Critical Infrastructure in the Future City
Developing Secure and Resilient Cyber–Physical Systems

Hugh Boyes, Roy Isbell, Tim Watson

Cyber Security Centre, WMG, University of Warwick, UK
{hb, ri, tw}@warwick.ac.uk

Abstract. Cities face serious challenges that affect competitiveness, sustainability and their occupants' safety & security. In response, investment is made in city infrastructure projects. Given the complexity of the systems architecture, and interactions between physical and cyber domains, this paper shows how a multi-disciplinary approach can be adopted to address the challenges. It introduces an analysis methodology for use by multi-disciplinary teams to allow the dependencies and interactions of cyber–physical systems in physical–cyber environments to be explored. The analysis methodology offers a systematic way to study the cyber–physical systems and identify safety, security or resilience issues that need to be addressed in the systems design or operation.

Keywords: Smart cities, cyber–physical systems, cyber security, resilience, trustworthy software, critical infrastructure, physical–cyber environment, future city

1 Introduction

Projections indicate that 60% of the world's population will be urbanised by 2030 [1]. This compares to less than 40% of the global population living in cities in 1990 and with fewer than 10% of urban dwellers living in cities with populations <500,000 people [2]. The WHO anticipates that population growth in cities over the next 30 years will occur in developing countries [2]. This indicates that by the middle of the 21st century, the urban population of developing countries will more than double. This growth will result in the expansion of existing cities and development of new ones. Areas where these cities develop are often on coastal plains, putting them at greater risk from severe weather events and changes in sea levels [3].

The increasing size of urban populations creates significant challenges for future cities, dubbed as 'smart cities', where complex interactions between Cyber–Physical Systems (CPS) will aim to improve the quality of life and to proactively manage demand for scarce or costly resources. Creating future cities will present significant technical and economic challenges for both developed and developing nations.

Use of technology is not without risks, particularly with regard to the resilience and cyber security of critical city infrastructure. Future cities will evolve into sophisticated platforms, comprising systems-of-systems-of-systems or physical–cyber environments. There will also be a greater degree of system autonomy where humans will be relegated to the role of supervisor or maintainer, giving birth to a new breed of 'Cyber Janitor'.

Future cities will challenge existing safety and security engineering models e.g. the United States electricity blackout in 2003 [4] showed that in interdependent networks a very small failure in one network might lead to catastrophic consequences [5]. New and complex cascading failure modes will arise out of unforeseen or emergent system characteristics as they are developed in an incremental and ad hoc fashion, especially where more sophisticated technologies are added to an already ageing physical infrastructure.

This paper examines some challenges to be addressed if we are to understand and manage the potential future impacts. It starts by examining the nature of CPS and the evolution of the city as a platform. To understand the requirements this paper considers a city from three perspectives: the context of its data and systems, understanding resilience of systems and services, and an approach to deriving its cyber security needs. These perspectives form the basis of an analysis methodology under development by the authors.

2 Cyber–physical systems and The City as a Platform

There are a number of definitions of CPS [6–9]. Common features effectively describe control systems, networked and/or distributed, incorporating a degree of intelligence (adaptive or predictive), and work in real time to influence outcomes in the real world. These definitions point to the diverse nature of CPS found in transportation, utilities, buildings, infrastructure, manufacturing, and health care.

Although CPS have similarities with traditional data processing systems, e.g. their networked or distributed nature and a degree of automation, the real-time nature of their interactions with the physical world is a significant difference. Interactions are sensors detecting and measuring physical parameters with actuators to control physical processes. Feedback loops allow data about the environment and the physical processes to be collected and computed. Actuation may be automatic or by an alert to a human operator.

Critical infrastructure systems are CPS, whose failure would have economic or social impact. Society expects systems will operate in a safe, secure and consistent manner [10]. In response to environmental, demographic and societal pressures, cities may no longer conduct business as usual. Traditional city models are no longer appropriate, as transport and utility infrastructures becomes unsustainable and requires significant investment [11].

