Chapter 11

Risks, Safety and Security in the Ecosystem of Smart Cities

Stig O. Johnsen

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.70740

Abstract

We have performed a review of systemic risks in smart cities dependent on intelligent and partly autonomous transport systems. Smart cities include concepts such as smart transportation/use of autonomous transportation systems (i.e., autonomous cars, subways, shipping, drones) and improved management of infrastructure (power and water supply). At the same time, this requires safe and resilient infrastructures and need for global collaboration. One challenge is some sort of risk based regulation of emergent vulnerabilities. In this paper we focus on emergent vulnerabilities and discussion of how mitigation can be organized and structured based on emergent and known scenarios cross boundaries. We regard a smart city as a software ecosystem (SEC), defined as a dynamic evolution of systems on top of a common technological platform offering a set of software solutions and services. Software ecosystems are increasingly being used to support critical tasks and operations. As a part of our work we have performed a systematic literature review of safety, security and resilience software ecosystems, in the period 2007–2016. The perspective of software ecosystems has helped to identify and specify patterns of safety, security and resilience on a relevant abstraction level. Significant vulnerabilities and poor awareness of safety, security and resilience has been identified. Key actors that should increase their attention are vendors, regulators, insurance companies and the research community. There is a need to improve private-public partnership and to improve the learning loops between computer emergency teams, security information providers (SIP), regulators and vendors. There is a need to focus more on safety, security and resilience and to establish regulations of responsibilities on the vendors for liabilities.

Keywords: safety, security, resilience, smart cities, software ecosystems

1. Introduction

This paper contains a discussion and review of safety, security and resilience of smart cities, considered as software ecosystem (SEC). The purpose is to provide an overview of research in the field, identify emergent risks in a systemic perspective and identify possible issues that existing literature is not addressing adequately. The article is initiated by a discussion of the concept of software ecosystems and the need for safety, security and resilience in smart cities.

1.1. Smart cities and software ecosystems

In Ref. [1] there is a fairly general definition of a smart city, described as a place when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure, fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance. From [2], looking at specific systems, smart cites are described as a city that monitors and integrates conditions of its critical infrastructures, traffic (including roads, bridges, tunnels, rails, subways, airports, seaports), communications, water, power and major buildings. All this is done in order to optimize resources, plan its preventive maintenance and monitor security aspects while maximizing services to its citizens.

A literature review of software ecosystems in general was performed in [3] identifying 90 papers in the period from 2007 to 2012. The review identified the software ecosystem (SEC) as a fruitful systemic perspective. The review inspired us to find papers discussing safety, security and resilience of SEC published in the period from 2007 to 2016.

A software ecosystem (SEC) describes the complex environment of a smart city. A SEC will consist of components developed by actors both internally and externally, and solutions will spread outside the traditional borders of software companies to a group of companies, private persons and entities. In [3] they defined a software ecosystem as: "*the interaction of a set of actors on top of a common technological platform that results in a number of software solutions or services. Each actor is motivated by a set of interests or business models and connected to the rest of the actors and the ecosystem as a whole with symbiotic relationships, while, the technological platform is structured in a way that allows the involvement and contribution of the different actors….*"

When discussing software ecosystems, we include the legal and organizational framework in addition to applications and supporting infrastructure as described in **Figure 1**. Scope of digital ecosystems.

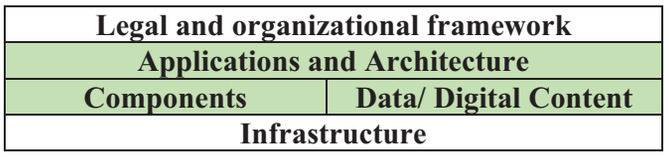

Figure 1. Scope of software ecosystems.

Software ecosystems are often based on the internet as infrastructure. The internet economy makes up a significant part of the GDP in 2016 since it is 5.3% of GDP [4]. SEC has gained more importance due to mobile platforms such as iPhone and android. Examples of SEC are:

- Digital learning environments;
- Mobile systems (phone applications);
- Shopping and payments systems;
- Social networking systems;
- Personal wellness and healthcare (training, food, medical equipment and surveillance…);
- Smart cities with transportation, infrastructure control (water, power). A part of Smart cities is intelligent transport systems (ITS) controlling vehicles, traffic management systems, electronic payments…;
- "Smart farming" with systems to track livestock and harvest/yield; outside cities.

Arguments for discussing software ecosystems has been the speed of development; increased competition and reduction of development costs due to the opening up of development outside of organizational silos. Some of the software ecosystems are critical, in that a malfunction can severely affect the functioning of society or personal well-being. Examples are systems used in transportation, car control systems and health systems (such as pacemakers).

1.2. Safety, security and risks

In this paper we have used the definition of safety as a state, as described by Department of Defense - [5], "*freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.*" This definition describes safety as being free from conditions causing a mishap or accident, i.e., safety is in some sense a "non-event."

