Levent Kartal

# Techno-economic feasibility analysis of remote maintenance connectivity in factories

**School of Electrical Engineering**

Thesis submitted for examination for the degree of Master of Science in Technology.

Espoo 20.11.2017

**Thesis supervisor:**

Prof. Heikki Hämmäinen

**Thesis advisors:**

Prof. Martti Mäntylä

M.Sc. Jaspreet Singh Walia

Aalto University
School of Electrical
Engineering

AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING

ABSTRACT OF THE
MASTER'S THESIS

Author: Levent Kartal

Title: Techno-economic feasibility analysis of remote maintenance connectivity in factories

Date: 20.11.2017 Language: English Number of pages: 10+71

Department of Communications and Networking

Professorship: Network Economics

Supervisor: Prof. Heikki Hämmäinen

Advisors: Prof. Martti Mäntylä, M.Sc. Jaspreet Singh Walia

Maintenance activities play a major role in factory operations, as they prevent breakdowns and extend machine life. With the advances in sensor, computing and communications technology, sensor data can be increasingly exploited for real-time supervision of machine condition. However, the acquisition of the data is challenging due to proprietary technologies and interfaces applied in Industrial Networks. Therefore, sensor data is rarely utilized in other processes than automation. As the industry is heading towards a new industrial era, also referred to as Industrial Internet or Industrie 4.0, there is growing need to improve data availability for applications that can realize its potential value.

In this research, the focus is on the feasibility of remote maintenance deployment in factories. The topic is approached from the connectivity viewpoint. The research is conducted by reviewing the literature, and by interviewing numerous industry experts regarding the connectivity and data exploitation in factories. These form the basis for the value network analysis, in which Value Network Configuration (VNC) method is applied, to analyze the value distribution among different actors in alternative remote connection cases.

As a result of the VNC analysis, three alternative value network configurations are formed. They provide a high-level technical architecture of the remote connection implementation and discuss the accumulated value of each actor concerning remote maintenance service. The insights gained from the VNCs and literature are then employed to propose a future technical architecture for remote maintenance connectivity in factories.

Keywords: remote maintenance, industrial networks, Industrial Internet, 5G, remote connection, Value Network Configuration

AALTO-YLIOPISTO
SÄHKÖTEKNIIKAN KORKEAKOULU

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Levent Kartal

Työn nimi: Teknoekonominen toteutettavuusanalyysi etäylläpidon liitettävyydestä tehtaissa

Päivämäärä: 20.11.2017 Kieli: Englanti Sivumäärä: 10+71

Tietoliikenne- ja tietoverkkotekniikan laitos

Professuuri: Tietoverkkotalous

Työn valvoja: Prof. Heikki Hämmäinen

Työn ohjaaja: Prof. Martti Mäntylä, DI Jaspreet Singh Walia

Huoltotoimet ovat suuressa roolissa tehtaan toiminnassa, sillä ne ehkäisevät konerikkoja ja pidentävät koneen käyttöikää. Sensori-, laskenta- ja tietoliikennetekniologian kehittymisen johdosta sensoridataa voidaan hyödyntää yhä enemmän koneen kunnon reaaliaikaiseen valvontaan. Datan saanti on kuitenkin haastavaa teollisissa verkoissa käytettyjen sovelluskohtaisten teknologioiden ja liitäntöjen takia. Sen vuoksi sensoridataa hyödynnetään harvoin muissa prosesseissa kuin automaatiossa. Teollisuuden suunnatessa kohti uutta teollista aikakautta, joka tunnetaan myös nimillä Teollinen Internet ja Teollisuus 4.0, on datan saatavuutta parannettava sovelluskohteille, jotka voivat realisoida sen potentiaalisen arvon.

Tämä tutkimus tarkastelee etäylläpidon käyttöönoton toteutettavuutta tehtaissa. Aihetta lähestytään liitettävyyden näkökulmasta. Tutkimus suoritetaan tarkastelemalla kirjallisuutta sekä haastattelemalla lukuisia teollisuuden asiantuntijoita koskien liitettävyyttä ja datan hyödyntämistä tehtaissa. Nämä muodostavat perustan arvoverkkoanalyysille, jossa sovelletaan arvoverkkokonfiguraatio-menetelmää, jolla analysoidaan arvon jakautumista eri toimijoiden kesken vaihtoehtoisissa etäyhteystapauksissa.

Arvoverkkokonfiguraatioanalyysin tuloksena muodostetaan kolme vaihtoehtoista arvoverkkokonfiguraatiota. Ne tarjoavat korkean tason teknisen arkkitehtuurin etäyhteyden implementaatiosta ja tarkastelevat toimijoiden kerryttämää arvoa etäylläpitopalvelun osalta. Arvoverkkokonfiguraatioista ja kirjallisuudesta saatujen näkemysten pohjalta esitellään lisäksi tulevaisuuden tekninen arkkitehtuuri etäylläpidon liitettävyydelle tehtaissa.

Avainsanat: etäylläpito, teollisuusverkot, Teollinen Internet, 5G, etäyhteys, arvoverkkokonfiguraatio

# Preface

First of all, I want to thank Professor Martti Mäntylä for providing me with an opportunity to conduct my thesis as part of 5G@II project. Moreover, I want to express my deep gratitude to Professor Heikki Hämmäinen for supervising my thesis and providing insightful feedback throughout the whole process. My gratitude also goes to my advisor Jaspreet Singh Walia, who offered his assistance in all relevant matters regarding the thesis.

During the time of the thesis, I got the chance to meet and discuss with various experts from industry and academia. I want to thank all of them for interesting discussions and insights, which helped me to better understand the world of industry. Furthermore, a special thanks to all my colleagues, Alexandr, Jaume and Ben, for inspiring conversations during the coffee and lunch breaks.

Last but not least, I want to thank my family and friends for their support and understanding during the thesis. I am grateful to my girlfriend, who was supportive and patient, especially during the last months of the writing process when I did not have enough time for her. My special thanks also goes to my brother, who has always pushed me to try harder, no matter the circumstances. Finally, Mom and Dad, I cannot thank you enough for all the support and love you have given me. I never would have made it here without you.

Otaniemi, 20.11.2017

Levent Kartal

# Contents

# List of Abbreviations and Acronyms

| | |
|---|---|
| 3GPP | 3rd Generation Partnersh+B2:B16ip Project |
| 5G | Fifth generation of mobile telecommunications technologies |
| 5GPPP | 5th Generation Public-Private Partnership |
| API | Application Programming Interface |
| CAD | Computer Aided Design |
| CAN | Control Area Network |
| CapEx | Capital Expenses |
| CBA | Component Based Automation |
| CBM | Condition-Based Maintenance |
| CIM | Computer Integrated Manufacturing |
| CNC | Computer Numerical Control |
| CPS | Cyber-Physical Systems |
| DCS | Distributed Control System |
| DoS | Denial-of-Service |
| E2E | End-to-End |
| ERP | Enterprise Resource Planning |
| EtherCAT | Ethernet for Control Automation Technology |
| ETSI | European Telecommunications Standards Institute |
| GDP | Gross Domestic Product |
| GE | General Electric |
| GSM | Global System for Mobile Communications |
| HMI | Human-Machine Interface |
| HTTP | Hyper Text Transfer Protocol |
| HTTPS | Hyper Text Transfer Protocol Secure |
| ICT | Information and Communication Technology |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IoT | Internet of Things |
| IP | Internet Protocol |
| IRT | Isochronous Real-Time |
| ISA | International Society of Automation |
| ISP | Internet Service Provider |
| IT | Information Technology |
| ITU-T | International Telecommunication Union-Telecommunication |
| LSA | Licensed Shared Access |
| LTE | Long-Term Evolution |
| M2M | Machine-to-Machine |
| MAC | Media Access Control |
| MAP | Manufacturing Automation Protocol |
| MEC | Mobile Edge Computing |
| MES | Manufacturing Execution System |
| MIMO | Multiple-Input Multiple-Output |
| mMTC | massive Machine-Type Communications |

| | |
|---|---|
| MNO | Mobile Network Operator |
| MVNO | Mobile Virtual Network Operator |
| NB-IoT | Narrowband Internet of Things |
| NF | Network Function |
| NFV | Network Functions Virtualization |
| NFVI | Network Functions Virtualization Infrastructure |
| NGMN | Next Generation Mobile Networks |
| OPC | Object linking and embedding for Process Control |
| OPC UA | OPC Unified Architecture |
| OSI | Open System Interconnection |
| OT | Operational Technology |
| PDA | Personal Digital Assistant |
| PLC | Programmable Logic Controller |
| PROFIBUS | Process Field Bus |
| PROFINET | Process Field Net |
| QoS | Quality-of-Service |
| RAN | Radio Access Network |
| RAT | Radio Access Technology |
| RCS | Resilience Control System |
| RTE | Real-Time Ethernet |
| SCADA | Supervisory Control And Data Acquisition |
| SDN | Software-Defined Networking |
| SERCOS | Serial Real-Time Communications |
| SIM | Subscriber Identity Module |
| SOAP | Simple Object Access Protocol |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| WAN | Wide Area Network |
| WLAN | Wireless Local Area Network |
| VLAN | Virtual Local Area Network |
| VNC | Value Network Configuration |
| VNF | Virtual Network Function |
| WPAN | Wireless Personal Area Network |
| VPN | Virtual Private Network |
| WSAN | Wireless Sensor and Actuator Network |
| XML | Extensible Markup Language |

# List of Figures

# List of Tables

# 1 Introduction

In the coming years, the fifth generation of mobile telecommunications technologies (5G) will initiate a new industrial era, which will entirely change the way machines operate and communicate with each other. This era, also known as Industrial Internet or Industrie 4.0 (also referred to as Industry 4.0), will not only transform isolated industrial systems to globally connected entireties but also advance our society and economy. Futuristic applications, such as self-driving cars, and fully autonomous manufacturing and supply chains will be some of the many outcomes arising out of the radical transformation of industry and evolution of mobile and computing technologies. The advancements will create a totally connected world where physical devices, vehicles, home appliances, and other "things" embedded with electronics, software and sensors would be able to communicate with each other via a network, also known as Internet-of-Things (IoT). The amount of these things, according to the IHS forecast 2016 (available at [1]), is expected to grow from 20 billion in 2017 to 75 billion in 2025. The growth – following the Network Externality theory [2] – will generate a vast amount of business opportunities, which can, according to McKinsey [3], have an economic impact of $3.9 trillion to $11.1 trillion per year in 2025. Part of the impact ($1.2–3.7 trillion) will result from advanced industrial applications, such operations optimization, predictive maintenance and inventory optimization.

In industrial operations, maintenance activities play an important role, as they prevent breakdowns and increase the life-cycle of machines, hence directly affecting production availability and reliability [4], as well as competitiveness and profitability of a company [5]. With the advances in Information and Communication Technology (ICT) and rapid decrease in sensor costs, maintenance strategies are gradually evolving from simple run-to-failure or time-based maintenance to more advanced ones, such as Condition-Based Maintenance (CBM) or predictive maintenance. Advanced strategies are based on diagnostics tools that measure and exploit sensor data of, e.g., temperature, pressure and vibration, to provide real-time information about the machine condition. Consequently, maintenance activities can be conducted at the right time rather than on a certain time or date intervals which, on the other hand, increases the efficiency of the maintenance function (better utilization of spare parts) and decreases the risk for unexpected breakdowns.

Advances in computing, electronics, software and sensor technology have allowed machines to evolve into autonomous, automated systems, which increasingly perform various tasks without human assistance. These systems generate massive amount of data since their operation depends on sensors and actuators (from tens to hundreds per machine), which in coordination with the controller unit(s), control the performance of machine(s). In a typical factory setting, the autonomous systems are connected to a larger production system via industrial communications technologies, thus forming an industrial network.

Industrial Networks are special kind of networks that are different from conventional networks due to the hostile environment, and strict communications requirements regarding latency and jitter. For this reason, communication protocols and interfaces are often proprietary and not compatible with standard communications

protocols such as Ethernet. This impedes machine data to be utilized in applications other than, the ones used in industrial automation and production management. Moreover, the complexity of network structure (multi-level network structure with different communication technologies on each level) inflicts challenges in cases where, for example, a remote connection to a factory machine needs to be established for troubleshooting. In such a case, the remote connection is typically established via a wired connection, whereupon it must pass through the factory's internal network, thus causing complications regarding the deployment of remote service. With the mobile solution, the complexity of internal network can be avoided, although at the expense of security and access control. This thesis analyzes the feasibility of alternative remote connection solutions concerning remote maintenance by approaching the topic from a techno-ecnomic viewpoint. The analysis will provide insight on the characteristics of alternatives and the value creation logic of remote maintenance solutions.

## 1.1 Motivation

Over the last decades, sensor and network technologies have evolved substantially. This has allowed factories to supervise their operations more efficiently and enhance the overall performance of the production by exploiting the data collected from machines, logistics and other factory-related functions. Machines typically collect a vast amount of data, of which most are used merely for real-time control in automation systems or anomaly detection [3]. Consequently, there remains an additional value to be captured by applications, such as predictive maintenance or production optimization. With the emergence of Industrial Internet, there is also a growing need for more open machine data, which can be utilized by more than one entity. However, the incompatibility of industrial ICT with the conventional ICT hinders the implementations regarding data sharing, e.g., for remote maintenance operations. Hence, the feasibility of alternative connectivity solutions, including 5G, should be studied.

## 1.2 Research question

Factories are generally considered as closed systems in which machine operational data and external connections are controlled strictly. Normally, the data is not shared with other actors, like machine providers because the implementation of remote connection for data collection purpose is considered to be an unnecessary security risk, and burdensome due to the complexity of industrial networks. Moreover, the machine data is regarded as a valuable asset, which is not provided to the third parties without substantial benefits. Nevertheless, remote maintenance or monitoring can be valuable for machine providers and factories, for example, in terms of revenue and reduction of downtime, respectively. To find the most feasible solution benefiting both parties, different connectivity options should be studied. Thus, the main research question is as follows:

*What are the alternative connectivity solutions for remote maintenance deployment in factories?*

To answer the main question, different remote connection options and value network configurations are studied, thus the sub-questions are following:

RQ1: How does connectivity and data policy choice affect the functionalities of remote maintenance?

RQ2: What is the value network configuration in each remote connection case?

## 1.3 Research methods and scope

The scope of this thesis is limited to the remote connection cases which enable machine providers to maintain or monitor factory machines remotely. The focus of the thesis is solely on the remote maintenance or monitoring of machines located in a factory, thus remote monitoring of production, logistics or other factory functions are beyond the scope. The implementation of remote maintenance is studied from a techo-economic viewpoint by analyzing alternative remote connection solutions qualitatively. The cost analysis of the solutions and the actual realization of the implementation are excluded from the thesis.

The research in the thesis is based on literature review and semi-structured interviews. The literature review includes publications from academia, industry consortia and other major standard development organizations, including 3GPP (3rd Generation Partnership Project), ETSI (European Telecommunications Standards Institute) and 5GPPP (5th Generation Public-Private Partnership). The interviews are conducted with experts from different industry fields, to gain insights about the current status in factories regarding remote maintenance, network technologies and connections, and data utilization. Additionally, the information from the interviews is used as an input for the case studies, which establish the foundation for the value network analysis.

In order to determine how value is distributed among different actors in alternative remote maintenance solutions, Value Network Configurations (VNCs) are formed. The configurations provide information about the roles each actor can take within the limits of current or future technology, and which actor will accumulate most value in terms of money, data or other indirect benefits. Moreover, they illustrate the underlying technical architecture of each solution. The VNC method is discussed more closely in Chapter 4.1.

## 1.4 Outline of the thesis

After the introductory chapter, the thesis is structured in the following manner. Chapter 2 reviews the publications regarding e-Maintenance, Industrial networks, Industrial Internet and 5G, which form the basis for understanding maintenance activities and network connectivity in factories, and the possible impact of future technologies on industrial operations. Chapter 3 presents three different factory

and remote connection cases, which are based on the information obtained from the interviews, and also partly on literature. The case studies are the basis for Chapter 4, which involves the VNC of each remote connection case and the possible future technical architecture for remote maintenance connectivity in factories. The final form of VNCs is the result of iterative improvement, which was based on the feedback gained from the thesis supervisor and advisor, and industry experts during the multiple workshop sessions. Chapter 5 discusses the results of the analysis and the insights gained from the case studies. Chapter 6 concludes the thesis. The visual representation of the structure is illustrated in Figure 1.

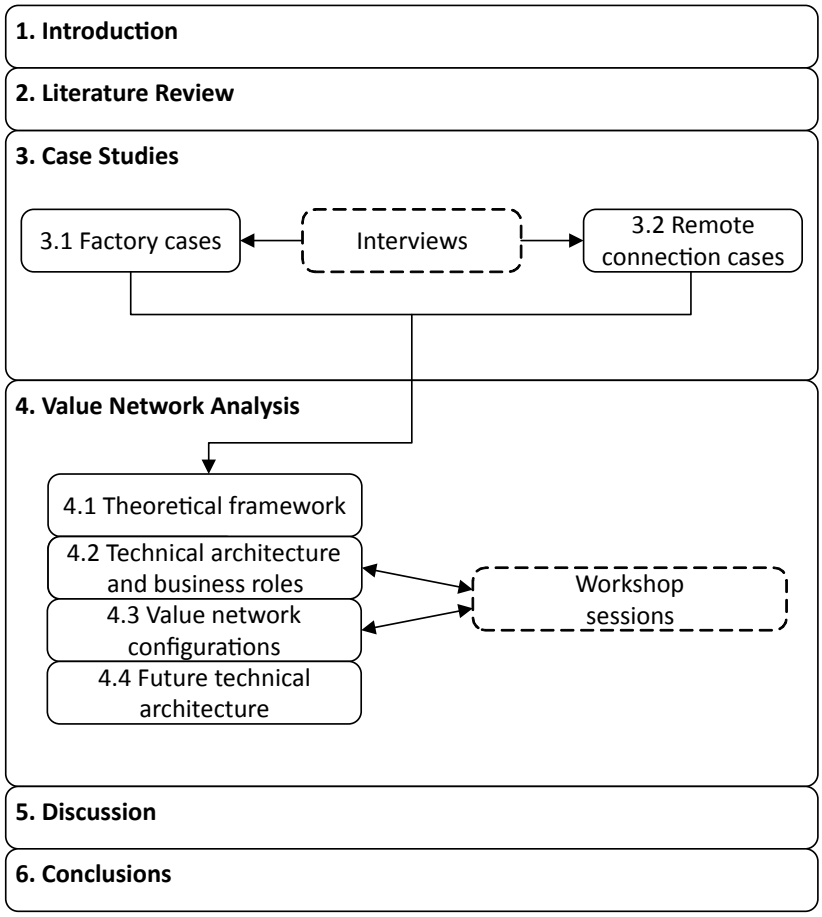


Figure 1: Structure of the thesis.

# 2 Literature Review

## 2.1 E-maintenance

The importance of maintenance function is increasing in today's factories due its role to improve availability and safety of equipment, as well as product quality [6], which, on the other hand, affect production performance and competitiveness [4]. Maintenance function has increasingly been supported by ICT, thus allowing the emergence of e-maintenance concept [6]. The definition of the concept and different type of remote maintenance strategies are presented in the following chapters.

### 2.1.1 Definition

The term e-maintenance appeared in early 2000 and is now widely used in maintenance-related literature. It covers many maintenance-related functions which has lead to inconsistent definitions and usage of the term. [7] To better understand the concept, possible roles of e-maintenance need to be determined, that is, whether e-maintenance is a maintenance strategy, maintenance plan, maintenance type or maintenance support [6].

- *E-maintenance as a maintenance strategy*: E-maintenance can be seen as a management method in which real-time machine data, obtained through ICT, is utilized in different tasks and systems [8]. Hence, it can be interpreted as a maintenance management process [9], which handles massive amount of data and ensures that information is available at functions where it is needed at the right time in order that maintenance decisions can be performed strategically, in synchronization with the production [10].

- *E-maintenance as a maintenance plan*: E-maintenance can also be viewed as a maintenance plan, which explores new approaches, such as CBM, collaborative maintenance, remote maintenance and service, and integration of maintenance function with the production, in order to conduct more efficient maintenance and prepare for the future e-automation manufacturing world. The implementation of the plan requires a proactive e-maintenance scheme, which is an interdisciplinary approach consisting of monitoring, diagnosis, prognosis and control processes. [10]

- *E-maintenance as a maintenance type*: Generally, e-maintenance is seen as gradual replacement of traditional maintenance practices with more proactive or predictive ones, such as CBM [11].

- *E-maintenance as a maintenance support*: E-maintenance can be referred as distributed artificial intelligence environment, which involves an information processing resources, decision support and communication tools, as well as cooperation between maintenance processes and expert systems [12].

Based on the review of the possible roles, the term e-maintenance can be defined as follows:

*A maintenance management concept which includes the resources, services and technology necessary to enable a proactive execution of maintenance process in synchronization with the production, logistics and upper-level enterprise functions.*

E-maintenance is an extremely broad concept as it covers many direct and indirect functions regarding maintenance. In this thesis, the focus is on remote maintenance, which is a part of factory's e-maintenance system. Remote maintenance can consist of services, such as monitoring, diagnostics, prognostics and optimization, which are performed over the Internet by the service provider autonomously, or in collaboration with the factory personnel.

### 2.1.2 Maintenance strategies

Maintenance is a critical function in any factory since it minimizes machine breakdowns and extends the life-cycle of machines. Formulating a proper maintenance plan requires a factory or maintenance manager to evaluate different maintenance strategies in order to minimize the combined cost of operating the business and maintaining the factory [4]. The strategy can vary from basic maintenance, such as run-to-failure, time-based maintenance or "design out", to more advanced one, like CBM. Additionally, the strategy may consist of maintenance-related functions which are performed remotely. The remote maintenance strategies are presented in Figure 2.

The most basic strategy, which can be applied to maintaining equipment, is run-to-failure (also known as maintain-on-failure or breakdown maintenance) [4]. In this strategy, equipment is maintained only when there is a failure, as the name refers. Organizing this type of maintenance is simple, and it does not require additional scheduling work. However, a failure might occur at an inconvenient time which might lead to whole production being stalled. Moreover, a large spare part inventory and maintenance team may be needed, to ensure a rapid response to a failure.