Some cities have embraced the concept of the 'city as a platform', a hyper-connected urban environment that harnesses the network effects, openness, and agility of the real-time web [12]. The focus has been on access to data, leading to development of smartphone apps and portals allowing citizens to 'connect' with city services and institutions [13, 14]. To address cyber security requirements we need to understand the proliferation of functions in this hyper-connected world [15]. Where functions in individual CPS interact, they will create new functions that will proliferate over time. To protect these complex systems we need to understand their network of functions, relationships and interdependencies. A study of critical infrastructure interdependencies [16] led to the identification of six dimensions, which can be used to examine CPS and supporting infrastructures:

- Type of interdependency, e.g. cyber, physical, logical or geographic;
- Environment, e.g. business, economic, public policy, legal, regulatory, security, technical, health/safety, or social/political;
- Coupling and response behaviour, e.g. adaptive, inflexible, loose/tight or linear/complex;
- Infrastructure characteristics, e.g. spatial, operational, organisational or temporal;
- Type of failure, e.g. common cause, escalating or cascading;
- State of operation, e.g. normal, stressed/disrupted, restoration or repair.

The study is a useful starting point in understanding interdependencies between city systems and infrastructure, however, the sophistication of solutions today is greater than those contemplated in 2001. The increased integration and automation of city systems requires a broader understanding of the 'city as a platform' if solutions are to deliver resilience and cyber security.

3 Future Cities Analysis Framework

We propose an analysis framework, which examines the critical city infrastructure and services from three perspectives: context, resilience, and cyber security. The analysis framework (Figure 1), builds on our work regarding the cyber security of buildings [17], adapted to focus at a city level on critical infrastructure and related services.

3.1 Identifying critical city infrastructure

Whilst there are a number of definitions for critical national infrastructure [18–20], from a city perspective the concept of critical infrastructure is not well defined. The UK's definition of critical national infrastructure (CNI) is: "those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends" [19]. Where criticality is determined based on a Criticality Scale [21], which assesses impact of events or scenarios on a national scale. From a city perspective, we propose that criticality addresses elements necessary for the delivery of essential services to the populace who are resident and/or work in the city and that impact is focused at city rather than national level. The critical infrastructure must encompass both the city's normal operating state, and its ability to effectively respond to natural or other disasters [22]. Our definition of a city's critical infrastructure translates the principles underlying criticality at a national level to apply them at a city level based on four factors:

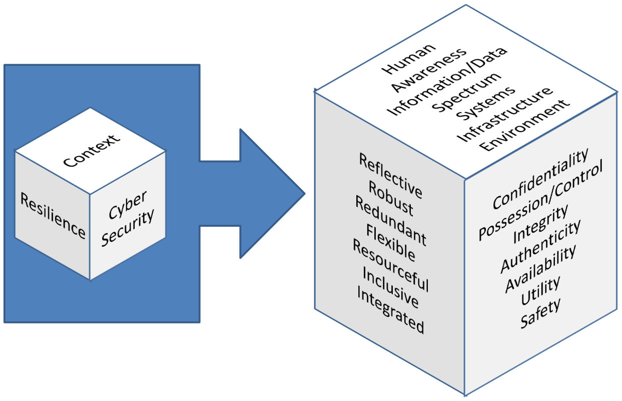

Fig. 1. Analysis Framework for secure and resilient Future Cities

- the impact on delivery of essential societal functions and services, e.g. to provide water, food and shelter, and to maintain law and order;
- the economic impact on the well-being and viability of the city, e.g. the ability to operate as a business and financial centre and provide employment;
- the impact on life, health and well-being of city occupants, e.g. to provide medical and social services to protect and care for citizens;
- the ability to respond to major incidents or disasters, e.g. to provide emergency services including sites to manage emergency operations and to provide housing in the event of a disaster.

The result of applying these factors to a typical city's infrastructure is illustrated in Table 1, which also identifies whether an element would normally be regarded as part of the critical national infrastructure.

Critical City Infrastructure	**Critical National Infrastructure**
Communications	Yes
Education (Schools, Colleges, Universities)	No
Emergency Services	Yes
Energy (Electricity, Gas, Oil/Petroleum products)	Yes
Financial Services	Yes
Food	Yes
Government (City administration)	Yes
Health	Yes
Leisure (Parks, Sport Facilities)	No
Transport (Road, Rail, Air, Waterborne)	Yes
Water	Yes

Table 1. Proposed components of critical city infrastructure

The extension of generally accepted critical infrastructure to include education and leisure facilities recognises the critical role they can play in emergencies.