Security is used to describe conditions of intentional harm. The relationships to safety are discussed in [6]. Security is defined as "*the degree to which malicious harm is prevented, reduced and properly reacted to*" and safety is defined as "*the degree to which accidental harm is prevented, reduced and properly reacted to*" from [7]. In information systems, there has often been a focus on "*information security.*" Information security is defined as *"protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: integrity, confidentiality and availability"*, from [8]. Since software ecosystems not only handle information, but also actual critical processes in smart cities, in automobiles and other applications the software ecosystems must both be secure (i.e., protected from malicious harm) and safe (i.e., protected from accidental harm). The systems must be able to handle unanticipated risks, and the ecosystem must be able to handle breakdowns and ensure that the systems has a safe state and/or a secure state.

In [9], the following definition of risk is given, "*Risk: two dimensional combination of the consequences (of an activity) and associated uncertainties (what will the outcome). Probabilities*

are used to express the uncertainties. When risk is quantified in a risk analysis, this definition is in line with the ISO/IEC Guide 73 (2002) standard definition [10]*: combination of the probability of an event and its consequence*." Related to new emerging risks and complexities of interactions, there may be challenging to establish the probability of an event since they may be unanticipated.

Systemic risk is defined as "*Probability of loss or failure common to all members of a class or group or to an entire system."* When discussing systemic risks related to smart cities we are exploring failures common to members of a smart city.

A key element when assessing systemic risks are the scope and prioritization of systems to be evaluated. We have focused on critical systems of common interest in a city. In the following we have discussed risks and protection of what is defined as part of critical infrastructure. Definition and protection of critical infrastructure has been a key concern in the US and EU. In the US the establishment of the national infrastructure protection plan (NIPP) from 2009 has been updated systematically. The latest, [11], has the title "Partnering for Critical Infrastructure – Security and Resilience." The successive NIPP has identified specific areas of concern such as interdependencies, cyber security and the international nature of threats. The risk management framework of NIPP is interesting since it is broad and systemic including physical, cyber and human elements. In the EU, the directive 114/08 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection was established as a council directive in 2008 [12]. In **Table 1**, we have described critical infrastructure sectors.

The main elements and areas of this list of critical infrastructure, is highly relevant when discussing smart cities, of special interest are smart city applications related to: Transportation systems, energy systems (power supply), bank and finance; communication systems; Technologies of information (including navigation systems); Water supply and health systems. The following areas are critical when impacted by loss or failures (**Table 2**).

The criticality or potential loss due to failures, breakdowns or attacks increases the need to be able to support critical operations even when the system is under stress or may fail, thus the ability to handle unanticipated incidents (or ability to go to a safe and secure state) are gaining importance. The concept of resilience engineering is an important strategy to handle these unanticipated incidents. In [13] resilience is defined as "*the intrinsic ability of a system to adjust*

US-NIPP sectors	EU 114/08 sectors
Energy	Energy—electricity, oil, natural gas
Transportation systems	Transport—roads and highways, railroads, aviation, inland waterways, shipping and ports
Agriculture and food; bank and finance; communications; military installation and defense; technologies of information; national monuments and icons; drinking water treatments plans	(NA—not applicable yet)

Table 1. Critical infrastructure sectors in US-NIPP and EU 114/08.

Areas impacted by smart cities	Examples of critical loss or failures
Transportation systems—Intelligent transportation, management and control of transport being impacted by surveillance, Google Map used to recommend routes, autonomous transport, traffic control centers managing transport and road signals	Breakdown of transport; impacting emergency services (police, fire, ambulance) or flow of material. (trough exploiting vulnerabilities in autonomous car systems; or influencing traffic control systems/halting control systems)
Energy systems—smart metering and improved management through centralized or more technology-based power grid systems	Breakdown of power supply – breakdown of power grids through exploiting vulnerabilities in new technology, on a control level and in smart metering systems
Bank and finance—many areas—one example payments systems integrated in toll roads and parking to manage traffic (reduce traffic in selected areas) and to make parking more user friendly and efficient	Breakdown of payment systems, halting/delaying key services
Communication systems and technologies of information (including navigation systems)—autonomous cars, traffic control, route planning and signaling systems dependent on information technology and navigation systems.	Breakdown (accidents) in transportation due to nonfunctioning supporting technology
Water supply—managed and optimized by control systems	Breakdown, contamination of water supply due breakdown (hacking) of control systems
Health systems—dependent on sensors (such as in pacemakers) and communication systems (sending and receiving data from health professionals), "just in time" management of health,	Breakdown/errors in health systems used to manage critical operations, such as in peacemakers

Table 2. Systemic risks in smart cities.

its functioning prior to or following changes and disturbances, so that it can sustain operations even after a major mishap or in the presence of continuous stress." In [14], Woods focuses on unanticipated disturbances and adaptations, and describes resilience as: "*How well can a system handle disruptions and variations that fall outside of the base mechanisms/model for being adaptive (adaptive defined as the ability to absorb or adapt to disturbance, disruption and change).*" The handling of the unanticipated and continued functioning has been a key property of resilient systems.