Time-based maintenance or preventive maintenance is a strategy, which focuses on preventing failures by replacing machine parts based on predetermined useful life, or at certain calendar days [4]. With this strategy, spare parts are ordered only when they are required. Hence, there is no need for excessive spare parts supply. Furthermore, the probability of unexpected failures is minimized by not waiting until the machine parts are completely threadbare. Despite the preventive measures, failures may still occur because suitable and correct failure data are not always available, to construct a right estimation of the life of components [4]. Consequently, a factory may overmaintain its equipment, leading to unnecessary production stoppages and inefficient use of spare parts.

Sometimes, continuous failures stem from deviating behavior of a process or software. In these type of cases, "design out" strategy aims to prevent or reduce future breakdowns by updating the process design or software. This strategy only

addresses the problems with continuous breakdowns, thus time-based maintenance or CBM may still be needed to prevent failures that are not related to design issues. [4]

Advanced maintenance plans such as CBM differ from the strategies mentioned above, as they exploit sensor data to detect early deterioration of components, hence enabling timely and efficient maintenance process. The functionality of CBM is based on continuous monitoring of sensor data, which is utilized for measuring a specific parameter that indicates the condition of a machine. The parameter can be, for example, a performance indicator, or a diagnostic measurement, which provides a warning of deterioration. [4]

A maintenance strategy can also consist of application areas which are performed remotely. Figure 2 presents the most common remote services for industrial applications. The starting point for all remote services is that the machines, which need to be remotely maintained, are equipped with sensors and can be connected to the Internet. Additionally, the sensor data needs to be stored in a private or public cloud, from which it can be utilized in various remote and web services.

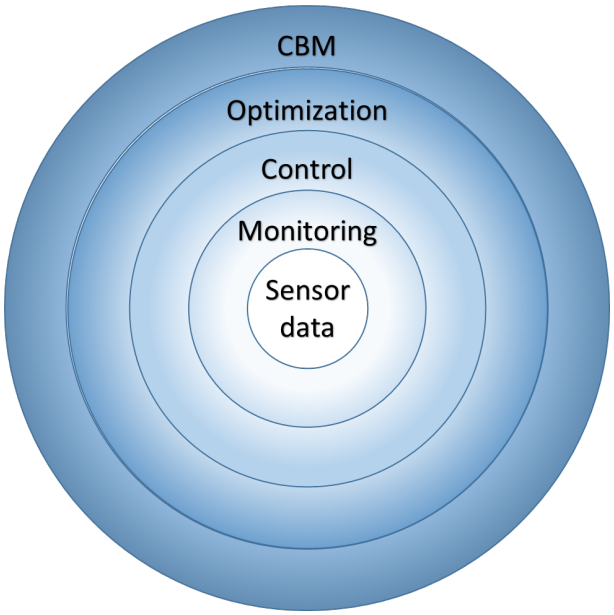


Figure 2: Remote services which can be built around sensor data (modified from [13]).

Remote monitoring is the foundation for all the other services seen in Figure 2, since it provides the possibility to supervise the condition and performance of equipment, through which decisions about a potential remote control or remote optimization can be conducted. Remote monitoring also enables a service provider to know how its machines are used and where they are located, thus providing an opportunity to develop better machines and improve logistics (spare parts and maintenance personnel). From a customer's viewpoint, remote monitoring allows machines to be supervised around the clock, and it can also reveal information, which was not formerly available. A customer can use this information, for example, to

improve maintenance activities.

After sensor data can be stored in a cloud and utilized for monitoring, the next step would be the implementation of remote control. In factories, machines are typically controlled remotely when an untypical malfunction is observed in machine's controlling system. The control, in these type of cases, would actually refer to remote diagnosis and remote repair, although it is possible, for example, to start a machine tool or control an industrial robot remotely if the customer allows it. In addition to the remote diagnostics and repair, remote control also enables remote updates, which can be used, for example, to repair software errors, re-calibrate sensors and change measurement parameters [13, p. 67].

In remote optimization, the settings of machines can be changed in real-time – at least close to real-time – to enhance the performance and improve the reliability of equipment. Additionally, the use of resources and raw material can also be optimized, on condition that other information (i.e., utilization rate of equipment and physical properties of raw materials) apart from sensor data is accessible to the service provider. [13, p. 66] Optimizing equipment and processes requires more advanced analytical methods than in remote monitoring and control, since data need to be combined from various sources and analyzed is such a manner that it provides concrete benefits to the customer.

Remote CBM or predictive maintenance offers most opportunities to exploit data (see Figure 3). For example, it can improve productivity by increasing the utilization rate of machines, by decreasing unexpected failures and by reducing maintenance breaks [13, p. 73]. This can be realized by monitoring the condition of machines and by estimating when the maintenance is needed. The estimations rely on anomalies which are tried to be observed from the real-time data [13, p. 73]. To improve the accuracy of estimations even further, historical data of a monitored machine – or even global historical data of the similar machine model – can be exploited in the assessment of maintenance need. Although remote CBM can provide the most concrete benefits compared to the other remote services, it is also most challenging one to implement and requires large investments.

Implementing a correct maintenance plan always requires a careful inspection of alternative strategies and the possible benefits that can be realized with them. Obviously, the best option would be to apply CBM as an overall policy to all machines, but it would not be cost-effective because some techniques related to CBM are expensive. Therefore, it is necessary to evaluate which machines are critical from the viewpoint of safety, capital value and production, and require more advanced maintenance strategies, and which ones would manage with typical maintenance procedures. [4]

## 2.2 Industrial networks

In the past decades, automation has had a central role in many industry areas, including manufacturing, electricity generation, food and beverage processing, and chemical refinement. It has allowed plants to be operated more efficiently by saving in labor costs, and by improving quality, accuracy and precision in processes, such

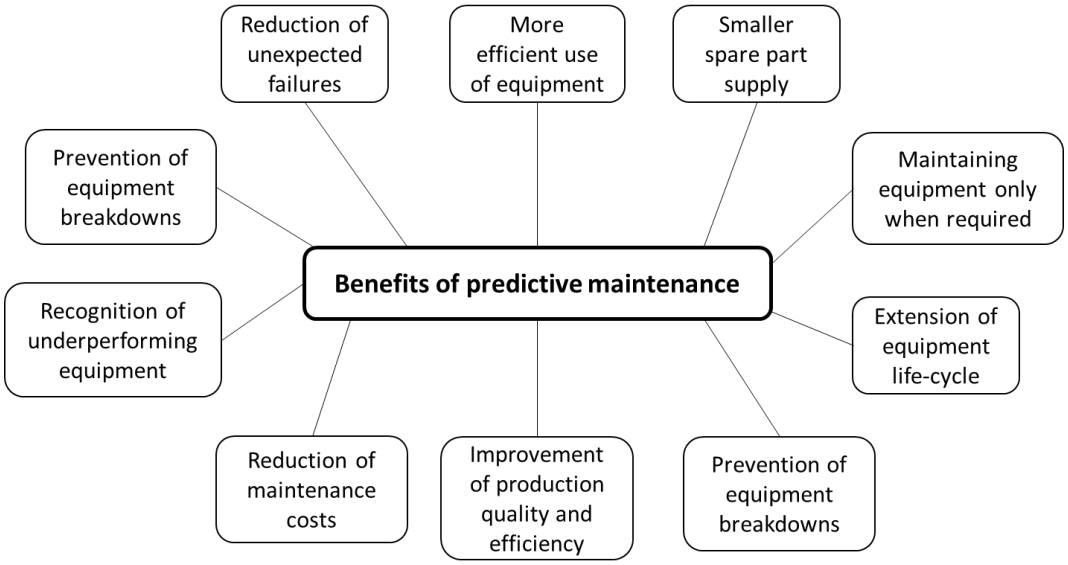


Figure 3: Potential benefits that can be realized by predictive maintenance (modified from [13, Fig. 7]).

as manufacturing and assembling. One of the key factors of modern automation systems have been industrial control networks, which have allowed horizontal (e.g., peer-to-peer coordinated control among sensors and actuators) and vertical (e.g., control among a machine, a cell and a system) integration of distributed devices and functions [14], [15]. Following chapters discuss the characteristics of industrial networks and present the overview of current fieldbus and control systems, and wireless technologies.

### 2.2.1 Network characteristics

In recent years, industrial networks have gradually started to resemble conventional networks due to the employment of Ethernet standard in industrial equipment and control networks. Although similarities can be found on some levels (e.g., management and enterprise level), the requirements in networking and communications differ significantly, especially in lower level control networks (see Table 1). [16] For example, the requirements regarding jitter and delay are very stringent; packets must be received periodically and before a certain time. Additionally, the hierarchy of industrial networks is very deep, meaning that each level – even the field level is divided to multiple subnetworks – may apply different protocols and physical standards. Consequently, the devices on one level cannot communicate directly with devices on another level, unless there is a gateway that can convert, for example, fieldbus traffic to Ethernet traffic [17].

Table 1: Differences between industrial and conventional networks [16].

| | Industrial | Conventional |
|---|---|---|
| **Primary function** | Supervision and control of machinery | Data processing and routing |
| **Environment** | Manufacturing and process industry | Corporate and household |
| **Hierarchy** | Deep, functionally separated hierarchies with many protocols and physical standards | Shallow, integrated hierarchies with uniform protocol and physical standards |
| **Failure severity** | High | Low |
| **Required reliability** | High | Moderate |
| **Round trip times** | 250 $\mu s$ - 10 ms | 50+ ms |
| **Determinism** | High | Low |
| **Data composition** | Small packets of periodic and aperiodic traffic | Large, aperiodic packets |
| **Temporal consistency** | Required | Not required |
| **Operating environment** | Hostile, often involving high levels of dust, heat and vibration | Clean environments |

### Architecture

Industrial networks normally consist of various network levels which are often connected through divergent interfaces and protocols. Figure 4 shows the well-known automation pyramid which describes the functionality of each level and the most common communication technologies connecting them. Additionally, it shows the time constraints for each level, that is, the time on which decisions are performed based on the collected data. The levels are:

- *Field Level:* This level represents all field equipment embedded with sensors (optical, magnetic, thermal etc.) and actuators (pneumatic, hydraulic, electronic etc.) [18]. The control structure of equipment can be either closed-loop or open-loop (see figure 5). In a closed-loop system, a sensor measures the effects caused by the actuator and provides feedback, for example, whether the action of the actuator should be stopped or continued. In an open-loop system, on the other hand, the actuator does not receive any feedback and acts solely on the input signal. Open-loop control is rarely used in industrial automation because it requires continuous supervision, and manual operation when the behaviour of a system needs to be changed. [19, pp. 28–32]

- *Control Level:* The purpose of this level is to control field level equipment by executing preprogrammed commands on controllers, such as Programmable

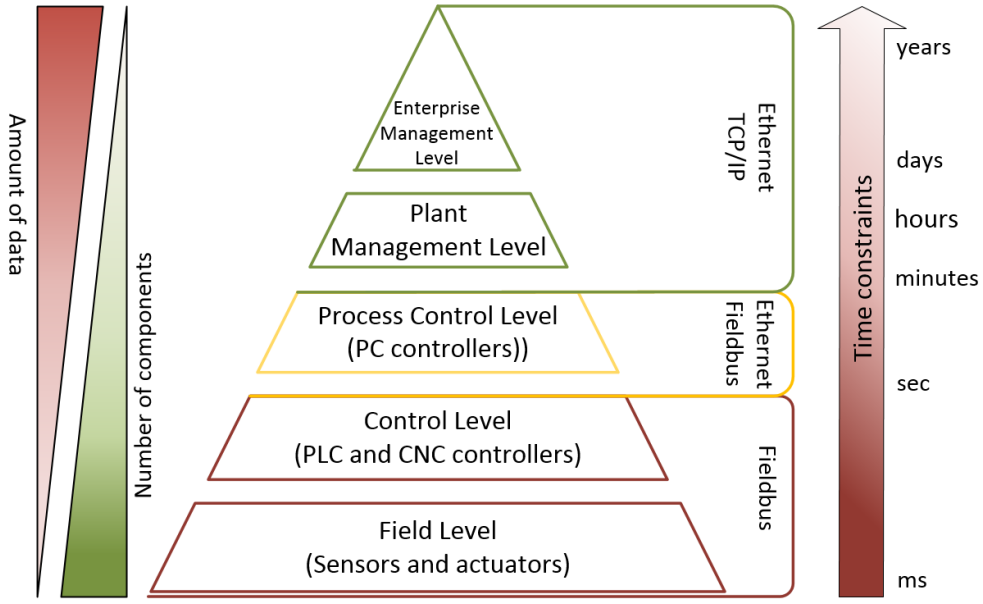


Figure 4: Automation pyramid (modified from [20], [21]).

Logic Controller (PLC) or Computer Numerical Control (CNC) [15]. The communication between the controllers and field level machinery often has high requirements regarding the Quality-of-Service (QoS). This type of communication is known as Isochronous Real-Time (IRT) communication, which has an upper limit of 1 $\mu s$ for jitter and 10 $ms$ for latency. Today, only field bus technologies, such as PROFIBUS (Process Field Bus), INTERBUS, CAN (Control Area Network), DeviceNet and some of the adapted Ethernet protocols, like PROFINET (Process Field Net) IRT and EtherCAT (Ethernet for Control Automation Technology) can satisfy IRT requirements. [17]

- *Process Control Level:* Process Control or Supervisory Control And Data Acquisition (SCADA) level coordinates lower level machinery and processes through supplier-specific process control software or some 3rd party software, which applies OPC (Object linking and embedding for Process Control) standard [20], [22]. The software is usually installed on a PC-based system, such as industrial, desktop or Panel PC. Typically, PC-based systems communicate with the lower levels via standard Ethernet using industrial Ethernet switches. [22] The focus of these systems is data acquisition from field level equipment and processes, and information visualization through a Human-Machine Interface (HMI) [16].

- *Plant Management Level:* This level consists of Manufacturing Execution Systems (MESs) that integrate shop floor processes with top-level systems by delivering status information of ongoing lower level processes to the higher level, and by optimizing the allocation of the resources (e.g., machines, robots, labor, tasks and parts) based on the received production orders from the enterprise

level. MESs are highly modular, and they include various functions, such as maintenance management, product tracking, performance analysis and quality management, which can be applied according to the operational needs of a company. [23]

- *Enterprise Management Level:* Top level of the automation pyramid contains the business intelligence of an enterprise. The objective of this level is to provide a unified view to all functions and departments through information systems, like Enterprise Resource Planning (ERP) that cover functional areas, such as financial and accounting, human resources, supply chain management, and customer relationships. [24]

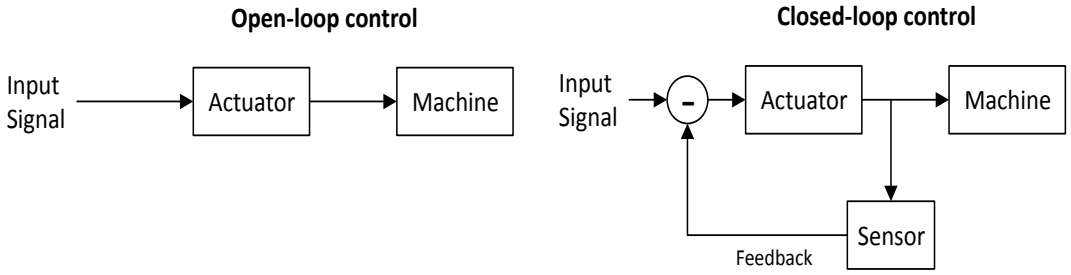


Figure 5: Open-loop and closed-loop control (modified from [19, Fig. 2-1 and 2-4]).

Although the architecture presented above is applicable in many cases, it is slowly becoming obsolete due to the gradual adaptation of Ethernet standards to all automation levels [15]. For example, Sauter [14] and Rotondi et al. [17] present a three-tier communication-focused automation pyramid, which consists of production and field level, SCADA level, and enterprise level. There are numerous other versions of the pyramid in literature, but in general, the following statement applies to almost all; the amount of data increases and the real-time requirements for data transmission decrease when moving towards the top of the pyramid [25].

### 2.2.2 Communication protocols

Today, a wide variety of communication protocols are used in industrial networks which results from rigorous requirements regarding the real-time control of field equipment, as well as, the specialized needs of different industry sectors [16]. Industrial protocols can roughly be divided into three classes: fieldbus, Ethernet-based fieldbus and wireless [14].

#### Fieldbus

Fieldbus systems, just like Internet, apply internationally accepted communications reference model OSI (Open Systems Interconnection) in the definition of communication functions. However, the model used in industrial systems is a simplified version with only three layers (see Figure 6): application, data link and physical. In addition

to the aforementioned layers, a user layer is required in fieldbus systems, to include function blocks, which specify how different type of data or information (pressure, temperature, speed, etc.) should be managed. The OSI layers in fieldbus systems have similar functionalities as in Internet systems. *Physical* layer defines voltages and physical connections and specifies how the conversion between electrical signals and bits should be performed. *Data link* layer, on the other hand, determines the protocol, encodes and decodes messages, and provides the means to detect errors that may occur on the physical layer. Moreover, it ensures deterministic data exchange between network nodes. *Network* and *Transport* layers, which are very important from networking perspective in conventional networks, have been omitted by almost every fieldbus protocol producer. [26, pp. 252–254] One of the reasons have been the conclusion that the simplified model would improve the performance of data transmission (reduction of layer data processing and passing delays), which was a problem in the first implementations of seven layer profile defined by Manufacturing Automation Protocol (MAP) Task Force [27]. Even though the simplified model does not include all the layers, it can still provide similar functionalities (e.g., networking) as in OSI model within the application layer. However, the mechanisms of accomplishing these functionalities are considerably different from general-purpose networks. [16]

In today's industrial networks, one can find a diverse set of fieldbus protocols due to the specialized requirements of different field level systems, as was stated before. For example, in some system, low latency could be crucial from the operations viewpoint, while in some other system, the priority could be high link bandwidth and network capacity.

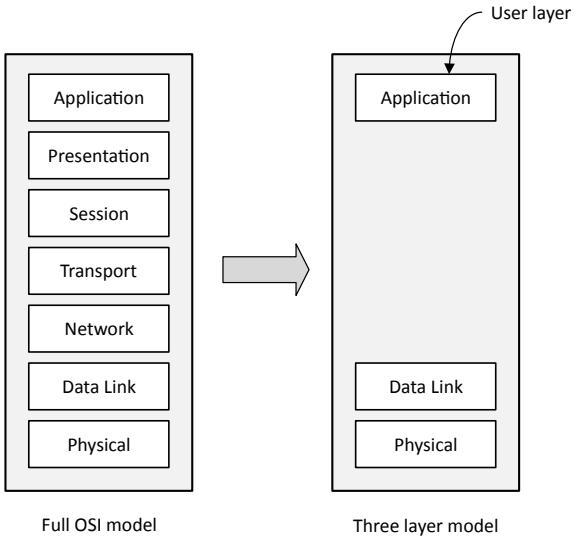


Figure 6: OSI and simplified three layer model [26, Fig. 12.3]).

### Ethernet-based fieldbus

One of the major problems in industrial networks has been the fact that different levels in the automation pyramid are controlled by networking technologies that are incompatible with each other which has inflicted many issues in the vertical integration of the automation pyramid levels. With Ethernet and IP (Internet Protocol) suite, the data exchange across all pyramid levels can be alleviated, thus making the structure of the pyramid flatter and easier to handle. [14] However, Ethernet as such is not applicable for field level communications because it cannot fully satisfy the real-time requirements needed in industrial automation [28]. Nevertheless, Real-Time Ethernet (RTE) properties and backward compatibility with the Fieldbus systems can be achieved with one of the three approaches discussed in [29]. They are presented in Figure 7. Common to all approaches is that they use Ethernet cabling and TCP (Transmission Control Protocol)/UDP (User Datagram Protocol)/IP protocols for non-real-time communications. The real-time capabilities are achieved by concentrating all real-time modification to the application layer, by bypassing TCP/UDP/IP and accessing Ethernet functionality directly, or by modifying the Ethernet mechanisms and infrastructure itself. These approaches are called "On top of TCP/IP", "On top of Ethernet" and "Modified Ethernet", respectively.

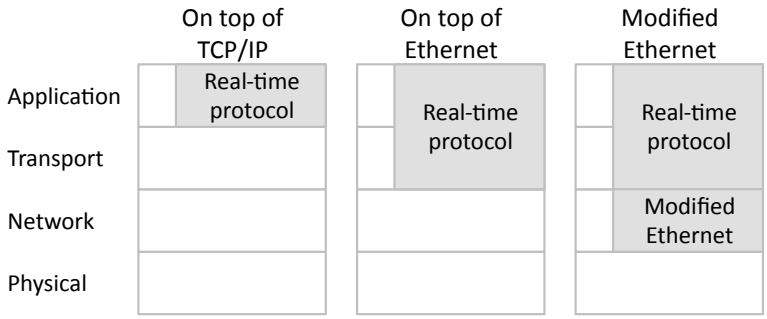


Figure 7: Ethernet-based fieldbus stack implementations on TCP/IP reference model [16], [29].

When the RTE is implemented on top of TCP/IP, only the application layer functionalities are modified which allows transparent communications over network boundaries as well as through routers. This enables, for example, to build automation networks that could be extended over the local network boundaries. Handling the protocol stack over larger networks would, however, introduce non-deterministic delays and require devices that are equipped with a reasonable amount processing power and memory. Currently, RTE protocols, such as EtherNet/IP and MODBUS/TCP, implement real-time functionalities on top of TCP/IP.

Should the RTE realized on top of Ethernet, the physical layer remains unaltered, but a custom ethertype is specified in the Ethernet frame. The ethertype allows RTE protocols to use their own protocol stacks alongside the standard IP which, on the other hand, enables the allocation of bandwidth and prioritization between devices within the network. However, the connected devices must have the understanding of

the ethertype, to use the real-time properties of the RTE protocol. One example of RTE protocol, which is implemented on top Ethernet, is PROFINET CBA (Component Based Automation).

The RTE solutions that modify the Ethernet mechanisms or network infrastructure stem from the Fieldbus solutions where starbus topology was replaced with bus or ring topologies in order to reduce cabling costs. Since the default topology of Ethernet is a star, modifications to the hardware or infrastructure are mandatory in order to have real-time functionalities in bus-like or ring-like topologies (see Figure 8). This can be realized by integrating the switching functionality inside the field device. Consequently, every connected device must be compatible at the hardware level in order that the real-time properties of the protocol can be used. Some of the well-known protocols, which apply "Modified Ethernet" approach, are SERCOS (Serial Real-Time Communications), EtherCAT and PROFINET IO.

