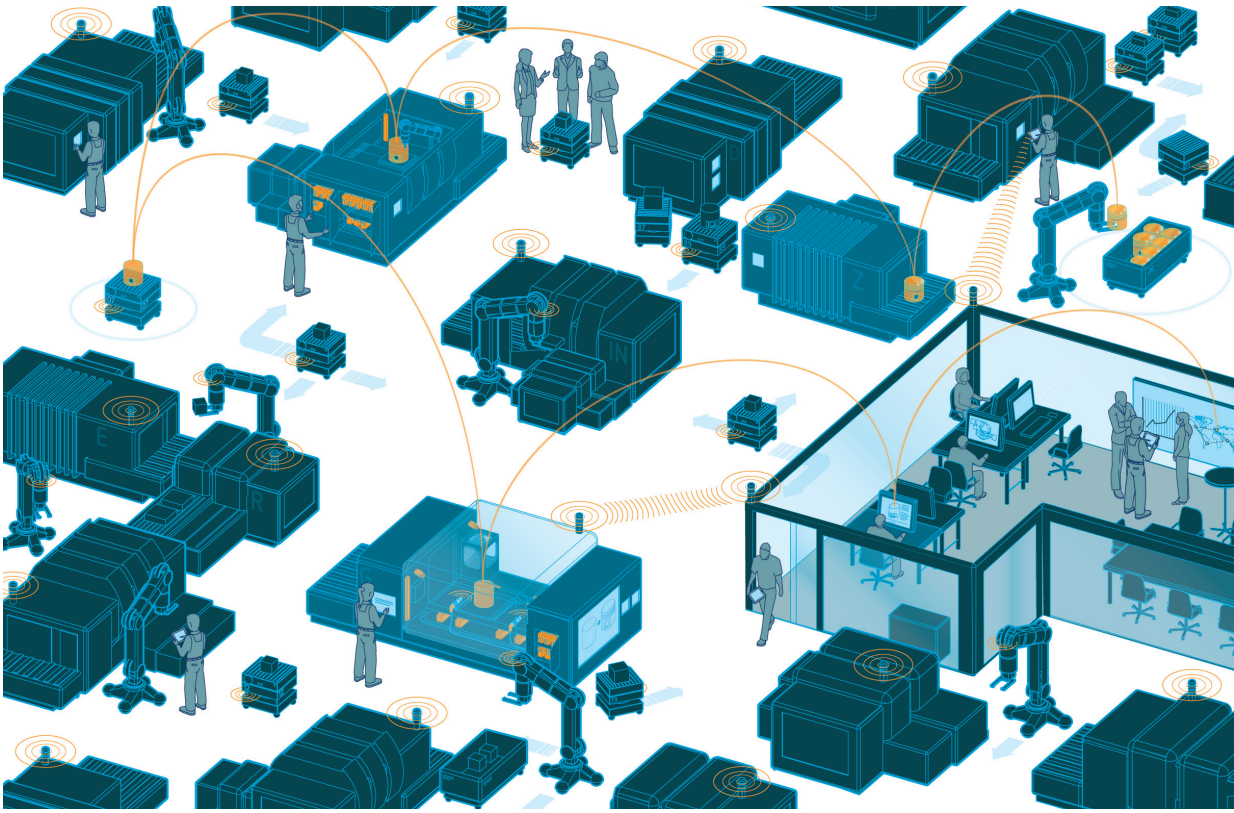
ZVEI:
Die Elektroindustrie

Consumer Devices in the Industrie 4.0 Environment

What challenges arise when using mobile devices in industrial applications?



White Paper – Part 3

Automation Division

Consumer Devices in the Industrie 4.0 Environment

Publisher:

ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
German Electrical and Electronic Manufacturers' Association
Automation Division
Lyoner Strasse 9
60528 Frankfurt am Main, Germany

Phone: +49 69 6302-440
Fax: +49 69 6302-386
E-mail: automation@zvei.org
www.zvei.org

Responsible:
Meik Billmann

Created by the working group System Aspects

This publication is part of a series of white papers:

Part 1 – Industrial Software 4.0?
Part 2 – Electrical Connectivity for Industrie 4.0?
Part 3 – Consumer Devices in the Industrie 4.0 Environment
… further parts to follow

A White Paper from the Working Group System Aspects in the Automation Division

Within the German Electrical and Electronic Manufacturers Association (ZVEI), the Automation Division works on topics and challenges from the perspective of manufacturers and users of automation equipment. By far the most discussed topic in this context is Industrie 4.0 and the associated potential, architectures, standards and technologies. The working group System Aspects is conscious of the significant importance of this topic area and has set itself the goal of examining and identifying the specific potential impact on basic technologies in our domains. This is being pursued as part of a small series of white papers, and this document on the subject of consumer devices is the third part in this series. As the basic work on Industrie 4.0 topics is still in its early stages, the members of the working group do not see the white paper as additional solution proposals, but rather as a (to some extent) critical examination of the anticipated implementation and application scenarios.