In the European Union, safety, security and resilience are prioritized in the cybersecurity strategy [15]. Three of the top five strategic issues mentioned are: Develop the industrial and technological resources for cybersecurity; Achieving cyber resilience; and establish a coherent international cyberspace policy for the EU. Thus, safety, security and resilience of smart cities are important issues that should be explored further. In addition, it is important to understand how risk governance of smart cities is addressed and established in order to support a coherent cyberspace policy of the key issues.

2. Problem definition and methods

Based on the preceding introduction, and the summary above, the three research questions we wanted to explore are:

- RQ1: How is safety, security and risks of smart cities (software ecosystems of cities) framed and defined?
- RQ2: How is risk governance of smart cities (software ecosystems of cities) addressed?
- RQ3: What are key issues in Governance of the ecosystem?

In the following we have described some of the challenges and problems of these research questions and our methodology (i.e., approach).

2.1. Challenges and problems

There is often poor focus on emerging risks, safety and security. These issues have been identified late when vulnerabilities have been exploited and unwanted incidents have been published. The suppliers and vendors (software vendors) seldom has to pay for unwanted incidents even if they are due to poor quality issues in the systems such as safety, security or resilience. The bill has been given to the users, the organizations and/or society.

Critical infrastructure is in most cases regulated by the authorities. Safety and security regulation is often reactive, and lags technological innovation. New software is implemented and societal consequences are discussed later. Internet of things (IoT) is an example of new technology that are introduced in software ecosystems that may affect operations of critical infrastructure. IoT has introduced a broad set of vulnerabilities and can challenge safety, security and resilience of software ecosystems. As an example the Mirai botnet was used in a Denial of service (DoS) attack on the internet firm Dyn, Ref. [16], using unsecured devices on a large scale. The attack affected Dyn's clients such as Twitter, Reddift, Spotify, and SoundCloud. The cyber-attacks caused outages across the whole East Coast in the US in October 2016. When discussing vulnerabilities in a software ecosystem such as in smart cities, one challenge is that there is not one single supplier, but a set of suppliers that must be involved. Incident handling moves to a broader area where it can be difficult to identify responsibilities and manage competencies. This is relevant, in [17] the author points out that there are serious vulnerabilities (poor quality control) in systems used in smart cities (i.e., traffic control systems), which could be used to cause traffic jams or collisions.

2.2. Methodology

The literature review started by a keyword search based on combination of "software ecosystems" "smart cities" and "safety, security, resilience." Using Google Scholar and then searching the ACM Digital Library, IEEE Explore, Springer Link and Science Direct. The literature body was selected based on that software ecosystems/smart cities and safety (security and resilience) was the main theme. In addition, papers were selected based on a set of criteria i.e., have been peer reviewed and published in a scientific context (journal, conference), available in English, and more than one-page long. Since software ecosystems involves governmental rules, relevant white papers were also identified. The identified literature body is gathered in Section 5, numbered from [18–29] [LIT BODY:13] and [LIT BODY:14]. In addition, we have listed other general references that could not be included in the literature body, in Section 6.

The concept of Risk and Risk Governance has been an issue in the review, and we have structured papers based on risk governance, see [30], starting with problem framing; then risk appraisal (hazards and vulnerabilities); risk judgment; risk communication and risk management.

3. Findings and reflections

We found 14 papers in total, 13 papers published in the interval 2007–2016; and we included a paper from 2003 that had an illuminating discussion of resilience of systems. The following three sections are based on our research questions (RQ1 to RQ3 as described in Section 2) and have been used as title of the chapter:

- Framing of safety, security and risks in smart cities (RQ1)
- Risk Governance of smart cities (software ecosystems) (RQ2)
- What are key issues in Governance of the ecosystem? (RQ3)

3.1. Framing of safety, security and risks

In [31] there is a discussion of the convergence of safety and security, pointing out that a successful integration of both requirements needs the collaboration of both safety and security disciplines, aided by a common understanding. In [28, 32], it is pointed out that both safety and security issues must be assessed to build trustworthy software ecosystems. Issues identified through security analysis (i.e., threats) must be combined with issues from safety analysis (i.e., hazards). In [33] there is a focus on of the development of industrial control systems and how safety and security must be integrated in the development methodologies. These control systems are similar to control systems employed in smart cities. An overview and comparison of methodologies is given.