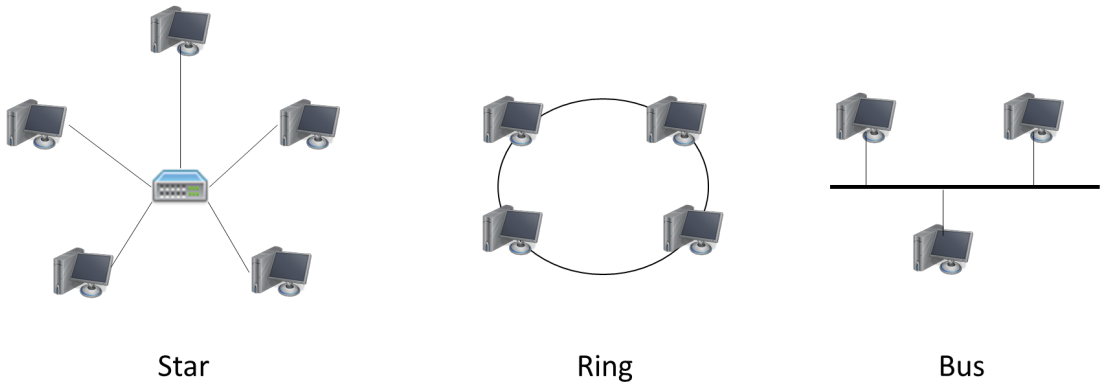


Figure 8: An example of star, ring and bus topology.

### Wireless

As Ethernet-based fieldbus is slowly becoming a dominating technology in field-level communications, the next logical step in the evolution of Industrial networks would be the inclusion of wireless technologies. The topic has been studied in many publications [14], [30], [31], [32], but is still far away from being resolved. The issue in wireless communications is varying transmission channel conditions (e.g., interference, attenuation, path loss and thermal noise) which cause challenges for satisfying the stringent real-time and reliability requirements of many industrial applications [33], [31]. Nevertheless, with proper designs and technical solutions, wireless technologies will become more common in the field-level networks in the near future due to the benefits and possibilities they can offer [14]. By using wireless solutions, a factory could, for example, save in cabling costs, unlock new information from sensors, deploy new devices quicker, alter the shop floor setup flexibly, and use wireless control applications [30], [33]. In the industrial setting, wireless networks are usually referred to as Wireless Sensor and Actuator Networks (WSANs). In WSANs, sensors

and actuators are equipped with transceivers, which enable a wireless transmission of collected data not only between the sensors and actuators embedded in the same machine but also with other machines as well [34]. In order that WSANs would experience a wide-spread penetration in industrial automation, especially process and discrete manufacturing automation, the following challenges should be addressed:

- *Safety:* WSANs should be designed in such a manner that they guarantee the safety of humans, environment and property. The design should address the issues caused by connection losses and packet errors [30].
- *Security:* A possible manipulation of sensor and actuator data should be prevented with proper safety measures. Moreover, possible external Denial-of-Service (DoS) attacks should be reckoned with safe state features included to the automation systems. [30]
- *Availability:* Should a communication error occur in some production section, the influence of it to the overall production should be minimized [30].
- *Latency:* In automation systems, data is only valid for a short time, and therefore delivery of data should not exceed a certain time limit [32].
- *Network size:* The network should be capable of satisfying the required refresh rates of sensors (expresses the frequency of sensor readings) [30]
- *System integration:* WSANs need to be integrated seamlessly with the IP architecture so that machine data could be utilized more efficiently in production management and remote services [32].
- *Wireless channel conditions:* A wireless communication link is exposed to the interference of many sources, which decreases the quality of a link [32]. Therefore, proper interference cancelling methods are required so that the real-time properties could be achieved in WSANs [30].
- *Energy consumption:* Due to required refresh rates in automation systems, it is difficult to decrease the energy consumption of sensors. Therefore, it is not expected to have completely wireless field equipment equipped with battery-powered sensors and actuators in process and manufacturing industries in the near future. However, temporary battery-powered sensor installations could be used, e.g., for machine optimization purposes. [30]

Many challenges need to be resolved before wireless technologies can widely be adopted in industrial automation as can be noticed from the list above. It is also not expected that they would fully replace existing wired systems in form WSANs, but are more likely to be implemented as complementary solutions to wired field-level networks [14]. For example, Sauter [14] proposes a hybrid wired/wireless network topology which consists of isolated wireless clusters that are connected to the field-level backbone network through access points (see Figure 9). The clusters do not

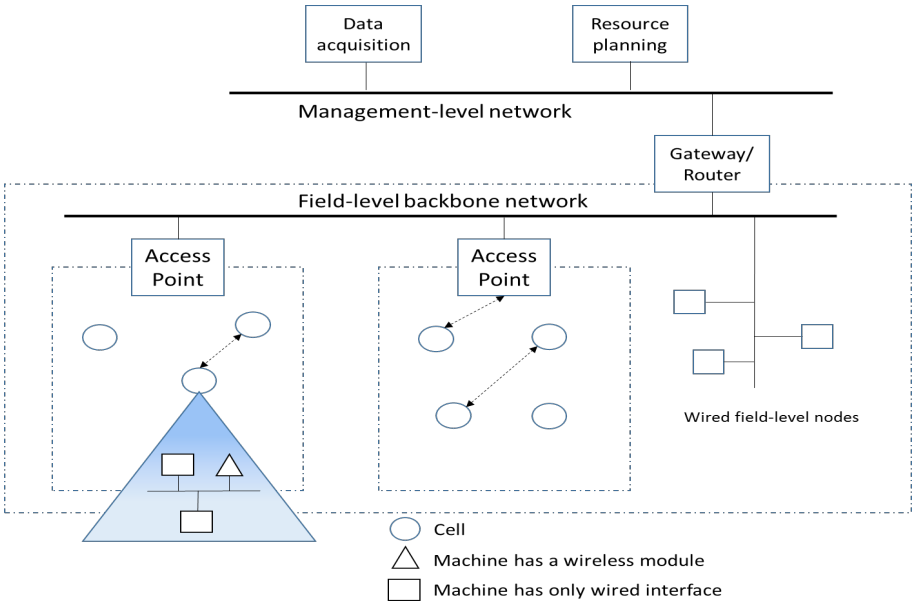


Figure 9: Hybrid network topology with isolated clusters (modified from [14]).

exchange data, or at least not with real-time requirements. This type of setup in factories could be, for example, wireless clusters consisting of multiple cells.

Currently, IEEE (Institute of Electrical and Electronics) wireless technologies, such as 802.11; WLAN (Wireless Local Area Network), 802.15.4; WPAN (Wireless Personal Area Network) and 802.15.1; Bluetooth, are used in many commercial applications. Even though the requirements for reliability and latency in consumer applications are less stringent than in industrial applications, standardized technologies can potentially contribute to the wireless technologies being widely adapted to Industrial networks as well. However, the aforementioned wireless technologies as such would not be suited to more critical factory operations, like automation because they cannot meet the real-time communication requirements [14]. Therefore, communications standards, such as WirelessHART and ISA 100.11a, which are designed for applications founded in process automation, have modified the MAC (Media Access Control) layer of IEEE 802.15.4 (the PHY layer is adapted without modifications) in order to make it more applicable for the industrial environment. These communications standards are mainly targeting applications (e.g., condition monitoring) that do not have high requirements for latency. Therefore, it is very likely that some improvements are needed before the current IEEE standards would be able to serve time-critical applications. [30] On other hand, another alternative for IEEE solutions are mobile technologies, particularly 5G, which are developed by 3GPP. One of the main objectives of 5G is to provide technology and infrastructure which would meet the requirements of mission-critical communications (i.e., time-critical communications) [35]. For example, Yilmaz et al. [36] studies the use of 5G in industrial automation by simulating an LTE (Long-Term Evolution) system with modified physical layer attributes and convolution code modulation. The simulation results showed that it

is possible to guarantee sub-millisecond wireless transmission with very low failure rate. 5G is covered more closely in subchapter 2.4.

### 2.2.3 Industrial control systems

Interconnection of various production related functions and assets through communication networks is of primary importance in today's factories because it enables diagnostics, supervision and control of equipment [37]. Communication networks in industrial setting are normally comprised of components and applications, such PLCs, SCADA and Distributed Control System (DCS) [16]. These components and applications with other ICT resources, like servers, routers and desktops, form Industrial control systems or networks [37]. An example of Industrial control network can be seen from Figure 10. The two rightmost blocks (Control Networks and Field Area) in the figure are the core of every Industrial control network. In a typical industrial network, these blocks contain sensors and actuators, which are controlled by PLCs. However, in some industries, like manufacturing, the blocks also include CNC controllers in addition to the PLCs. These controllers are used to operate movements of machine tools and robots by means of numerical values, which are produced by Computer Aided Design (CAD) software [38].

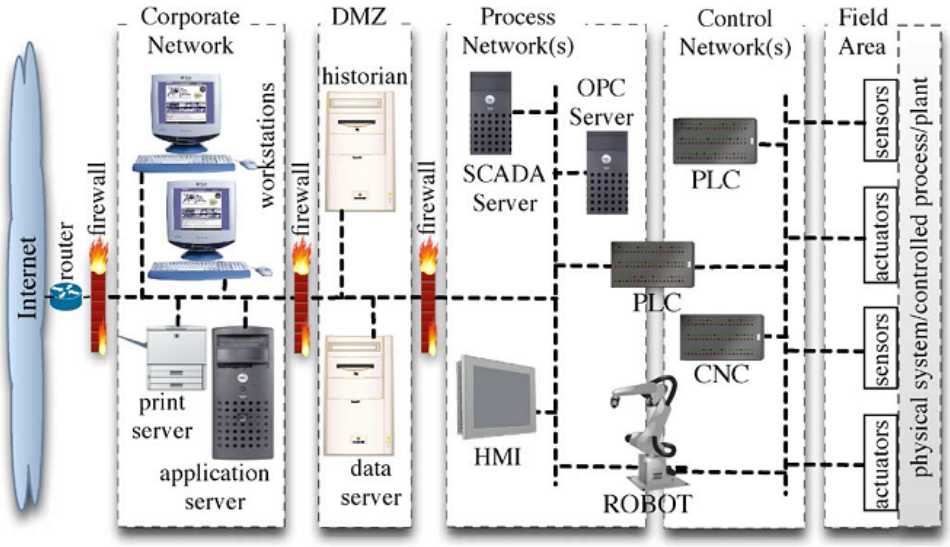


Figure 10: An example of Industrial control network and typical connections between field-level and corporate-level equipment [37].

PLCs are specialized and solid-state electronic devices which can be programmed through a dedicated port or network by using a special programming language and software. They are highly modular devices, which generally consist of a power supply, processor, input/output module and communication module. The modularity enables easier maintenance and installation of larger PLCs, which can be composed of more than one module of each type. Moreover, modules with different functionalities can

be combined, depending on the system requirements. [16] PLCs can be used, for example, to control motor rotation speed or fluid flow.

The middle block in Figure 10 represents the process network, which is designed to support monitoring and management of field devices through SCADA, DCS and other specialized process control software, such as OPC UA (Unified Architecture) based applications [37]. Most of these systems are purely software based and are normally applied at the process control level (see Figure 4) [16]. SCADA, for example, is a system which main focus is data acquisition and data presentation through centralized HMI, and as such, it does not perform any substantial control of equipment. SCADA systems are usually comprised of two application layers; client applications and server applications. The client-side applications are responsible for presenting machine data through HMI, whereas the server applications manage the communication with controllers, and coordinate and store the information which is being displayed by the clients. Server and client applications are connected to each other via Ethernet, and the controllers communicate with the servers through fieldbuses. [39] SCADA systems are tailored for geographically diverse control hardware, which can be dispersed over long distances. Therefore, it is often required to use communication services offered by third parties, like Internet Service Provider (ISP) in order to connect the hardware. Since the third-party communication media is often unreliable or have limited bandwidth, SCADA systems are normally event-driven (only changes in variables reported) rather than process-driven (a continuous stream of process variables). [16]

DCSs, on the other hand, are process-driven and resemble SCADA systems in many functions, as they are also software based and have a centralized HMI. Since the focus of DCSs is on presenting a steady stream of process information, a much higher level of interconnection between software layer and control hardware is required than in SCADA systems. In DSCs, the whole control hardware is comprised of powerful PLCs that often implement multiple closed-loop controls. Because of the aforementioned matters, DCSs are less suitable for geographically distributed systems. Many DSCs need only a single engineering tool for programming control hardware and configuring software due to the high level of interconnection. In order to implement such a functionality, the equipment and software need to be bought from the same vendor which tends to restrict the purchase of equipment from other vendors. Moreover, implementing a proprietary system is a substantial investment which often leads to situations where control hardware have much longer life-cycles than the computer equipment. This is a growing concern from the overall security viewpoint – especially in SCADA systems – since in many cases newer computers and operating systems are not compatible with the control hardware which leads to communication being implemented using obsolete hardware and drivers. [16] The summary of the differences between a DCS and SCADA system are presented in Table 2.

In recent years, a new automation concept named OPC UA has increasingly been used in Industrial networks for transferring data between automation pyramid levels in a standardized manner. Today, there exist over 35 000 different OPC products in more than 17 million applications [40]. In industrial automation, OPC UA servers

Table 2: Differences between a Distributed Control System (DCS) and Supervisory Control And Data Acquisition (SCADA) system [16].

| **DCS** | **SCADA** |
|---|---|
| Process-driven | Event-driven |
| Small geographical areas | Large geographical areas |
| Suited to large, integrated systems, such as chemical processing and electricity generation | Suited to multiple independent systems, such as discrete manufacturing and utility distribution |
| Good data quality and transmission media reliability | Poor data quality and transmission media reliability |
| Powerful, closed-loop control hardware | Power efficient hardware, often focused binary signal detection |

typically exist on the process control level, although as such, OPC UA is not a process control system, but more like a framework and a set of standards which interconnect different systems by providing a common interface for communications between products from various vendors. The functionality of OPC UA is entirely based on state-of-the-art Web services technology, excluding the functionalities of Classic OPC, which are included to ensure compatibility with older systems. [41] Consequently, OPC UA functions can be implemented to any operating system such as Apple, Android, Linux with JAVA and Microsoft Windows, or hardware platform such as traditional PC hardware, cloud-based servers and PLCs [40]. The communication of OPC UA is implemented into layers on top of standard TCP/IP stack. The layers manage sessions and ensure that communication between clients and server(s) is secured. [42] The data between clients and server(s) is encoded to binary or XML (Extensible Markup Language) messages and is exchanged using numerous transport protocols, including TCP, which provide options, such as OPC binary and SOAP-HTTP(S) (Simple Object Access Protocol-Hyper Text Transfer Protocol(Secure)) [40]. In Industrial networks, OPC UA server(s) typically collect data from field level devices and communicate with OPC UA clients, which can be, for example, ERP, MES, SCADA system, or Windows-based HMI (see Figure 11).

## 2.3 Industrial Internet

New levels of connectivity provided by the Internet, and the convergence of industrial systems and exponentially growing technologies, such as advanced computing, analytics and low-cost sensing, have enabled the emergence of new concept named Industrial Internet. It promises to revolutionize the interaction of industrial machines and change the way business is done. [43] Next chapters present the waves of innovations, industrial revolutions, and the term Industrie 4.0, which is similar to Industrial Internet, but with more focus on industrial production applications. Moreover, the

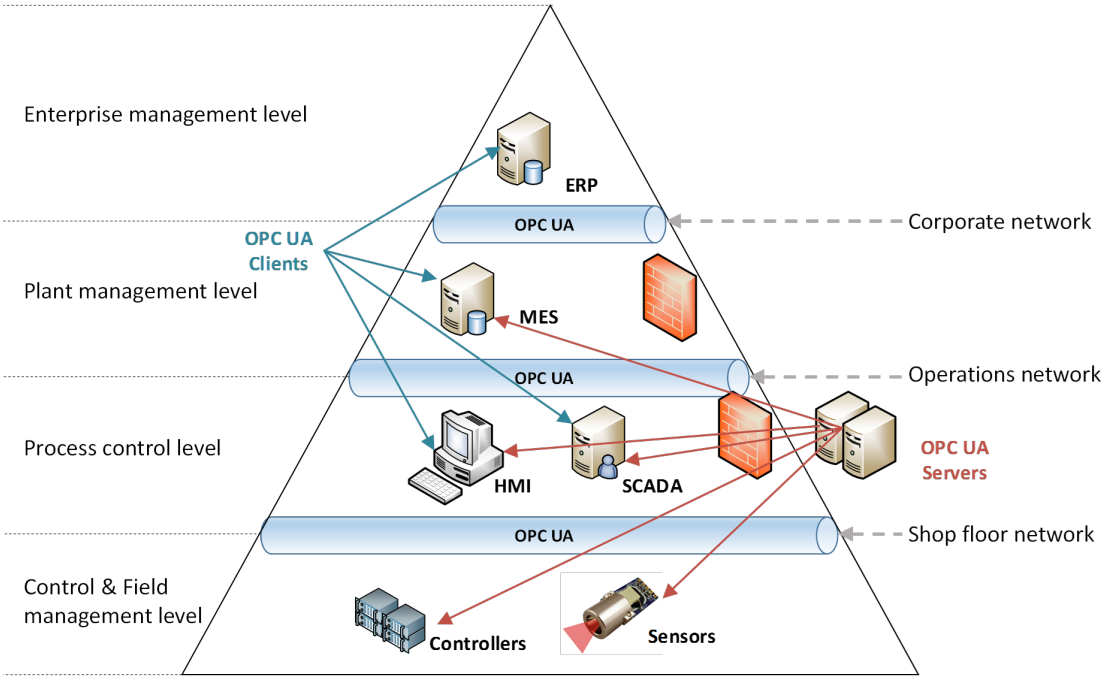


Figure 11: OPC UA communication within the automation pyramid (modified from [41]).

prerequisites for materialization of Industrial Internet and the economic and technical forces driving the change are discussed.

### 2.3.1 Industrial revolutions and waves of innovations

Both Industrial Internet and Industrie 4.0 refer to a new industrial era which is supposed to change our society and economy. The name "Industrial Internet" was invented by General Electric (GE), whereas "Industrie 4.0" was first used in Hanover Fair in 2011, and since then it is frequently used by the German government bodies and media with relation to the German industry, and discussed in academic publications [44]. While these terms share similar vision of the forthcoming industrial era, their view of the past revolutions differ.

Industrie 4.0, as the name refers, is the Fourth Industrial Revolution. The previous three revolutions spanned almost 200 years starting from the introduction of steam engines in the 1780s, followed by the mass production based on the division of labor and electrification, and ending to the presentation of the first PLC (invented by Modicon in 1969), which enabled the automatization of production systems (see Figure 12) [44]. Common to all the previous revolutions was that the productivity increased dramatically due to the introduction of novel technology. The Fourth Industrial Revolution, on the other hand, is not driven by a revolutionary innovation, but by the transformation of technological advances, such as cloud computing, "big data" and analytics, augmented reality and autonomous robots, to support and integrate production and business related functions across the entire value chain [45].

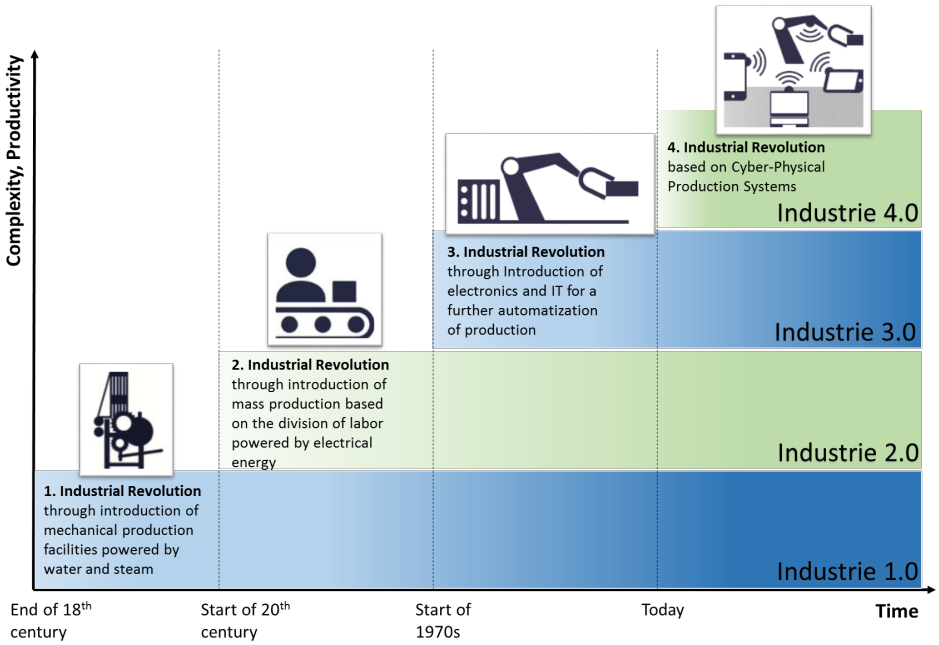


Figure 12: An overview of the industrial revolutions (modified from [46]).

General Electric's interpretation of the next revolution differs from the view of Industrie 4.0, as it discusses the waves of innovations (see Figure 13), of which Industrial Internet is meant to be the third one. According to the GE, the first wave, i.e., the Industrial Revolution, spanned from 1750 to 1900. During this time, innovations, including the steam engine, internal combustion engine and electricity, were applied to manufacturing, energy production, transportation and agriculture, initiating a period of economic growth and transformation. The Industrial Revolution had an enormous impact on society, economy and culture since it introduced radical advancements in transportation (railways, steamboats and trucks), communications (telephone and telegraph) and living standards (electricity, running water, sanitation and medicine). [43]

The second wave, i.e., The Internet Revolution, which is currently ongoing, has been information and knowledge centric rather than resource centric that was characteristic for the Industrial Revolution era. The Internet Revolution began in 1950's with the introduction of large main frame computers, software and data packets that allowed communication between computers via a transmission medium. The major breakthrough in this era was the invention of the World Wide Web, which enabled communication between heterogeneous networks and devices all around the world. With continuously increasing transmission speeds and more rapid exchange of larger data volumes, new powerful platforms for commerce and social exchange were created. The forerunners in this were companies, such as Google, Facebook and eBay. [43] In the industry, the invention of the digital controller and the application of networking and computing to production related functions allowed more flexible operations and deeper integration [16], thus increasing the efficiency and productivity

in industry fields, like process and manufacturing industry.

