Chapter 16
Internet of Things

Marilia Curado, Henrique Madeira, Paulo Rupino da Cunha, Bruno Cabral, David Perez Abreu, João Barata, Licínio Roque, and Roger Immich

1 Introduction: Next-Generation Cyber-Physical Systems

Internet of Things (IoT) technologies and applications, as a prominent example of large-scale cyber-physical systems (CPS), will be ubiquitously embedded in our daily life in the near future. Available technology reports on IoT (van der Meulen 2014; Manyika et al. 2013) point to a massive transformational impact on industry and society, changing dramatically the way we work and live. IoT is expected to reach impressive figures ranging from $2.7 trillion to $6.2 trillion per year by 2025 as the potential economic impact of its related technologies (van der Meulen 2014). In specific domains such as the automotive, Gartner predicts that more than 250 million vehicles will be globally connected by 2020, laying the ground for future mobility scenarios but, above all, changing the drivers/people perspective that will tend to see cars as "smartphones on wheels", extending (not simply allowing) their capacity to be connected, to be productive, and to be a consumer all the time.

Embedded intelligence, smart actuation/control, and high requirements on resilience, safety, and security are vital elements of future Cloud-based IoT that will drastically move apart from initial IoT paradigms, mainly focused on sensors and basic connectivity of "things". Future IoT will include the classical view of the Web of Things, where simple equipment such as coffee machines, refrigerators, washing machines, heating systems, and so forth are connected to the Internet in order to allow remote control and simple services supporting modern lifestyle, and, at the same time, will also encompass edge-oriented areas and applications, which are usually focused on a dedicated user group and often safety and security critical.

M. Curado (✉) · H. Madeira · P. R. da Cunha · B. Cabral · D. P. Abreu · J. Barata · L. Roque
R. Immich
Centre for Informatics and Systems, Department of Informatics Engineering,
University of Coimbra, Coimbra, Portugal
e-mail: marilia@dei.uc.pt; henrique@dei.uc.pt; rupino@dei.uc.pt; bcabral@dei.uc.pt; dabreu@dei.uc.pt; barata@dei.uc.pt; lir@dei.uc.pt; immich@dei.uc.pt

A. Kott, I. Linkov (eds.), *Cyber Resilience of Systems and Networks*, Risk, Systems
and Decisions, https://doi.org/10.1007/978-3-319-77492-3_16

According to the National Institute of Standards and Technology (NIST) (Mell and Grance 2011), cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Although the Cloud Paradigm supports the deployment of a vast amount of applications, it has lacked in providing some characteristics for emergent IoT services such as location awareness, low latency, and mobility support among others. In order to achieve the requirements of new services, a decentralised environment where a plethora of heterogeneous devices communicate and eventually cooperate with each other to perform tasks such as storage and processing autonomously referred as Fog computing paradigm emerged (Vaquero and Rodero-Merino 2014; Bonomi et al. 2014). The Fog rises as an extension to the well-known cloud computing paradigm to address services that are not fitted for the last one.

The prospective of an open Web of Things mixing up traditional IoT and critical areas, composed of trillions of smart objects capable of producing event information and learning with specific scenarios, publishing such knowledge and, at the same time, being able to search for the best response to a given situation and take decisions and actuate, assuring resilience, security, privacy, and even safety in specific Fog areas, faces formidable research and innovation challenges.

Massive scaling and complexity, unprecedented levels of data production, and the need to smartly actuate in the surrounding environment to truly fulfil the visions of a smart world will require future IoT, the prominent features of a pervasive and colossal Cyber-Physical System of Systems (CPSoS) where intelligent behaviour must go together with high resilience, security, and trustworthiness. Assuring correct and trustable response and behaviour are essential in IoT, but guarantying timely and safety actuation in a smart world involving both things and humans is also mandatory to gain the confidence of consumers and society in general.

Within the context of CPS and CPSoS, information systems deal with the sociotechnical change that emerges from the use and adaptation of technology and organisational processes by the users (Paul 2007). Organisational change can have periods of minor mutations followed by punctuated drastic transformations or "revolutions" that involve people, processes, technology, and structure (Lyytinen and Newman 2008). The fourth industrial revolution is the most recent case that affects the organisation and its supply chain, requiring the development of digital competencies (Prifti et al. 2017; Brettel and Friederichsen 2014), redesigned business processes (Lasi et al. 2014), cyber-physical systems, and structural changes that also involve political, economic, environmental, and legal aspects. How to continue their mission after disruption is now a concern for organisations, but also for the collaborative value networks in which they participate.

There are four main design principles for the next-generation processes in industry 4.0 scenarios, namely, interconnection, information transparency, decentralised decisions, and technical assistance (Hermann et al. 2016). Dematerialised business processes are increasingly deployed across most sectors of the economy, taking advantage of Cloud, Fog, mobile, and IoT devices.

Therefore, going mobile is a priority for organisational managers that want to compete in global markets (Barata and Cunha 2016).

One of the main issues in next-generation cyber-physical systems is how they can assist end-to-end digital integration of business processes and industrial workflows (Brettel and Friederichsen 2014). In recent years, many organisations have been changing their digital infrastructure and building new digital services that shape their business strategy (Bharadwaj et al. 2013). Information has an increasing value in this context of change and the strategic posture "*defined as a focal firm's degree of engagement in a particular class of digital business practices relative to the industry norm*" (Mithas et al. 2013) is affected by the competitive environment and turbulence. As a consequence of the increased speed and scale of the internal and external transformations, organisational managers must bring resilience of their processes and practices to the top of their agenda. A possible model to assist them in this task is the CERT-RMM (Caralli et al. 2010), which addresses security management, business continuity management, and IT operations management.

The grand challenges for the next generation of CPS, already sketched above, should be understood in a constant evolving IoT setting, assuming the availability of common technology and infrastructures, such as networking infrastructure and typical elastic Cloud features and services. Furthermore, existing developments, such as FI-WARE (FI-WARE n.d.) comprise entities to gather sensors information and to trigger commands to actuators, or SOFIA2 (http://sofia2.com/home_en.html), which includes middleware to facilitate the interoperability of multiple systems and devices, are also assumed as available building blocks. Elaborating on top of this scenario (i.e. the current IoT technology), we can translate the general grand challenges of future CPS in a set of concrete requirements by stating that the next generation of CPS (seeing them in an IoT environment) should:

- Deal with the extreme complexity of future IoT and provide sustainable means to cope and manage such complexity, even in highly dynamic IoT environments.
- Deal with the massive amount of event data generated in future IoT and be able to convert such data/event information into usable knowledge for the relevant domains and deliver effective publishing strategies to allow efficient use of such knowledge in the IoT.
- Assure resilient and trustworthy service, even in complex and heterogeneous networked system-of-systems, including secure, available, reliable, and timely response/actuation, particularly in Fog areas with safety-critical requirements.
- Cope with mixed criticality IoT environments where open and highly exposed noncritical IoT areas are mixed up with safety-critical Fog-oriented application areas by providing an integrated safety and security approach.
- Guarantee individual and organisation privacy and provide a clear framework to deal with existing and forthcoming ethical issues, namely, the ethical challenges related to the new forms of interactions among, people things, and organisations.
- Provide cost-effective solutions/applications in spite of the need to assure strong properties in quality attributes such as resilience, safety, security, and privacy.