In [34], a broad overview of security and safety challenges of digital systems are given based on an ecological perspective. Ecology is used both as a metaphor to learn from the development in the nature, but also to have a more holistic perspective of systems involving human actors in a society. The ecosystem perspective is as an important viewpoint when discussing safety and security in a changing word, and especially when exploring risks and risk governance of smart cities.

In [35] there is a discussion of infrastructure resilience from an organizational context. Adaptive capacity, resource robustness is discussed related to infrastructure and a conceptual framework for assessing resilience is outlined. The conceptual framework seems to be useful when discussing resilience in software ecosystems, especially of critical (infrastructure) ecosystems. In [36] different elements of resilience are discussed. The paper presents a framework for system resilience, consisting of five aspects: time periods, system types, events, resilience actions and properties to preserve. It is followed by principles for emergence, and factors affecting resilience, including improving resilience, trade-offs, and loss of resilience.

Not many textbooks (that can be used in teaching) have been found related to implementation of security and resilience in control systems of smart cities. However, in [37] guidelines for secure and resilient software development are discussed. The development guidelines are targeted toward software ecosystems; and the goal is to improve developer skills related to security and resilience. It is pointed out that security and resilience must be integrated from concept/early design, it reviews security design methodologies and suggests how to measure the development process. The discussion of security in Industrial Automation setting, is discussed in [38], including the challenges of adapting general software security principles to industrial automation and control systems.

In [29] resilience and cyber security of the ecosystems is seen as a part of the maturity of governance and collaboration between industry and government. Thus, cyber resilience is seen as the next step of cyber security.

In [24] there is a discussion of the security dynamics of software ecosystem (SEC), pointing out that SEC reduces cost and are increasing efficiencies for the software producers while society get the costs of software failures (i.e., issues related to security, safety and poor resilience). The paper has a quantitative examination of 27,000 vulnerabilities disclosed over the past decade (1996–2008). The paper identifies the interest of several stakeholders in the market of software vulnerabilities such as the vendors, safety experts/consultants, security information providers (SIP), and criminals. The paper explores several policies such as security trough obscurity, responsible disclosure of vulnerabilities (as a suggested policy) or security trough transparency. One of the key insights is that secrecy prevents people from assessing their own risks, which contributes to a false sense of security. The process of responsible disclosure is that the researcher discloses full information to the vendor, expecting that a patch is developed within a reasonable timeframe. An increasing number of vendors and security organizations have adopted some form of responsible disclosure. The role of security information providers (SIP) as risk-communicators is discussed in the vulnerabilities market.

In summary, there has been a positive development in identifying the need to explore both safety and security in development and to use resilience as a mitigating strategy. The concept of software ecosystems benefits the developers and industries, but it seems that at present that society gets the costs of software failures. Responsible disclosure of vulnerabilities to the vendors, expecting a patch, seems to be a beneficial policy. The role of actors in the software ecology, such as security information providers should be explored further.

3.2. Risk governance of smart cities (software ecosystems) –vulnerabilities and risks

In [26] a set of vulnerabilities in cars are pointed out such as the possibility to control a wide range of automotive functions and completely ignore driver input from dashboard, including disabling the brakes, selectively braking individual wheels on demand, stopping the engine, and so on. Attacks were easy to perform and the effects were significant. It is possible to bypass rudimentary network security protections within the car, and perform attack that embeds malicious code in the car that will completely erase any evidence of its presence (after a crash). There is a discussion of the challenges in addressing these vulnerabilities while considering the existing automotive ecosystem.

http://dx.doi.org/10.5772/intechopen.70740

In [27] Semi-autonomous and fully autonomous cars are described as coming from the development stage to actual operations. The autonomous systems are creating safety and security challenges. These challenges require a holistic analysis, under the perspective of ecosystems of autonomous vehicles. The perspective of ecosystems is seen as useful to understand and mitigate security and safety challenges. These systems will become important critical information infrastructures, simultaneously featuring connectivity, autonomy and cooperation. Threat analyses and safety cases should include both (random) faults and (purposeful) attacks.

In [39], there is a discussion of Cyber-Physical infrastructure risks in the future smart cities. Several examples of unwanted incidents are described in transportation systems (autonomous vehicles; Trains; …) in electricity distribution and management and in the water and wastewater systems sector. It is suggested to the regulator to work with standards and regulations in addition to communication and increased engagement by giving direct assistance. Challenges mentioned are the need to establish goal based standards and regulations as new technology is implemented and to focus on dissemination of best practices in combination with systematic education.

In [17] there is an empirical evaluation of "smart cities" looking at a broad set of technologies of traffic control, management of energy/water/waste and security. Known vulnerabilities are in traffic control systems, mobile applications used by citizens, smart grids/smart meters and video cameras. The issues are in line with peer-reviewed papers, i.e., lack of cyber security testing and approval, lack of encryption, lack of City Computer Emergency Response Teams (CERT), and lack of cyber attack emergency plans. There are reasons to anticipate that we establish potential for serious incidents, if these issues are not addressed and mitigated.

