identify patterns and trends that may indicate a potential threat. For example, predictive analytics may be used to analyse data from social media, CCTV cameras, and other sources to identify potential threats and take proactive measures to prevent attacks.

4. Geographic information systems (GIS) technology can map and analyse data about potential threats and vulnerabilities in public spaces. For example, GIS can identify areas at higher risk of an attack based on population density, proximity to potential targets, and previous incidents.

Effective data analysis requires a multi-disciplinary approach that involves not only technology and data science experts but also security professionals and law enforcement agencies. By working together to collect and analyse data from various sources, they can develop a more comprehensive understanding of the risks associated with attacks on public spaces and take proactive measures to prevent them.

5.7 Scenarios and Best Cases

SemAttack: Natural Textual Attacks via Different Semantic Spaces

Authors: Boxin Wang, Chejian Xu, Xiangyu Liu, Yu Cheng, Bo Li. Published at Findings of NAACL 2022

Recent studies show pre-trained language models (LMs) are vulnerable to textual adversarial attacks. However, existing attack methods either suffer from low attack success rates or fail to search efficiently in the exponentially large perturbation space. The authors propose an efficient and effective framework SemAttack to generate natural adversarial text by constructing different semantic perturbation functions. In particular, SemAttack optimises the generated perturbations constrained on generic semantic spaces, including typo space, knowledge space (e.g., WordNet), contextualised semantic space (e.g., the embedding space of BERT clusterings), or the combination of these spaces. Thus, the generated adversarial texts are semantically close to the original inputs. Extensive experiments reveal that state-of-the-art (SOTA) large-scale LMs (e.g., DeBERTa-v2) and defence strategies (e.g., FreeLB) are still vulnerable to SemAttack. The authors further demonstrate that SemAttack is general and able to generate natural adversarial texts for different languages (e.g., English and Chinese) with high attack success rates. Human evaluations also confirm that our generated adversarial texts are natural and barely affect human performance.

6. Recommendations

6.1 Research Recommendations

Research plays a key role in evolving technologies for Crisis Preparedness and Management, therefore, some recommendations should be taken into consideration, such as:

- Fostering innovative tools, technologies and processes aimed at enabling and improving operations and its efficiency, as well as data sharing between stakeholders and different organisations
- Assurance of interoperable and secure incident management and better integration of IoT for early warning systems and simultaneous data collection for analysis, learning, decision-making and efficient communication with organisations and stakeholders;
- Resilience improvement of critical infrastructures, such as transport, energy and communication
- Ensure the creation of relations between topics such as Innovation, Testbeds and Standardisation to accelerate the RandD and enable early testing and validation of ideas and concepts
- Design and leverage methodologies already available to guide the initiation and the realisation of testbeds for IoT and Crisis Preparedness, where the AIOTI testbed methodology is one of them.

6.2 Standardisation and Interoperability Recommendations

While standards like ISO 22320, ETSI TS 103 463, and NG-112 have made significant contributions to improving crisis preparedness and IoT-based security systems, there are still gaps and challenges that require further research and efforts. Some of these gaps and challenges include:

- **Interoperability**: Achieving seamless interoperability between different IoT devices, communication networks, and emergency response systems remains a challenge. There is a need for further research and standardisation efforts to deliver protocols and frameworks that enable effective data exchange and communication among diverse systems
- **Scalability**: As IoT deployments and data volumes continue to grow, there is a need to address the scalability of IoT-based security systems for public spaces. Research efforts should focus on developing scalable architectures, data management approaches, and analytics techniques that can handle the increasing volume and velocity of data generated by IoT devices
- **Privacy and data protection**: The collection and analysis of data in IoT-based security systems raise concerns about privacy and data protection. Research is needed to develop robust mechanisms for ensuring privacy compliance, secure data storage and transmission, and informed consent from individuals whose data is being collected
- **Human factors**: The successful implementation of IoT-based security systems relies not only on technology but also on human factors. Research efforts should explore human-centred design principles, user interfaces, and training programs that promote effective utilisation of IoT systems by first responders and other relevant stakeholders.

While standards such as ISO 22320[31], ETSI TS 103 463[32], and NG-112[33] exist, there may still be gaps and inconsistencies in terms of coverage and implementation. Research and collaborative efforts are needed to address these gaps, ensure comprehensive coverage, and foster harmonisation between different standards and guidelines.