The third wave, as was stated before, is the Industrial Internet era, in which open computing, communications and Internet-based digital technology are meant to merge with industrial systems, thus offering new possibilities to accelerate productivity, reduce inefficiency and waste, as well as improve the working experience of employees [43]. The realization of Industrial Internet heavily depends on the assimilation of advanced information and communication technologies in traditional industries [47], as well as on the deployment of intelligent devices and systems, with which machines, factories, fleets and networks can more deeply be integrated with the big data, analytics and other advanced applications [43].

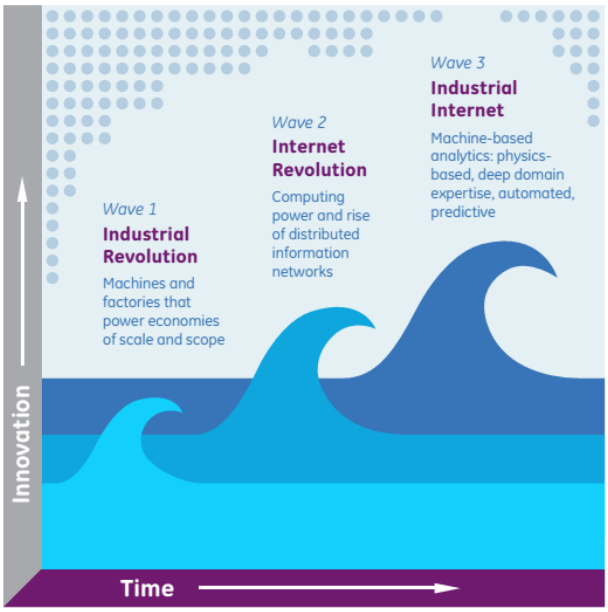


Figure 13: The three waves of innovation and change [43].

### 2.3.2 Economic and technical catalysts

There are many explanations why Internet Industrial is emerging now. Firstly, the capabilities of machines are not being fully utilized and inefficiencies at the system level continue to rise due the increasing complexity of industrial networks and systems which create incentives to apply novel solutions arising from Internet-based innovations [43]. Secondly, with rapid evolution of computing, information, network and sensor technologies in the 21st century, it is now possible to support widespread instrumentation, monitoring and analytics [13, pp. 44–47]. Thirdly, the cost of instrumentation and cloud computing is declining, and advanced cloud-based analytic tools are maturing and becoming widely available [43]. Lastly, the potential economic benefits of Industrial Internet are significant, thus accelerating investments in Industrial Internet applications and technology. In 2015, McKinsey predicted that potential economic impact of IoT in 2025, including consumer surplus, is $3.9

trillion to $11.1 trillion, of which factories (definition includes hospitals, agricultural settings and manufacturing facilities) generate $1.21 billion to $3.7 billion due to more efficient operations, maintenance and inventory management as well as improvements in worker health and safety [3]. Merely in Germany, the next Industrial Revolution is expected to contribute about 1 percent per year to GDP (Gross Domestic Product) over the next ten years and create approximately 390,000 new jobs [45]. In addition to the aforementioned factors, there are also many other economic and technical catalysts which are affecting the transition to next industrial era. The catalysts are:

- *Costs of deployment:* Instrumentation and sensor costs have declined radically in recent years which have enabled more economical installation of sensors and monitoring of industrial machines [43].

- *Computing power:* During the past 50 years, the number of transistors in microprocessors have doubled every year, as was predicted by the Moore's Law. At the same time, the performance of microchips has increased radically and the price level declined, leading to the situation where it is feasible to equip physical machines with more advanced digital intelligence [43].

- *Advanced analytics and big data:* Advances in software tools and analytic methods have provided the means to collect and extract valuable information from large data sets acquired from many different sources (e.g., equipment, MES, ERP and customer-management systems) [45].

- *Autonomous robots:* Today, robots are an essential part of industrial automation systems. They have long been used to perform complex tasks, which require unprecedented precision and often power. [48] They are also gradually becoming more autonomous, flexible and cooperative, and in the future, will be interacting with one another as well as working safely abreast with human operators [45].

- *Simulation:* The importance of simulations in plant operations will rise in the future, as they will be used to test and optimize machine settings for the next products in line in a virtual environment before the actual physical changes are made, thus decreasing machine setup times and improving quality [45].

- *Horizontal and vertical system integration:* Due to lack of standards and proprietary solutions, most of today's Information Technology (IT) systems in factories – not to mention the linkage of IT systems across the value chain – are not fully integrated [45]. However, the use of Ethernet in all automation levels and implementation of standards, such as OPC UA, are gradually integrating systems vertically. With the Industrial Internet, the vertical and horizontal integration will evolve even further, leading to truly automated value chains [45].

- *The Industrial IoT:* Today, sensor data is not fully utilized due to the limited use of embedded computing in machines. With the Industrial IoT, machines will be more intelligent due to smart sensors and smart computing, and with

standard technologies, they will able to communicate and interact seamlessly with one another as well as with the centralized controlling systems. [45]

- *The cloud:* Cloud-based software and analytics are slowly penetrating the industrial market, but with emerging Industrial Internet applications, more production-related data will be transferred across sites and factory boundaries, hence leading to a growing need for cloud services [45]. As the price of processed data is declining and industrial cloud platforms are emerging, cloud services will eventually be adapted by the industry due to the productivity gains provided by the Industrial Internet applications [43].

- *Additive manufacturing:* Additive manufacturing, also known as 3D printing, is gradually becoming an important manufacturing technology. As a part of Industrial Internet, it has a potential to revolutionize parts manufacturing and logistics by means of decentralized manufacturing systems and parts-on-demand production. [49]

- *Augmented reality:* Augmented reality is a novel HMI system, which overlays computer-generated information on the physical world [50]. Augmented-reality-based systems are currently at an early development stage [45], but they are expected to introduce an innovative and efficient solution for workers in order to improve decision making in maintenance, design, planning and machining tasks through the real-time information provided by an augmented-reality-based HMI [50].

The list above is by no means exhaustive, but it presents the key technologies and economic factors that are driving the change towards Industrial Internet.

### 2.3.3 Prerequisites for materialization

Most of the technological elements as well as economic incentives for Industrial Internet are already in place to initiate the change. However, there are some prerequisites that need to be considered and studied before Industrial Internet can truly materialize. Otherwise, it may remain as a vision and promises, as happened with the Computer Integrated Manufacturing (CIM) in the 1970s and 1980s [51]. At that time, CIM promised a highly automated production and had a vision similar to present-day Industrial IoT [51]. The vision and promises proved to be just a marketing hype, resulting in wide investment losses [52]. In order to avoid the destiny of failed market cases, like CIM, the realization of Industrial Internet presumes at least a sufficient infrastructure to support the massive growth of data and devices, proper cyber security measures, stakeholder involvement, new business opportunities, talent development and education, and an architecture to support the implementation of advanced industrial systems.

According to Gartner, the amount of connected "things" (devices, machines, sensors, etc.) is expected to grow from 8.6 billion to 20.4 billion in the next three years [53]. Therefore, the ICT infrastructure, including data centers, mobile and fixed

networks, and broadband spectrum, has to be developed further in order to support the significant growth of these things, as well as data volumes which will increase as a consequence of the growth. From the industry perspective, the infrastructure should be capable of providing adequate service for various machines, systems and networks throughout industries and geographies.

With the emergence of Industrial Internet, more machines, devices, sensors as well as industrial systems will be connected to the public networks which will increasingly emphasize the importance of proper cyber security regimes. Many of today's factories still rely on closed networks and systems that are not designed to encounter the cyber security threats involved with increasing connectivity [45]. Therefore, proper cyber security strategies should be designed in terms of both network security (defense strategy) and the security concerning devices that are connected to the public network. The defense strategies should consider every layer, starting from the public network down to the device. Additionally, sufficient measures regarding the data and transmission encryption should be implemented in order to protect sensitive and valuable information during its transmission, e.g., to a public cloud. [43]

The realization of Industrial Internet heavily depends on the co-operation of various stakeholders, such as technology and machine vendors, asset owners/operators, regulators and policymakers, international institutions, and academia [43], as well as on the convergence of IT and Operational Technology (OT) [48]. The parties involved in the development of Industrial Internet need to reach a consensus on the technology standards, data privacy policies and cyber security strategies, which would promote innovative business-to-business and business-to-consumer solutions and encourage data sharing among businesses. Moreover, the traditional barriers between IT and OT systems, processes and people need to be removed since one of the major requirements for the realization of Industrial Internet is the seamless interconnection between field-level machines, management-level systems and cloud platforms [48].

With the Industrial Internet, the number of connected machines, devices and sensors will radically increase which will provide new business opportunities for different type of actors. Ehret and Wirtz [54] identify three opportunity categories with respect to Industrial IoT. They are asset-based, service-innovation based and service-driven opportunities. The asset-based opportunities focus on leveraging assets with Industrial IoT systems, for example, by providing manufacturers the machine output as a service. The service-innovation-based opportunities are in Industrial IoT data aggregation and analysis with other data from similar environment. The service-driven opportunities are in the empowerment of designers, customers and other stakeholders with direct access to manufacturing. Although the opportunities mentioned above are centered around asset owners and providers, there are also business opportunities for other actors. For example, cloud providers could offer a platform, which enables the integration of various Industrial Internet services. Mobile operators, on the other hand, could provide localization or network resource allocation (i.e., network slicing) services for remote service providers.

With the rise of Industrial Internet, new cross-disciplinary talents will be required. These talents can be developed from the existing workforce, or they can be trained

through the university educational programs that address the needs of Industrial Internet [45]. One of the most demanded job categories will be "digital-mechanical" engineers (combination of mechanical engineering with information and computing competencies), data scientists and user interface experts. In addition to the talent development and employing, companies will also have to develop or hire a new generation of leaders, which promote the vision of Industrial Internet through investments in novel technologies and applications, changes in organization culture, and embrace of innovative production methods. [43]

Next generation industrial systems will require an architecture to support the implementation of novel industrial applications. In Industrie 4.0 concept, these systems are defined as Cyber-Physical Systems (CPS), and one of the most well-known architecture linked with CPS is the 5C model (see Figure 14) proposed by Lee et al. [55]. It consists of five levels, which are:

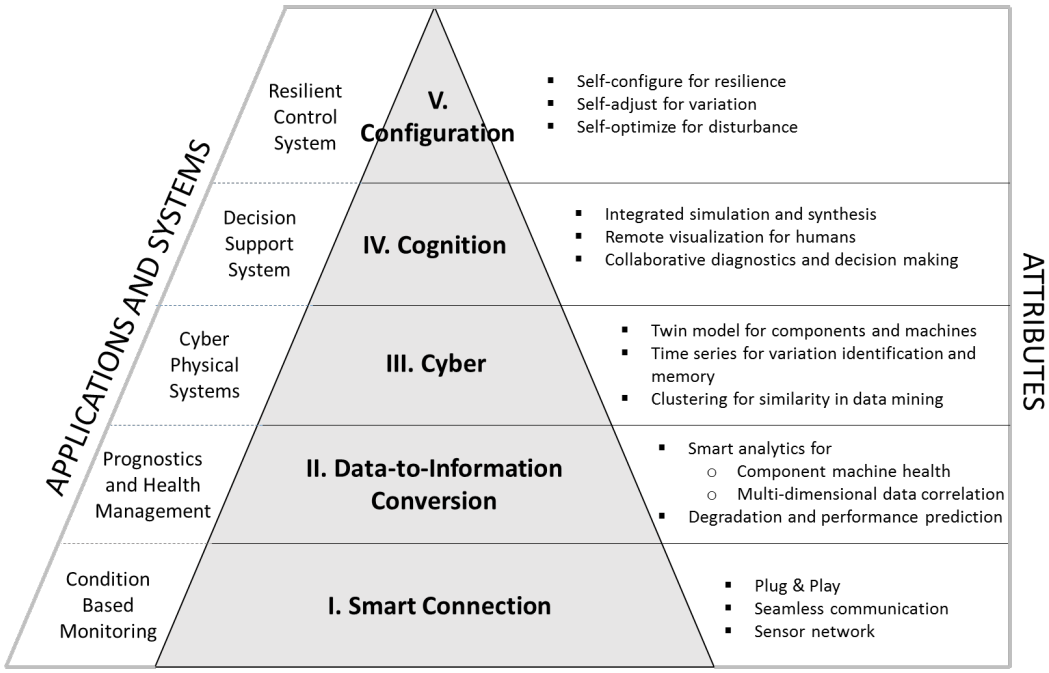


Figure 14: 5C architecture for the implementation of Cyber-Physical System (modified from [55]).

- *Smart **C**onnection:* Reliable and accurate data is seamlessly acquired from sensors, controllers, and systems, such as MES and ERP using wired and wireless communication. The important factors at this level are the management of various type of data from wireless and wired sources, as well as the selection of proper sensors (type and specification)

- *Data-to-Information **C**onversion:* Data is transformed to meaningful information with analyzing tools and methodologies. This enables, for example, to

predict the remaining useful life of equipment which, on the other hand, is the first step towards self-awareness of machines.

- ***C**yber:* This level acts as a central information hub to which data is transmitted from every connected machine that together form the machines network. The massive data combined with advanced analytics provide machines self-comparison ability, which enables the performance comparison and rating of a single machine among the fleet, as well as the prediction of future behavior by exploiting the historical data of previous assets. The actual CPS are formed at this level.

- ***C**ognition:* This level provides a thorough knowledge of the monitored system to users. The acquired knowledge is transferred through info-graphics and HMIs. By way of visual information, users can perform correct and rapid decisions regarding production-related tasks.

- ***C**onfiguration:* The top level of the pyramid provides the feedback from cyber space to physical space and acts as a Resilience Control System (RCS). The RCS applies the corrective and preventive decisions, which were performed at the cognition level, to the monitored system. The configuration level is also the topmost supervisory control level that provides the means to make machines perform self-configuration and self-adaptation.

The 5C model presented above is a fairly abstract representation of CPS, but nevertheless provides the guideline for the implementation of different stages and development of novel applications.

## 2.4 5G vision

Numerous standardization and industry bodies, including 3GPP, IETF (Internet Engineering Task Force), ITU-T (International Telecommunication Union - Telecommunication), ETSI, IEEE, NGMN (Next Generation Mobile Networks) and oneM2M as well as academia are tirelessly working to solve the technical specifications of 5G in order to fulfill the requirements of novel applications, such as autonomous driving, tactile Internet and e-Health. The latest publications regarding the architecture, technical requirements and enabling technologies of 5G, as well as its impact on the industry are discussed in the next chapters.

### 2.4.1 Technical requirements

The technical requirements of 5G heavily depend on the use cases proposed by different industry fields, governmental bodies, and organizations. The use cases (a 3GPP study [56] defined over seventy use cases) can be categorized into four groups: Massive Machine-Type Communications (mMTC), Critical Communications, enhanced Mobile Broadband, and Network Operation (see Figure 15). Each group has its own technical requirements. *mMTC* consists of densely populated (1 M/km$^2$ [57]) sensors and devices, which are mobile with low to moderate speeds (e.g., 50 km/h)

and require low transmission speeds (e.g., 1 Mb/s) [56]. Novel vertical services in this category are smart home and city, smart utilities, smart wearables, and e-Health [58]. *Enhanced Mobile Broadband* category includes use case families, which require higher data rates (e.g., augmented reality and ultra-high definition services), higher mobility (e.g., high speed trains) and variable data rates (e.g., moving hot spots), as well as higher coverage with guaranteed minimum data rate (e.g., 50+ Mb/s). *Critical Communications* group is comprised of services, to which high reliability and availability, and low latency are critical from the operations viewpoint. These type of services are industrial automation and control, life-critical applications in e-Health, automated traffic control and driving, and public safety. [59] The last use case group is *Network Operation*, which function is to address the system requirements of 5G with functionalities, such as network slicing, connectivity and routing, migration and interworking, optimization and enhancements, and security [58].

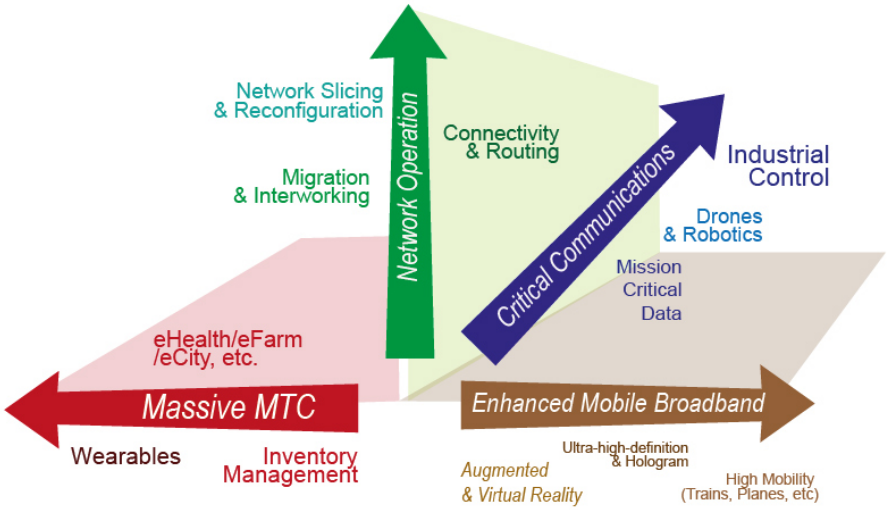


Figure 15: The main use case groups of 5G [58].

With the introduction of novel use cases, the mobile and wireless traffic is expected to grow enormously over the next decade which will be driven by the massive increase in connected devices. These devices will need to have an access to the Internet and a possibility to share data, anywhere and anytime. The growth of data and the amount of connected devices will require a new type of technical solutions so that the diverse services required by the connected devices can be met. The aim of future 5G systems is to support [57], [60]:

- 1000-fold increase in data volume per area (10 Tb/s/km$^2$)
- 10- to 100-fold increase in number of connected devices

- 10- to 100-fold increase in typical user data rate (up to 10 Gb/s)
- 10-fold extension in battery life for low power mMTC devices
- 5-fold reduction in End-to-End latency ($<$ 5ms)

### 2.4.2 Architecture

With the introduction of numerous challenging use cases and novel technologies, a new type of architecture is required for the next generation mobile communications. Many propositions for the 5G architecture has already been published by the academia and consortia. For example, the architecture working group of 5GPPP proposes an overall architecture [61], which consists of five different views (Applications and Business Services, Infrastructure Control, Logical & Functional, Physical Resources, and System Management) and supporting functions (Network Slicing, End User and Operational Services, Integration of Heterogeneous Technologies, Native Softwarization, and Integration of Communication and Computation) that together form the 5G architecture. Walia [62], on the other hand, presents a 5G architecture for machine-to-machine communications, which is formed by different technical components in device, network and application domains. Both propositions are applicable descriptions of possible future architecture, but this subchapter will discuss more specifically about the NGMN's vision of the 5G architecture [59], as it provides an explicit view of the infrastructure and business applications. The architecture is illustrated in Figure 16. It consists of Infrastructure resources, Business enablement and Business application layer, and End-to-End (E2E) management and orchestration entity, which together provide communications and business services to different type of devices equipped with 5G Radio Access Technology (RAT).

The infrastructure in the architecture is comprised of physical resources, such access nodes, cloud nodes (may act as processing or storage units), networking nodes and associated links. 5G devices, such as mobile phones, wearables and machine type modules, may also be included as a configurable infrastructure resource if they possess capabilities to act, for example, as a relay/hub or computing/storage node. The resources are available to the higher layers and E2E management and orchestration entity through Application Programming Interfaces (APIs).

The business enablement layer contains modular architecture building blocks, including software-realized function modules that can be retrieved from the repository to the needed location, as well as a set of parameters that are used to configure certain parts of the network (e.g., radio access). The functions and capabilities can be requested by the orchestration entity through relevant APIs. Certain functions can have multiple performance variants and different characteristics, as they are used to determine network functionalities among divergent services (e.g., a mobility function defining parameters for nomadic, vehicular or aviation mobility).

The business application layer includes specific services and applications of different actors, which utilize the 5G network. The applications can build dedicated network slices by requesting resources from the orchestration entity. Network slicing is addressed more closely in the next chapter.

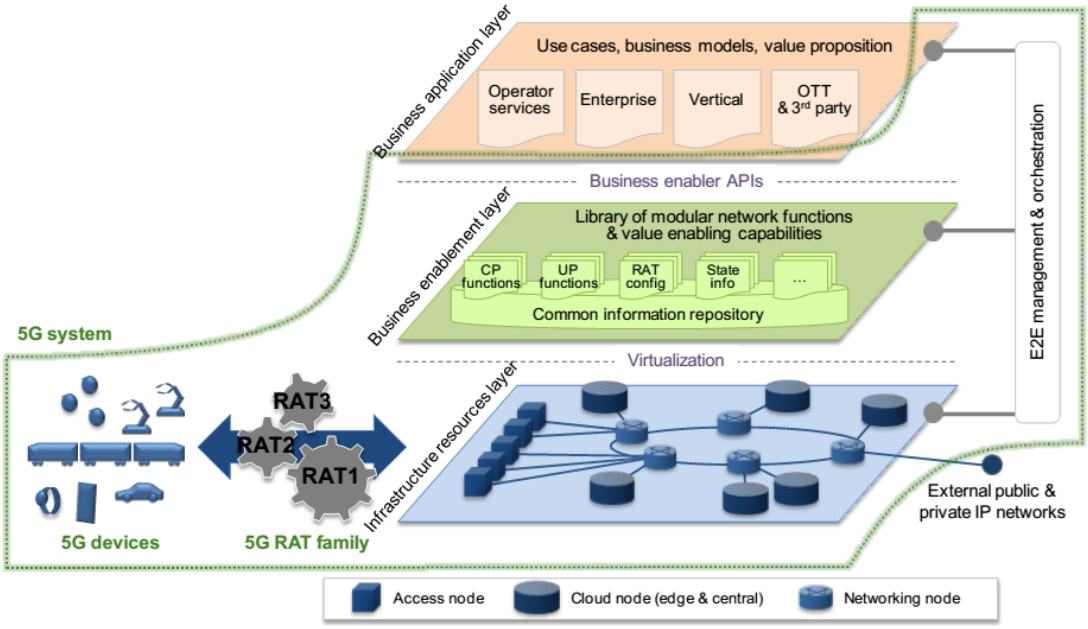


Figure 16: 5G Architecture [59].