In [20] there is a discussion of the expanded use of federated embedded systems (FES) in automotive and process automation. Expected benefits include the possibility of third-party actors developing add-on functionality; a shorter time to market for new functions; and the ability to upgrade existing products in the field. This is a substantial area for innovation and change, the responsibilities of the manufacturer will change, and a key challenge will be ecosystem management. However, it is suggested that the liabilities and responsibilities of the total product must rest with the manufacturer. The regulator has a key role to define responsibilities. These issues highlight the need for Risk Governance of systems to be used in smart cities.

In [21] open software ecosystem is proposed as an approach to develop software for embedded systems in the automotive industry. The focus is on the need to deliver functionality to customers faster. The paper describes quality attributes and defines a reference architecture. Both safety, security and dependability are explored.

In [22] they model the architecture of a cloud-based ecosystem, showing security patterns for its main components; and discuss the value of such an approach. The ecosystem approach provides a holistic view and is valuable in security, by indicating places where security mechanisms can be attached. Holistic views are seen as important to combine quality factors such as safety and reliability with security. By using this abstraction level, it is argued in the paper that this unified approach reduces complexity, one of the important weaknesses used by attackers and can enable analysis of the propagation of threats and data leaks.

In [28] they cover research on Enterprise Architectures of ecosystems (i.e., software ecosystems) discussing resilience and adaptability as a key area and suggest reference architectures mentioning security. However, safety is not mentioned.

In [25] there is a discussion on how to build robust and evolvable resilient software systems, discussing redundant data structures, transformer middleware and service-oriented communities. The use of transformer middleware may lead to more complex systems and higher costs or latency. Exploration of service-oriented communities may support adaptation and spontaneous emergence of resilience, but may lead to higher costs due to high degree of redundancy and challenges with deterministic behavior.

In summary, there has been documented several vulnerabilities in smart cities, intelligent transport systems and autonomous cars. However, software ecosystems have beneficial elements since more actors are developing functionality and enabling a shorter time to market. Liabilities must rest on the manufacturer and the regulator must define responsibilities. The ecosystem provides a holistic view that is seen as important to combine safety and reliability with security. It is argued in several papers that this approach reduces complexity; one of the weaknesses used by attackers and can enable improved analysis of propagation of threats and data leaks.

3.3. Key issues in governance—responsibilities, management and communication

International governance of security of the infrastructure of software ecosystems is addressed through several channels such as standards (ISO, IEC) or international bodies such as OECD, EU, NATO and UN. Software Ecosystems are international—involving many actors with different agendas. In [40] there is a discussion of governance of emerging technology (such as IoT) as it is integrated into critical infrastructure. It is suggested that manufacturers should follow the principle of privacy and security by design, when developing new products, and must be prepared to accept legal liability for the quality of the technology they produce. Buyers should collectively demand that manufacturers respond effectively to concerns about privacy and security. Governments can play a positive role by incorporating minimum security standards in their procurement. It is suggested that government regulations should require routine, transparent reporting of technological problems to provide the data required for a transparent market-based cyber-insurance industry. It is suggested to establish an agreement (a compact) based on collaboration between government, industry and private society supporting evidence based decision making.

In [19] the focus is on software assurance of safety-critical and security-critical software (i.e., conceptualized as SEC). The perception is that the use of current methods has not achieved the wished-for level of protection, and that there are missing security principles and standards. The industry continues to see an expansion of major breaches occurring in both the public and private sectors. There need to be incentives or regulations for implementing protective and immunizing measures. Such measures could be a mandatory part of the security architecture of all applications. A formal requirement could be that implementation of protective and immunizing measures is included in any certification process. On governance it

is suggested to establish software assurance standards at the UN level; to have a risk based approach; to share best of breed methods; and the need to discuss liabilities for damages occurring as a result of an attack or security-related errors.

In [18] the issue of Information security is highlighted in national governance. They propose a comprehensive conceptual framework for building a robust, resilient and dependable Information Security Infrastructure, based on the perspective of software ecosystems.

Development of security and resilience is seen as a maturity process in [41], referencing the CERT Resilience Management Model (CERT RMM) from the Carnegie Mellon Software Engineering Institute. Resilience as a strategy is not simple to implement, in [42], the analysis of resilience strategies in the US agencies revealed that most of the plans only focus on a few of the stages of resilience. Plans do not focus on resilience in the information and social domain, and do not consider long-term adaptation.

In [23] there is a discussion of resilience as a high level design principle. There is an argument for resilience in systems, i.e., distributed systems composed of independent yet interactive elements may deliver equivalent or better functionality with greater resilience. Guidelines for resilience are given such as robustness through resilience rather than resistance, and intervention rather than control. It is argued for the perspective of resilience and to use an ecological perspective in system design and deployment, thus this article describes a design methodology on the ecology level based on resilience principles.