For example, in Hurricane Katrina the New Orleans Superbowl was used as an emergency relief centre. Large open spaces, such as parks or sports fields can also be used as locations for temporary accommodation or to provide alternative sites for managing disaster operations in the event of a natural disaster [22].

3.2 Understanding the context

The resilience and cyber security requirements of a future city require a holistic view of the relevant systems, services and their interdependencies. This is important where a network of independently operated systems including systems operating external to the city provides the essential functionality. A smart environment must be able to both detect the current state or context in the environment and determine what actions to take based on this context information [23].

To establish the resilience and cyber security requirements for a future city's CPS, the seven dimensions of cyber [24, 25] need to be analysed and the context under which they are operating understood. The dimensions are: human, awareness/understanding, information/data, spectrum, systems, infrastructure, and the environment. E.g. understanding the spectrum and channels used for communications and sharing both data and control signals will help to understand the impact of interference, jamming, electro-magnetic pulses and solar weather events on the city's infrastructure.

3.3 Resilience of a city's cyber–physical systems

The Rockefeller Foundation and Arup developed a City Resilience Framework [26]. The Framework defines a resilient system as having seven qualities: reflective, robust, redundant, flexible, resourceful, inclusive, integrated. These indicators are important as they provide a holistic view of resilience as it applies to a city. E.g. a resilient city has effective city leadership, good infrastructure, social cohesion, collective identity and relative prosperity. This is illustrated in the contrast between the recovery of Port au Prince, Haiti following an earthquake in 2010 and New York's response to Hurricane Sandy in 2012 [26].

3.4 Defining cyber security for cyber–physical systems

The future city will be a complex environment comprising a variety of technologies, existing and emerging. The cyber security approach adopted may vary considerably, depending on factors such as asset and systems complexity, ownership and use. The supply chain supporting design, construction, operation and occupation of individual assets or systems also affect the future city. Applying current information security practice to deliver cyber security of the city as a platform is extremely complex if not impossible. The fragmented ownership of individual components within the platform, diverse interfaces and constant change will all limit the effectiveness of traditional control measures. Cyber security of

CPS is complicated by the real-time nature of the systems and the potential safety critical elements of their functionality. Applying the traditional CIA triad [27], used by the information security community, does not adequately address the safety and control aspects of CPS. An alternative approach that combines engineering good practice with information security may be achieved by adapting the Parkerian Hexad [28] with the addition of safety as a seventh element [25]. This results in cyber security being considered using the following elements: confidentiality, possession and/or control, integrity, authenticity, availability, utility, safety. Table 2 illustrates how these elements relate to the design and operation of the city's CPS.

Element	**Relevance to cyber–physical systems**
Confidentiality	Protection of personal and other sensitive data
Possession/Control	Prevent unauthorised manipulation or control of systems
Integrity	Prevention of unauthorised changes to or deletion of data, and maintenance of system configuration
Authenticity	Prevention of fraud or tampering with data
Availability	City infrastructure able to operate without disruption or impairment
Utility	Maintaining data and systems in a useful state throughout their lifecycle
Safety	Prevention of harm to individuals, assets and the environment

Table 2. Application of cyber security elements

4 Applying the framework to city infrastructure

With the increasing sophistication and integration of city systems and the need to protect their growing populations, there is a need for city planners to consider risk, resilience and cyber security in a holistic manner. The two examples below illustrate how critical CPS and poor planning may disable generators and transport systems. The example from Hurricane Sandy of cross-sector dependencies was the impact of the storm on energy supplies. A post storm study [29] exposed risks that were not understood by dependent critical sectors and government officials, due in part to their limited understanding of sector operations and distribution. The study highlights that:

- without power, even well stocked gasoline service stations were unable to pump fuel to customers;
- emergency managers struggled to determine which gasoline stations had both fuel and power;
- refineries and supply terminals that lost power also had major water damage to primary switch gear and other critical electrical components that delayed restoration long after power was restored;
- many critical dependent sites limited to 24 hours of fuel storage required repeated daily refuelling runs for generators;
- the regulation on fuel storage creates disincentives to store greater supplies.

The analysis framework, which is summarised in Figure 2, is a structured approach to analysing city infrastructure and systems. Due to the interdependencies between city systems and services, it should be applied on a citywide basis rather than focused on single systems or services. Whilst the framework is intended to work at an overall systems level, by addressing the interactions and dependencies of the 'city as a platform', it may also be used within systems to understand complex sub-system relationships and behaviour. The framework has been tested on the CCTV and associated area management systems in a major UK city [30].