In summary, the next generation of CPS will have to provide enhanced functionality in a resilient IoT environment with 24/7 availability, will require online maintenance and evolution to keep up with a fast-changing world, will address Fog-oriented application areas where safety and security are critical, will handle the production of large amount of event information, and will learn with specific scenarios in order to better address user needs but, at the same time, will need to assure strict privacy, and finally all these features should be available at a reasonable cost, maybe following completely new business models.

2 Resilient Software and Internet Services

This section addresses resilience challenges and solutions within cyber-physical systems, with a holistic perspective that comprises infrastructure and communications, software systems, and organisations.

2.1 Communications and Software Resilience

The communication infrastructure of the Internet plays a crucial role since it enables the connection between devices, services, applications, and users; thus, it is necessary to guarantee its availability. The ability of the network to keep an acceptable level of service in the presence of challenges, such as malicious attacks, software and hardware faults, misconfigurations, and natural disasters is known as network resilience (Smith et al. 2011).

A resilient communication system has at its disposal self-healing mechanisms capable of discovering, diagnose, and react to internal and external disruptions. From the network infrastructure point of view, the general idea is to have primary and backup paths to activate the backups if something is going wrong in the primary ones. This approach usually is performed using a proactive method, where the backup paths are computed and assigned to the primaries from the beginning, or a reactive method, where the backup paths are computed and assigned just after a failure is detected.

Different metrics could be used to measure the quality of resilience of a network. The mean time to recovery (MTTR) is a traditional metric that denotes the time that a device, link, or service will take to recover from any failure (Smith et al. 2011). Considering the fact that a network infrastructure is made up of devices, links, and services, it is not easy to determine the level of resilience in a simple way given the complexity of the new arising paradigms such as the Internet of Things. Further details about metrics related to cyber resilience can be found in Chap. 2.[1]

[1] Cybenko, metrics for cyber resilience.

IoT introduces a novel paradigm consisting of uniquely addressable “things” (e.g. sensors, actuators, home appliances) permanently communicating to one another and with the Internet (Borgia 2014). This paradigm has new and particular challenges, such as energy awareness and large density that require evaluating new ways to enable a reliable and secure communication system. The communication in IoT environments is dominated by wireless technologies, making the network infrastructure very dynamic. The IPv6 routing protocol for low power and lossy networks (RPL) (Gaddour and Koubâa 2012) is a routing protocol specifically designed for low power and lossy networks following the guidelines of the 6LoWPAN IETF working group supporting autoconfiguration, self-healing, and multiple-edge routers as resilience features.

Considering the constraints of IoT systems, and the vast amount of data and software applications involved, alternative ways to process data and support applications requirements are needed. The Cloud and Fog computing paradigms allow tackling these barriers, offloading heavy computations to data centres (Zanella et al. 2014).

The cloudification of the IoT introduces new challenges from the network and software resilience perspectives since the end-to-end communication is now supported by a multilayer approach where different technologies are used to carry on the data from the IoT devices to the users through the Fog and Cloud. Figure 16.1 depicts this complex scenario, where the resilience mechanisms should be applied to each layer and interlayers to achieve the proper quality of resilience. In the picture, the green arrow depicts normal behaviour, and the red arrow represents behaviour in case of failure.

To enhance an end-to-end resilient communication infrastructure in a scenario as the one described in Fig. 16.1, the resilience mechanisms must be articulated. At the bottom layer, the IoT network is managed by a routing protocol (e.g. RPL) guaranteeing the availability of the wireless communication. At the edge of the Fog, gateways allow the aggregation of IoT data to be sent to upper layers for processing. At the Cloud and Fog levels, resilience mechanisms have to deal with the virtualization methods applied to devices, networks, and software. From the network perspective, resilience takes care of the path computation (primary and backup) of the substrate network and the virtual networks (embedded in the physical one). From the devices and services perspective, software robustness is required, as well as smart placement strategies.

Network function virtualization (NFV) and software-defined networking (SDN) paradigms support end-to-end resilience in communication infrastructures (Jammal et al. 2014). The first one allows instantiating on-demand specific network functions, enabling reactive mechanisms to failure recovery. The second decouples the forwarding and data planes of the network making easy to reroute the traffic between paths, besides providing a complete view of the network infrastructure. The outcome of these resilience mechanisms is to work together through multiple layers to achieve an end-to-end resilient and scalable system in a seamless way.

On top of the components described so far, data plays a fundamental role in IoT environments. Having a huge number of distributed sensors is a synonym of having

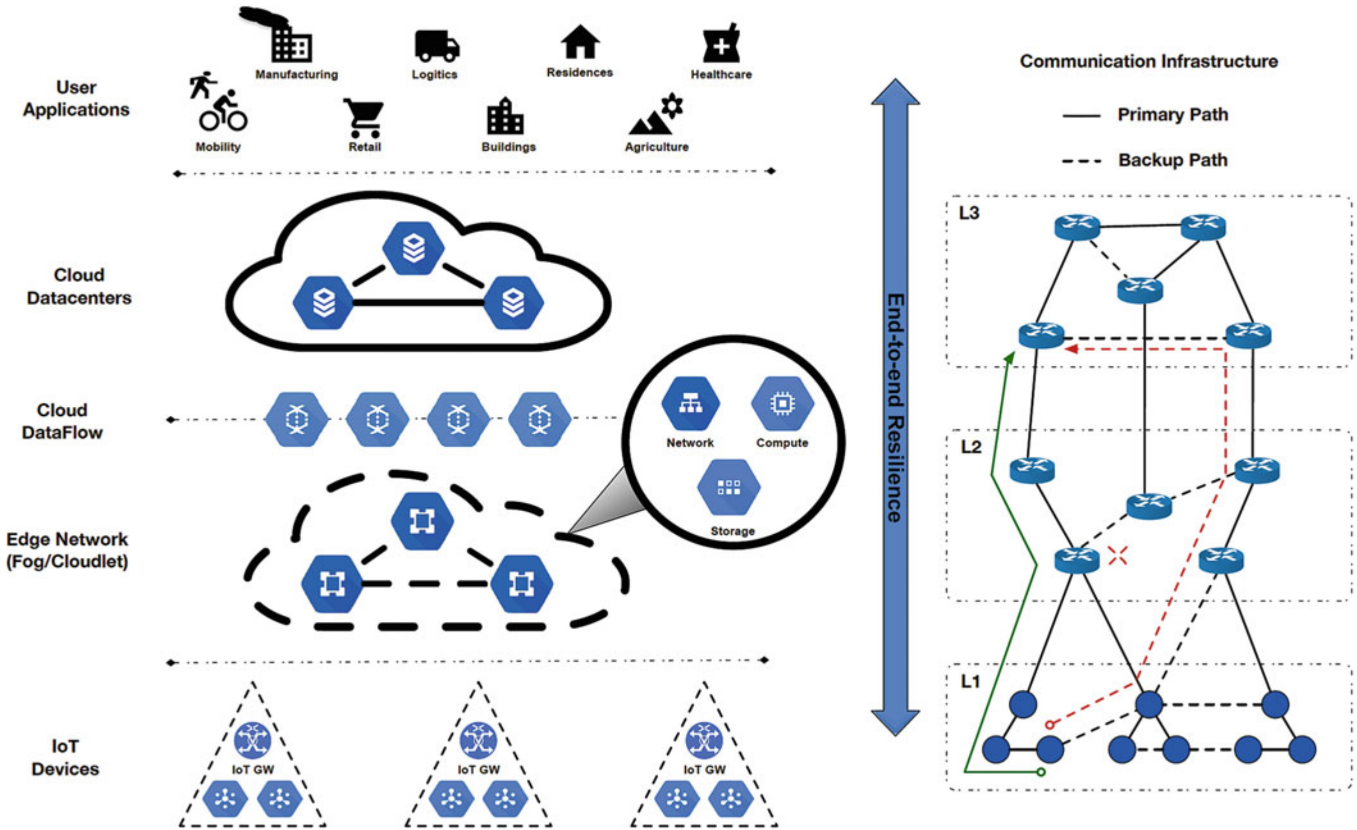

Fig. 16.1 Resilience in an IoT communication infrastructure

massive amounts of data to acquire, integrate, store, process, and use. This is becoming a pressing and important challenge for enterprises to achieve their business goals (Ashton 2009). Both engineers and researchers are working on finding new solutions for handling massive heterogeneous data in highly distributed environments, especially for Cloud-based architectures.