In [43] there is a discussion of development of software-systems, and ignoring some perspectives of software ecosystems. If we want systems that are secure and reliable, both security and reliability must be built together. Applications, middleware and operating systems must be built in the same way, to get systems that are inherently secure and that can withstand attacks from malicious applications and resist errors. The suggested approach is based on security patterns that are mapped through the architectural levels.

3.4. Key issues related to methods of risk assessments

The papers identified that the risk assessment was complex, thus there is a need to use methods that integrates the following issues:

- Technology, ensuring that scope of methodology includes safety issues (such as described by IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems) security issues (ISA/IEC-62443 to ensure secure Industrial Automation and Control Systems) in addition to a Certification Framework such as the European IACS components Cybersecurity Certification Framework (ICCF).
- Human Elements: Risk understanding and perceptions of the involved actors, including understanding of both safety issues and security issues
- Organizational issues, ensuring that responsibilities are in place, and that necessary organizational structures are in place both to specify, implement, operate and handle deviations critical components of the system.

In summary, if we want systems that are secure and reliable, both security and reliability must be built together. The suggested approach is based on security patterns that are mapped through the architectural levels of the system. However, there is missing international regulation or compacts based on private public partnerships to ensure privacy, safety, security and resilience. Vendors must ensure this quality by design, and must be prepared to accept legal liability for the quality of the technology they produce. Regulations should require routine, transparent reporting of technological problems to provide data for a transparent market-based cyber-insurance industry. There is an argument for resilience in systems, composed of independent yet interactive elements that may deliver equivalent or better functionality with greater resilience. However, the maturity of resilience in use is varying.

4. Summary

In this review, we have used the concept of software ecosystems on systems used in smart cities. Our review indicates that the "smart cities" concept are vulnerable and subject to increased emerging risks due to introduction of new technology (such as autonomous transport systems) unsecured components and new connections that has not been foreseen or thought of. Threats, new vulnerabilities and new unwanted incidents are emerging and can be observed through media attention and exploration.

Software assurance of safety-critical and security-critical software (conceptualized as the software system ecosystem) is strongly needed. Current methods have not achieved the necessary level of protection, and are missing security principles and standards. The industry continues to see an expansion of major breaches occurring in both the public and private sectors. Incentives or regulations are needed to implement protective and immunizing measures.

The ecosystem approach seems a promising approach since it provides a holistic view of security needs, by indicating places where security mechanisms can be attached. This approach reduces complexity; one of the important weaknesses used by attackers and can enable analysis of the propagation of threats and data leaks.

Due to the increased proliferation of the IoT and the vulnerability of the Internet, there is a strong need to establish a social compact (agreement) ensuring that the Internet continues to be accessible, inclusive, secure and trustworthy. To ensure that all actors in the value-chain understand the vulnerabilities and the risks, a silo-based "need to know" principle must be replaced by transparent and open reporting. This may support a market based cyber-insurance industry.

In the literature body and in [32] there is an increased understanding of the need for collaboration between the safety and security disciplines to understand and mitigate risks and vulnerabilities. The differences in perspectives between security and safety are due to different adversity models. The security community addresses threats (directed, deliberate, hostile acts) and the safety community addresses hazards (undirected events). Software ecosystems are so pervasive across all sectors of economic activity that this silo approach can no longer be regarded as acceptable.

There is a need for international rulemaking and regulation. This may be difficult to achieve. Vendors must ensure safety, security and resilience by design, and must be prepared to accept legal liability for the quality of the technology they produce. Prescriptive and detailed rulemaking on a national level is missing and is difficult to achieve. This is an international challenge. The Mira denial of service (DoS) attack was due to components produced in China but used in the US. No penetration testing, acceptance or testing of robustness was performed prior to release of the product.

In general, there is a need to establish functional standards, responsibilities of liabilities and practices cross-countries. There must be a specific responsibility of the producer to ensure safety, security and resilience, and ideally, a formal process of product acceptance or certification or safety case exploration before a product can be sold or offered. Thus, there is a need for regulatory action from government to set minimum standards, establish responsibility, and follow up of incidents/accidents. The suppliers should establish a proactive focus on (best practice) safety/security standards.

In **Table 3**, we have exemplified critical ecosystems such as smart cities/intelligent transport systems. Based on our review so far, these critical systems have no mandated test criteria (neither safety cases nor security cases, thus it is described as "Poor") and there are no organizations such as CERTS to handle and systematize unwanted incidents.

Ecosystem	Vulnerability	Test	CERT
Smart cities and intelligent transport systems	Disruption of services (transport, power, water)	Poor	No

Table 3. Critical digital ecosystems and learning.

