UTILIZATION OF RADIO COMMUNICATIONS IN PRODUCTION FACILITIES FOR INDUSTRY 4.0

Friedrich K. Jondral
Karlsruhe Institute of Technology, Communications Engineering Lab
76128 Karlsruhe, Germany
Friedrich.Jondral@kit.edu

ABSTRACT

The digitization of our world irresistibly proceeds towards the internet of things and services. With her industry 4.0 initiative the German Federal Government stimulates growth, employment, and innovation. After methods of information technology have been increasingly installed for industrial automation, further developments promise a migration to cyber physical systems in fabrication. In this connection radio communications will increasingly be applied. This contribution is dedicated to the corresponding challenges.

Keywords: Industry 4.0, radio transmission in a factory, 5. generation of mobile communications, standardization, frequency administration, industrial automation, safety & security

INTRODUCTION

With her initiative *Industry 4.0 and Digital Economy* the German federal government, keeping in mind the internet of things and services, supports networking of production facilities and processes by means of information technology [1]. In this connection, the reliable and secure information transmission in factories is of paramount relevance. An important component is radio communications that, on the other hand, involves particular challenges targeted in this contribution.

The rest of this paper is organized as follows: The second section points out the importance as well as the diversity of radio technologies deployable in production. Afterwards, it is shown that different radio transmission technologies have to be applied for different purposes. The third section discusses the possible influence of the ongoing standardization efforts for the fifth generation (5G) of mobile communications on the tasks to be solved in *industry 4.0*. Section four highlights problems of operational, transmission as well as data security connected with the application of radio technology in manufacturing plants. The fifth section summarizes the results of the discussion derived in the previous sections and draws some conclusions.

RADIO TRANSMISSION IN PRODUCTION FACILITIES

Radio, the wireless information transmission via electromagnetic waves, may be flexibly employed and combines the mobility of terminals with low installation costs and high ease of maintenance. Today, in mobile communications preferably electromagnetic waves from the frequency region between 400 MHz and 6 GHz are used because of their favorable physical propagation properties [2]. The utilization of higher frequencies is a hot topic of current research. As drawbacks for the application of radio communications appear the stochastic properties of its transmission channels

that result from reflection, refraction, deflection, multipath propagation, interference of electromagnetic waves, and further natural distortions like, e.g., noise. Radio transmissions may intentionally be injured by wire-tapping, tampering, or by deploying mocking or jamming transmitters.

Already today, smart phones, tablets, smart glasses as well as machine-to-machine communications, which all use radio transmission, are established in manufacturing in order to monitor and control production processes. The application of wireless communications in factories leads to various questions concerning operational, transmission, and data security.

In public perception, radio communications, because of the of the associated technologies' great distribution rates, is tightly connected with cellular mobile communications or wireless local area networks (WLANs). Mobile communications and WLANs are preferably employed in offices or apartments i.e. in, from a radio propagation point of view, rather harmless environments compared to production facilities. Their subscribers are very sensitive with respect to costs. The installed technology is mainly based on highly specialized ASICs (application specific integrated circuits). Their fundamental figures of merit are data rate and energy efficiency.

Radio communications in factories is confronted with a rather harsh environment. Frequently, a great number of terminals are installed per unit area. Rotating machines and other production facilities disturb the propagation of electromagnetic waves. Robust transmissions using low data rates but high repetition rates (reports from sensors, commands to actors) as well as the creation of ad-hoc networks that, in contrast to cellular networks, do not rely on central base stations often become necessary. Sensitivity to costs may not be as high as for commercial mobile communications. The technology to be employed for radio transmission in production lines will strongly depend on the quantities of terminals that will be demanded. The most important figures of merit in these applications are (network and link) reliability, (transmission) latency, and (operational, transmission as well as data) security.

Altogether, we have to record that the requirements upon radio transmission in fabrication facilities distinctly differ from and usually are considerably higher than those put upon current commercial mobile radio systems. A certain order may be introduced into these challenges with regard to the automation pyramid that, considering a factory as a cyber physical system, is depicted in figure 1. On the left side the time scales, in which the appertaining systems have to react, are mentioned. (Here we have to observe that electromagnetic waves in the air cover a distance of about 300 kilometers per millisecond.) The scales on the right side indicate the layers on which smart phones, tablets, smart glasses, and machine-to-machine communications are employed. The information transmitted from sensors as well as to actors on the pyramid's base is of tactical nature, i.e. situation aware and instant actions are required. The more we climb up the layers' hierarchy the more the strategic nature of the information to be handled comes to the fore. At the pyramid's top, information describes systematic procedures. From this presentation we conclude that the protection of the information at the pyramid's base from a time duration point of view must not be as reliable as at the pyramid's top. This is because tactical information becomes obsolete much faster than strategic information. Certainly, this approach approaches

its limits if sensor or actor data critical for the production process have to be transmitted.