IoT data is characterised by its (Ma et al. 2013):

- Heterogeneity: Distributed sensors will generate different types of data (integers, characters, semi-structured data, and unstructured data, such as images, audio, and video streams).
- Inaccuracy: One of the primary factors limiting the widespread adoption of IoT is the inaccuracy of the data produced (Derakhshan et al. 2007).
- Massive real time: Communications between thousands of objects generate a large volume of heterogeneous, real-time, high-speed, and uninterrupted data streams (Aggarwal et al. 2013).
- Implicit semantics: To support higher-level applications, such as smart home and intelligent healthcare, complex semantics need to be abstracted from the raw data generated by IoT devices (Wang et al. 2006).

These characteristics are, in practice, important and complex research challenges. Solutions to reduce and eliminate data-quality issues have been proposed for RFID systems, but there is still a lot to be done in terms of extending these approaches into IoT. Also, when trying to convert low-level raw events into higher-level applications, complex event processing (CEP) systems play an important role. Some authors (Ma et al. 2013) pointed out that ontology-based IoT semantic event processing is a promising research topic. A different challenge is providing for intelligent data processing and at the same time ensuring the usability and reliability of services. Also, as the complexity of the relationship between devices, data, and users continues to increase, data security and privacy become problems that need to be handled with urgency.

2.2 *Organisational Resilience*

In the context of CPS and CPSoS, where the solutions demanded are beyond the technical aspects, the organisations have to be prepared to deal with newly arrived challenges in a holistic way. This is especially important when considering the heterogeneity and scale of IoT environments, the multiple business processes, as well as the stakeholders involved. It is therefore of utmost importance to provide organisational resilience within IoT ecosystems.

Organisational resilience can be defined as its "*capability to face disruptions and unexpected events in advance thanks to the strategic awareness and a linked operational management of internal and external shocks*" (Annarelli and Nonino 2016). These authors present a comprehensive review of 194 papers and conclude that organisational resilience can be static – to reduce threats and its impacts, or dynamic – when the focus is on managing disruption and unexpected events, aiming to increase the speed of recovery or even reach an improved state. The goal of resilience can be found, for example, in the design of quality management systems that use quality procedures to deal with unpredictability (Øgland 2008).

There are features of resilience common to different knowledge domains, which include organisations but also engineering, technology, or psychology. According to (Connelly et al. 2017), those features are the critical services provided, the thresholds, recovering time (and scale), and the memory/adaptive management required to adapt. Therefore, organisations must be prepared to continuously plan, execute, evaluate, and improve their human and technical resources to deal with uncertainty (Shewhart 1939).

Enterprise modelling can be used to identify potential risks and increase strategic awareness of the organisation. rISk-around is a possible approach to use that suggests the combination of risks and workarounds (alternative procedures to the official process) at global, strategic, and operational levels (Barata et al. 2015). Operational and compliance risks emerge from business processes (e.g. information security and privacy, regulatory issues). These risks are more predictable and related to standard operation procedures. Strategy risks involve, for example, environmental, customer relations, human resources, and IT-related risks. At the highest level, there are the global enterprise risks that may occur due to the most improbable events, usually called *"black swan"*. Managers, for example, should also tackle it with scenario planning (Kaplan 2009). Alternatively, the risk model proposed by (N. I. of S. and T. NIST 2010) distinguishes the organisation, the mission and the business processes, and the information system at a separate level. An enterprise-wide-risk framework must consider distinct layers, for example, the strategic and the cultural, at all levels of the organisation (Popescu and Dascalu 2011). Figure 16.2 presents the rISk-around framework that extends conventional risk approaches by including unexpected events.

First (as seen on the left of Fig. 16.2), it is necessary to identify the sources of uncertainty (e.g. events, variability, mishaps) and certainty (e.g. quality principles, strategy, formal process maps) that exist in the organisation. Second, move to identify (1) global enterprise risks; (2) strategic risks, by assessing the strategic plan; and (3) operational risks at the process and service level. The approach involves sessions of modelling business processes and the potential workarounds. These sessions require a reflection about the "formal" process and the alternative "informal" practices that occur in the organisation, promoting debate among process participants. Third, assess impacts, and then (fourth) establish actions to avoid, mitigate, or accept the identified risks.

According to rISk-around, risks and workarounds can be represented in process models, allowing participants to redesign the processes to reduce threats, contributing to static organisational resilience. One example process model is presented in Fig. 16.3.

Figure 16.3 depicts a formal BPMN process model, similar to the ones used in ISO 9001-certified companies, and the potential workarounds or unexpected events. One advantage of this approach is to make organisational staff aware of existing

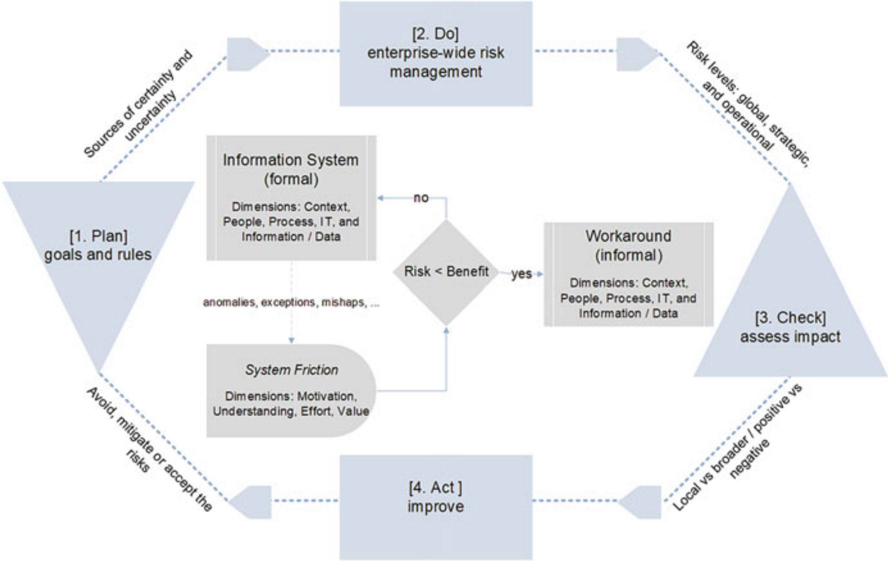
[2. Do]
enterprise-wide risk management
Sources of certainty and uncertainty
Risk levels: global, strategic, and operational
[1. Plan]
goals and rules
Information System (formal)
Dimensions: Context, People, Process, IT, and Information / Data
no
Risk < Benefit
yes
Workaround (informal)
Dimensions: Context, People, Process, IT, and Information / Data
[3. Check]
assess impact
anomalies, exceptions, mishaps, ...
System Friction
Dimensions: Motivation, Understanding, Effort, Value
Avoid, mitigate or accept the risks
Local vs broader / positive vs negative
[4. Act]
improve

Fig. 16.2 rISk-around framework. (Adapted from Barata et al. 2015)

practices, highlight potential problems, and redesign the process execution. It also recognises that traditional *fail-safe* mentality must be complemented by *safe-fail* preparations, towards resilience-based design which "*acknowledge risks that are not known but have some probability of occurrence*" (Park et al. 2011). Yet, workarounds are only a facet of informal practices that occur in the organisation and contribute to process elasticity. Dealing with organisational resilience is a complex endeavour that involves different technical aspects, for example, the impact of enterprise systems as presented by (Ignatiadis and Nandhakumar 2007) or the IT management solutions related to business continuity and disaster recovery plans (Sahebjamnia et al. 2015). Moreover, it mixes organisational and individual aspects (Riolli and Savicki 2003), tolerance for the uncertainty, empowerment in the decision process, and ability to deal with permanent change (Mallak 1998).