The E2E management and orchestration entity performs the translation of use case requirements and business models into actual network functions and slices. The translation involves the definition of network slices for a given application scenario, linkage of relevant modular network functions, determination of relevant performance configuration, and reservation of infrastructure resources.

### 2.4.3 Enabling technologies

The commercialization of 5G will require a new type of technological solutions due to challenging requirements of novel applications. The technological enablers, which can address these requirements, are fog/edge computing, network virtualization, network slicing, and advancements in the utilization of extended radio spectrum.

#### Fog/edge computing

During the last decade, cloud computing has established itself as a computing paradigm that provides on-demand computing and storage resources for users who cannot afford to have their own computing servers, as well as, for organizations that want to reduce Capital Expenses (CapEx) [63]. The economic benefits are realized through flexible access to computing resources, meaning that users pay only for the resources their applications or services need. Moreover, with cloud computing organizations do not have to bear the risks of overprovisioning (underutilization of data centers) or underprovisioning (not enough computing capacity for service requests) anymore. [64] While cloud computing can offer a feasible solution in many cases, like big data analytics, it does not, however, perform very well in scenarios

where devices or machines need to make real-time decisions based on data analytics [65]. Therefore, a new paradigm called fog computing or edge computing is introduced in literature to answer the strict latency and reliability requirements in these type of use cases [66].

Fog, as its name refers to, is closer to the ground, thus closer to the end devices that produce and act on data. The purpose of the fog is to extend either local or public cloud, or both, to be closer to the end devices while providing similar kind of services as cloud computing, yet on a smaller scale (see table 3) [66], [67]. Any device with computing and storage resources, and network connectivity can operate as a fog node. Possible devices can be, for example, industrial controllers, switches, routers and embedded servers. [66]

Table 3: Differences between fog and cloud computing [66], [68].

| | Cloud | Fog |
|---|---|---|
| **Response time** | Minutes, days, weeks | Milliseconds to subsecond |
| **Access** | Fixed and wireless | Mainly wireless |
| **Control** | Centralized/hierarchical (full control) | Distributed/hierarchical (partial control) |
| **Service access** | Through core | At the edge |
| **Availability** | 99.99% | Highly volatile and highly redundant |
| **Application examples** | Big data analytics | M2M (Machine-to-Machine) communication, including automation, robotics and telemedicine |
| **Duration of data storage** | Months or years | Transient |
| **Geographic storage** | Global | Very local (e.g, production process) |

The utilization of fog computing can benefit companies in many different manners. Firstly, it accelerates awareness and response to events by not transferring all data to the cloud for analysis. Secondly, the operating expenses will decrease, as most of the data is processed locally, thus reducing the use of Internet bandwidth. Finally, it provides better security, and deeper and faster insights, since data is analyzed closer to the end devices. [66]

The emergence of 5G has also introduced another computing paradigm in addition to the fog. This paradigm is known as Mobile Edge Computing (MEC). MEC provides cloud-computing capabilities within the Radio Access Network (RAN), hence enabling better responsiveness for content, services and applications. Placing computing capabilities at the edge of the mobile network improves the Quality of Experience (QoE) of mobile users and infrastructure efficiency due to the reduction

of latency and optimization gains, respectively. Moreover, having intelligence closer to the end devices, new type services for scenarios, such as indoor M2M, can be created. [69] The comparison of the paradigms presented in this chapter can been seen in Figure 17. The fog aggregator seen in the figure can also be an access point equipped with MEC capability, depending on how the mobile services are provided to the end devices.

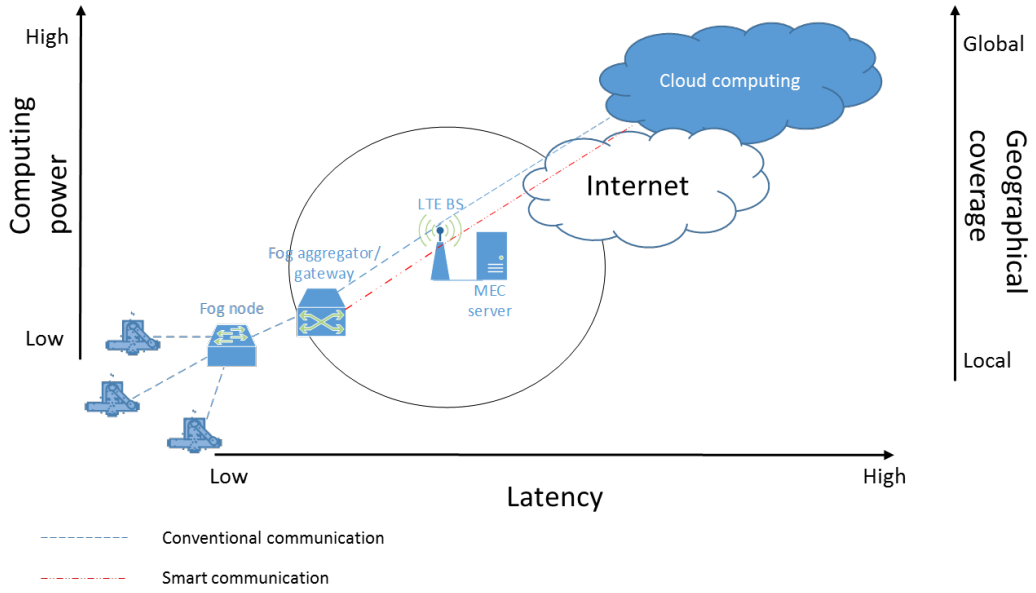


Figure 17: Fog comparison with other computing paradigms.

Currently, the technical implementation of novel computing paradigms is under investigation. One possible architecture for the functionalities of a fog device is presented in Figure 18. It describes the basic tasks, which can be performed by a fog node on several functional layers. The layers are:

- *Physical and Virtualization Layer:* In this layer, both physical and virtual sensors, and wireless and virtual sensor networks are managed and maintained based on their types and service needs [70].
- *Monitoring Layer:* This layer monitors the performance of underlying devices and networks, and collects the heterogeneous data sent by different devices and machines regardless of the protocol they are using [66], [71].
- *Preprocessing Layer:* The collected data is analyzed, filtered and trimmed in this layer. It is also responsible for finding the problems that can, for example, affect the functionality of the monitored devices. The data that does not need immediate action and is meaningful by some preimposed criteria is passed to the next layer for further analysis.
- *Temporary Storage Layer:* The role of this layer is to act as a sort of data buffer for upper and lower layer services. The data is maintained in storage media as

long as it is needed by some of the layers, or when the data is uploaded to the cloud and is not needed locally anymore [70].

- *Security Layer:* In many cases, the data produced by the devices might be sensitive or private, and therefore it should be protected using proper measures. Security layer is responsible for ensuring that the data passed to the transport layer is secured with proper encryption algorithms. [71]
- *Transport Layer:* After the data is secured and is ready to be sent to the cloud, the transport layer takes control of the connection through which the data is transferred [71].

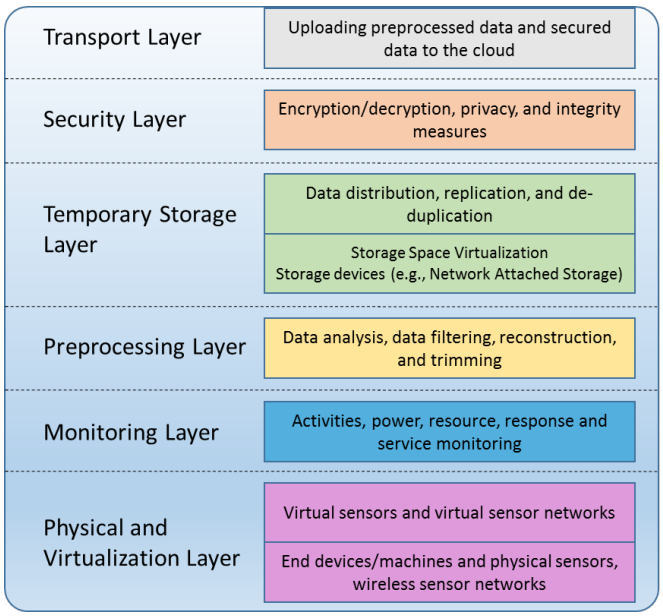


Figure 18: Layered architecture of fog (modified from [71]).

### Network virtualization

Network virtualization has been one the fundamental enabler to realize the requirements of 5G, since it allows greater flexibility, in terms of reconfigurability, reusability and infrastructure sharing, as well as provisioning of services, such as MEC, network slicing and autonomic network management [61]. In literature, the concept of network virtualization is often associated with Software-Defined Networking (SDN) and Network Functions Virtualization (NFV)

In non-virtualized networks, the functions controlling the network resources, i.e., Network Functions (NFs), are implemented as a combination of vendor-specific software and hardware (also referred as network elements or network nodes). In NFV, these elements no longer consist of integrated software and hardware, but they are comprised of separated software and hardware entities. The separation allows

both entities to perform different functions at various times, hence allowing flexible NF deployment and dynamic network operation. Figure 19 illustrates a high-level framework for the implementation of Virtual Network Functions (VNFs). The VNFs are purely software instances that run over NFV Infrastructure (NFVI) and are managed by the NFV Management and Orchestration entity. [72] The function of the orchestration entity is to control the composition of VNF chains, which are the basis for the virtualization of service delivery [73].

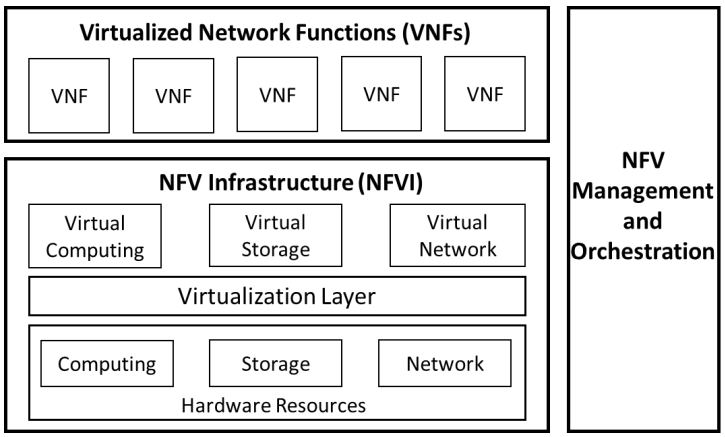


Figure 19: High-level NFV framework [72].

Software-Defined Networking, like NFV, introduces a network virtualization concept which enables dynamic utilization of network resources through the exploitation of server scale out and cloud technologies [57]. The approach of SDN is, however, a slightly different compared to NFV. The functionality of SDN is based on the separation of network control and forwarding, whereas in NFV, the virtualization is realized by decoupling the software and hardware entities in physical devices. By migrating control (typically bounded in individual network devices) into the programmable entity, the underlying infrastructure can be abstracted and provided as virtual network resources for applications and network services. The migration of control also allows the network intelligence from individuals devices to be centralized in software-based SDN controllers, which sustain a global view of the network. Consequently, the network can be controlled from a single logical point, since it appears as a single logical switch from outside. [74]

NFV and SDN are complementary technologies that both can independently enable network virtualization. However, when applied in combination, they can provide greater value in service delivery, especially in future 5G networks. [73] Figure 20 represents a framework for the potential utilization of SDN and NFV in 5G networks (i.e., softwarization), including the radio access, transport and core network segments, as well as the Internet segment [61].

In 5G RAN, the software network technologies enable virtualization of radio functions and physical NFs which allows virtual instances, i.e., VNFs, to be flexibly shifted to locations (e.g., radio edge or mobile edge cloud) where they are required.

Consequently, functions, such as data plane and control can be executed from the edge cloud or central cloud, leveraging the centralization of computation maximally.

The softwarized transport network acts as a platform for applications and network services and adapts the operation according to the needs of RAN through NFV and SDN framework. The transport network and RAN can also jointly coordinate aspects, such as mobility and load balancing. The VNFs of the transport network allow dynamic allocation and on-demand provisioning of underlying network resources.

In the core network, the majority of infrastructure and service plain functions are expected to be implemented as VNFs, meaning that they will be running on virtual machines over standard servers, and potentially centralized to cloud computing infrastructures. The VNFs can flexibly be deployed to different network sites, depending on the requirements with respect to latency, processing and storage capacity, and available bandwidth. The core network VNFs together with the VNFs from other segments can be used to form different service chains or network slices. The composition of the service chains or slices is directed by the orchestration and management entity, which is also responsible for integrating and coordinating physical or virtual resources needed to fulfill the requirements of services or slices with particular attributes.

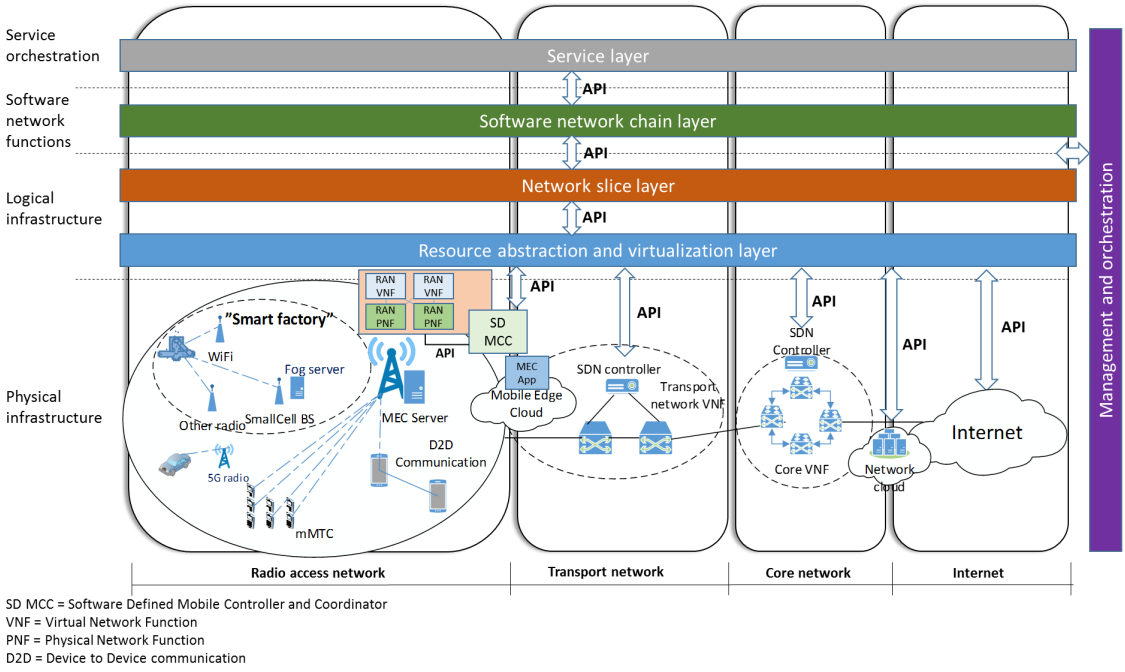


Figure 20: Software network technologies in 5G overall architecture (modified from [61]).

## Network slicing

The utilization of network software technologies and provisioning of network resources to support communication service of a specific connection type, i.e., network slicing,

is a novel concept to address the requirements of use cases, such as autonomous driving, mMTC and industrial automation. The object of network slicing is to provide "slices" for different type services by allocating necessary network resources and configuring relevant network functions, depending on the requirements of a use case. For example, for a network slice supporting mMTC devices, some of the basic control plane functions, such as mobility, could be omitted, since machines (e.g., in factories) are quite static and do not require such a service. Consequently, these functions would not be necessary at the edge due to low mobility, and therefore could be run in a central cloud. On the other hand, high mobility and low latency services, such as autonomous driving, would need all the necessary functions, which are responsible for ensuring high security and reliability, and low latency, to be run at the edge. [59] Dividing the network into slices with differing attributes enables a flexible and cost-efficient operation of underlying infrastructure which can create new business opportunities for various actors. For example, Mobile Network Operators (MNOs) could offer customized E2E cellular networks as a service for Mobile Virtual Network Operators (MVNOs), which could focus on serving specific markets, such as industrial automation or governmental bodies. [75]

**Efficient utilization of extended radio spectrum**

In the coming years, mobile traffic will continue to grow almost at exponential rate, reaching annual traffic of 600 Exabytes (approx. $6.3 * 10^{11}$ Gigabytes) by the end of 2021. The growth will be driven by the increasing usage of mobile video, virtual and augmented reality, and M2M devices. [76] In order that the mobile infrastructure would be able to serve every connected device with certain level QoS, more capacity will be needed. Densification of cellular networks (reduction of cell sizes) is one approach to increase network capacity, and another one is the extension of licensed spectrum below 6 GHz. However, these approaches are not cost-efficient ways to address the issue due to rising costs of installation and maintenance of cells, and the high price of the spectrum (Telefónica UK Ltd paid 500 million pounds for two channels of 10 MHz bandwidth on 800 Mhz frequency band in 2013 [77]). Hence, novel technologies and concepts are required to answer the rapid growth of mobile traffic and the emergence of 5G applications. The technological solutions expected to answer the challenges and enable more efficient utilization of radio spectrum are:

- *Millimeter wave:* Frequencies from several hundred Hz to a few GHz are almost fully occupied by terrestrial wireless systems. As a consequence, new techniques to exploit the millimeter wave range of 30–300 GHz are being studied by academia and consortia. Although this frequency range can raise bandwidth in mobile systems, the utilization of higher frequencies is a challenging task. This stems from the propagation qualities of millimeter wave spectrum, which are strong path loss, low diffraction around obstacles, atmospheric and rain absorption, and low penetration through objects. Regardless of the issues, the utilization of millimeter wave with relevant technology is still a feasible option – especially in short range line-of-sight deployments – to extend the available spectrum. [78]

- *Massive Multiple-Input Multiple-Output (MIMO):* After having introduced into WiFi systems around 2006 and into 3G cellular systems later on, MIMO has established itself as notable technology to provide increased capacity and spectral efficiency in cellular networks [78]. The functionality of MIMO is based on the use of multiple antennas at the transmitter and receiver, which enables signals to carry data through multiple paths, thus achieving space diversity gains [79]. LTE systems applying MIMO can include up to eight antennas per base station, but in 5G the amount may increase up to hundreds which has lead to the invention of the term "massive MIMO" [78].

- *Narrowband IoT (NB-IoT):* Although already being specified in 3GPP Release 13 regarding the narrowband of LTE for IoT, NB-IoT continues to be reckoned as s focal technology to address the requirements of massive MTC and IoT use cases in 5G. NB-IoT can be deployed to existing licensed frequency bands either as a guard-band or in-band implementation in LTE bands, or as a separate standalone carrier in GSM (Global System for Mobile Communications) band. It occupies 180 kHz bandwidth, which is the same as one resource block in LTE transmission. In GSM band, the bandwidth of one resource block is 200 kHz, thus it can also be deployed in GSM frequencies due to a guard interval of 10 kHz on both sides of the spectrum. The utilization of low bandwidth means that peak data rates of both downlink and uplink are extremely low (170kbps and 250kbps) which is ideal for sensors and other battery-powered devices that require very low transmission speeds and have long data sending interval.

- *Licensed Shared Access (LSA):* The LSA concept is a framework that allows existing spectrum user(s), e.g., MNO, to share spectrum with a single or multiple licensed LSA users (i.e., "LSA licensee(s)) in agreement of predefined conditions. The conditions can be either static (e.g., a certain time interval for operation) or dynamic (e.g., on-demand authorization by LSA licensees or geographic/time sharing). [80] Due to recent advances in network virtualization technologies, dynamic implementation of LSA, which allows spectrum sharing on the grounds of frequency, location and time, could be realized in next generation mobile networks. This would enable more efficient utilization of already scarce spectrum and provide new sources of income for existing spectrum user(s).

### 2.4.4 Manufacturing industry in 5G era

5G technologies are expected to create major opportunities for manufacturing industry by providing an intelligent infrastructure to support next-generation digital platforms (also called CPS). These platforms in combination with 5G will be the basis for intelligently connected production information systems, which enable operation beyond physical boundaries of factory premises, transforming factories from isolated entities to interconnected and service-oriented systems. This will lead to global and highly automated connected value chains where data is exchanged across a diverse

set of stakeholders, which capitalize on increased flexibility and efficiency in supply chain management and cooperate to create innovative products and services. [81]

In the vertical domain, which is comprised of connected production and management processes inside factory premises, 5G will play a key role as a unifying platform, which supports seamless communication among heterogeneous devices located both inside and outside factory premises. By utilizing softwarization technologies, the platform will enable a programmable and unified infrastructure through the integration of networking, computing and storage resources. The infrastructure will support the integration of novel applications, such as additive manufacturing and augmented reality, and interconnect machines, robots, processes and goods, hence establishing a highly automated operation, involving intelligent cooperation between machines and workers. [81]

5G technology platform will also provide the means to seamlessly integrate products and related services throughout their life cycle, including innovation, commercialization, delivery, maintenance and disposal. This will increasingly disrupt the way machine providers do business in 5G era, transforming them from product-centric to product-service centric organizations. [81] Consequently, customer relationship will change from a single transaction to a long-term partnership, in which both parties will accumulate significant value; exploitation of usage data creates opportunities to improve the design of products and increases availability through timely maintenance.

# 3 Case Studies

## 3.1 Factory cases

In order to the understand the current state of factories regarding the management systems, control networks and remote maintenance, factory employees from three different factories were interviewed. The interview with Factory A personnel was conducted on the spot and the other two interviews by phone. Following chapters present the results of the interviews.

### 3.1.1 Factory A

Factory A manufactures metal parts and assembles motors. Its production line consists of over ten cells that are connected to the local network but do not communicate with each other (see Figure 21). Therefore, the parts that are finished in one cell must be moved manually to another cell. Each cell is comprised of a single or several machines, such as robots and machine tools (can be from different machine providers). They are connected through wired technologies, such as fieldbus or fieldbus-based Ethernet. Although the cells are connected to the network, they are not monitored or controlled from a centralized management system, because the implementation of such a system would be too expensive, and there is no guarantee that the machines from different vendors could be monitored with it. This results from the proprietary software and communication technologies, which are applied to some of the machines.