Development of safety has often been dependent on exploration of publicized accidents and incidents, and a systematic learning loop between users, the regulator and industry. An important component in the learning loop of software systems has been structured reporting and analysis of incidents trough computer incident response teams, i.e., CERTS. There is a need to regulate and ensure that new technology is approved/tested (has some sort of quality control/safety case examination) and that there is some sort of a structured learning process when incidents happen.

Software ecosystems will be exposed to new strains as new unsecured technology are introduced—thus there must be an increased focus on how to handle surprises i.e., resilience and adaptability in software ecosystems to ensure that new demands/stress/failures are not impacting the infrastructure in a catastrophic way. In the review of resilience, [44], there is an increased use of resilience in papers from 2006 on. The resilience concepts are in development, and there is a need to be careful not to place the responsibility of resilience on the individual (i.e., expecting resilience from an individual only). Resilience is the integrated ability of the ecosystem as a whole consisting of an interplay between technology abilities, organizational abilities and human abilities. During the review process, several issues have not been addressed adequately, and are in need of further research, such as:

- There has not been an exploration of the different actors that can affect safety, security and resilience in smart cities (i.e., software ecosystems). Such an exploration should give insight into how to improve safety, security and resilience of systems, and how liabilities should be placed
- There has been no systematic discussion of the maturation of resilience in smart cities (specifics in software ecosystems) discussing technology, organizations and human awareness/human actions together
- There have been few definitions of patterns of resilience in smart cities and related software ecosystems and how these can be used at an architectural level. There is a missing discussion on how smart cities/critical ecosystems can become resilient, based on patterns
- How to perform ecosystem management of development of federated embedded systems (FES) used in smart cities (i.e., transportation, automotive systems…)

Author details

Stig O. Johnsen[1,2]*

*Address all correspondence to: stig.ole.johnsen@ntnu.no

1 NTNU, Faculty of Information Technology, Trondheim, Norway

2 SINTEF Technology and Society, Safety Research, Trondheim, Norway

References

[1] Caragliu A, Del C, Nijkamp P. Smart cities in Europe. Journal of Urban Technology. 2011;**18**(2):65-82. DOI: 10.1080/10630732.2011.601117

[2] Chourabi H, Nam T, Walker S, Gil-Garcia JR, Mellouli S, Nahon K, et al. Understanding smart cities: An integrative framework. In: IEEE Computer Society, Proceedings of the 45th Hawaii International Conference; 2012. pp. 2289-2297

[3] Manikas K, Hansen KM. Software ecosystems–a systematic literature review. Journal of Systems and Software. 2013;**86**(5):1294-1306

[4] Boston Consulting Group. The Internet Economy in the G-20. 2012 Retrieved from: www.bcgperspectives.com

[5] DoD. U.S. Department of Defense, "Standard Practice for System Safety" MIL-STD-882D 2000

[6] Pietre-Cambacedes L, Chaudet C. The SEMA referential framework: Avoiding ambiguities in the terms "security" and "safety". International Journal of Critical Infrastructure Protection. 2010;**3**:55-66

[7] Firesmith DG. "Common Concepts Underlying Safety, Security, and Survivability Engineering", Technical Note CMU/SEI-2003-TN-033. Carnegie Mellon University; Pittsburg, USA, 2003

[8] U.S. Code Title 44, Chapter 35, Subchapter III, § 3542 retrieved at 2006-12-31. Uscode. House.Gov/Download/Pls/44c35.Txt

[9] Aven T. Risk Analysis: Assessing Uncertainties beyond Expected Values and Probabilities. Wiley; Chichester, UKT, 2008

[10] ISO Guide 73, I. E. C. (2002): Risk Management. Vocabulary. Guidelines for Use in Standards. Geneva, Switzerland

[11] NIPP (2013) Department of Homeland Security: Partnering for critical infrastructure security and resilience. Washington D.C.: Department of Homeland Security. Retreived from www.dhs.gov

[12] EU (114/08) On the identification and designation of European critical infrastructure and the assessment of the need to improve their protection. Council directive (2008)

[13] Hollnagel E, Woods D, Leveson N. Resilience Engineering. Ashgate; Hampshire, England, 2006

[14] Woods D. In: Hollnagel E, Woods D, Leveson N, editors. Essential Characteristics of Resilience. "Resilience Engineering" Ashgate; Hampshire, England, 2006

[15] EU (2013) European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyber Space (7 February 2013)

[16] CSM. 2016. Retrieved from: www.csmonitor.com/World/Passcode/2016/1026/What-you-need-to-know-about-the-botnet-that-broke-the-internet

[17] Cerrudo C. (2015). An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks. Securing Smart Cities – White paper – IOActive. www.ioactive.com/pdfs/IOActive_HackingCitiesPaper_cyber-security_CesarCerrudo.pdf