The rapid evolution of IoT technologies poses challenges for existing legal and regulatory frameworks. Research efforts should focus on developing flexible and adaptive frameworks that address the unique characteristics and challenges of IoT-based security systems, while also ensuring compliance with data protection, cybersecurity, and privacy regulations.

[31] ISO 22320:2018 - Societal security - Emergency management - Requirements for incident response: this international standard by ISO provides requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving incident response capabilities. It focuses on the coordination and interoperability of organisations involved in emergency management to effectively respond to incidents. ISO 22320 was published in 2018 and is currently in use worldwide, providing a framework for organisations involved in crisis management to establish effective incident response capabilities. It promotes a systematic and coordinated approach to managing crises, improving interoperability and coordination between different entities involved in emergency response.

[32] ETSI TS 103 463 - Cybersecurity for Consumer Internet of Things: this technical specification, developed by ETSI, provides guidelines and best practices for ensuring cybersecurity in consumer IoT devices. It addresses the unique security challenges posed by IoT devices and offers recommendations for protecting against cyber threats. ETSI TS 103 463 was published in 2017 and has undergone subsequent revisions and updates, to ensure cybersecurity in IoT devices for maintaining the resilience of critical infrastructure and systems during crises. ETSI TS 103 463 provides guidance to device manufacturers, service providers, and consumers to enhance the security of IoT devices, reducing the risk of cyber attacks that could disrupt emergency response systems.

[33] NG-112, also known as Next Generation 112, is an initiative focused on improving emergency communications and response systems, specifically for public safety answering points (PSAPs) or emergency call centres. NG-112 aims to enhance the capabilities of emergency services by leveraging advanced technologies and communication networks, including IoT. NG-112 is being developed by various standardisation organisations and industry alliances, which includes stakeholders from the public safety and telecommunications sectors. These specifications include the use of IP-based networks, multimedia capabilities, and the integration of various communication channels (voice, video, text, and data) to enable more efficient and effective emergency response, to provide enhanced situational awareness and improved communication capabilities to emergency services, allowing them to respond more effectively to incidents and emergencies.

IoT-based security systems need to be resilient and robust to withstand various threats and disruptions. Research is needed to identify vulnerabilities, develop countermeasures, and conduct comprehensive risk assessments to enhance the resilience of IoT systems against natural disasters, cyber attacks, and other disruptions.

Addressing these gaps and challenges requires collaboration among researchers, industry experts, policymakers, and practitioners. Continued research and concerted efforts are essential to drive innovation, improve standards, and develop best practices that enhance the effectiveness, reliability, and security of IoT-based security systems for crisis management and public safety.

These collaborations within the standardisation and innovation ecosystem, which can also be incorporated into funded projects or associations such as AIOTI, are expected to accelerate the standardisation and technology deployment processes and support the provision of validated solutions to standards development process allowing for a faster specification of standards with no decrease of quality.

6.3 Business-driven Recommendations

In the context of crisis preparedness, businesses can play a critical role in leveraging IoT technologies to enhance response coordination, resource deployment, monitoring, and surveillance.

Response Coordination and Resource Deployment:

To facilitate better response coordination and deployment of resources, businesses should:

- Implement IoT-enabled platforms that enable real-time communication and collaboration between different response agencies and stakeholders. These platforms streamline information sharing, resource allocation, and coordination efforts, ensuring a synchronised response to crisis situations.

- Develop automated resource management systems that leverage IoT technologies to track and manage the availability and deployment of resources. By monitoring resource usage in real-time, businesses can ensure efficient allocation based on evolving demands and optimise their response capabilities.

- Integrate IoT sensors and data analytics to monitor resource usage, identify bottlenecks, and optimise the allocation of resources. Real-time insights derived from IoT data enable businesses to make data-driven decisions, ensuring effective resource utilisation during crisis situations.

Monitoring and Surveillance Systems/Strategies:

To enhance monitoring and surveillance capabilities, businesses should:

- Deploy IoT sensors and monitoring systems in critical infrastructure and public spaces to gather real-time data on environmental conditions, security threats, and potential risks. This data can be analysed to detect anomalies, identify patterns, and trigger early warnings, enabling timely response and mitigation efforts.