Frankfurt am Main, February 2018

Günter Feldmeier
Chairman of the System Aspects working group

Authors from the working group System Aspects

- Thomas Debes — CodeWrights
  Thomas.Debes@codewrights.de
- Holger Dietz — Janitza
  holger.dietz@janitza.de
- Heinz Scholing — Emerson
  heinz.scholing@emerson.com
- Jens Wickinger — Schneider Electric
  jens.wickinger@schneider-electric.com
- Günter Feldmeier — TE Connectivity
  GFeldmei@te.com
- Johannes Kalhoff — Phoenix Contact
  jkalhoff@phoenixcontact.com
- Dr. Jan Michels — Weidmüller
  janstefan.michels@weidmueller.de
- Arnd Ohme — Harting
  arnd.ohme@harting.com
- Carsten Risch — ABB Automation
  carsten.risch@de.abb.com
- Prof. Martin Wollschlaeger — TU Dresden
  martin.wollschlaeger@inf.tu-dresden.de
- Meik Billmann — ZVEI
  billmann@zvei.org

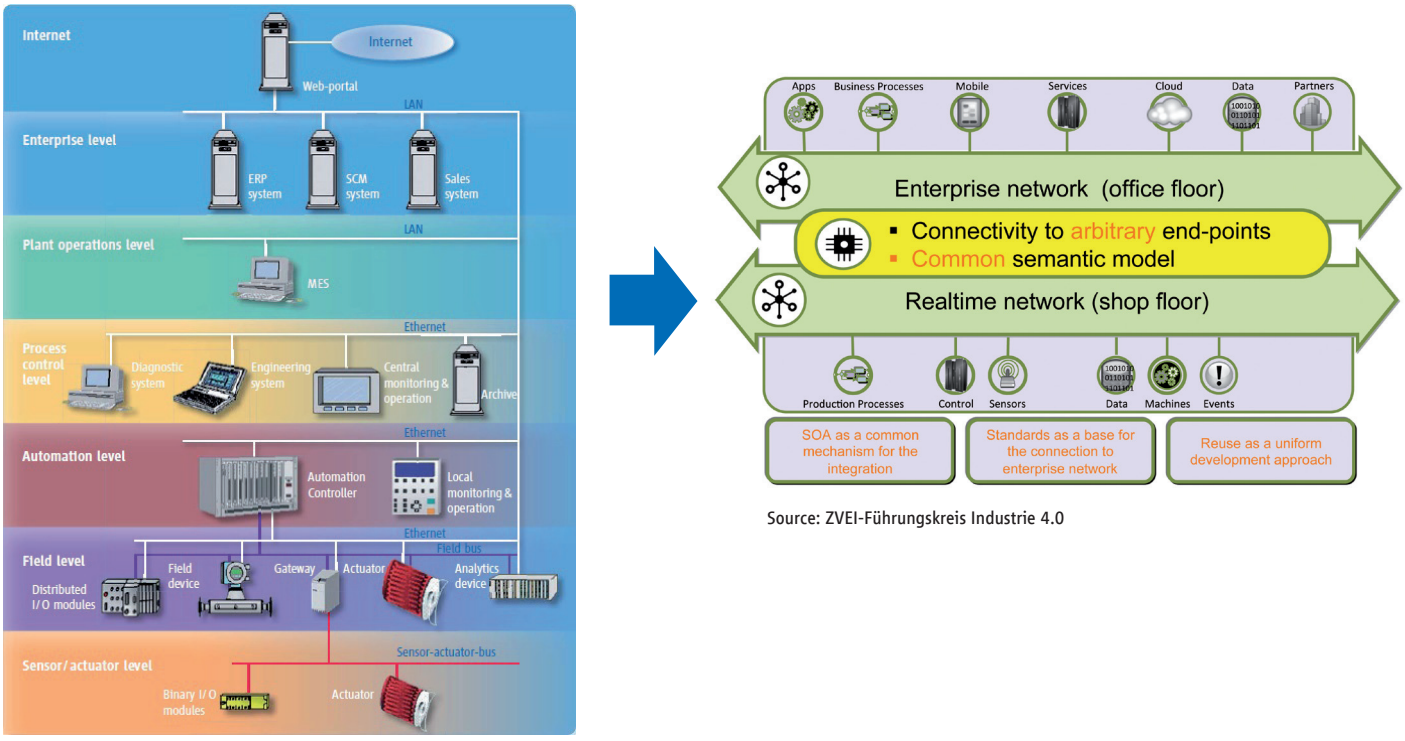
Content

1 Introduction

"Industrie 4.0" is surely one of the most commonly used terms in the field of industrial automation today. Also known as the fourth industrial revolution, numerous experts see in it major potential for far-reaching changes, not only for the economy but also societal politics. Within ZVEI, too, substantial contributions are being elaborated in various committees, including the System Aspects working group in the Automation Division. This working group is considering cross-sectorial topics in the area of system technology for automation. In particular, its task is to observe and evaluate the system-related framework conditions in automation technology in the Automation Division's area of application and to influence them in the Association's favour, if necessary. The previously published White Papers [1] and [2] formed the basis for a series of publications that shed more light on various aspects of Industrie 4.0 and consider the implications for specific target groups. This document investigates the challenges and opportunities that arise as a result of the immense technological development of devices in the consumer area and that will be further strengthened with future applications in the Industrie 4.0 environment. The focus here is on mobile devices (tablets and smartphones), as these now no longer only have a direct impact on the personal daily life of many users, but, thanks to their performance and interfaces, represent a key element in human-to-machine and human-to-human communication. Use of this type brings with it numerous side effects for users as well as system operators and system developers, which need to be analysed and assessed for the specific use case.

The following sections describe selected problems and potential solutions that may serve to support decisions regarding the use of mobile devices.

Figure 1: From the automation pyramid to Industrie 4.0



Source: Prof. Martin Wollschlaeger, TU Dresden

Source: ZVEI-Führungskreis Industrie 4.0

2 Anticipated User Benefits from Industrie 4.0 and Devices from the Consumer Area

Industrie 4.0 is not only known as the fourth industrial revolution in terms of the technical and technological changes, but also as a process that will significantly influence and change the world of work. In the future, production, logistics and service processes will be intelligently networked over the entire lifecycle of a product – from its creation until the end of its lifecycle – allowing a flexible response to market and customer requirements. Based on the opportunities that arise as a result of a more flexible production, the employees' areas of activity and the technical equipment will change. Connectivity, in particular the wireless kind, is becoming increasingly important here. In this context, extensive new options for information processing emerge for employees. New conditions are arising