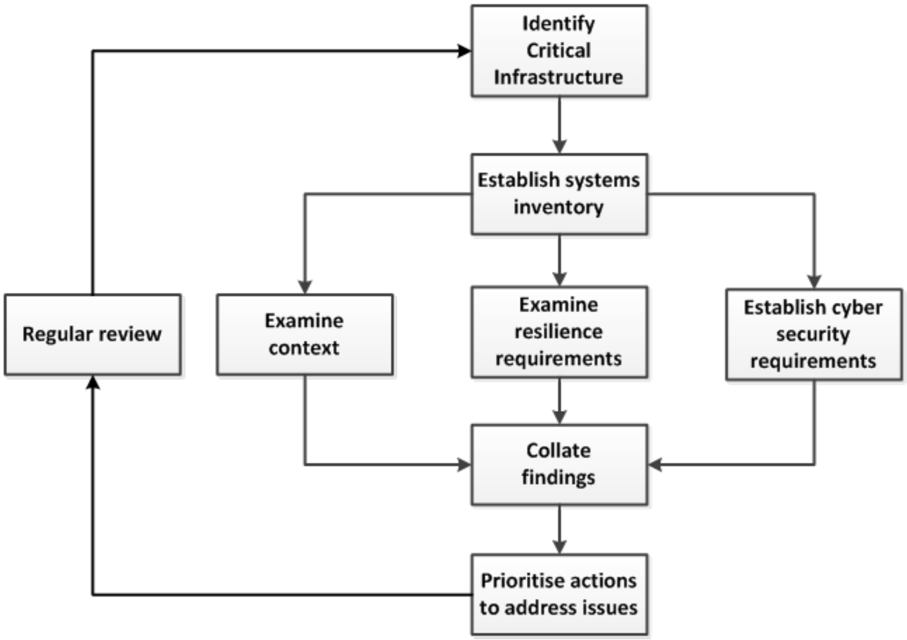
Identify Critical Infrastructure
Establish systems inventory
Regular review
Examine context
Examine resilience requirements
Establish cyber security requirements
Collate findings
Prioritise actions to address issues

Fig. 2. Applying the analysis framework to a city

The approach used to test the framework was to identify the set of affected systems, which included a number of control rooms. The context and role of the control rooms was examined, including the relationships between the areas of coverage. The resilience requirements were investigated, taking into account the need to manage major annual events and public safety incidents. Finally the cyber security requirements and current systems issues were investigated. In collating the results a number of deficiencies were identified, including a significant loss of capability following a system upgrade. The discovery of this loss and the rapid advances in the technology employed in 'smart' cities confirmed the need for regular reviews, to monitor changes in systems and infrastructure, identify new dependencies and emergent functionality arising from systems integration or interconnectivity.

The framework draws together information that may not be apparent to an infrastructure owner or operator, e.g. one recently discovered correlation between the three perspectives occurred in a power distribution network. The operator is increasing the use of the mobile telephony network to manage the field maintenance workforce. The mobile telephone network is not robust when there are power supply interruptions. In the event of a major supply outage, e.g. following a severe weather incident, due to the operator's reliance on the mobile telephone network (Context – Spectrum), the field workforce will not have access to a robust communications platform (Resilience – Robust), leading to a potential loss of command and control communications (Cyber Security – Availability).

5 Discussion

Development of smart cities where there is greater reliance on information and communications technologies represents a significant challenge for city authorities. Even as standalone IT and communication systems, as a consequence of component failure or due to software design and coding errors, these technologies are significantly less reliable than the physical assets. A city suffering frequent systems outages and/or disruptions may become a volatile environment, particularly during seasonal weather extremes.

In the past, resilience studies focused mainly on geophysical issues and on the physical engineering aspects related to the protection of infrastructure from natural events, such as earthquakes, tsunami and extreme weather, or from terrorism related activity. However, the increasing volumes of CPS necessitate the development of new techniques to allow the complexity of, and relationships between, these systems to be understood. The situation is further complicated by the emergent nature of many CPS, with incremental deployment of enhancements and upgrades onto existing infrastructure.