- Enhance existing video surveillance systems with IoT technologies, such as intelligent video analytics and behaviour recognition, to improve situational awareness. IoT-enabled video surveillance can detect and identify suspicious activities, track individuals of interest, and provide valuable insights for effective crisis management.

- Develop predictive analytics models that leverage IoT data and machine learning algorithms to identify patterns and trends related to crisis events. By analysing historical data, businesses can anticipate potential threats, optimise resource allocation, and implement proactive measures to mitigate risks.

The following recommendations focus on improving the effectiveness and efficiency of crisis management across the four phases of the process: mitigation, preparedness, response, and recovery.

Mitigation Phase:

Mitigation involves measures taken to minimise the impact of potential crises. During this phase, businesses should focus on identifying vulnerabilities, assessing risks, and implementing strategies to prevent or reduce the severity of crises. By utilising IoT-enabled risk assessment tools and predictive models, businesses can identify potential hazards and vulnerabilities. This data-driven approach enables them to develop targeted mitigation strategies and allocate resources efficiently.

Preparedness Phase:

Preparedness is centred around planning, readiness, and capacity building to effectively respond to crises. Businesses should focus on developing comprehensive emergency response plans and procedures that outline roles, responsibilities, and communication protocols for all stakeholders involved. IoT technologies can support preparedness efforts by facilitating real-time communication and enabling seamless information sharing among response teams. Additionally, conducting drills and simulations using IoT technologies allows businesses to test response plans, identify gaps, and refine strategies. IoT sensors and monitoring systems provide real-time data during simulations, allowing for evaluation and improvement of preparedness efforts.

Response Phase:

The response phase involves the immediate actions taken to address a crisis event. Businesses should deploy IoT-enabled situational awareness platforms that integrate data from various sources, such as sensors, social media, closed-circuit television (CCTV), and other relevant sources. By leveraging IoT data analytics, businesses can gain real-time insights into the evolving situation, enabling informed decision-making and effective response coordination. Furthermore, utilising IoT devices and wearables can enhance responder safety by monitoring their well-being and providing timely assistance during response operations.

Recovery Phase:

The recovery phase focuses on restoring normalcy and facilitating the recovery of affected communities and infrastructure. Businesses can leverage IoT technologies for post-crisis data collection and analysis to assess damages, evaluate response effectiveness, and inform recovery strategies. IoT-based monitoring systems can track the progress of recovery operations, monitor infrastructure rehabilitation, and ensure the safe return of affected communities.

By implementing these business-driven recommendations across the four phases of the crisis management process, organisations can effectively utilise IoT technologies to enhance response coordination, improve monitoring and surveillance capabilities, and build resilience against natural and man-made hazards.

6.4 Policy-driven Recommendations

The role of policymakers in crisis preparedness is crucial for ensuring effective response coordination, resource allocation, and the use of IoT technologies to enhance monitoring and surveillance. The following recommendations focus on policy initiatives that can strengthen crisis management efforts across all phases: mitigation, preparedness, response, and recovery.

Mitigation Phase:

Invest in research and development initiatives focused on leveraging IoT technologies for risk assessment, hazard mapping, and early warning systems, support collaborations between research institutions, industry partners, and government agencies to develop innovative IoT-based solutions for hazard mitigation and prevention and encourage the use of IoT-enabled predictive analytics models and machine learning algorithms to identify potential risks, optimise resource allocation, and inform mitigation strategies. By defining strong requirements beforehand, one can ensure that any strategic planning previously designed and defined is carried out without any predicament or additional difficulty.

Besides fostering Research and Development, promote Public Awareness and Education by implementing public awareness campaigns to educate citizens about the benefits of IoT technologies in crisis preparedness and mitigation, develop educational programs and training initiatives to enhance digital literacy and promote the responsible use of IoT devices and technologies during emergencies, and, finally, foster partnerships with educational institutions, community organisations, and the private sector to disseminate information, best practices, and guidelines related to IoT and crisis management.