for interaction between humans and machines, which have an impact not just on content but also the time response of the communication. This all results in different requirements regarding the qualifications of those who work directly in this dynamic environment and are confronted with new technologies and methods. For this reason, the topics of work and training are a key component of the German National Platform Industrie 4.0. People entering the professional world today are frequently referred to as Generation Y or Digital Natives [3]. They grew up in a world that was already digital and are familiar with today's technologies. While employees from previous generations need to adapt to numerous changes, the industry and Digital Natives as users benefit as users immensely from technologies and known procedures that are already established in the consumer area. However, very few of these originated in an industrial environment. Many of these are developments from the consumer area (e.g. personal computers and their peripheral devices) that are now used in the industrial field or that are adapted to the specific requirements of the respective industry. The hybrid use of consumer devices has increased significantly with the widespread availability of mobile terminal devices, such as tablets and smartphones. The primary reason for this is the way these devices influence our lifestyle. People can access information at any time and from any location. The networking of people via social applications has established an entirely new form of communication. The extensive amount of sensors that are now commonly integrated into the devices also allow new applications. With integrated location sensors (GPS), it is possible to localise people regardless of where they are or to use the mobile terminal device for navigation. The integrated near-field communication (NFC) can be used to communicate with payment systems for purchases in supermarkets or as digital museum guides, to provide visitors with additional information about the exhibits. Due to the intelligent combination of the sensor information and their frequently cloud-based aggregation, new business models are developing that will result in the displacement of established systems. Mobile technologies are a major driver of digitisation. New information can be gained through networking data, and user benefits and the user experience can be improved considerably. When mobile consumer devices are used in an industrial environment, a distinction can be made between different scenarios:

- For example, customers use information that a company provides as part of business processes and customer relationships. This includes mainly e-commerce applications which allow customers to configure their products individually and to be continuously informed by the company about the manufacturing and delivery process.
- Another scenario is the use of private electronic devices that use the infrastructure at the workplace. The available infrastructure is used for private communication (e.g. e-mails, Facebook).
- Im Gegensatz dazu werden Geräte auch In contrast to this, devices are also used as a integral component of business or production processes. Especially where mobile access to business data is required (e.g. monitoring of production data and key figures), numerous mobile applications have already established. This allows sales representatives or other field staff to access up-to-date order and customer data. Service staff can learn about the current status of production systems or processes at any time. In

these various scenarios, many challenges arise for all those involved, which need to be mastered and which are described in the remainder of this document.