Where upgrades involve information and communications technologies, system designers often attach Internet facing elements to legacy systems or make use of wireless technologies. Both of these developments introduce cyber security and resilience vulnerabilities.

The systems architecture of a future city is likely to be constantly evolving, with new components added and existing elements progressively upgraded or replaced. At any instant, the future city is therefore likely to be a complex hybrid of established, proven systems, with known constraints and defects, and newer systems whose behaviour and performance are still being established. It is likely that technical standards will also evolve over time, so systems will be built to differing risk profiles, availability and security standards.

This analysis framework provides a structured, systematic way of examining CPS, to identify any safety, security or resilience issues that need to be addressed in the design or operation of the systems. The three perspectives combine information about environmental, societal, process and technical dependencies and risks. This approach is not intended to replace the technical risk assessment techniques used in systems engineering, such as Failure Mode and Effects Analysis (FMEA), Hazard and Operability studies (HAZOP), Fault Tree Analysis (FTA) or Cause and Effect Analysis. Instead it provides an approach, which may be used at city level to explore vulnerabilities in the design and use of complex integrated CPS.

6 Conclusions

The expectation of future cities is that information and communications technologies, autonomy and CPS will be harnessed to deliver a safe, secure and sustainable environment for their rapidly growing populations. This dependence on technology is not without significant risk as the complex CPS that are already being developed will increasingly interact with each other. When the systems start to behave as a platform, the city becomes exposed to cascading failure modes, where apparently unrelated events may cause significant disruption or even loss of life.

The analysis framework described in this paper is intended to provide an approach for analysing the city level risks and vulnerabilities to inform both system planning and design. It should also enable the city authorities and infrastructure owner to make informed decisions about where systems need to be reinforced or reengineered to improve resilience and reduce cyber security risks.

Without a clear framework such as the one proposed here, it will be difficult to analyse the complex interactions and relationships between cyberÃśphysical systems in a future city. The approach to systems thinking outlined in this paper enables multi-disciplinary teams to adopt a common approach to sharing information about the operation, dependencies and potential vulnerabilities of their systems or infrastructure. Using this consolidated view should enable security and resilience issues to be identified and addressed.

A comprehensive analysis methodology is under development by the authors, which builds on the framework outlined in this paper. Further work is also underway regarding the definition of cyber security of CPS. The work in both of these areas will be published in due course.

References

1. Doytsher, Y., et al.: Rapid urbanization and mega cities: The need for spatial information management. Research study by FIG Commission 3. FIG Publication No 48. (2010).
2. World Health Organisation: Global Health Observatory (GHO) – Urban population growth. (2014). Available: http://www.who.int/gho/urban_health/situation_trends/urban_population_growth/en/. Last accessed: 17 April 2014.
3. Campbell-Lendrum, D., Corvalan, C.: Climate change and developing-country cities: implications for environmental health and equity. J Urban Health, 84(Suppl 1), 109–117. (2007). doi: 10.1007/s11524-007-9170-x.
4. Biello, D.: Is the US grid better prepared to prevent a repeat of the 2003 blackout?. Scientific American. (2013). doi:10.1038/nature.2013.13559 Available: http://www.nature.com/news/is-the-us-grid-better-prepared-to-prevent-a-repeat-of-the-2003-blackout-1.13559. Last accessed: 17 April 2014.