According to Park et al. (2011) "whereas the call for incorporating resilience into systems design and management has increased dramatically, the development of practical methods to implement resilience in an engineering context is still in an incipient stage". We highlight the need to shift from the static to the dynamic focus of organisational resilience.

3 Use Cases of Resilient Software and Internet Services

This section introduces two use cases of resilient CPS where different approaches for resilience are being developed, one focused on smart cities and the other on large-scale systems. These use cases try to capture how the users and other systems will

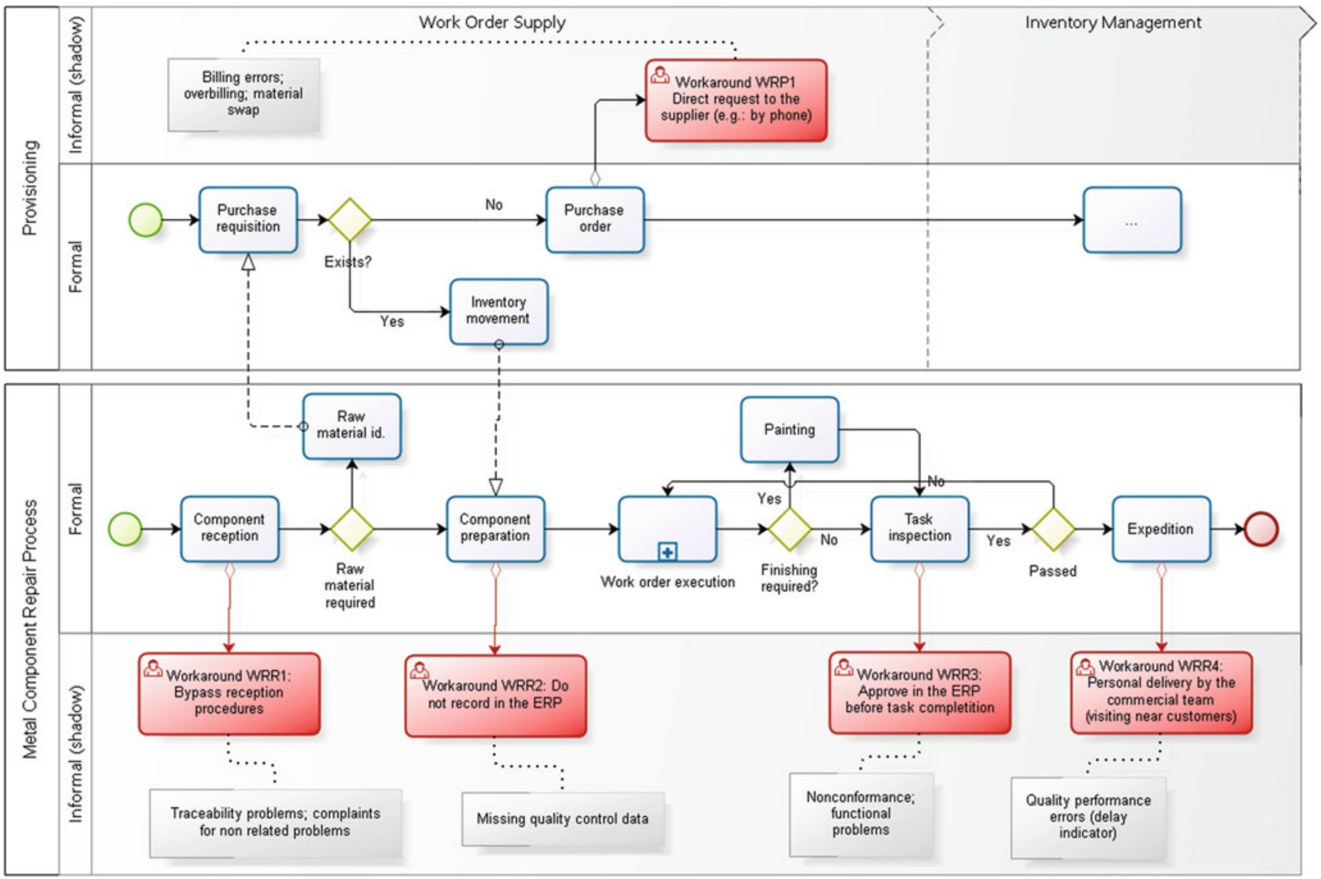
Provisioning
Informal (shadow)
Formal
Work Order Supply
Inventory Management
Billing errors; overbilling; material swap
Workaround WRP1 Direct request to the supplier (e.g.: by phone)
Purchase requisition
Exists?
No
Yes
Purchase order
Inventory movement
...
Metal Component Repair Process
Formal
Informal (shadow)
Component reception
Raw material required
Raw material id.
Component preparation
Work order execution
Yes
No
Finishing required?
Painting
Task inspection
No
Yes
Passed
Expedition
Workaround WRR1: Bypass reception procedures
Workaround WRR2: Do not record in the ERP
Workaround WRR3: Approve in the ERP before task completition
Workaround WRR4: Personal delivery by the commercial team (visiting near customers)
Traceability problems; complaints for non related problems
Missing quality control data
Nonconformance; functional problems
Quality performance errors (delay indicator)

Fig. 16.3 Example of a business process model to deal with uncertainty. (Adapted from Barata et al. 2015)

interact with the proposed solutions on how to improve the resilience. In addition, they will give context and present innovative solutions for the resilience challenges named in the previous section.

3.1 Resilience in the Smart Cities Context: The MobiWise Project

The "MobiWise: from mobile sensing to mobility advising" project is composed of four partners, namely, the Center for Informatics and Systems of the University of Coimbra (CISUC), the Centre for Mathematics of the University of Coimbra (CMUC), the Centre for Mechanical Technology and Automation (TEMA), and the University of Aveiro (UA). The project is funded by the European Regional Development Fund through COMPETE2020 – Operational Program for Competitiveness and Internationalization (POCI) and by the Portuguese Foundation for Science and Technology (FCT) and has a global budget of 2.4 M Euro. There are around 40 people working on the project, including professors, researchers, and grant holders. The kick-off of the project was on January 2017 with the end date set to January 2020.

MobiWise aims to develop a 5G platform to support the mobility of users in urban environments. The main challenges of the MobiWise platform pertain highly demanding services within dense areas with requirements concerning latency, resilience, and energy consumption. Such challenging goals are being addressed within the context of IoT devices and platforms integrated into a Cloud infrastructure.