2.1 Use of consumer devices as part of business processes

2.1.1 For customer interaction

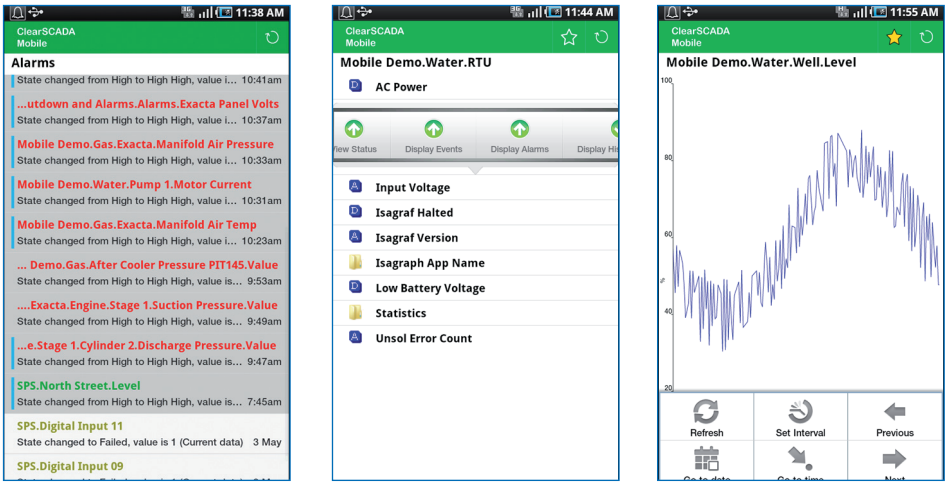
Industrie 4.0 applications are characterised by the flexible combination of various individual modular processes across the value-creation chain and the product lifecycle. Data that is relevant to the order process or to products must be organised and processed. The integration of mobile terminal devices into these processes also gives rise to new possibilities for interaction with customers and interested parties. On the one hand, status changes such as delivery progress or product updates can be communicated faster and more directly. On the other hand, new possibilities for manufacturers and customers to intervene in the processes for producing a product also arise.

Figure 2: Accessing process data with smart device

Source: Janitza

Figure 3: SCADA pages specially prepared for Smart Devices

(left: alarm side, centre: structuring of diagnostic data, right: trend curve)

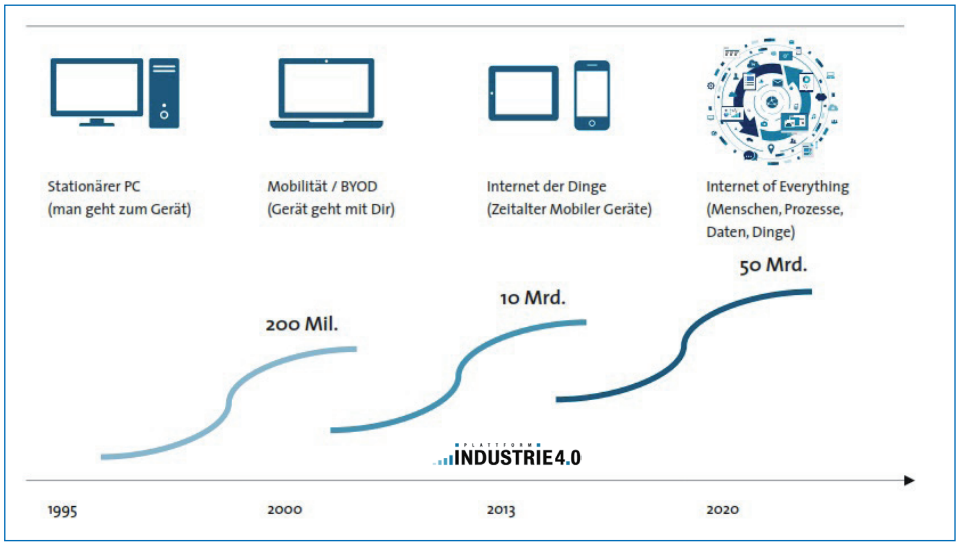


Source: Schneider Electric

2.1.2 For process control and monitoring

All companies have business processes to achieve specified objectives. In principle, these consist of various individual activities, which can in turn be divided into sub-tasks. The production of goods, and even customer management and financial reporting are defined as business processes. It is no longer possible to imagine these processes without IT support. While in office environments, it is possible to use consumer devices without making adjustments to the standard hardware, in industrial applications this is often not the case. Specific requirements due to the environmental conditions or the intended purpose were and often still are the reason for proprietary developments. For example, in explosive areas, special hardware must be used, or the environmental characteristics of the deployment environment (e.g. temperature, air humidity, dust) may require a different selection of the electronic components used or a different mechanical design of a device. Here, there is an increasingly apparent trend to use hardware and software components from consumer devices and make specific adjustments where required (e.g. housing to achieve protection class IP65). There are numerous reasons for this development – however, the main aspects are probably the mobility of users, the cost attractiveness, and rapid technological development and improvement. In most cases, proprietary development of high-performance hardware and software cannot keep up with the rapid developments for the consumer market in terms of development costs, unit costs, and time-to-market. This is a consequence of the extremely high quantities in the consumer sector and the resulting optimised mass production. In 2015 and 2016 alone, more than a billion smartphones were sold worldwide. While the first industrial use of consumer devices only supported early stages of a product lifecycle, such as planning, project planning and engineering, it can be expected that, with the development of industrial applications, later stages of the product lifecycle will also be supported. Examples of this are industrial solutions that allow consumer devices to access plant control and SCADA systems. Here, data prepared for the specific purpose is provided for visualisation (see Figure 2). During project planning for these systems or for operating terminals, special pages can be stored for smartphones or tablets, which can then also be accessed during the plant's lifetime (see Figures 2 + 3).