[18] Ranjan S, Maurya MK, Malviya AK, Yadav R, Gupta R, Mishra M, Rai S. Building an information security infrastructure-a comprehensive framework towards a robust, resilient and dependable infrastructure. International Journal of Computer Science Issues. 2012;**9**:414-419

[19] Axelrod CW. Reducing software assurance risks for security-critical and safety-critical systems. In: Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island, IEEE; 2014, May. pp. 1-6

[20] Axelsson J, Papatheocharous E, Andersson J. Characteristics of software ecosystems for federated embedded systems: A case study. Information and Software Technology. 2014;**56**(11):1457-1475

[21] Eklund U, Bosch J. Architecture for embedded open software ecosystems. Journal of Systems and Software. 2014;**92**:128-142

[22] Fernandez EB, Yoshioka N, Washizaki H. Patterns for security and privacy in cloud ecosystems. In: Proceedings of the 23rd IEEE International Requirements Engineering Conference, Ottawa, ON, Canada; 2015. pp. 24-28

[23] Fiksel J. Designing resilient, sustainable systems. Environmental Science & Technology. 2003;**37**(23):5330-5339

[24] Frei S, Schatzmann D, Plattner B, Trammell B. Modeling the security ecosystem-the dynamics of (in) security. In: Economics of Information Security and Privacy. Springer Boston, MA; 2010. p. 79-106

[25] De Florio V. Robust-and-evolvable resilient software systems: Open problems and lessons learned. In: Proceedings of the 8th workshop on Assurances for self-adaptive systems, ACM; 2011, September. pp. 10-17

[26] Koscher K, Czeskis A, Roesner F, Patel S, Kohno T, Checkoway S, Savage S. Experimental security analysis of a modern automobile. In: 2010 IEEE Symposium on Security and Privacy; 2010, May. pp. 447-462

[27] Lima A, Rocha F, Völp M, Esteves-Veríssimo P. Towards safe and secure autonomous and cooperative vehicle ecosystems. In: Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, ACM; 2016. pp. 59-70

[28] Zimmermann A, Schmidt R, Jugel D, Möhring M. Evolving enterprise architectures for digital transformations. DEC. 2015;**15**:25-26

[29] Sharkov G. From cybersecurity to collaborative resiliency. In: Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense, ACM; 2016, October. pp. 3-9

[30] Renn O. (2005). Risk governance—Towards an integrative approach, white paper no.1—International risk governance council

[31] Piggin R. S. H. (2013). Process safety and cyber security convergence: Lessons identified, but not learnt? In: IET Conference Proceedings. The Institution of Engineering & Technology

[32] Bryant IRC. Towards a trustworthy software ecosystem. International Software Quality Management Conference (SQM); 2012. pp. 1-7

[33] Kriaa S, Pietre-Cambacedes L, Bouissou M, Halgand Y. A survey of approaches combining safety and security for industrial control systems. Reliability Engineering & System Safety. 2015;**139**:156-178

[34] Carlsson B, Jacobsson A. (2012). Om säkerhet i digitala ekosystem. Studentlitteratur AB, Lund, Sverige

[35] Longstaff PH, Armstrong NJ, Perrin K, Parker WM, Hidek MA. Building resilient communities: A preliminary framework for assessment. Homeland Security Affairs. 2010;**6**(3):1-22

[36] Sheard S, Mostashari A. A framework for system resilience discussions. In: Proc Eighteenth Annual Int Symp INCOSE; 2008

[37] Merkow MS, Raghavan L. Secure and Resilient Software Development. CRC Press; London, UK, 2010

[38] Krutz RL. Industrial Automation and Control System Security Principles. ISA; NC, USA, 2013

[39] DHS. Department of Homeland Security, Office of Cyber and Infrastructure Analysis: The Future of Smart Cities: Cyber-Physical Infrastructure Risk. 2015

[40] GCIG. 2016 Global Commission on Internet Governance, "One Internet" www.ourinternet.org

[41] Payette J, Anegbe E, Caceres E, Muegge S. Secure by design: Cybersecurity extensions to project management maturity models for critical infrastructure projects. Technology Innovation Management Review. 2015;**5**(6):26

[42] Larkin S, Fox-Lent C, Eisenberg DA, Trump BD, Wallace S, Chadderton C, Linkov I. Benchmarking agency and organizational practices in resilience decision making. Environment Systems and Decisions. 2015;**35**(2):185-195

[43] Fernández EB, Washizaki H, Yoshioka N, Van Hilst M. An approach to model-based development of secure and reliable systems. In: Sixth international conference on availability, reliability and security, ARES, Vienna. 2011. pp. 260-265. DOI: 10.1109/ARES.2011.45

[44] Bergström J, Winsen R, Henriqson E. On the rationale of resilience in the domain of safety: A literature review. Reliability Engineering & System Safety. 2015;**141**:131-141

IntechOpen