The MobiWise project uses a comprehensive amount of technologies; thus, to give a proper resilient communication support, it is necessary to ensure the security, dependability, as well as robustness of the services, applications, and infrastructures. Because of that, the main targets to embed resilience behaviour in MobiWise are the access infrastructure and the IoT platform.

At the access infrastructure level, the main mechanisms for resilience are multihoming, resilient data gathering, and distribution mechanisms. One example is the multihoming-aware decision-making MeTHODICAL mechanism (Sousa et al. 2014; Mallak 1998). This mechanism uses an optimisation technique to assign weights objectively considering two main parameters, namely, traffic performance and multihoming. Each parameter has a collection of benefits (advantages) that must be maximised and also several costs (disadvantages), which must be minimised. In order to provide the best results, the optimisation algorithm uses analytic hierarchy process (AHP) to define the weights that are also mapped to the users/application preferences. In the end, MeTHODICAL outperforms the competitors providing optimal path selection with higher-ranking stability and better adaptation to the network conditions.

Another approach is a multihoming architecture that improves the transmission performance in a heterogeneous environment (Capela and Sargento 2015). It uses an algorithm to optimise the best traffic allocation based on real-time context information, which encompasses the access network state, the characteristics of the communication channels, and details about the end-user terminal as well as the actual network traffic. The advantages of this architecture are twofold; it provides load balancing over multiple interfaces and also resilience against errors, yielding the best results when the Points-of-Attachment (PoA) are reaching their maximum capacity.

Apart from the access infrastructure level, the IoT platform also has to enclose resilience features. The IoT middleware of MobiWise aims at the integration of IoT systems with Cloud systems. To achieve this goal, a software-defined network approach is followed. With this paradigm, there is a separation of data and control planes, giving more flexibility for network management, also providing abstraction functions, which facilitate the control in heterogeneous environments. At this level, multiple options are available to improve resilience, at infrastructure, data, and service levels.

In this context, a three-layer IoT architecture (Fig. 16.4) was proposed to ensure a high-resilience level to services and infrastructure (Abreu et al. 2017). The layers are the IoT infrastructure, IoT middleware, and IoT services. Each layer is responsible for tackling specific challenges in supporting the smart city paradigm. The first layer (IoT infrastructure) handles the physical devices (smart objects) which are responsible for data gathering and to react to specific situations. The IoT middleware layer is responsible for providing seamless integration of data and devices, wrapping all the functionalities and abstractions in order to provide easier interactions between

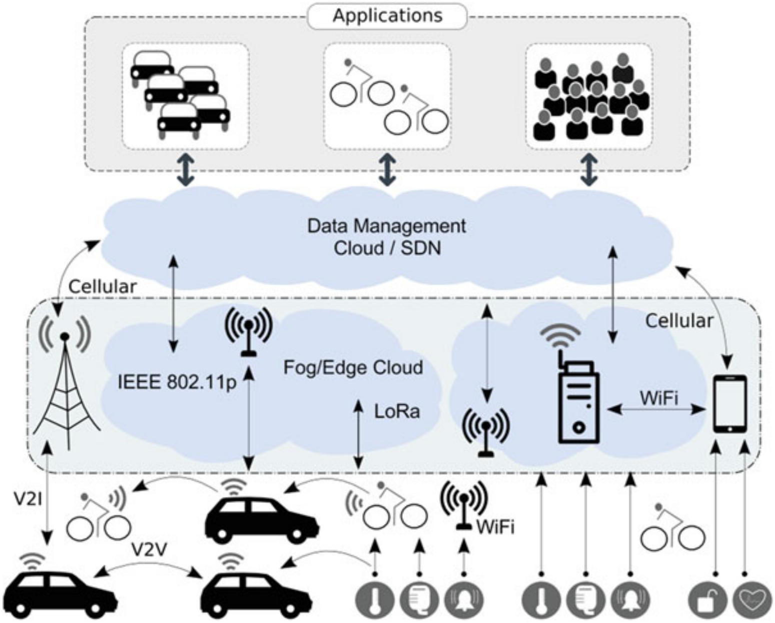

Fig. 16.4 MobiWise architecture for IoT

them. This layer is required due to a large number of technologies infused in an IoT scenario. The last layer (IoT services) supervises the applications and services as well as holds the urban analytics components which will feed information to the smart services. All the layers provide virtualization, caching, and replication capabilities deployed to the Cloud to reduce latency and increase resilience. In addition, the resilience-related tasks follow a distributed approach being disseminated throughout the layers, which also increases the resilience.

One of the core aspects of resilience is addressed in MobiWise through a distributed decision mechanism supported by multiple SDN controllers. Such mechanisms will be able to deal with the services available to the users, their context and users mobility profiles. The decision mechanism will receive monitoring information, and this information will be used as input to learning algorithms able to cope with limited information. At this level, one key aspect towards resilience is the use of several controllers, which will be able to provide redundancy and enhance recovery mechanisms.

Several proposals of distributed SDN controllers can be found in the literature, such as Onix (Koponen et al. 2010), HyperFlow (Tootoonchian and Ganjali 2010), and ElastiCon (Dixit et al. 2013). Onix provides a platform on top of the network control plane allowing the implementation of a distributed system. To achieve this, Onix hands over a general application programme interface enabling flexible distribution primitives. Although the platform, by itself, does not solve management problems, it allows designers to choose the trade-offs between durability, consistency, and scalability. HyperFlow makes use of a different approach by offering a distributed event-based control plane. It allows deploying an indiscriminate number of synchronised controllers in the network and at the same time provides a holistic view of all of them. This enables HyperFlow to be physically distributed but logically centralised, resulting in both scalability and consistency. Another example is the ElastiCon, which is able to dynamically increase and decrease the controller pool based on traffic conditions. It also enables dynamic load balancing when the aggregate load changes, suppressing the need for over-provisioned controllers.

MobiWise will develop a multi-application IoT platform which will embed mechanisms for energy efficiency, low latency, resilience, and scalability. One example of energy efficiency method in machine-to-machine (M2M) communication is the two-tier aggregation for multi-target applications (TTAMA) (Riker et al. 2016). It adaptively aggregates data based on the Constrained Application Protocol (CoAP) configurations, groups, communication periodicity, and aggregation functions. To achieve this, the first TTAMA tier is responsible for reducing data redundancy and the second one to reduce the costs due to message overhead.

A key contribution of MobiWise for resilient 5G services targets the IoT-oriented coupling of middleware and Cloud resources. Mechanisms for on-demand provisioning of networking overlays to interconnect IoT and Cloud platforms, incorporating awareness about the characteristics of services in terms of resilience and latency will be developed. This objective will be achieved through the integration of Fog computing and overlay disjoint paths computation.

An architecture for intelligent service placement at Fog level was proposed to provide higher availability and resilience (Velasquez et al. 2017a). This architecture adopts a modular approach with a constant monitoring of the current network conditions, the popularity of the services, and the user status to steer the placement decisions. The service placement model takes into consideration multi-objective parameters and is optimised using integer linear programming, allowing the orchestration algorithm to decide the most convenient location for the services as well as start the migration process whenever necessary. Besides the higher availability and resilience, another advantage of this architecture is its low latency levels due to single-hop destiny to end users.

In the context of overlay networks, MobiWise has looked into a GEOgraphically Correlated Resilient Overlay Networks (GeoCRON) which provides resilient communications in the case of large-scale geographically correlated failures such as the one caused by a large seismic event (Benson et al. 2016). GeoCRON uses the geographic placement of nodes and information about the IoT underlying routing infrastructure to define a set of multiple geo-diverse routes aiming to increase the chances of delivering the messages.