Figure 4: Growth curve of connected devices



Source: Nach Studie / Hrsg. Bitkom, Fraunhofer IAO: Industrie 4.0 – Volkswirtschaftliches Potenzial für Deutschland, Berlin, 2014

2.2 Use of consumer devices when using third-party infrastructures

The use of private devices in the workplace is mainly a result of the wide spread of mobile terminal devices. In today's society, these have become people's constant companions. In April 2016, 49 million smartphone users were registered in Germany [4]. Statistically, there are 1.7 smartphones per household [5]. An important aspect in the spread of these devices is their connectivity and simple networking.

Although the development of portable computers has already resulted in a hybrid use, this was not a mass phenomenon. The demand for and availability of IT solutions for integrating and using these devices in a business environment were correspondingly low. Typically, restrictive security settings prevented integration into office networks (e.g. Ethernet). As the costs for the data volumes used in the mobile communications network were high in the early days, the use of WLAN-based accesses was attractive not only for reasons of speed, but also from a costs perspective. Guest accesses in the wireless access points enabled access to public services. However, it was often only possible to connect to the operator's internal infrastructure via a VPN (Virtual Private Network). This situation changed with the significant increase in "smart" mobile phones, which enabled the simple use of Internet-based services and applications. The use of an already available infrastructure with private devices is also known as "Bring Your Own Device" (BYOD). This type of use is not restricted to a corporate environment, but also extends to public areas such as universities and administrative offices. A distinction must be made between this and the use of devices that belong to a company and are provided to employees with the option of (also) using them privately. The term "Corporate Owned, Personally Enabled" (COPE) has become established for this.

3 Overview of Technology

3.1 Application fields

Technological development has advanced massively over the past few years. The progressive miniaturisation of electronic components has resulted in a continuously increasing packing density in the devices. Today, the standard equipment in mobile devices includes numerous communications interfaces and a variety of sensors. The aggregation of sensor data opens up new application fields, which are also relevant for the industrial field. See Table 1 for information. A typical example for this is combining sensor data from various sources to determine the flow of traffic. The location data (GPS) is used to determine speed profiles, which in turn are used to detect traffic jams and calculate alternative routes.

Today, mobile devices are primarily based on three platforms (operating systems and application development environments): Apple iOS, Google Android and Windows Phone/Mobile [6]. The three manufacturers, Apple, Google and Microsoft, follow different strategies with regard to the licencing of their platforms for terminal-device manufacturers. What they have in common is the strategy for tying end customers to their respective ecosystem, which allows them access to services, free and paid applications ("apps"), multimedia offers, etc. Table 2 provides an overview of the key characteristics of the three platforms:

Table 1: Application fields of the consumer-device sensors

Application field	Function	Used sensors
Position determination and navigation	Localizing the device for position-based services (weather forecast, routing planning)	• GPS receiver • Acceleration sensor • Magnetometer
Movement detection (safety and healthcare)	Pedometer Distance capture	• GPS receiver • Acceleration sensor • Barometer • Temperature sensor • Pulse monitor
Authentication, access control	User identification by capturing and validation of the fingerprint	• Fingerabdrucksensor • Kamera
Logistics and warehousing, Service	Product information via RFID or QR code and cashless payment	• Kamera • NFC
Workplace lighting, energy efficiency	Illumination measurement and control	• Helligkeitssensor
Augmented reality	Visualization of information on the basis of a real-life environmental representation (Data glasses for warehouse management or service, indoor navigation)	• Camera • GPS receiver • Acceleration sensor
Voice and gesture control	Touchless (remote) operation of machines and other devices	• Microphone • Camera

Table 2: Comparison of mobile operating systems

	Apple iOS	Google Android	Windows Phone/Mobile
Development	By Apple	Open source (Linux kernel)	By Microsoft
Licensing of devices	Exclusively used by Apple devices	By Google, also open for unlicensed distributions, in case of unlicensed distribution, Google applications are not available (closed source)	By Microsoft
Device manufacturer	Only Apple	Samsung, LG, HTC, Motorola, Sony, ZTE, many more…	Microsoft (Lumia), others marginal
Usage without registration	No, Apple ID required	Yes, use without Google account possible, but some services and applications are not available (e. g. Google Play Store)	Yes, use without Microsoft account possible, but some services and applications are not available (e. g. OneDrive, Windows Store, Cortana)

As a result of their evolution, there are multiple versions of the operating systems for the platforms named above. It can thus be assumed that a user group uses various versions. The manufacturers no longer support some older versions, meaning software updates are no longer performed, and even known security gaps remain in place.