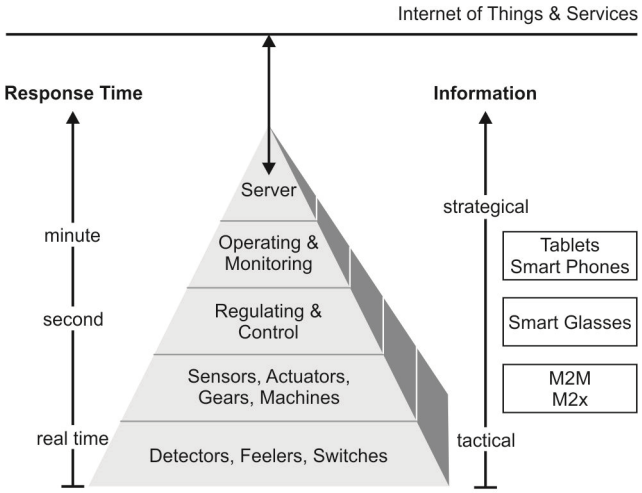


Figure 1: The Factory as Cyber Physical System

THE FIFTH GENERATION OF MOBILE COMMUNICATIONS

When discussing radio applications in factories, 5G that currently is prepared by standardization bodies, research institutions, and the relevant industries is, of course, a hot topic.

The most important goals pursued by 5G are [4]:

- Increase of the data rate such that the area capacity (measured in bit per second and area unit) compared with the fourth generation by a factor of thousand. At the same time the data rates at the cell edges shall lie between 100 Mbit/s and 1 Gbit/s and the peak data rate shall amount to several 10 Gbit/s.
- The roundtrip latency (e.g. control computer – actor – control computer) may not exceed 1 millisecond.
- Altogether, the overall energy consumption and cost in 5G shall not be higher than with the fourth generation of mobile communications (4G). I.e. that the energy to be spent to transmit one bit as well as the cost for this has to be lowered by at least a factor of 100 with respect to 4G.

These ambitious goals are to be reached by ultra-high densification of the networks (what means the application of femto cells) the installation of heterogeneous networks, the exploitation of the microwave range (28 to 90 GHz), the application of (massive) multiple input multiple output (MIMO) technology [2], the utilization of new wave forms at the physical layer, and the virtualization of the infrastructure. For all these intentions the effects of standardization by the worldwide acting fora and of regula-

tion by the nationally and internationally responsible agencies cannot be overestimated.

New application areas for radio communications within 5G are identified with the internet of things and services, the tactile internet, smart metering, in smart cities and smart grids, with coordinated autonomous car driving, and, of course, also with industry 4.0. The producing industry has to answer the question, whether it actively takes part in standardizing 5G, or, at least for radio applications at the automation pyramid's base, opts for different solutions. For a universal solution pursued by 5G to emerge as too complex for practical applications in production lines, the real risk should not be denied.

SECURITY

Security aspects are of paramount importance for radio transmissions in production facilities. Disturbances appear not only because of physical or technological insufficiencies but may be, e.g. with the goal of obstruction or targeted espionage of confidential data, deliberately effectuated by an offender on all layers of the automation pyramid.

1 Operational Security

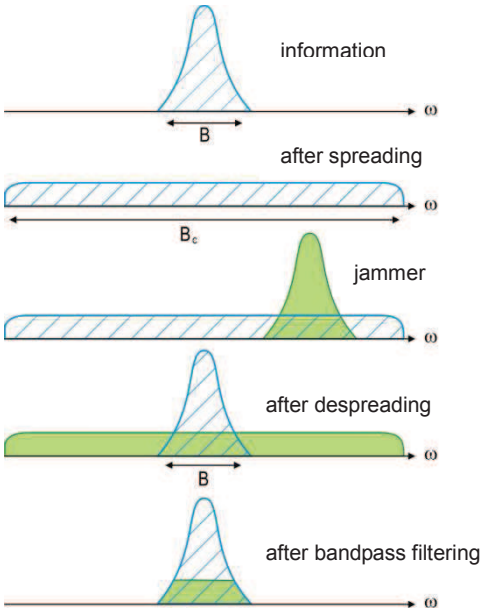
Operational security means that no danger for men and environment may emanate from production facilities. Below we are going to point out that operational and data security are tightly connected. This means that e.g. the transmission of defective or faked sensor data, leading to an erroneous evaluation of a reactor's state in a control center, are avoided or certainly recognized just as the transmission of defective or faked instructions to actors, that become, by means of incorrect actions, hazardous for operational staff or environment.