In addition to mechanisms to support resilience, security and privacy issues are also addressed in MobiWise. In particular, mechanisms for identification, data authentication, confidentiality, and integrity at the infrastructure level, in the presence of heterogeneous devices and technologies, are addressed. Approaches to user privacy will be developed at the application level, protecting users from the regular gathering of personal information.

Data validation and storage will be deployed over the MobiWise infrastructure in such a way that all ecosystem is involved, including end users mobile devices, and thus, while bringing additional players into to data scenario, also introducing additional opportunities concerning system resilience (e.g. prediction, detection, and recovery).

In SDN and Cloud-based IoT systems, it is possible to perform autonomic configurations to protect the transmissions. In order to achieve that, several link quality indicators, such as the bit-error rate and signal-to-noise and distortion ratio, as well as the mobility patterns, signal strength, and the importance of the data that is being transmitted have to be taken into consideration to programmatically configure the network control layer. This allows maximising the resources usage in a quick and dynamic fashion leading to a better transmission quality and higher energy efficiency. Additionally, by identifying the most important data, which can be generated by sensors, mobile devices, vehicles, or any device attached to the network, it is possible to add an extra layer of protection to specific portions of data with the aid of unequal error protection mechanisms (Immich et al. 2016).

The impact of the developed resilience mechanisms will be assessed through fault injection tools and network, software, and service robustness testing tools. At the system level, MobiWise will assess the uncertainty related to the usage of Cloud resources and its services by incorporating a feedback control loop. This run-time provision of robustness should be able to continuously monitor, evaluate, and correct any discrepancies that might exist between the specified functional and non-functional goals of the Cloud platform and its actual behaviour. In addition, experiments will be executed in an urban pilot in the city of Porto, integrating fixed and mobile sensors, crowd sensing, and applications to provide Fog-based enhanced mobility to users.

In summary, MobiWise will design, integrate, and deploy a 5G platform that encompasses several different types of technologies and networks. The advantages are twofold: first, it will contribute to the advance of the state of the art in resilient communication, as several heterogeneous devices will have to efficiently communicate with each other. Second, this enables a unified access infrastructure providing support for mobility, services, and applications. In order to do that, a comprehensive data collection and analysis from sensors, people, and vehicles will be performed leading to improved urban mobility for both commuters and tourists.

3.2 Resilience in Large-Scale Networks: The SORTS Project

Internet services are usually interconnected between each other by an extremely complex network of technology infrastructure providers that encourage the workflow of the applications offered to end users (Senna et al. 2011). Nowadays, the automation of the activities that mould applications' workflows is supported by orchestrated Cloud/Fog tasks, where the activities belonging to different services are combined to achieve specific goals.

In Cloud and Fog, applications and services should provide different levels of Quality of Service (QoS) which implies that the orchestration mechanisms should be able to provide on-demand services, low latency, high mobility, high scalability, and real-time execution to achieve the QoS requirements; nevertheless, this support is only partly met by existing Cloud computing solutions (Zhang et al. 2010). In Fog computing, services are available as close as possible to users, allowing for greater geographic coverage, sensitivity to context, load balancing, and flexible mobility support. These characteristics are essential in new applications for the Internet of Everything (Albrecht and Michael 2013), such as transport and traffic control systems, or M2M environments, which have special requirements like real time and low latency.

In a distributed scenario with high mobility requirements, like the Fog ones, it is required to support the orchestration of services on demand, with adaptability, while providing a flexible and reliable performance; this is the main challenge of the Supporting the Orchestration of Resilient and Trustworthy Fog Services (SORTS) project.

SORTS is a cooperation project between the University of Coimbra in Portugal and the University of Campinas in Brazil, funded by the Coordination for the Improvement of Higher Education Personnel (CAPES) and by FCT. This project encourages the cooperation of nine researchers attached to the Institute of Computing of the University of Campinas and ten researchers attached to the Centre for

Informatics and Systems of the University of Coimbra. The project started in February 2016 and will last until January 2019.

The primary goal of the SORTS project is to research, design, implement, and evaluate a new service orchestrator able of guaranteeing the resilience and trustworthiness of open, large-scale, dynamic services on the Fog. The service orchestrator will be in charge of composing service elements residing in the Fog environment (e.g. sensing, connectivity, processing, storage, platform service, and software services) into more complex Fog services (e.g. trip planning services and traffic crowd sensing) so they can be offered to users in the Fog environment.

The execution of the Fog services comprehends different components and entities spread in a wide geographical area, incrementing the complexity of the decision-making process for the resource allocation tasks aimed at accomplishing the required QoS levels. To manage the execution of the Fog services, different orchestration mechanisms will be designed and developed. These mechanisms will coordinate the functioning of the different service elements to reach the requirements of the composed Fog services, namely, scalability, resilience, and low latency.

Since the Fog services are continuously spreading over a large area, to guarantee resilience and scalability, the service orchestrator will work in a loosely coupled mode, in which some functions constrained by real-time requirements will be assigned/distributed to Fog regional service orchestrator (RSO) placed at the edge of the Fog environment, facilitating semi-autonomous operation of the different Fog regions, under a lightweight supervision of the Fog domain service orchestrator (DSO) responsible for the Fog domain. The management of such independent domains is necessary to guarantee the participation of autonomous entities disseminated throughout the Fog. The DSOs must support federation mechanisms that allow the collaboration among different Fog domains (i.e. belonging to various entities or under the administration of different authorities) and the creation of a multidomain Fog environment capable of supporting Fog service ubiquity in the federated Fog environment.

The Fog enables a new generation of services and applications, and there will be a constructive cooperation between Cloud and Fog, especially concerning the data management and analysis. Thus, the Fog will be closer to the points of information generation, and the Cloud will execute the “work behind the scenes” getting data from the different distributed Fogs, addressing them globally and making them available as the reference for the entire federation of Fogs.

To carry out the management among Fog and Cloud domains, a hybrid environment service orchestrator (HESO) will be integrated. The HESO will support different technologies of Fog and Cloud and will have functionalities similar to the DSOs, adapted to work in a federated Cloud environment. Figure 16.5 depicts the architecture discussed.

By the end of the project, and included in the design of the service orchestrator, it will be defined (1) a model for building the hybrid and heterogeneous environments composed by the integration of Fog and Cloud domains and (2) a model for the integration between management inside one domain (virtual network management, execution management, monitoring management). The final output of the SORTS

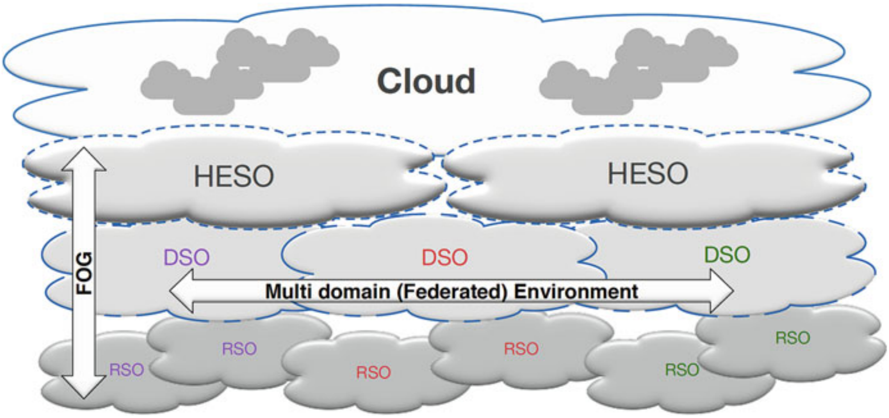

Fig. 16.5 Architecture levels of the SORTS fog orchestrator

project will be a prototype of the service orchestrator integrated system, including all the defined domains (regional and hybrid). With these outcomes, the SORTS project will contribute to the advance of knowledge of resilience using mechanisms for service placement and path computation to improve the MTTR of applications and services deployed in Cloud/Fog environments.