4 Challenges and Potential Solutions when Using Mobile Devices

The use of mobile devices poses major challenges for the companies and/or operators of the applications. No matter whether the devices are personal or provided by the company, numerous requirements must be taken into account.

4.1 Security

4.1.1 Security of the infrastructure

If the network is available, the network gateway is the first barrier to decide whether the user is to be granted access or not. Depending on the number of users, there are various possible solutions. Classic "guest access" can be implemented though simple web-based portal solutions, which are often part of the firmware of the access points (so-called "captive portals"). Here, when an address is entered in the web browser of the device, the user is automatically redirected to a log-in page where he or she must enter the relevant access data and/or accept conditions of use. If the communication is unencrypted, such solutions can easily be circumvented (e.g. through man-in-the-middle attacks). Secure implementations therefore always use special procedures to secure the access using dedicated authentication and authorisation (e.g. RADIUS = Remote Authentication Dial-in User Service). The disadvantages here are the fact that not all terminal devices support such procedures, and the increasing configuration effort. Once users have gained access to the infrastructure, a suitable network segmenting (VLAN) must ensure that they only gain access to the systems that are required for the specific use case (e.g. logistics, service, production control). By installing firewalls or proxy servers, additional measures can be taken to restrict the access to certain systems and services. Additional challenges arise when a provider makes the infrastructure available. In this case, the transparent access for the administration of users and devices is often only possible to a certain extent. The provider's availability guarantees thus have a direct impact on the company's own business processes. When selecting a provider, we recommend auditing them and performing a risk analysis.

4.1.2 Security of the terminal devices in operation

The ever shorter innovation cycles are giving rise to new challenges, such as security problems due to operating systems being updated later or not at all as well as the termination of use (also refer to [7]). New and further developments are not only ongoing in the area of hardware; updates are also released regularly for the software in use. While for end users of applications these are usually coming with new features, for the devices' operating systems the reason is often to close critical security gaps. Here, the individual manufacturers differ greatly when it comes to their response speed when rolling out the updates. In the worst case, older devices are no longer provided with updates at all, meaning detected safety gaps remain and thus pose a risk for the company and the users.

If mobile devices are used as components of business processes in the corporate environment, central inventorying and registration is not only desired by the company but also a mandatory requirement. In this way, the company specifies or restricts security guidelines, the software applications that can be used and the use of data. Other functions, such as the rollout of software updates, localisation and deletion of the device in the event of loss, can be implemented using a Mobile Device Management system (MDM). Well-known examples of these systems include VMware AirWatch, Blackberry Enterprise Service or Citrix XenMobile. The management of terminal devices is particularly challenging when various different mobile platforms (see Section 3) are used. Often not all functions are available and implemented in the same way on all platforms. Furthermore, there is the acceptance among users when the company guidelines also result in restrictions to their private use. For example, these may lock the device following inactivity and require a password with a specified minimum complexity to unlock it again.

The use of the device depends on various factors. If these devices are used solely for business purposes, the company specifies which applications and services can be used.

This is done either by contractual exclusion of personal use or by installing technical barriers that make it impossible for users to access applications that have not been approved to use. The basic challenge is that the flow of information between apps and services is only known to a limited extent and can thus also only be monitored and controlled to a certain extent. For example, if e-mails, contacts and appointments can only be used via the company infrastructure, users often wish to synchronise these with a personal account. In the worst case, data that was previously transmitted and stored on the device in encrypted form is now sent to another, potentially untrustworthy provider, as plain text information with no encryption, and is then no longer under the company's control. Calendar entries in particular frequently provide confidential information regarding the subject, participants and any documents provided for preparations. These are also synchronised and thus potentially visible to third parties. In an industrial environment, this is often the weak spot for industrial espionage. Furthermore, the increasing availability of voice assistants with cloud-based speech recognition and processing presents a security risk that has not yet been precisely defined.

4.1.3 Security in the event that devices are lost

The loss of devices, and thus the data stored on them, represents a high risk. In addition, in many cases access data to other systems is also stored on the devices. With company-owned devices that are provided for personal use, a Mobile Device Management system can be used to trigger remote clean-up of the devices. When private devices are used at the company, this depends on the user's settings. As long as no agreement was made between the users and the company, this may involve significant security risks in the event that a device is lost. Damage due to malware, Trojans and other harmful applications that may be introduced by an inadequately protected private device should also not be underestimated.