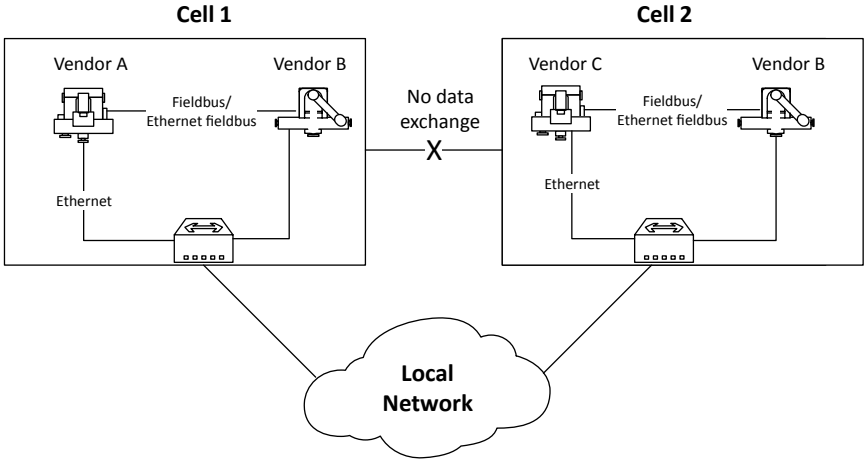


Figure 21: An example of cell communication in Factory A.

The average life-cycle of the factory machinery is 10–15 years, but some of the older machines have been in use for more than 30 years. The problem with long life-cycles is that the software which controls the machine can be, in some cases, too outdated, and it would be a major risk, for example, to allow the machine to be remotely monitored by the machine provider. Old machines and outdated software are factors why Factory A has not ongoing remote maintenance contract with any

machine provider. However, one of their machine can be remotely diagnosed when it detects a problem in its operation. In such a case, the machine sends a connection request to the remote service provider. Thereafter, the factory manager decides together with the maintenance team whether a remote diagnosis is necessary, and if it is, a temporary access right through the firewall for the service provider is created in order to allow the machine to be connected and repaired remotely.

The size of the maintenance team in Factory A is quite large because the machines require continuous maintenance due to the challenging manufacturing process; several malfunctions may occur per day. In addition to repairing the malfunctions, the task of the team is to ensure that the machines are working properly by inspecting them visually and lubricating the parts on a daily basis. Every month, the team also conducts a comprehensive maintenance operation in which the inner machinery of the machines is checked, and the worn-out parts are replaced based on the visual checking. Moreover, those parts that have a predefined useful life are also changed even if no sign of abrasion is detected.

Since in Factory A the machines are not monitored through a centralized system and sensor data is not exploited for preventive maintenance purposes, the machines may sometimes break unexpectedly. This often leads to the production being halted for many hours until the reason for the breakage is found and repaired, respectively. In worst case, the spare part needs to be ordered from another country which even prolongs the downtime of the production.

Currently, Factory A employs wireless technologies only in the office spaces, even though the signal strength of both WiFi and LTE is high throughout the factory. WiFi has not been used due to its unreliability and the lack of WiFi modules in the machines. On the other hand, LTE has been seen as an infeasible solution for remote monitoring implementation due to the factory's rigid security policy regarding the data and communications.

### 3.1.2 Factory B

Factory B operates in the electronics industry and manufactures telecommunications equipment. It has an almost fully automated assembly-based production line which consists of numerous robots and composing machines. Each robot and machine is preprogrammed to perform a certain task on the manufactured product. They are connected with industrial Ethernet cables and apply Ethernet/IP protocol to exchange data between each other. The production line consists of cells, as in Factory A's case (see Figure 21), but they are considerably lower in number. Each cell is connected to the local network and managed through MES. Although MES is functioning properly and it enables the supervision of the operations, the factory would still like to be able to integrate more information from different systems and machines to it, and with each other in order to improve the performance of the whole production. The problem is that most of their automation systems, which are designed for certain vendor-specific machines, are proprietary solutions. As a consequence, the compatibility issues are not only experienced with MES but also with the other automation systems as well.

The average life-cycle of the factory equipment is under five years, even though some of the composing machines are over ten years. The factory has a small service unit which is responsible for ensuring that the machines are working properly by conducting basic preventive maintenance tasks, such as visual inspection of the machinery condition and lubrication of the machinery parts. For more comprehensive maintenance operations, the factory applies the hybrid model, meaning that the service unit workers are responsible for the monthly operation whereas the machine providers for the annual, respectively. All maintenance operations must be performed on the spot, since the factory do not have an ongoing contract for remote maintenance. If a machine must be accessed remotely for troubleshooting, then there is possibility to establish a VPN (Virtual Private Network) connection to it through the firewall.

Factory B's network solutions are mainly based on wired technologies, but in some functions, like logistics, WiFi is used. Since the factory manufactures telecommunications equipment and is specialized in wireless technologies it is eager to replace all wired solutions into wireless in the near future. The factory is also in good position to test the next generation wireless technologies because, firstly, the personnel have knowledge about them and secondly, the signal strength is high throughout the factory.

### 3.1.3 Factory C

Factory C produces electrical equipment for various industry fields, and it has a highly automated assembly-based production line, which consists of over 20 robots. The production line is divided into several cells which are connected to the local network and controlled from the centralized system. The controlling logic of the cells is built on top of the PLCs, thus if the network is down the whole production stops.

Factory C has different type of machines, but the most critical ones from the production viewpoint are robots. Normally, the robots have a life-cycle of 15 years, even though some of them are still operational after 20 years. The robots are mainly maintained by the factory's own maintenance team and in some cases by the software engineers. The maintenance function includes daily activities, such visual inspection and cleaning, as well as monthly and annual activities, such as full inspection of the inner machinery of the robots and interchange of threadbare parts. Currently, all maintenance tasks are conducted by the factory personnel, and there is no contract with any machine provider regarding the remote maintenance. The factory has, however, a functional VPN which can be used for remote maintenance if needed. Some of the employees already use it to check the status of the robots and repair the software errors remotely.

The factory rarely has machine malfunctions because machinery is maintained regularly. If for some reason a machine breaks unexpectedly, the maintenance team is called. Typically, it takes a couple of minutes to repair the faulty machine since the malfunction is usually related to a software error.

Network connections in Factory C, excluding the office space, are mainly based on wired fieldbus and Industrial Ethernet solutions. The signal strength of WiFi and LTE is high inside the factory, but only WiFi is applied to production-related functions,

of which one is PDA (Personal Digital Assistant) utilization in the supervision of factory operations.

### 3.1.4 Summary of factory cases

Previous chapters presented three factories from different industry fields and discussed the characteristics of each factory, which are summarized in Table 4. Many similarities were found regarding network technologies, maintenance functions and automation systems. However, the supervision of the machines and overall automation in Factories B and C were on a more advanced level than in Factory A. Still, the interviewees from each factory agree that more data should be collected and exploited so that the maintenance tasks could be conducted more efficiently and the performance of the production improved.

Table 4: Summary of the factory cases.

| | **Factory A** | **Factory B** | **Factory C** |
|---|---|---|---|
| **Industry** | Metal | Electronics | Electronics |
| **Type of production line** | Manufacturing and assembly | Assembly | Assembly |
| **Automation level** | Medium | High | High |
| **Control system** | Distributed | Centralized (MES) | Centralized (MES and OPC UA) |
| **Machinery life-cycle (avg.)** | 10–15 years | 5–10 years | 15–20 years |
| **Remotely maintained machines** | 1 (event-based) | None | None |
| **Maintenance interval** | Calendar and usage based | Calendar based and annual (by suppliers) | Calendar based and annual |
| **Machine malfunctions / day** | Several | - | Almost none |
| **Average repairing time** | Couple of hours | - | Minutes |
| **Maintenance team** | Large (6–8) | Small | Small (2–3) |
| **WiFi and LTE signal strength** | Good | Good | Good |

## 3.2 Remote connection cases

It is well known that factories do not allow any remote monitoring to be established to their machines because they consider it as a security risk and unnecessary service. Moreover, the deployment usually requires additional configuration to network and

firewall settings, and possibly new equipment and software. However, allowing machines to be remotely monitored can be beneficial for the factory owner and machine provider. Therefore, it is an interest for both parties to find a solution that provides additional value from the operational data, which is collected by the machines. Next chapters present three remote connection cases and discuss the characteristics of each case.

### 3.2.1 Through mobile network

Remote connection through mobile network offers many advantages for both parties because the implementation is straightforward, and it can be established to any machine inside the factory where signal strength is high enough. However, older machines and even most of the newer ones are not equipped with a 3G/4G module which inflicts some problems to the implementation. Usually, they can be solved by embedding a separate module to the machine, or by using a cellular router that can convert fieldbus traffic to standard Ethernet traffic.

This type of remote service scales very well because more machines can be monitored without having to consider about the limitations of physical equipment (limited number of interfaces) or length of network cables (e.g., maximum length of CAT5 Ethernet cable is 100m). The only restricting factor is the capacity of the cellular tower to which the machines are connected. Additionally, the configuration part from the factory owner's viewpoint is simple because the connection is established directly to the mobile network and not through the Intranet. Although this allows the customer to avoid the complexity of the local network, it also reduces the control on data and increases the security risk. However, these issues can be managed with proper measures; allowing only outbound connection from the machine, installing a firewall to the gateway device or machine's operating system, and defining terms regarding the data collection in the contract (e.g., how often and what data can be collected).

A factory, in general, is a very challenging environment for all types of communications. For example, establishing a reliable wireless connection inside the factory can be extremely difficult because many factors, such as metal, wall thickness and heat, affect the quality of the signal, which again is directly reflected to the reliability of the connection. However, it is possible to improve the connection by deploying, for example, a smaller base station inside the factory. Even though mobile-based remote service cannot offer the same reliability as wired solutions, it can still be a feasible alternative in many use cases, in which high latency or packet loss do not have a significant influence on the quality of the provided service.

### 3.2.2 Through firewall

As was stated before, factories are closed systems where communications and data are strictly managed. Therefore, establishing a remote connection to a machine through a factory Intranet requires always additional configuration to the firewall and network settings, because new policies have to be created and the connection needs to be separated from the other network, for example, by creating a VLAN (Virtual

Local Area Network) on top of the physical network. In addition to the VLAN separation, the connection is also logically separated from the public network with VPN. Since many of the older machines do not have VPN possibility, the machine vendor provides a preconfigured router, which enables the remote connection between the machine and service provider's cloud to be established. This type of solution can be burdensome from the configuration viewpoint because the more machines are monitored remotely the more logical connections have to be created which, in turn, increases the complexity of the local network and complicates the supervision of ongoing remote connections. Regardless of the aforementioned issues, firewall solution provides more control over data and better security compared to the mobile connection solution because the customer can control inbound and outbound traffic with firewall policies. Although a firewall provides the means to inspect packets, and block or allow connections based on some predefined criteria, it cannot, however, control the data which is sent over an encrypted connection such as VPN.

Most remote services, in which the connection must go through the factory's own firewall, usually rely on wired solutions. On the one hand, wired implementations provide better reliability compared to the wireless ones, but on the other hand, they increase the amount of cabling and network complexity (the machine might be located behind several routers). However, it is important to remember that local connection choices can guarantee a certain level of reliability only for the factory part of the remote connection. They cannot affect, for example, through what kind of links the connection is established over the Internet. Therefore, the functionality of the remote service depends widely on the reliability of the Internet connection.

### 3.2.3 Isolated

In the isolated case, factory machines are connected to the local management system or cloud platform and supervised centrally through an HMI. As no remote connections to the machines are allowed from outside the factory, the machine vendor provides a special software or an industrial PC whose function is to collect and analyze data and offer performance information locally. This type of solution not only eases the configuration part of the implementation from the customer's viewpoint (no need to add new firewall policies) but also allows more machines to be monitored without having to establish separate connections outside the local network. In some situations, however, the machine provider may have to connect to a malfunctioning machine remotely if the problem cannot be solved locally either by the factory's own maintenance team or by the software provided by the vendor.

Since the machines are first connected to the local system, the customer decides what data can be collected by the machine provider's software. Moreover, the customer determines whether the software is allowed to send or receive data over the Internet, for example, for database synchronizing purposes.

One of the major advantages of local remote service is the high level of security and reliability which results from the policy of not allowing any remote connections through the firewall and relying only on local communications, respectively. However, factors, such as network congestion, capacity and topology, as well as communication

technologies, can affect the reliability of the service even if it is based entirely on a local solution.

### 3.2.4 Summary of remote connection cases

Providing a feasible and functioning remote maintenance service requires an evaluation of many factors. For example, what communication technologies should be used and how the data should be collected. Previous chapters presented three remote connection cases and described the characteristics of each case. Table 5 summarizes the differences between them. Each alternative has its strengths and weaknesses, and possible applications. Therefore, one should not conclude that, for example, the isolated case superior to the other cases.

Table 5: Comparison table of the remote connection cases.

| | **Mobile** | **Firewall** | **Isolated** |
|---|---|---|---|
| **Scalability** | HIGH | LOW | MED |
| **Configuration** | LOW | HIGH | MED |
| **Data control** | LOW | MED | HIGH |
| **Reliability** | LOW | MED | HIGH |
| **Security** | LOW | MED | HIGH |

# 4 Value Network Analysis

The chapter analyzes remote maintenance connectivity through several value network configurations and introduces a future technical architecture based on the results of the analysis, and the insights gained from the interviews and literature.

## 4.1 Theoretical framework

Business of any form is driven by transactions, in which value is exchanged in form of tangible assets, such as money, goods or services, or intangible assets, such knowledge, trust or reputation [82]. In other words, value is created and traded for another type of value. Value creation process involves numerous activities (i.e., inputs) that are performed to produce some output (e.g., physical product). When these activities are linked together they form a value chain. Porter's value chain framework [83] is a widely accepted tool to represent and analyze value creation logic of a firm, that is, which are the strategically important activities and what are their impact on cost and value. However, companies rarely operate on their own which is why the framework is not applicable for analyzing a value chain consisting of several actors, which cooperate to produce some output. Value chain as a concept is also gradually becoming outdated since in many today's industries, such telecommunications and banking, products and services do not have a physical dimension (value chain concept defines activities that exist in the physical world) [84]. Moreover, in these industries, value is not typically created linearly, but realized through a network-like interaction between different actors, thus defining a value network concept [85].

This thesis applies the value network analysis method defined by Casey et al. [86], according to which a value network is comprised of interlinked *technical components* and business *actors* that in conjunction create economic value. The interaction of the components and actors are presented in the form of Value Network Configuration (VNC), which consists of several interlinked blocks. The VNC notation is illustrated in Figure 22.

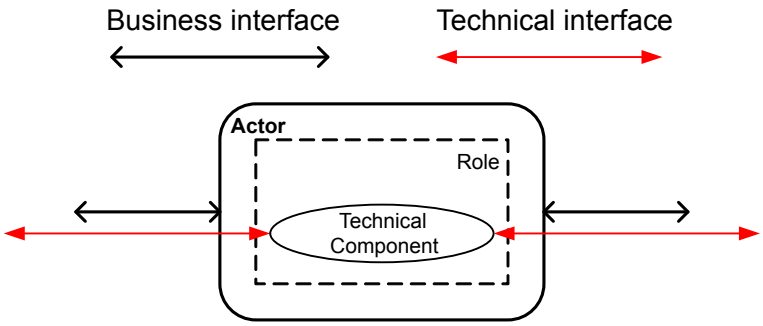


Figure 22: VNC notation adapted from Casey et al. [86].

## 4.2 Technical architecture and business roles

Technology is the key factor when defining the value creation logic of an ecosystem, and the possible functional roles actors can take in that. In a value network configuration, technology is defined as a technical component, which is a compilation and realization of technical functionalities, involving the interfaces to other components. Technical architecture, on the other hand, consists of technical components which are interconnected by technical interfaces. Typically, technical architecture remains almost unchangeable when defining different VNCs, but in remote connection cases the architecture varies significantly, and therefore the illustration of the generic architecture is omitted from this chapter, and only the descriptions of the components are presented. The descriptions of both the "business" roles and technical components can be seen from Table 6 and Table 7, respectively.

Table 6: Business role descriptions used in the VNCs.

| **Business Role** | **Description** |
|---|---|
| Machinery Supervision | Monitoring and control of a machine through an HMI. |
| Service Provisioning | Management of cloud resources, including billing, if public cloud is in question. |
| Machinery Operation | Collection and analysis of sensor data, and automatization of machinery functions. |
| Traffic Management | Management of bandwidth, and firewall policies. |
| Connectivity Provisioning | Providing the functions and interfaces for collecting data from a machine remotely or locally. |
| Remote Supervision | Involves the supervision of performance and condition of customer's assets, customer informing activities (e.g., email, phone call or SMS), and management of remote maintenance operations. |
| Network Operation | Management and monitoring of network resources, and provisioning of mobile and broadband services. |

Table 7: Descriptions of the technical components.

| **Technical component** | **Description** |
|---|---|
| Human-Machine Interface (HMI) | A software that translates data from an automation system into a human-readable form and allows an operator to monitor and control the status of a process. |
| Cloud Platform | An infrastructure that provides on-demand delivery of compute power, database storage, applications, and other IT resources via the Internet with pay-as-you-go pricing (Public Cloud), locally (Private Cloud), or using both (Hybrid Cloud). |
| Firewall | Monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on predefined security rules. A firewall can be hardware, software, or both. |
| Automation System | Controls the movements of robots and machine tools, and collects and analyses sensor data (e.g., ABB IRC5 [87] and Siemens 840d [88]). Additionally, it can be connected to the network through wired or wireless interface. |
| Gateway | A networking device that connects two or more devices through an unsecure network, such as Internet. Moreover, it can be a converter, which connects devices that use divergent protocols. It is configured to pass, block or route traffic from predefined IP address(es). |
| Wide Area Network (WAN) | Connects two or more geographically distributed local area networks over wired and/or wireless links. |

## 4.3 Value network configurations

### 4.3.1 Through mobile network

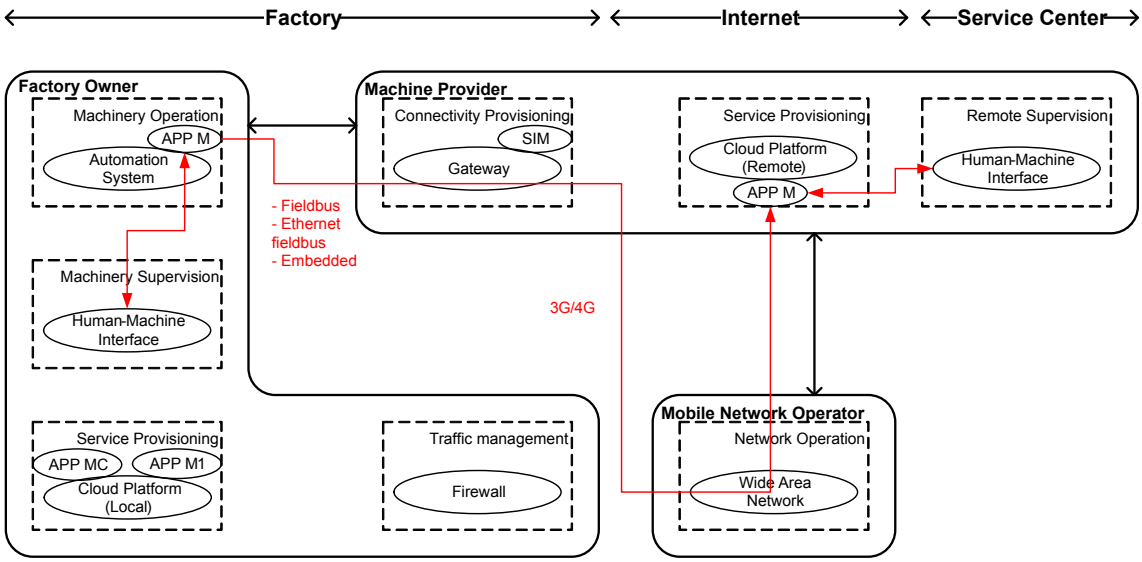


Figure 23: VNC - "Through mobile network"

The VNC shown in Figure 23 presents the high-level architecture for mobile-based remote connection. It is formed by the factory owner, mobile network operator and machine provider. The connection between the automation system and machine provider's cloud is established through the WAN by using a gateway, which enables data from the automation system to be sent wirelessly. The gateway, in this VNC, is owned by the machine provider, which is responsible for establishing the remote connection and monitoring the machine. It can be either 3G or 4G module embedded in the machine or a separate device. The machine provider also purchases the necessary SIM (Subscriber Identity Module) card from the MNO and decides what connection type should be used for remote monitoring service. Hence, the machine provider controls how much and how often the data is sent over the Internet. MNO, on the other hand, offers the machine provider M2M service, which enables the management of transmission speeds, packet sizes and other network related features. However, the gateway or module prevents the MNO from knowing what type of machine is connected to its network, thus it cannot, for example, estimate the number of specific machine types which, on the other hand, decreases the opportunity to offer more innovative services.

For the factory owner, mobile-based remote connection offers a possibility to supervise those machines that cannot be connected to the local monitoring system due to the proprietary interfaces or protocols, or have a basic embedded HMI that does not provide enough information about the machine performance. Additionally, it provides the means to bypass the local network, which is usually one of the major factors preventing the use of remote services. The supervision is normally conducted

by the machine provider's employees working in the service center, but it is also possible that the factory owner receives the information about the performance of the machines through a web application or by email, if the machine providers includes them in the offered service. However, the data volumes collected by the machine provider might be too low so that it could offer, for example, real-time information about the machines, because the cost of M2M data rates are currently quite high.

Every actor in this value network receives benefits whether they are tangible or intangible. The actors accumulate value as follows:

- *Factory Owner*
  - Information about the machines (the quality depends on the amount of data collected by the machine provider)
  - Less downtime due to faster delivery of spare parts and quicker response of the machine provider's maintenance team
- *Mobile Network Operator*
  - New revenue opportunities with M2M service
- *Machine Provider*
  - Steady income
  - More efficient use of resources (e.g., better geographical positioning of spare part warehouses and maintenance personnel) due to the location information of the monitored machines

### 4.3.2 Through firewall

Figure 24 describes the VNC in which the remote connection is established through the factory's firewall. The machine provider still delivers the gateway, which is preconfigured to establish a VPN connection between the machine and machine provider's cloud. The gateway, in this case, can be, for example, a VPN router or an industrial PC. Since the connection must bypass the firewall, the factory owner manages the inbound and outbound traffic which allows more control on the connection. The control is, however, limited to the traffic management, thus the factory owner cannot regulate the data that is collected by the machine provider via the remote connection.