Preparedness Phase:

For the preparedness phase the overall recommendations are to develop national IoT preparedness strategies and foster Public-Private Partnerships. One approach is to formulate national strategies that emphasise the integration of IoT technologies into crisis preparedness plans, including provisions for IoT infrastructure, data governance, and interoperability standards, and collaborate with relevant stakeholders, including government agencies, industry experts, and academia, to establish guidelines for the implementation and adoption of IoT technologies in crisis management.

Another is to allocate resources for capacity building, training, and awareness programs to enhance the understanding and utilisation of IoT technologies among emergency responders and relevant personnel, and encourage partnerships between government entities and private sector organisations to promote the development and deployment of IoT solutions for crisis preparedness. Deploy secure communication systems for real-time, enabling decision makers with all the tools necessary for informed and structured decision making as well as strategic thinking and planning.

Facilitate information sharing and collaboration among stakeholders to promote innovation, exchange best practices, and leverage expertise in the field of IoT and crisis management and establish mechanisms to incentivize private sector investments in IoT technologies for crisis preparedness through grants, tax incentives, or research funding.

Response Phase:

Ensure Interoperability and Data Sharing by implementing policies that promote interoperability among IoT devices, systems, and platforms used by various response agencies to enable seamless data sharing and collaboration during crisis events. Furthermore, establish data governance frameworks and protocols that ensure privacy, security, and ethical use of IoT-generated data during response operations, and encourage the development of common data standards and formats to enable effective integration and analysis of IoT data across different response systems.

Invest in Communication Infrastructure to enhance it, including high-speed networks and resilient connectivity, to support real-time data transmission and communication during crisis situations, while promoting the use of IoT-based communication systems, such as satellite communication and mesh networks, to overcome communication challenges in remote or disrupted areas. Finally, develop policies that prioritise the continuity and reliability of communication networks during emergencies, ensuring seamless information exchange among responders and affected communities.

Recovery Phase:

Encourage the use of IoT-enabled data analytics and visualisation tools to assess damages, evaluate the effectiveness of response efforts, and inform recovery strategies. This data-driven recovery strategy should facilitate the integration of IoT data with existing recovery databases and systems to streamline data collection, analysis, and decision-making processes. Moreover, establish guidelines for the ethical and responsible use of IoT-generated data in recovery planning, respecting privacy rights and data protection regulations.

With the purpose of supporting smart infrastructure rehabilitation, promote policies that incentivise the integration of IoT technologies in infrastructure rehabilitation efforts to enhance resilience and ensure future preparedness, while encouraging the adoption of smart building technologies, sensor networks, and IoT-enabled monitoring systems in the reconstruction and retrofitting of critical infrastructure.

Last but not least, provide financial support and grants to encourage the deployment of IoT solutions that enhance the safety, efficiency, and sustainability of recovered infrastructure.

By implementing these policy-driven recommendations, policymakers can create an enabling environment that supports the integration of IoT technologies in crisis preparedness and facilitates effective response coordination, recovery efforts, and mitigation strategies.

7. Conclusions

In this paper, we have explored various aspects of crisis management and the role of IoT technologies in addressing challenges related to pandemics, natural disasters, cybersecurity, and attacks on public spaces. Through an analysis of the current state of play, research challenges, ideal scenarios, risk analysis, behavioural and cultural challenges, and data analysis, we have identified key insights and best cases in each domain. These findings provide valuable recommendations for research, standardisation, business strategies, and policy initiatives.

For the era of pandemics, the adaptation of smartphones within Europe and the use of contact tracing apps have demonstrated the potential of IoT technologies in enhancing public health surveillance and response. However, challenges such as privacy concerns and behavioural acceptance need to be addressed for wider adoption and effectiveness. In the context of natural disasters, the integration of IoT in disaster management has shown promising results in improving early warning systems, response coordination, and post-disaster recovery. Nevertheless, there are still challenges to overcome, including interoperability issues and the need for robust data analysis frameworks to leverage the full potential of IoT-generated data.

The cybersecurity aspect of crisis management highlights the importance of protecting critical infrastructure and ensuring the resilience of communication networks. IoT-based solutions offer innovative approaches to enhance cyber crisis management, but risks such as data breaches and sophisticated cyber-attacks require continuous research and proactive measures to mitigate. The threats posed by attacks on public spaces require innovative IoT technologies to enhance surveillance, threat detection, and emergency response. While there have been advancements in this area, challenges related to privacy, ethical considerations, and data analysis methods need to be addressed to ensure effective and responsible use of IoT technologies in securing public spaces.