4.1.4 Security after use ends

The lifecycle of terminal devices is also determined by contract terms. The providers subsidise the procurement of new terminal devices through monthly contract fees. In Germany, at least, in recent years this has resulted in the majority of users switching to a new device every two years. The old devices are frequently sold on and used elsewhere. Any existing data may remain on the device and thus accessible to unauthorised persons.

4.2 Administration

Due to the variety of devices, corresponding requirements arise with regard to handling and managing the huge range of devices, operating systems and their versions. For one thing, smooth operation must be ensured within the selected infrastructure. In addition, individual applications need to be developed, tested and maintained for a number of very different platforms. This presents a cost factor that should not be underestimated and that occurs for the entire lifecycle of the device.

4.2.1 Infrastructure for terminal devices

The infrastructure is an essential component of the considerations that a company must take into account when using mobile devices. In the majority of cases, this is based on wireless LAN, for which access points have to be integrated into the existing company infrastructure. Depending on the environmental conditions, the positioning of the access points determines the subsequent signal quality. In production environments, in particular, significant attenuation and reflections often occur. A signal strength measurement prior to the installation helps to avoid later problems. If the area to be covered is very large, a correspondingly high number of access points must be established. Depending on the expected number of users, the backbone must be dimensioned accordingly to avoid subsequent bandwidth issues. For larger installations, the efficient installation, commissioning and administration in operation mode play a major role, as the management of individual devices with different configurations is often extremely time-consuming. Many manufacturers of network components provide management platforms, which enable central administration even for widely distributed systems.

4.2.2 Interoperability – terminal devices and applications

Requirements in the interoperability area arise as a result of the heterogeneous device landscape and the associated different lifecycles of hardware and software [7].

4.3 Legal requirements

The legally compliant handling of personal and company data is certainly one of the most important requirements. This is not only because not complying with these requirements results in legal consequences, but also due to the potential ramifications that could arise for the company due to negligent disclosure or distribution or as a result of loss of data.

Tax-legislation and licence-related aspects may also be relevant when the company hands over the devices to the user with the resulting possibility for personal use. This is particularly relevant if the conditions of use for the respective software prohibit commercial use. Consideration of various national provisions is a major challenge for global companies with central IT administration.

It is important to note that, when devices are used for both business and privately, at least in Germany the relevant data protection requirements apply and personal data can only be processed with the user's permission.

5 Decision Guide for Use

Generally, the use of mobile devices in an industrial environment depends on the use case. The crucial factor is the cost/benefit ratio during development and use of such devices and the costs for operating these devices.

5.1 Application-dependent cost/benefit ratio

One of the main features of Industrie 4.0 is communication, meaning it should be possible to exchange data without obstacles and this data should be available always and from anywhere. Mobile terminal devices such as tablets and smartphones can provide an important contribution here by complementing existing technology in order to ultimately realise the required data flow and information exchange.

If we consider the introduction of mobile terminal devices into the industrial environment under the aspect of the cost/benefit ratio, the respective application is a key criterion for the decision. Access to typical business data such as e-mails, notes or contacts is already commonplace and can be covered with the available applications from the personal environment. When it comes to accessing data from the production or manufacturing environment, the costs must be considered in comparison to a conventional implementation. An example of this is visualisation by means of a fixed remote terminal compared with the use of a tablet as an operating and monitoring interface. In both cases, it is important to take into account to what extent it is possible to use the existing infrastructure or whether the environmental conditions require additional installation or protection measures.

It is also necessary to consider how frequently the mobile data communication should be used. Is this a daily, weekly, monthly or even a non-cyclical application? A typical application case here could be a maintenance process using a smart device and RFID compared with a traditional walk round with a checklist. If it is merely an annual visual check of a small number of non-critical assets, the case for an investment in an RFID or a smart-device-based maintenance process would be difficult to convey. The situation is different if the number of assets is larger, the check cycles are shorter and/or official regulations require corresponding documentation of critical applications.

5.2 Social components

As mentioned at the start, the use of mobile devices in an industrial environment depends on the use case. When using multiple devices, guidelines should be provided: if the user is expected to be permanently available, is there already a set of rules for this within the company, e.g. works agreements? Other criteria apply when using these devices in a process-related environment. Here, it may be necessary to check whether these devices are so open that any apps can be installed on them, which, in some circumstances, could pose a risk of distraction. A further aspect is the level of training: Are the employees sufficiently qualified for the use of such devices, and will employees accept such devices?