4 Open Issues

This section outlines the main open issues regarding mechanisms to support resilience in cyber-physical systems considering the requirements of emerging systems architectures as well as environmental and societal challenges.

The next-generation Internet of Things is evolving towards an Internet of Everything, where everybody and everything are connected to provide multiple services within various contexts such as smart home, wearables, smart city, smart grid, industrial internet, connected car, connected health, smart retail, smart supply chain, and smart farming (Diaz et al. 2016). The main challenges of such cyber-physical systems include different perspectives, from devices and networks, through data and services, towards users, and businesses, as summarised next.

- Complex CPS: How to provide sustainable means to cope and manage such complexity, even in highly dynamic IoT environments?
- Vast amount of event data generated in CPS: How to convert such data into usable knowledge for the relevant domains while preserving user's privacy?
- Critical services: How to assure resilient, secure, trustworthy, and low latency services in complex and heterogeneous CPS?
- Large-scale, heterogeneous, and dense environments: How to achieve scalability while providing cost-effective high quality and resilient services?

The research community, including the MobiWise and SORTS projects presented in the previous section, is addressing these issues as highlighted next:

- Development of solutions based on the Fog paradigm: Placing content and services closer to the users reduces latency and improves resilience as neighbouring Fogs can take over the responsibilities in case of failure (Velasquez et al. 2017a). This is especially important when considering critical services and mobile nodes. There is thus the need to perform research in the areas of content and service placement in Fog environments, considering aspects such as services popularity and requirements as well as users' interests and locations, and giving adequate care to privacy.
- Layered architectures: Creating different tiers to manage the infrastructure, middleware, services, and businesses eases the integration of heterogeneous entities (e.g. data, devices, technologies) at the different levels and has the potential to provide multiple levels of redundancy (Abreu et al. 2017). This approach raises issues concerning the definition of the different layers, their roles, as well as their interactions, which need to be addressed in order to provide adequate service levels.
- Distributed decision mechanism: Distributed control based on multiple controllers provides redundancy and supports enhanced recovery mechanisms (Dixit et al. 2013). By decoupling data and control planes, network management becomes more flexible while providing an abstraction layer that simplifies handling of heterogeneous environments. In addition, such approach potentiates context-aware decisions with a direct impact on the quality of the services provided to the users.
- Hybrid orchestrators: Management of large-scale and geographically distributed Fog environments requires service orchestration at different levels. A hybrid approach to manage Fog and Cloud domains is needed in order to support the coordination of resources, applications, and services in a dynamic and responsive way (Velasquez et al. 2017b). Research on the optimisation approaches to be used by the orchestrators is needed in areas such as disjoint path computation for resilience and service placement for time-critical services.
- Digital ecosystems of "People, Process, Technology": The full sociotechnical nature of these contexts must be acknowledged in the design and operation of intra- and inter-organisational business processes, caring for their sustainability, managing innovation, ensuring transparency and interoperability in the supply chain, and by implementing appropriate governance structures. New models to assess and guide strategic and operational management in the context of these significant changes are needed. One of the most popular research streams in this area is the development of maturity models and industry 4.0 roadmaps for specific sectors of the economy (Leyh et al. 2016, 2017).

Acknowledgements The work presented in this chapter was partially carried out in the scope of the MobiWise project: From mobile sensing to mobility advising (P2020 SAICTPAC/0011/2015), cofinanced by COMPETE 2020, Portugal 2020 – Operational Program for Competitiveness and Internationalization (POCI), European Union's ERDF (European Regional Development Fund), and the Portuguese Foundation for Science and Technology (FCT). David Perez Abreu wishes to acknowledge the Portuguese funding institution FCT – Foundation for Science and Technology for supporting his research under the Ph.D. grant SFRH/BD/117538/2016.

References

Abreu, D. P., Velasquez, K., Curado, M., & Monteiro, E. (2017). A resilient internet of things architecture for smart cities. *Annals of Telecommunications, 72*, 19–30. https://doi.org/10.1007/s12243-016-0530-y.

Aggarwal, C. C., Ashish, N., & Sheth, A. (2013). The internet of things: A survey from the data-centric perspective. In C. Aggarwal (Ed.), *Managing and Mining Sensor Data*. Boston: Springer.

Albrecht, K., & Michael, K. (2013). Connected: To everyone and everything (guest editorial: Special section on sensors). *IEEE Technology and Society Magazine, 32*(4), 31–34.

Annarelli, A., & Nonino, F. (2016). Strategic and operational management of organizational resilience: Current state of research and future directions. *Omega, 62*, 1–18, 2016.

Ashton, K. (2009). That 'internet of things' thing. *RFiD Journal, 22*, 97–114.

Barata, J., & Cunha, P. R. (2016). Mobile supply chain management: Moving where? In *Proceedings of the 13th European, Mediterranean and middle eastern conference on information systems (EMCIS)* (pp. 1–13).

Barata, J., Cunha, P. R., & Abrantes, L. (2015). Dealing with risks and workarounds: A guiding framework. In *The practice of enterprise modeling. Lecture notes in business information processing 235* (Vol. 235, pp. 141–155).

Benson, K. E., Han, Q., Kim, K., Nguyen, P., & Venkatasubramanian, N. (2016). *Resilient overlays for IoT-based community infrastructure communications*. 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), Berlin, pp. 152–163. https://doi.org/10.1109/IoTDI.2015.40

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly, 37*(2), 471–482.

Bonomi, F., Milito, R., Natarajan, P., & Zhu, J. (2014). Big data and internet of things: A roadmap for smart environments. In *Fog computing: A platform for internet of things and analytics* (pp. 169–186). Springer International Publishing. https://doi.org/10.1007/978-3-319-05029-4_7 isbn= 978-3-319-05029-4, url=https://doi.org/10.1007/978-3-319-05029-4_7.

Borgia, E. (2014). The internet of things vision: Key features, applications and open issues. *ELSEVIER Computer Communications Journal, 54*(1), 1–31.

Brettel, M., & Friederichsen, N. (2014). How virtualization, decentralization and network building change the manufacturing landscape: An industry 4.0 perspective. *International Journal Mechanical Aerospace, Industrial Mechatronic Manufacturing Engineering, 8*(1), 37–44.

Capela, N., & Sargento, S. (2015). An intelligent and optimized multihoming approach in real and heterogeneous environments. *Wireless Networks, 21*(6), 1935–1955.

Caralli, R. A., Allen, J. H., & White, D. W. (2010). *CERT resilience management model: A maturity model for managing operational resilience* (1st ed.). Addison-Wesley Professional.

Connelly, E. B., Allen, C. R., Hatfield, K., Palma-Oliveira, J. M., Woods, D. D., & Linkov, I. (2017). Features of resilience. *Environmental System Decision, 37*(1), 46–50.

Derakhshan, R., Orlowska, M. E. & Li, X.(2007). *RFID data management: Challenges and opportunities*. 2007 IEEE International Conference on RFID, Grapevine, TX, pp. 175–182. https://doi.org/10.1109/RFID.2007.346166

Diaz, M., Martin, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing. *Journal of Network and Computer Applications, 67*, 99–117. ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2016.01.010.