In this VNC, the actors remain the same apart from the WAN operator, which in this case is ISP since the remote service is based on wired connection. It is also often the case that the same actor provides both mobile and broadband service. Since the remote connection is established via the factory's current Internet connection, the factory owner has a contract with the ISP in addition to the contract with the machine provider. The factory owner pays either for normal broadband service if the VPN is realized on the application layer, or for dedicated VPN service if more secure and reliable remote connection is needed. The dedicated VPN is usually realized on

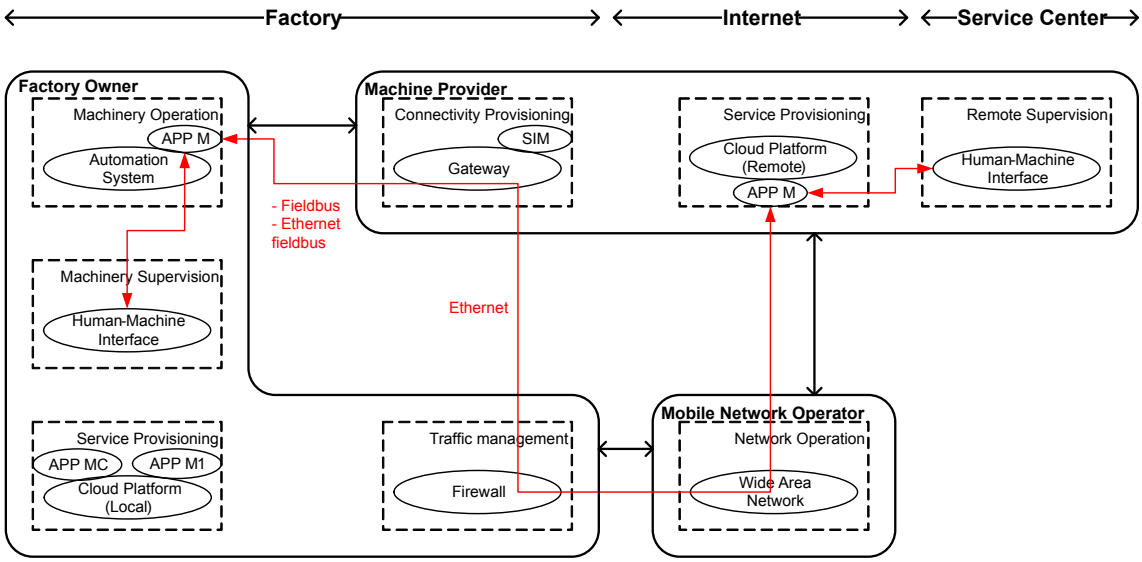


Figure 24: VNC - "Through firewall"

the layer 2 or layer 3 of the OSI model, thus it is considerably more expensive than normal VPN service. Typically, dedicated VPN is used for highly valuable assets such as paper machines that require real-time monitoring.

In the VNC, seen in Figure 24, the actors have opportunity gain following benefits:

- *Factory Owner*
  - Possibility to fully or partly outsource the maintenance function
  - Downtime decreased significantly due to the faster response to malfunctions
- *Mobile Network Operator*
  - Possibility to gain more revenue by offering advanced broadband services
- *Machine Provider*
  - Steady income
  - Higher data volumes allow to gain more information about the machines, thus allowing to notice malfunctions earlier and conduct more efficient maintenance in terms of spare parts delivery and response time reduction of the maintenance personnel

### 4.3.3 Isolated

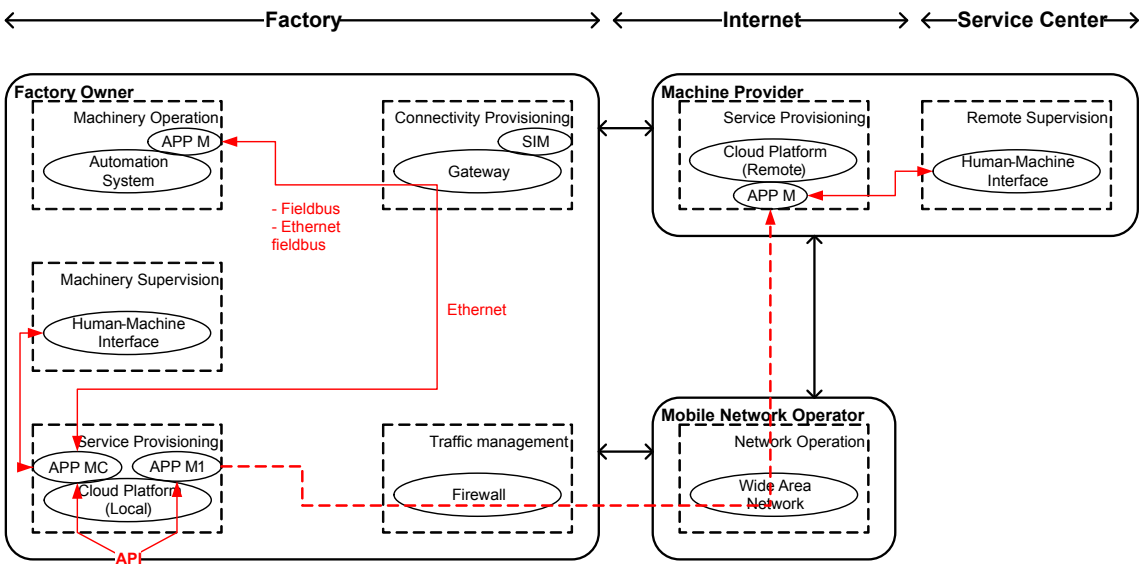


Figure 25: VNC - "Isolated"

The VNC seen in figure 25 presents the isolated solution in which the factory owner does not want any of its machines to be remotely monitored. Consequently, the machine provider offers an application (e.g., ABB Virtual Support Engineer [89]) that collects machine data locally and provides information about the machine performance and condition. Moreover, it assists the factory personnel in a case of a malfunction. If the application cannot solve the problem, it sends a connection request to the machine provider. The factory owner can then decide whether the machine provider's employee working in the service center can access the machine and solve the issue. Since the factory owner controls the gateway, he or she can also decide what data can be collected by the application. Additionally, by owning the gateway, the factory owner is not completely dependent on the remote service because shall the contract be terminated, the machine could still be monitored locally with the factory's own management system.

The remote connection in this VNC is used rarely, and therefore the machine provider and factory owner have a contract with the ISP solely for the basic broadband service. The value in the VNC is divided in the following manner:

- *Factory Owner*
  - Local "remote maintenance" solution
  - Reduction of downtime due to better utilization of machine data
- *Mobile Network Operator*
  - Basic broadband service

- *Machine Provider*
  - Monthly payment for the use of the application and possibly additional income from the remote operations

## 4.4 Future technical architecture

5G will enable a technological platform for a great variety of industrial applications, including remote maintenance. The utilization of 5G connectivity for remote maintenance in factories will require an architecture that exploits both wireless and wired transmission media in data communications. Figure 26 illustrates a possible architecture that could provide a feasible solution for 5G utilization in remote maintenance operations. The architecture consists of four different levels, of which the three bottommost (i.e., field level, cloud platform and management level) define the factory communications and functions. The field level involves the machines used in the production, as well as other functions, such as logistics. All field level functions are connected to the field-level backbone network, through which they communicate with the cloud servers and production management system. Logistics function may, however, be either physically or logically separated, since the requirements for communications deviate from production functions (e.g., automation) and logistics data is not typically utilized by the machines directly. The cloud platform acts as an integrative layer that collects and analyses machine and logistics data and provides computing resources for relevant applications and systems. The level above, i.e., management level includes production and enterprise management systems (e.g., MES and ERP), and a remote maintenance system, which provides access for remote service providers to the relevant virtual twins of the machines (exact digital copies of their physical counterparts, including all relevant data). The remote maintenance system is separated (e.g., Extranet) from the management-level network, to decrease the security risk of the service. It also acts as a single point of access for machine providers' cloud applications, thus enabling more efficient management of remote connections.

The problem in most today's factories is the rigid and complex hierarchical network structure, which hinders the economical and straightforward deployment of remote maintenance, especially for moderate and low-value assets. Mobile technologies such as 3G and 4G enable a wireless alternative for remote maintenance connectivity, but they are often unfeasible due to the hostile environment of factories and high cost. 5G is expected to transform the current static hierarchical network structure toward more dynamic need-based infrastructure, which would be able to provide communication resources, depending on the needs of an application. Hence, the future infrastructure would be able to serve industrial applications, which require low data rate communications (e.g., remote monitoring) or low latency (e.g., automation). Therefore, the architecture presented in the figure above introduces 5G as the main technology to enable flexible, reliable and economical mobile connectivity in industrial environments, such as factories. Connectivity can be provided either through a macro- or microcell base station (located outside the factory) or through a picocell base

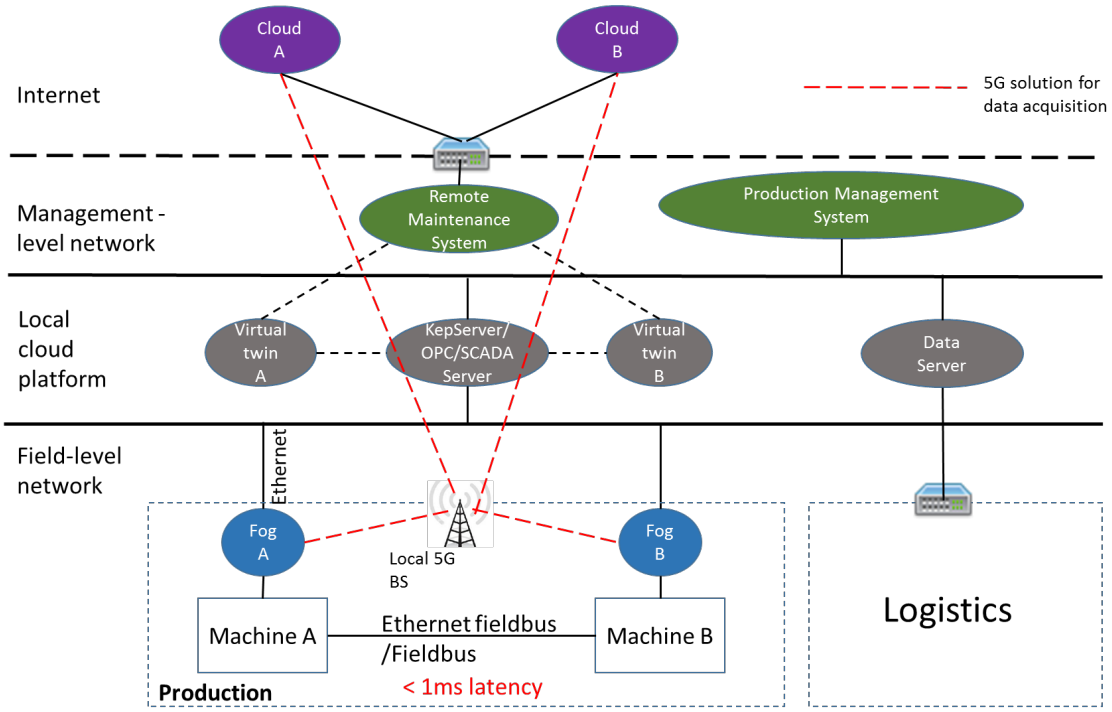


Figure 26: Future technical architecture for remote maintenance connectivity in factories.

station(s), as seen in Figure 26. The base station acts as a central connection point for fog devices, and together with emerging computing concepts (e.g., MEC) and softwarization technologies allows machine data to be flexibly and economically (cp. network slicing concept) transmitted to the relevant machine providers' clouds. The function of the fog device is to perform a pre-analysis of sensor data and send the analyzed data to the local cloud servers (see Figure 18 on page 33 for more specific information of the functionalities). Additionally, it controls the mobile data transmission between a machine and machine provider's cloud. The fog device only allows outbound remote connection(s), thus machines cannot be controlled through the mobile network. The fog unit can be either embedded in a machine, or a separated device. The capabilities of the fog can also be centralized to a single, more powerful device, which serves, for example, different machine models from a same vendor, or machines belonging to a same production cell.

The architecture presented in this chapter allows both the machine owner and provider to reach a feasible solution regarding data utilization for maintenance operations. It combines the positive sides of each remote connection type, as well as exploits emerging technologies, such as 5G and fog computing. Although 5G is only employed for remote monitoring, and wired connection for remote control, the architecture allows either connection type to be used for both functions. In mobile connection case, this would be realized by running the virtual twin instance in the fog device. However, allowing remote control function to bypass factory's firewall and

remote maintenance system, the security risk for unauthorized control of the machine increases. To limit this type of risk, the virtual twin could be configured to not accept any remote operations (e.g., software updates or configuration of functionalities) to the physical machine without the approval of factory personnel.

# 5 Discussion

An Industrial System is a complex entity, which consists of deviating set of functions, networks and people that in combination aim to create value through products and services. Hence, if some section is inoperative or not functioning properly, the impact is almost immediately reflected to the efficiency of plant operations. Therefore, Industrial Systems, such as factories, are often reluctant regarding the alteration of a functioning system, even though the deployment of a novel technology or service would most likely improve the system as a whole. Consequently, deploying, for example, a remote maintenance service in factories is challenging task, although there have been many successful remote service deployments, such as ABB's pilot in SSAB steel mill [90]. In that case, the value of the remote service was almost immediately realized, thus the customer saw the real benefits of the deployment. This is not always obvious because machines can function properly for many years without breakdowns, whereupon the customer cannot observe the real value of the service, as was in the Factory A's case. This leads to an impression that allowing machines to be maintained remotely is unnecessary and costly. Hence, a remote service should not operate as a separate function, but as a part of an Industrial System, in which case the value of the machine data would not only be realized in the service provider's side but also in the customer's premises. This could be realized, for example, through the integration of predictive maintenance and spare parts inventory which would automatize the orders based on the condition of machine parts. However, due to proprietary technology (e.g., communication protocols and management systems) applied in Industrial Systems, the integration is challenging, and sometimes even impossible to execute.

Currently, there are lots of ongoing research projects that aim to address the incompatibility issues through standardized platforms and technologies so that the concept "smart factory" would be realizable in the near future. One of the major projects in Finland is the "Reboot factory" [91], which aims to create the first wave of digitalization through the exploitation of IoT technology and standardized communications in factories. Even though the expectations for the adaptation of standard technology and open data are high, there is, however, an uncertainty whether the present platform and industrial protocol producers are willing to adapt to the changes because as industrial ICT becomes standardized, the competition would increase and there would not be a possibility to reap the benefits of proprietary solutions. Eventually, standard technology will be adapted to factory systems, but the initiative must come from the industry itself.

5G is expected to change the static factory networks into dynamic and need-based wireless systems. Since 5G technology will be used for local communications, in addition to the mobile communications (e.g., for remote service), it is still unclear whether MNO will operate these type of networks or the factory's IT personnel which has lead to the emergence of Micro Operator [92]. The concept of Micro Operator is similar to MVNO, but the focus is on operating and serving indoors/small cell 5G environment such as future factories. The Micro Operator type of operation could be realized, for example, through an LSA agreement with the MNO. The local operator

would most likely be the factory's own employees, but there is also an opportunity for a third party to serve, for example, specific industry field(s), or factories on a particular geographical area.

As more machines, sensors and actuators will utilize mobile communications to transmit data to various external applications in the future, there is a need to change the policy with SIM cards. Today, the problems arise especially in cases where hundreds of SIM cards need to be installed on machines located in different countries. This inflicts considerable logistics costs and is unpractical. Moreover, if the SIM cards are bought from the same operator, the machines are bound to use services of that particular operator. This is problematic especially in locations where the MNO does not have coverage. With the introduction of embedded SIM, these type of issues could be solved, as it enables "over the air" provisioning and possibility to change from one operator to another [93]. Moreover, the card would be embedded into equipment during the manufacturing phase, thus decreasing logistics costs.

With the evolution of computing, and diagnostics methods, maintenance activities will be optimized to the point where the abrasion level of machinery parts can be monitored in real-time, leading to exact predictions when the parts need to be changed. However, conducting predictive maintenance will require a massive amount of machine operational data, which is currently difficult to obtain since factories do not want to share the data with other actors such as machine providers without concrete benefits. This is an intractable equation because, on the one hand, providing the data to machine providers will enable the development of better diagnostics methods and services but, on the other hand, sharing the data without visible benefits is not rational from the factory's viewpoint. 5G and novel computing concepts will allow more flexible utilization of machine data both locally and externally, but there is a still need to develop better data sharing frameworks that would maximize the value of the operational data in different remote service solutions.

# 6 Conclusions

This thesis analyzed the feasibility of remote maintenance connectivity in factories by applying the VNC method by Casey et al. [86] in alternative remote connection cases. Additionally, it presented a future technical architecture based on the VNCs, literature review and case studies. A wide-ranging literature study, involving numerous publications regarding e-maintenance, Industrial Networks, Industrial Internet and 5G, was conducted for gaining insight of the relevant topics and establishing the basis for the analysis part.

## 6.1 Results

The importance of maintenance function is growing in factories due to manufacturing processes being increasingly performed by machines, robots and other equipment. By managing this function efficiently, a factory can save in costs through reduced downtime, prolonged machine life, and better utilization of spare parts, thus improving its productivity and competitiveness. Maintenance strategies can vary from "no maintenance" to predictive maintenance; the selection of proper strategy requires a thorough evaluation of the strategy implementation cost with respect to the machine value. The implementation of more advanced strategies presumes that the relevant machines are connected to a network, via which they can send measurement data for further analysis.

In factories, machines are typically connected to an industrial network, which consists of various real-time communication technologies that are often proprietary and not directly compatible with standard networking technologies. Consequently, acquiring measurement data from machines for utilizing it in other applications than automation-related supervisory and control systems is challenging. The introduction of OPC UA has, however, provided an architecture and technology to resolve the compatibility issues, and to have consistent communication and standard information models from controllers to the cloud. Now that the Fourth Industrial Revolution is approaching, having a standardized communication across all automation pyramid levels is of great importance in order to fully exploit machine data through applications, such as predictive maintenance, production optimization, and supply chain optimization. The realization of the next Industrial Revolution, also referred to as Industrial Internet or Industrie 4.0, will also highly depend on the global communications between all type of processes and equipment, including battery-powered sensors, and vehicles, located in factories, rural areas, and at seas. Hence, 5G will play a vital role in the materialization of Industrial Internet, as it aims to provide a flexible mobile communication infrastructure that enables dynamic resource utilization for diverse set of services, categorized into three communications categories: low data rate (mMTC), low latency (Critical Communications), and high data rate and mobility (Enhanced Mobile Broadband). The key enablers, which are considered to address the requirements of the communication categories, are network virtualization, efficient utilization of radio spectrum, network slicing, and novel computing concepts such as fog, edge and MEC.

The results from the case studies and interviews indicate that network communications in factories are still heavily depended on wired solutions and industrial protocols. Nevertheless, all case factories aim to exploit machine data in operations other than automation. Two of the case factories (Factory B and C) are already collecting a vast amount of machine data to the local cloud, but they have not been able to utilize it in functions, such as maintenance. Moreover, the exploitation of the data is meant to be performed with factory's own resources, and not by an external company, such as remote service provider. In all case factories, the mobile signal strength is high throughout the factory premises, thus there is a possibility to deploy a remote service via the mobile connection. However, due to long life-cycles of the majority of machines (3G/4G module is lacking) and high mobile costs, the mobile solution is not feasible in many cases.

The results from VNC analysis and remote connection cases state that the deployment of remote maintenance depends on the features of the remote connection and value of the corresponding service, as well as the current status of machines regarding the network connectivity and data acquisition. For example, if machine data can be acquired and processed in the local cloud, the customer would be more reluctant implement "through firewall" –type of solution, since, e.g., the control on data will decrease and the security risk will increase. Hence, in this case, the most obvious choice would be the "Isolated" solution. However, allowing a machine(s) to be maintained "through firewall" –type of solution, the customer would gain more value from the service, because the service provider would be able to respond more rapidly to malfunctions and provide, e.g., round-the-clock service. Moreover, the customer would save in computing costs, since the data will be processed in the service provider's cloud.

In the future, 5G is expected to transform rigid industrial networks into more transparent and flexible wireless systems. However, considering industry's tendency for slow adaptation of novel technology, the change will not occur in the few years after the introduction of 5G. Consequently, as a result of the VNC analysis and case studies, this thesis proposes a future technical architecture aimed to provide flexible remote maintenance connectivity in factories, through the exploitation of 5G and novel computing concepts.

## 6.2 Assessment of the results

The results are achieved through an extensive literature study and industry expert interviews, which provide valuable insights on the relevant topics and the current situation in factories regarding network connectivity and data exploitation. The experts are managers and specialists in the fields of manufacturing, engineering and service, process automation, Industrial Internet, and electrical equipment. The focus of the results is on the customer side of the remote maintenance service since the challenges of the deployment appear particularly inside the factory premises.

The case studies are for the most part based on interviews. They consider the focal features of a factory and remote connection solution which enables different cases to be compared, as well as establish the basis for value network analysis. The

results from the analysis are indicative of the remote maintenance deployment with the current and future technology, and they provide an insight of the benefits each actor can gain by participating in the value network. Hence, the results are valuable for all actors in the evaluation of remote maintenance initiative.

This research utilizes qualitative methods, including semi-structured interviews and VNC analysis, to gain insight into the current situation of remote maintenance usage in industry and assess the feasibility of remote connectivity in factories from techno-economic viewpoint. The interviews center around the insights of industry experts and employees on the topic, thus assumptions for MNO's relevance on the realization of remote maintenance are made. Additionally, the sample size of case factories is not large enough to make statistically relevant conclusions about the current state of remote maintenance and machine data exploitation with respect to industry field. Moreover, the case studies did not involve any factories from, e.g., process industry, thus the results from VNC analysis cannot be generalized to the whole industry. Also, if the sample size of case factories would be much larger and would include factories that currently employ remote maintenance, the VNCs could differ from the ones presented in this research, especially if more accurate information of the technical aspects of remote connection solution is gained. However, the remote connection cases are expected to be the same even if more case factories are included in the research.

The Value Network Configurations are high-level representations of the remote maintenance connectivity, and they consider only strategically important technology and business roles from the service realization viewpoint. Hence, the technical architecture of the VNCs cannot directly be applied to real-world deployments.