5.3 Infrastructure

The provision and management of the infrastructure must be included in the cost/benefit consideration. If the infrastructure is not yet in place and first needs to be set up, a provider solution may make sense. Here, an appropriate provider is responsible for providing the necessary components and central management of the users. The investment costs are lower compared with self-financed procurement; however, the operating costs are generally higher. To ensure smooth operation that meets the applicable requirements, the services to be performed must be defined. Agreements regarding availability, data protection, and data security are necessary to exclude legal risks due to third-party claims. We recommend auditing the service provider accordingly or requesting evidence of compliance with relevant standards (e.g. DIN ISO 27001).

5.4 Training costs

The use of consumer devices and their operating components reduces the training costs because, due the common acceptance in a personal environment, many users are already familiar with the use of the equipment. Self-owned applications benefit from this fact if they adhere to the design and operation guidelines of the mobile platform in question.

6 Future Prospects

The boundaries between personal and business use will become increasingly blurred in the future. Due to cloud technologies, fast data transmission with high bandwidths, and wireless connectivity, data and information are always available from anywhere. Mobile terminal devices will play a decisive role when it comes to accessing this data and information in the future. The increasing number of so-called "wearables" (e.g. smartwatches, fitness wristbands) show the potential that can be found in the technology. Today, such devices often require a smartphone as a connection to the Internet. However, this will change in the future as a result of increasing miniaturisation and further development of the technologies. The integration of sensors into items for everyday use, such as clothing and commodities, will lead to new data and application cases. With the launch of Google's data glasses in 2012 [8], we were able to see for the first time the possibilities that can arise when the real and virtual worlds are linked. Recording and continuous streaming of videos while at the same time showing additional information in the wearer's field of vision open up many new application areas, which had not been achievable until now due to the size, weight and performance of the hardware. The first solutions for maintenance and error localisation in machine and plant engineering that use cameras integrated into the device to record the environment and show additional information (such as 3D drawings, replacement part information) are already available today. Valuable working time is thus used more efficiently and the error frequency as a result of unavailable or incorrect information is reduced. If necessary, users can be supported remotely, as the camera image can simultaneously be transmitted to dedicated experts without the need for them to be on site. Due to the aggregation of extensive sensor information from the user's surroundings, he or she has completely new options for interacting and communicating with the environment, be that with other users or intelligent machines. Business processes will be fully digitised and can be performed regardless of location and time. Humans will become part of these processes and will be represented by digital copies of themselves.

Figure 5: Augmented Reality support in an industrial environment

Source: zapp2photo/Fotolia.com

7 Summary

The use of consumer devices in industrial environments holds risks and opportunities at the same time. The available hardware is extremely high-performing, somewhat robust, intuitive to operate, and provides numerous different sensors at attractive costs. The innovation cycles are extremely short and technological development in this area is being driven by numerous major IT companies worldwide. The number of available applications is constantly increasing – location-independent communication, data exchange, and networking at all levels characterise the continuing development. It can be expected that with the introduction of Industrie 4.0 concepts, the use of consumer devices in an industrial environment will cover all phases of the product lifecycle. However, the exploitation of these benefits in industrial applications also poses risks that need to be considered. The often lower investment costs when using consumer devices are offset by the corresponding lifecycle costs (Total Cost of Ownership) that arise from the continuous development and operation of the systems. Security aspects and legal requirements must not be neglected here and should also be checked and adjusted at regular intervals even if successfully implemented.

References:

[1] ZVEI, Arbeitskreis Systemaspekte (Hrsg.), Whitepaper „Industrie-Software 4.0?“, 2015

[2] ZVEI, Arbeitskreis Systemaspekte (Hrsg.),
Whitepaper „Elektrische Verbindungstechnik für Industrie 4.0?“, 2015

[3] Wikipedia: „Generation Y“, unter: https://de.wikipedia.org/wiki/Generation_Y

[4] Statista: „Anzahl der Smartphone-Nutzer in Deutschland in den Jahren 2009 bis 016“, unter: https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/

[5] Destatis: „Ausstattung privater Haushalte mit Informations- und Kommunikationstechnik - Deutschland“,
unter: https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/EinkommenKonsumLebensbedingungen/AusstattungGebrauchsguetern/Tabellen/Infotechnik_D.html

[6] Statista: „Zwei Systeme sie alle zu binden“, unter „https://de.statista.com/infografik/8311/marktanteil-der-smartphone-betriebssysteme

[7] ZVEI, Arbeitskreis Systemaspekte (Hrsg.), Life-Cycle Management für Produkte und Systeme der Automation, 2010, ISBN-13: 978-3939265009

[8] Wikipedia: „Google Glass“, unter: https://de.wikipedia.org/wiki/Google_Glass

Die Elektroindustrie

ZVEI - German Electrical and
Electronic Manufacturers' Association
Lyoner Strasse 9
60528 Frankfurt am Main, Germany

Telephone: +49 69 6302-0
Fax: +49 69 6302-317
E-mail: zvei@zvei.org