5. Bashan, A., Berezin, Y., Buldyrev, S. V. & Havlin, S.: The extreme vulnerability of interdependent spatially embedded networks". Nature Phys. 9. 667–672. (2013). Available: http://www.nature.com/news/us-electrical-grid-on-the-edge-of-failure-1.13598. Last accessed: 17 April 2014.
6. CHESS: CHESS – Center for Hybrid and Embedded Software Systems. (2013). Available: http://chess.eecs.berkeley.edu/. Last accessed: 17 April 2014.
7. Baheti, R. & Gill, H.: Cyber–physical systems. In: Samad, T. and Annaswamy, A.M. The Impact of Control Technology. New York: IEEE Control Systems Society. 161–166. (2011). Available: http://ieeecss.org/main/IoCT-report. Last accessed: 17th April 2014.
8. Poovendran, R.: Cyber–physical systems: Close encounters between two parallel worlds. Proceedings of the IEEE. 98 (8), 1363–1366. (2010).
9. Shafi, Q.: Cyber Physical Systems Security: A Brief Survey. In Computational Science and Its Applications (ICCSA), 2012. 12th International Conference on. 146–150. IEEE. (2012).
10. Boyes, H.A.: Trustworthy cyber–physical systems - A review. System Safety Conference incorporating the Cyber Security Conference 2013, 8th IET International, 1–8, 16–17 Oct. 2013. (2013). doi: 10.1049/cp.2013.1707.
11. Institution of Civil Engineers.: The state of the nation - Infrastructure 2010. London: Institution of Civil Engineers. (2010). Available: http://www.ice.org.uk/Information-resources/Document-Library/State-of-the-Nation--Infrastructure-2010. Last accessed: 17 April 2014.
12. Davis P.M.: How to Rebuild the City as a Platform. (2012). Available: http://www.shareable.net/blog/rebuilding-cities-as-platforms. Last accessed: 17 April 2014.
13. Coleman, E.: The City as a Platform - Stripping out complexity and Making Things Happen. (2014). Available: http://www.emercoleman.com/2/post/2014/02/the-city-as-a-platform-stripping-out-complexity-and-making-things-happen.html. Last accessed: 23 April 2014.
14. The Bartlett Centre for Advanced Spatial Analysis.: CityDashboard: London. (2014). Available: http://citydashboard.org/london/. Last accessed: 23 April 2014.
15. World Economic Forums.: Perspectives on a Hyperconnected World. (2013).
16. Rinaldi, S.M., Peerenboom J.P. & Kelly, T.K.: Identifying, understanding, and analyzing critical infrastructure interdependencies. Control Systems, IEEE, vol.21, no.6, pp.11–25, Dec 2001. (2001). doi: 10.1109/37.969131.
17. Boyes, H.A.: Cyber Security in the Built Environment. London: Institution for Engineering and Technology. (2014)
18. Moteff, J., & Parfomak, P.: Critical infrastructure and key assets: definition and identification. Library of Congress, Washington DC. Congressional Research Service. (2004)
19. Centre for Protection of National Infrastructure: The national infrastructure. (2014). Available: http://www.cpni.gov.uk/about/cni/. Last accessed: 17 April 2014.
20. Federal Office of Civil Protection and Disaster Assistance: Critical Infrastructure Sectors and Subsectors. Available: http://www.kritis.bund.de/SubSites/Kritis/EN/introduction/sectors/sectors_node.html. Last accessed: 23 April 2014.
21. Cabinet Office: Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. (2010). Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf. Last accessed: 23 April 2014.

22. O'Rourke, T.D.: "Critical infrastructure, interdependencies and resilience". The Bridge, 37, no. 1, 25–29. (2007). Available: http://www.nae.edu/File.aspx?id=7405. Last accessed: 23 April 2014.
23. Dey, A.K., Abowd, G.D., & Salber, D.: A context-based infrastructure for smart environments. Managing Interactions in Smart Environments. London: Springer. 114–128. (2000).
24. Isbell, R., Boyes, H., & Watson, T.: "Deconstructing Cyber: The Seven Dimensions of Cyberspace". In preparation.
25. Boyes, H.A.: Cyber security attributes for critical infrastructure systems. Cyber Security Review. Summer 2014. 47–51. ISSN 2055-6950. (2014).
26. Arup: City Resilience Framework. London: Arup. (2014)
27. Bishop, M.: Introduction to Computer Security. Amsterdam: Addison-Wesley Longman. (2004).
28. Parker, D.B.: Toward a new framework for information security. In: Bosworth, S., Kabay, M. (eds.) Computer Security Handbook, ch. 5, 4th edn. John Wiley & Sons. (2002)
29. National Infrastructure Advisory Council: Resilience through National, Regional, and Sector Partnerships: Draft Report and Recommendations. (2013). Available: http://www.dhs.gov/sites/default/files/publications/niac-rrwg-report-final-review-draft-for-qbm.pdf. Last accessed: 19 April 2014.
30. Boyes H.A., Isbell, R. & Watson, T.: The resilient city and the role of cyber–physical systems. In: Infrastructure Risk and Resilience: Managing Complexity and Uncertainty in Developing Cities. London: The Institution of Engineering and Technology. ISBN 978-1-84919-920-9. (2014).