Based on our analysis, we put forward a set of recommendations. Research recommendations call for further exploration of emerging technologies, such as AI, to enhance crisis management capabilities. Standardisation and interoperability recommendations emphasise the need for harmonised frameworks to facilitate seamless integration and communication among diverse IoT systems. Business-driven recommendations underscore the importance of better response coordination, resource deployment, and data-driven decision-making. Finally, policy-driven recommendations highlight the role of policymakers in creating an enabling environment that supports the adoption and responsible use of IoT technologies in crisis preparedness.

In conclusion, the integration of IoT technologies in crisis management holds great promise in addressing the complex challenges posed by pandemics, natural disasters, cybersecurity threats, and attacks on public spaces. By embracing the recommended strategies and approaches, stakeholders can unlock the full potential of IoT and foster a resilient and adaptive society better equipped to handle future crises.

8. References

(Butler et al., 2014, p. 3) Butler, D., Farmani, R., Fu, G., Ward, S., Diao, K., and Astaraie-Imani, M. (2014). A new approach to urban water management: Safe and sure.

(Chelleri et al., 2015) Butler, Ruth and Shibaz, Limor. (2013). Striving to connect and striving to learn: Influences of relational and mastery goals for teaching on teacher behaviors and student interest and help seeking. International Journal of Educational Research. 65. 10.1016/j.ijer.2013.09.006.

(Mannakkara et al., 2008) "Build Back Better" Principles for Reconstruction. Sandeeka Mannakkara*, Suzanne Wilkinson and Tinu Rose Francis. Department of Civil and Environmental Engineering, The University of Auckland, Auckland, New Zealand

(Twigg J ,2007) Characteristics of a disaster-resilient community – a guidance note. DFID Disaster Risk Reduction Interagency Coordination Group, London

Contributors

The document was written by several participants of the AIOTI FG Buildings and Communities.

Editor:

- Ricardo Vitorino, Ubiwhere

Reviewer:

- Damir Filipovic, AIOTI Secretary General

Contributors:

Name	Company/Organisation
Ana Pereira	Ubiwhere
Rita Santiago	Ubiwhere
Patricia Jimenez	NTT Data
Pietro Dionisio	Medea
Lazaros Karagiannis	ICCS
Evangelos Maltezos	ICCS
Panagiotis Michalis	ICCS
Dimitris Diagourtas	Satways
George Suciu	BEIA Consult
Monica Florea	SIMAVI
Asbjorn Hovsto	Hafenstrom
Flemming Sven	Hafenstrom
Tonny Velin	CENTIC
Dolores Ordonez	AnySolution
Karoline Krenn	Fraunhofer Fokus
Romain Vanhee	Yncrea ISEN
Rute Sofia	fortiss
Roumen Nikolov	Virtech
Amelie Gyrard	Trialog
Gabriel Petrescu	BEIA Consult
Mario Drobics	AIT

Editors and Contributions made by previous AIOTI members:

Name	Company/Organisation
Celine Prins (Co-Editor)	Institute for Future of Living
Fa Somers	Arthur's Legal
Arthur van der Wees	Arthur's Legal
Erik van der Wijk	DeWaarde Fabriek

Acknowledgements

All rights reserved, Alliance for IoT and Edge Computing Innovation (AIOTI). The content of this document is provided 'as-is' and for general information purposes only; it does not constitute strategic or any other professional advice. The content or parts thereof may not be complete, accurate or up to date. Notwithstanding anything contained in this document, AIOTI disclaims responsibility (including where AIOTI or any of its officers, members or contractors have been negligent) for any direct or indirect loss, damage, claim, or liability any person, company, organisation or other entity or body may incur as a result, this to the maximum extent permitted by law.

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT and Edge Computing Innovation in Europe, bringing together small and large companies, academia, policy makers and end-users and representatives of society in an end-to-end approach. We work with partners in a global context. We strive to leverage, share and promote best practices in the IoT and Edge Computing ecosystems, be a one-stop point of information on all relevant aspects of IoT Innovation to its members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of IoT and Edge Computing Innovation in society. AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT and Edge Computing ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability and defining policies.