## 6.3 Future research

This research applies VNC method to analyze the value creation logic of alternative remote maintenance solutions by focusing particularly on connectivity implementation. Thus, the same method could be used for application-level analysis of remote maintenance. Furthermore, the value network could be expanded to involve other actors, such as micro-operator and eSIM provider. In this case, a scenario planning tool by Schoemaker [94] could be utilized in combination with the VNC method to analyze the control of focal and new actors on strategically important technology concerning possible future scenarios.

This thesis is based on qualitative analysis, thus it does not evaluate the cost of remote maintenance deployment in different remote connection cases. To gain more accurate view on remote maintenance connectivity in factories, there is a need for quantitative analysis, which could, for example, focus on the cost structure of the deployment, including, e.g., data transmission cost, service cost and configuration cost.

# References


[1] IHS, "IoT installed base forecast," 2016. [Online]. Available: https://blogs-images.forbes.com/louiscolumbus/files/2016/11/IHS.jpg. [Accessed: Oct. 25, 2017].

[2] S. J. Liebowitz and S. E. Margolis, "Network Externality: An Uncommon Tragedy," *Journal of Economic Perspectives*, vol. 8, no. 2, pp. 133–150, 1994.

[3] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin and D. Aharon, "Internet of Things: Mapping the value beyond the hype," *McKinsey Global Institute*, June 2015, [Online], Available: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world. [Accessed: Sept. 2, 2017].

[4] A. Starr, B. Al-Najjar, K. Holmberg, E. Jantunen, J. Bellew and A. Albarbar. "Maintenance Today and Future Trends," in *E-maintenance*, K. Holmberg, A. Adgar, A. Arnaiz, E. Jantunen, J. Mascolo and S. Mekid, London: Springer, 2010, pp. 5–38. [Online]. Available: SpringerLink.

[5] A. Pehrsson and B. Al-Najjar, "Creation of industrial competitiveness". *Acta Wexionensia*, no. 69. Växjö University Press, Sweden, 2015. ISBN: 91-7636-467-4.

[6] A. Muller, A. C. Marquez, and B. Iung, "On the concept of e-maintenance: Review and current research," *Reliability Engineering and System Safety*, vol. 93, no. 8, pp. 1165–1187, Aug. 2008.

[7] A. Arnaiz, B. Iung, A. Adgar, T. Naks, T. Tommingas and E. Levrat. "Information and Communication Technologies Within E-maintenance," in *E-maintenance*, K. Holmberg, A. Adgar, A. Arnaiz, E. Jantunen, J. Mascolo and S. Mekid, London: Springer, 2010, pp. 39–60. [Online]. Available: SpringerLink.

[8] A. H. C. Tsang, "Strategic dimensions of maintenance management," *Journal of Quality in Maintenance Engineering*, vol. 8, no. 1, pp. 7–39, 2002.

[9] W. J. Moore and A. G. Starr, "An intelligent maintenance system for continuous cost-based prioritisation of maintenance activities," *Computers in Industry*, vol. 57, no. 6, pp. 595–606, Aug. 2006.

[10] M. Ucar and R. G. Qiu, "E-maintenance in Support of E-automated Manufacturing Systems," *Journal of the Chinese Institute of Industrial Engineers*, vol. 22, no. 1, pp. 1–10, Feb. 2005.

[11] T. Han and B.-S. Yang, "Development of an e-maintenance system integrating advanced techniques," *Computers in Industry*, vol. 57, no. 6, pp. 569–580, Aug. 2006.

[12] A. C. Marquez and J. N. D. Gupta, "Contemporary maintenance management: process, framework and supporting pillars," *Omega*, vol. 34, no. 3, pp. 313–326, June 2006.

[13] J. Collin and A. Saarelainen. *Teollinen Internet*. Helsinki: Talentum, 2016. ISBN: 978-952-14-2849-4.

[14] T. Sauter, "The Three Generations of Field-Level Networks—Evolution and Compatibility Issues," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 11, pp. 3585–3595, Nov. 2010.

[15] J. R. Moyne and D. M. Tilbury, "The Emergence of Industrial Control Networks for Manufacturing Control, Diagnostics, and Safety Data," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 29–47, Jan. 2007.

[16] B. Galloway and G. P. Hancke, "Introduction to Industrial Control Networks," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 2, pp. 860–880, Second Quarter 2013.

[17] H.-P. Huth, A. Houyou, J. W. Walewski and J. Claessens, "IoT@Work - State of the art and functional requirements in manufacturing and automation," Nov. 2010. [Online]. Available: https://www.researchgate.net/publication/282013984. [Accessed: July 20, 2017].

[18] M. Anjanappa, K. Datta, T. Song, R. Angara and S. Li. "Introduction to Sensors and Actuators," in *Mechatronic Systems, Sensors, and Actuators: Fundamentals and Modeling*, R. H. Bishop, $2^{nd}$ ed. CRC Press, 2007. ch. 17. ISBN: 978-1-4200-0900-2.

[19] D. R. Patrick and S. W. Fardo. *Industrial Process Control Systems*. $2^{nd}$ ed. Atlanta, GA: Fairmont Press cop., 2009. [Online]. Available: Knovel.

[20] M. Bajer, "Dataflow In Modern Industrial Automation Systems. Theory And Practice," Nov. 2014. [Online]. Available: https://www.researchgate.net/publication/267736303. [Accessed: July 20, 2017].

[21] SMAR Industrial Automation, "Industrial Networks – Part 1". [Online]. Available: http://www.smar.com/en/technical-article/industrial-networks-part-1. [Accessed: July 28, 2017].

[22] Infineon Technologies AG, "Industrial Automation: Products for Energy-Efficient Applications," Nov. 2010. [Online]. Available: https://www.infineon.com/dgdl/Industrial+Automation+2011.pdf?fileId=db3a30432c59a87e012c5ebb7edc3551. [Accessed: July 18, 2017].

[23] B. S. de Ugarte, A. Artiba and R. Pellerin, "Manufacturing execution system – a literature review," *Production Planning & Control*, vol. 20, no. 6, pp. 525–539, Sept. 2009.

[24] E. J. Umble, R. R. Haft and M. M. Umble, "Enterprise resource planning: Implementation procedures and critical success factors," *European Journal of Operational Research*, vol. 146, no. 2, pp. 241–257, Apr. 2003.

[25] R. Dietrich, "Industrial Ethernet... from the Office to the Machine - world wide-" *HARTING GmbH & Co. KG*, Dec. 2004. [Online]. Available: http://www.harting-usa.com/imperia/md/content/lg/hartingusa/news/hotlink/harting_industrial_ethernet_handbook.pdf. [Accessed: July 25, 2017].

[26] J. Park, S. Mackay and E. Wright. *Practical data communications for instrumentation and control.* Amsterdam; London: Elsevier, 2003. [Online]. Available: Knovel.

[27] J. P. Thomesse, "Fieldbus Technology in Industrial Automation," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1073–1101, June 2005.

[28] J. D. Decotignie, "Ethernet-Based Real-Time and Industrial Communications," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1102–1117, June 2005.

[29] M. Felser, "Real-Time Ethernet – Industry Prospective," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1118–1129, June 2005.

[30] J. Åkerberg, M. Gidlund and M. Björkman, "Future research challenges in wireless sensor and actuator networks targeting industrial automation," in *2011 9th IEEE International Conference on Industrial Informatics*, Caparica, Lisbon, 2011, pp. 410–415.

[31] A. Frotzscher, U. Wetzker, M. Bauer, M. Rentschler, M. Beyer, S. Elspass and H. Klessig, "Requirements and current solutions of wireless communication in industrial automation," in *2014 IEEE International Conference on Communications Workshops (ICC)*, Sydney, NSW, 2014, pp. 67–72.

[32] V. C. Gungor and G. P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[33] D. Miorandi, E. Uhlemann, S. Vitturi and A. Willig, "Guest Editorial: Special Section on Wireless Technologies in Factory and Industrial Automation, Part I," *IEEE Transactions on Industrial Informatics*, vol. 3, no. 2, pp. 95–98, May 2007.

[34] I. F. Akyildiz and I. H. Kasimoglu, "Wireless sensor and actor networks: research challenges," *Ad Hoc Networks*, vol. 2, no. 4, pp. 351–367, Oct. 2004.

[35] E. Dahlman, G. Mildh, S. Parkvall, J. Peisa, J. Sachs, Y. Selén and J. Sköld, "5G wireless access: requirements and realization," *IEEE Communications Magazine*, vol. 52, no. 12, pp. 42–47, Dec. 2014.

[36] O. N. C. Yilmaz, Y. P. E. Wang, N. A. Johansson, N. Brahmi, S. A. Ashraf and J. Sachs, "Analysis of ultra-reliable and low-latency 5G communication for a factory automation use case," in *2015 IEEE International Conference on Communication Workshop (ICCW)*, London, 2015, pp. 1190–1195.

[37] M. Cheminod, L. Durante and A. Valenzano, "Review of Security Issues in Industrial Networks," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 277–293, Feb. 2013.

[38] V. Ryan, "What Does CNC Mean?," 2009. [Online]. Available: http://www.technologystudent.com/cam/cnccut1.html. [Accessed: July 30, 2017].

[39] A. Daneels and W. Salter, "What is SCADA?," in *International Conference on Accelerator and Large Experimental Physics Control Systems*, Trieste, Italy, 1999.

[40] OPC Foundation, "Unified Architecture". [Online]. Available: https://opcfoundation.org/about/opc-technologies/opc-ua/. [Accessed: July 30, 2017].

[41] W. Mahnke and S.-H. Leitner, "OPC Unified Architecture – The future standard for communication and information modeling in automation," *ABB Review*, Mar. 2009. [Online]. Available: http://new.abb.com/about/technology/abb-review. [Accessed: July 30, 2017].

[42] Novotek AB, "OPC and OPC UA explained". [Online]. Available: https://www.novotek.com/en/solutions/kepware-communication-platform/opc-and-opc-ua-explained. [Accessed: July 30, 2017].

[43] P. C. Evans and M. Annuniziata, "Industrial Internet: Pushing the Boundaries of Minds and Machines," *General Electric*, Nov. 26, 2012. [Online]. Available: https://www.ge.com/docs/chapters/Industrial_Internet.pdf. [Accessed: Sept. 1, 2017].

[44] R. Drath and A. Horch, "Industrie 4.0: Hit or Hype? [Industry Forum]," *IEEE Industrial Electronics Magazine*, vol. 8, no. 2, pp. 56–58, June 2014.

[45] M. Rüßmann, M. Lorenz, P. Gerbert, M. Waldner, J. Justus, P. Engel and M. Harnisch, "Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries," *The Boston Consulting Group*, Apr. 9, 2015. [Online]. Available: https://www.bcgperspectives.com/content/articles/engineered_products_project_business_industry_40_future_productivity_growth_manufacturing_industries/. [Accessed: Sept. 2, 2017].

[46] W. Wahlster, "Industrie 4.0: Cyber-Physical Production Systems for Mass Customization," *German-Czech Workshop on Industrie 4.0*, Prague, Apr. 11, 2016. [Online]. Available: http://www.dfki.de/wwdata/German-Czech_Workshop_

on_Industrie_4.0_Prague_11_04_16/Industrie_4_0_Cyber-Physical_Production_Systems_for_Mass_Customizations.pdf. [Accessed: Sept. 1, 2017].

[47] J. Q. Li, F. R. Yu, G. Deng, C. Luo, Z. Ming and Q. Yan, "Industrial Internet: A Survey on the Enabling Technologies, Applications, and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1504–1526, thirdquarter 2017.

[48] J. Bloem, M. van Doorn, S. Duivestein, D. Excoffier, R. Maas and E. van Ommeren, "The Fourth Industrial Revolution – Things to Tighten the Link Between IT and OT," *Sogeti*, 2014. [Online]. Available: https://www.fr.sogeti.com/globalassets/global/downloads/reports/vint-research-3-the-fourth-industrial-revolution. [Accessed: Sept. 2, 2017].

[49] W. E. Frazier, ""Metal Additive Manufacturing: A Review," *Journal of Materials Engineering and Performance*, vol. 23, no. 6, pp. 1917–1928, June 2014.

[50] S. K. Ong, M. L. Yuan and A. Y. Nee, "Augmented reality applications in manufacturing: a survey," *International Journal of Production Research*, vol. 46, no. 10, pp. 2707–2742, May 2008.

[51] M. Hartmann and B. Halecker, "Management of Innovation in the Industrial Internet of Things," in *XXVI ISPIM Conference – Shaping the Frontiers of Innovation Management*, Budapest, 2015.

[52] T. Bauernhansl, M. ten Hompel and B. Vogel-Heuser. *Industrie 4.0 in Produktion, Automatisierung und Logistik*. Berlin: Springer, 2014. ISBN: 978-3-658-04681-1.

[53] Gartner, "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016," Feb. 7, 2016. [Online]. Available: http://www.gartner.com/newsroom/id/3598917. [Accessed: Oct. 10, 2017].

[54] M. Ehret and J. Wirtz, "Unlocking value from machines: business models and Industrial Internet of Things," *Journal of Marketing and Management*, vol. 33, no. 1, pp. 111–130, 2017.

[55] J. Lee, B. Bagheri and H.A. Kao, "A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems," *Manufacturing Letters*, vol. 3, pp. 18–23, Jan. 2015.

[56] 3GPP, "Study on New Services and Markets Technology Enablers," *The 3rd Generation Partnership Project*, 3GPP TR 22.891 v14.1.0, June 2016. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2897. [Accessed: Oct. 5, 2017].

[57] 5GPPP, "5G Vision brochure," 2015. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf. [Accessed: Oct. 1, 2017].

[58] 3GPP, "SA1 completes its study into 5G requirements," June 23, 2016. [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1786-5g_reqs_sa1. [Accessed: Oct. 5, 2017].

[59] NGMN Alliance, "5G White Paper," Feb. 2015. [Online]. Available: https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf. [Accessed: May 15, 2017].

[60] A. Osseiran, F. Boccardi, V. Braun, K. Kusume, P. Marsch, M. Maternia, O. Queseth, M. Schellmann, H. Schotten, H. Taoka, H. Tullberg, M. A. Uusitalo, B. Timus and M. Fallgren, "Scenarios for 5G mobile and wireless communications: the vision of the METIS project," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 26–35, May 2014.

[61] 5GPPP, "View on 5G Architecture," *5GPPP White Paper*, July 2016. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-5G-Architecture-WP-July-2016.pdf. [Accessed: May 10, 2017].

[62] J. S. Walia, "Techno-economic Analysis of 5G Local Area Access in Industrial Machine-to-Machine Communications," M.Sc. thesis, Aalto University, Espoo, Finland, 2016.

[63] Y. Yoon, D. Ban, S. Han, D. An and E. Heo. "Device/Cloud Collaboration Framework for Intelligence Applications," *Internet of Things: Principles and Paradigms*, R. Buyya, and A. V. Dastjerdi, Ed. Cambridge, USA: Morgan Kaufmann, 2016, pp. 49–60. ISBN: 978-0-12-805395-9.

[64] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia. "A view of cloud computing." *Commun. ACM*, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[65] M. Yannuzzi, R. Milito, R. Serral-Gracià, D. Montero and M. Nemirovsky. "Key ingredients in an IoT recipe: Fog Computing, Cloud computing, and more Fog Computing," in *2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Athens, 2014, pp. 325–329.

[66] Cisco, "Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are," *Cisco White Paper*, Apr. 2015. [Online]. Available: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf. [Accessed: Mar. 12, 2017].

[67] A. V. Dastjerdi, H. Gupta, R. N. Calheiros, S. K. Ghosh and R. Buyya. "Fog Computing: Principles, Architectures and Applications," in *Internet of Things:*

*Principles and Paradigms*, R. Buyya, and A. V. Dastjerdi, Ed. Cambridge, USA: Morgan Kaufmann, 2016, pp. 49–60. ISBN: 978-0-12-805395-9.

[68] L. M. Vaquero and L. Rodero-Merino. "Finding your Way in the Fog: Towards a Comprehensive Definition of Fog Computing." *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 27–32, Oct. 2014.

[69] ETSI, "Mobile-Edge Computing," *Introductory Technical White Paper*, Sept. 2014. [Online]. Available: https://portal.etsi.org/portals/0/tbpages/mec/docs/mobile-edge_computing_-_introductory_technical_white_paper_v1%2018-09-14.pdf. [Accessed: Oct. 4, 2017].

[70] M. Aazam and E. N. Huh, "Fog Computing Micro Datacenter Based Dynamic Resource Estimation and Pricing Model for IoT," in *2015 IEEE 29th International Conference on Advanced Information Networking and Applications*, Gwangiu, 2015, pp. 687–694.

[71] M. Aazam and E. N. Huh. "Fog Computing and Smart Gateway Based Communication for Cloud of Things," in *International Conference on Future Internet of Things and Cloud*, Barcelona, 2014, pp. 464–470.

[72] ETSI, "Network Functions Virtualization (NFV); Architectural Framework," *European Telecommunications Standards Institute*, GS NFV 002 V1.1.1, Oct. 2013. [Online]. Available: http://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.01.01_60/gs_nfv002v010101p.pdf. [Accessed: Oct. 4, 2017].

[73] J. Matias, J. Garay, N. Toledo, J. Unzilla and E. Jacob, "Toward an SDN-enabled NFV architecture," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 187–193, Apr. 2015.

[74] ONF, "Software-Defined Networking: The New Norm for Networks," *White Paper*, Apr. 13, 2012. [Online]. Available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf. [Accessed: Oct. 8, 2017].

[75] X. Zhou, R. Li, T. Chen and H. Zhang, "Network slicing as a service: enabling enterprises' own software-defined cellular networks," *IEEE Communications Magazine*, vol. 54, no. 7, pp. 146–153, July 2016.

[76] Cisco, "Cisco Mobile Visual Networking Index (VNI) Forecast Projects 7-Fold Increase in Global Mobile Data Traffic from 2016-2021," Feb. 7, 2017. [Online]. Available: https://newsroom.cisco.com/press-release-content?articleId=1819296. [Accessed: Oct. 8, 2017].

[77] Ofcom, "Ofcom announces winners of the 4G mobile auction," Feb. 20, 2013. [Online]. Available: https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2013/winners-of-the-4g-mobile-auction. [Accessed: Oct. 9, 2017].

[78] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What Will 5G Be?," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, June 2014.

[79] I. Poole, "What is MIMO? Multiple Input Multiple Output Tutorial," *Adrio Communications Ltd.* [Online]. Available: http://www.radio-electronics.com/info/antennas/mimo/multiple-input-multiple-output-technology-tutorial.php. [Accessed: Oct. 10, 2017].

[80] J. Khun-Jush, P. Bender, B. Deschamps and M. Gundlach, "Licensed shared access as complementary approach to meet spectrum demands: Benefits for next generation cellular systems," in *ETSI WORKSHOP ON RECONFIGURABLE RADIO SYSTEMS*, Cannes, 2012.

[81] 5GPPP, "5G and the Factories of the Future," *White Paper*, 2015. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Factories-of-the-Future-Vertical-Sector.pdf. [Accessed: Oct. 14, 2017].

[82] V. Allee, "Value network analysis and value conversion of tangible and intangible assets," *Journal of Intellectual Capital*, vol. 9 no. 1, pp. 5–24, 2008.

[83] M. E. Porter *Competitive Advantage: Creating and Sustaining Superior Performance*, New York: Free Press, 1985.

[84] C. B. Stabell and Ø. D. Fjeldstad, "Configuring value for competitive advantage: on chains, shops, and networks," *Strategic Management Journal*, vol. 19, pp. 413–437, 1998.

[85] J. Peppard and A. Rylander, "From Value Chain to Value Network: Insights for Mobile Operators," *European Management Journal*, vol. 24, no. 2–3, pp. 128–141, 2006.

[86] T. Casey, T. Smura and A. Sorri, "Value Network Configurations in wireless local area access," in *2010 9th Conference of Telecommunication, Media and Internet*, Ghent, 2010, pp. 1–9.

[87] ABB, "IRC5 – ABB's fifth generation robot controller". [Online]. Available: http://new.abb.com/products/robotics/controllers/irc5. [Accessed: Oct. 15, 2017].

[88] SIEMENS, "SINUMERIK 840D". [Online]. Available: http://w3.siemens.com/mcms/mc-systems/en/automation-systems/cnc-sinumerik/sinumerik-controls/sinumerik-840/sinumerik-840d/pages/sinumerik-840d.aspx. [Accessed: Oct. 15, 2017].

[89] ABB, "Remote Access Platform – Architecture and Security Overview". [Online]. Available: https://library.e.abb.com/public/ab7affaaa94041d448257d040035bb1a/RAP%20-%20Architecture%20and%20Security%20Overview.pdf. [Accessed: Nov. 5, 2017].

[90] ABB, "Internet of Things delivers innovative remote services for drives maintenance planning". [Online]. Available: http://new.abb.com/about/technology/iotsp/top-stories/customer-stories/innovative-remote-services-for-drives-maintenance-planning. [Accessed: Oct. 30, 2017].

[91] reboot Finland, "Reboot Factory". [Online]. Available: http://www.rebootfinland.fi/factory/. [Accessed: 14.11.2017].

[92] P. Ahokangas, S. Moqaddamerad, M. Matinmikko, A. Abouzeid, I. Atkova, J. F. Gomes and M. Iivari, "Future micro operators business models in 5G," *The Business & Management Review*, vol. 7, no. 5, pp. 143–149, June 2016.

[93] GSMA, "Remote SIM Provisioning for Machine to Machine". [Online]. Available: https://www.gsma.com/iot/embedded-sim/. [Accessed: 14.11.2017].

[94] P. J. H. Schoemaker, "Scenario Planning: A Tool for Strategic Thinking," *MIT Sloan Management Review*, vol. 36, no. 2, pp. 25–50, 1995.

# A List of interviewees

- Business Unit Technology Manager, Electrical Equipment. 21.12.2017, 09.03.2017, 19.04.2017
- Manager (Industrial Internet), Engineering and Service. 17.02.2017
- University Teacher, Department of Chemical and Metallurgical Engineering. 22.02.2017
- Factory Manager, Engineering and Service. 29.03.2017
- Service Manager, Engineering and Service. 29.03.2017
- Manufacturing Excellence and Development Manager, Telecommunications Equipment. 31.03.2017
- Product Development Specialist, Electrical Equipment. 10.04.2017
- Senior Project Manager, Electrical Equipment. 18.04.2017
- Technical Sales Manager; Technology, Engineering and Project Management Services. 27.06.2017