Dixit, A., Hao, F., Mukherjee, S., Lakshman, T. V., & Kompella, R. (2013). Towards an elastic distributed SDN controller. In ACM SIGCOMM computer communication review (Vol. 43(4), pp. 7–12). ACM New York.

FI-WARE. (n.d.). Future internet core platform. http://cordis.europa.eu/project/rcn/99929_en.html; https://www.fiware.org/

Gaddour, O., & Koubâa, A. (2012). RPL in a nutshell: A survey. *ELSEVIER Computer Networks Journal, 56*(14), 3163–3178.

Hermann, M., Pentek, T., & Otto, B.. (2016). *Design principles for Industrie 4.0 scenarios*. 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, pp. 3928–3937. https://doi.org/10.1109/HICSS.2016.488

Ignatiadis, I., & Nandhakumar, J. (2007). The impact of enterprise systems on organizational resilience. *Journal of Information Technology, 22*(1), 36–43.

Immich, R., Cerqueira, E., & Curado, M. (2016). Shielding video streaming against packet losses over VANETs. *Wireless Networks, 22*(8), 2563–2577.

Jammal, M., et al. (2014). Software defined networking: State of the art and research challenges. *ELSEVIER Computer Communications Journal, 72*(29), 74–98.

Kaplan, R. (2009). Risk management and the strategy execution system. *Balanced Scorecard Representative, 11*(6), 1–6.

Koponen, T., Casado, M., Gude, N., Stribling, J., Poutievski, L., Zhu, M., & Shenker, S. (2010). Onix: A distributed control platform for large-scale production networks. In *OSDI* (Vol. 10, pp. 1–6).

Lasi, H., Fettke, P., Kemper, H. G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business and Information Systems Engineering, 6*(4), 239–242.

Leyh, C., Bley, K., & Schäffer, T. (2016). *Digitization of German enterprises in the production sector – Do they know how 'digitized' they are?* In Americas conference on information systems - AMCIS 22nd Americas Conference on Information Systems - AMCIS 2016, San Diego, USA, pp. 1–10.

Leyh C., Schäffer T., Bley K., Forstenhäusler S. (2017). Assessing the IT and Software Landscapes of Industry 4.0-Enterprises: The Maturity Model SIMMI 4.0. In E. Ziemba (Ed.), *Lecture Notes in Business Information Processing: Vol 277. Information Technology for Management: New Ideas and Real Solutions. AITM 2016, ISM 2016*. Cham: Springer.

Lyytinen, K., & Newman, M. (2008). Explaining information systems change: A punctuated socio-technical change model. *European Journal of Information Systems, 17*(6), 589–613.

Ma, M., Wang, P., & Chu, C.-H. (2013). Data management for internet of things: Challenges, approaches and opportunities. In *Proceedings of IEEE international conference IEEE cyber, physical and social computing. green computing communications (GreenCom) IEEE internet things (iThings/CPSCom)* (pp. 1144–1151). Beijing.

Mallak, L. (1998). Putting organizational resilience to work. *Industrial Management, 40*(6), 8–13.

Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., & Marrs, A. (2013). Disruptive technologies: Advances that will transform life, business, and the global economy. In *Technical report*. McKinsey Global Institute. http://www.mckinsey.com/insights/business_technology/disruptive_technologies

Mell, P., & Grance, T. (2011). The NIST definition of Cloud computing. *NIST Special Publication 800–145, 1*(1), 1–7.

Mithas, S., Tafti, A., & Mitchell, W. (2013). How a Firm's competitive environment and digital strategic posture influence digital business strategy. *MIS Quarterly, 37*(2), 511–536.

N. I. of S., & T. NIST. (2010). Joint Task Force Transformation Initiative. 2010. SP 800-37 Rev. 1. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Technical Report. NIST, Gaithersburg, MD, United States.

Øgland, P. (2008). Resilience as a goal for quality management systems design. *Systemist, 30*(2), 247–265.

Park, J., Seager, T. P., & Rao, P. S. C. (2011). Lessons in risk- versus resilience-based design and management. *Integrated Environmental Assessment and Management, 7*(3), 396–399.

Paul, R. J. (2007). Challenges to information systems: Time to change. *European Journal of Information Systems, 16*(3), 193–195.

Popescu, M., & Dascalu, A. (2011). Considerations on integrating risk and quality management. In *Annals of "Dunarea de Jos" University of Galati, fascicle I* (pp. 49–54).

Prifti, L., Knigge, M., Kienegger, H., & Krcmar, H. (2017). *A competency model for 'Industrie 4.0' employees*. In 13th international conference on Wirtschaftsinformatik, St. Gallen, Switzerland, pp. 46–60.

Riker, A., Cerqueira, E., Curado, M., & Monteiro, E. (2016). A two-tier adaptive data aggregation approach for M2M group-communication. *IEEE Sensors Journal, 16*(3), 823–835.

Riolli, L., & Savicki, V. (2003). Information system organizational resilience. *Omega, 31*(3), 227–233.

Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research, 242*(1), 261–273.

Senna, C., Batista, D. M., & Milton, A. (2011). Experiments with a self-management system for virtual networks. In *II Workshop de Pesquisa Experimental Da Internet Do Futuro (WPEIF)*. Campo Grande.

Shewhart, W. (1939). *Statistical method from the viewpoint of quality control*. Washington, DC: Graduate School, Department of Agriculture.

Smith, P., et al. (2011). Network resilience: A systematic approach. *IEEE Communications Magazine, 49*(7), 88–97.

Sousa, B., Pentikousis, K., & Curado, M. (2014). MeTHODICAL: Towards the next generation of multihomed application. *Computer Networks, 65*, 21–40.

Tootoonchian, A., & Ganjali, Y. (2010). *HyperFlow: A distributed control plane for OpenFlow*. In Proceedings of the 2010 internet network management conference on Research on enterprise networking (INM/WREN'10). USENIX Association, Berkeley, CA, USA, pp. 3–3.

van der Meulen, R. (2014). Gartner says personal worlds and the internet of everything are colliding to create new markets. *Gartner*. http://www.gartner.com/newsroom/id/2621015

Vaquero, L. M., & Rodero-Merino, L. (2014). Finding your way in the fog: Towards a comprehensive definition of fog computing. SIGCOMM Comput. *The Communication Review, 44*(5), 27–32.

Velasquez, K., Abreu, D. P., Curado, M., & Monteiro, E. (2017a). Service placement for latency reduction in the internet of things. *Annals of Telecommunications*, 105–115. https://doi.org/10.1007/s12243-016-0524-9.

Velasquez, K., Perez Abreu, D., Gonçalves, D., Bittencourty, L., Curado, M., Monteiro, E., & Madeira, E. (2017b). Service orchestration in fog environments. In *IEEE 5th international conference on future internet of things and cloud* (pp. 21–23). Prague.

Wang F., Liu S., Liu P., Bai Y. (2006) Bridging physical and virtual worlds: Complex event processing for RFID data streams. In Y. Ioannidis et al. (Eds.), *Lecture Notes in Computer Science, vol 3896. Advances in Database Technology - EDBT 2006. EDBT 2006*. Berlin, Heidelberg: Springer.

Zanella, A., et al. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22–32.

Zhang, S., Zhang, S., Chen, X., & Huo, X. (2010). Cloud computing research and development trend. In *Second international conference on future networks, Sanya* (pp. 93–97).