2 Transmission Security

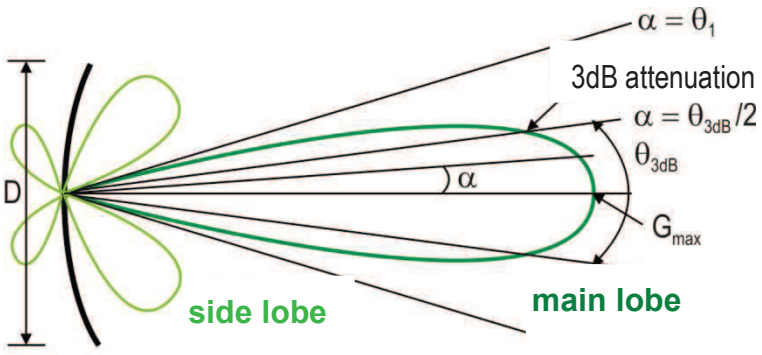
Transmission security is achieved by preventing or extenuating disturbances that may be traced back to the radio channel and that may impair communication. Transmission security requires the mastering of several technologies:

- In addition to the well-known effects like noise, multipath propagation, Doppler, attenuation, shadowing etc., the radio channel may be accidentally affected by production activities, e.g. from rotation machines or switching operations. In order to master such effects, an elaborate analysis of the current channel and, as a result of this, the application of perturbation resistant transmission methods becomes necessary.
- Protection against jammers is generally more difficult than protection against unintended disturbances because the offender may possibly have information about the employed transmission method (formatting, coding, modulation …) and uses it purposefully.
- Protection against spoofing may be achieved by authentication procedures, that certainly affect latency, or by application of other means (directional antennas, attenuation walls, short range devices …).

The following three technologies crucially contribute to the improvement of transmission security (c.f. figure 2). First of all robust transmission methods [5] are employed.



(a) Robust Transmission (Spread Spectrum)



(b) Trunked Radio (Directional Antenna)

$$\Delta \boldsymbol{E} = \mu_0 \varepsilon \varepsilon_0 \ddot{\boldsymbol{E}} + \mu_0 \sigma \dot{\boldsymbol{E}}$$

ε *Dielectric Constant*
σ *conductivity*

(c) Wave Equation (Absorption Walls)

Figure 2: Means for Transmission Security

These techniques, called spread spectrum technologies, use much higher transmission bandwidths than physically necessary. Herewith, resistance against intended as well as against unintended interferences is achieved. The application of trunked radio implies that information is spatially directed to its destination. This essentially makes wiretapping difficult. Last but not least, the wave equation's dependencies on the dielectric constant as well as on the propagation material's conductivity allow the design of absorption walls that may efficiently spatially limit the radio propagation.

3 Data Security

Data security algorithms and methods protect data and services against unauthorized access, alteration, or damage. We have to distinct active and passive attacks upon data security. As active attacks we identify in this connection denial of services, misuse of resources, spoofing (input of false data, modification of messages), and the disclosure of confidential information. Passive attacks are traffic analysis and wiretapping. Means of data security are identification of communications partners, authentication of messages, nonrepudiation of dispatch (e.g. by digital signature), access control of network subscribers, integrity, availability, jamming resistance, and interception resistance. Along with the ongoing digitalization, since the turn of the millennium cryptology evolved into an open science. This may easily be recognized by looking at the text books recently published about this subject [6-8]. However, scientific publications, especially in this area, often ignore application aspects.

Cryptology does not perform as an algorithm or as a device but as a system. This system must provide easy manageable and cost-efficient means for enciphering and deciphering by authorized users. Application of cryptology calls for a precise and nonambiguous definition of responsibilities (i.e. who may do what with the system?) The system must ensure that any intervention into its function by any nonauthorized person (or device) is extremely difficult, involved, and expensive. The people authorized for interventions into the system have to be trained as well as supervised continuously.

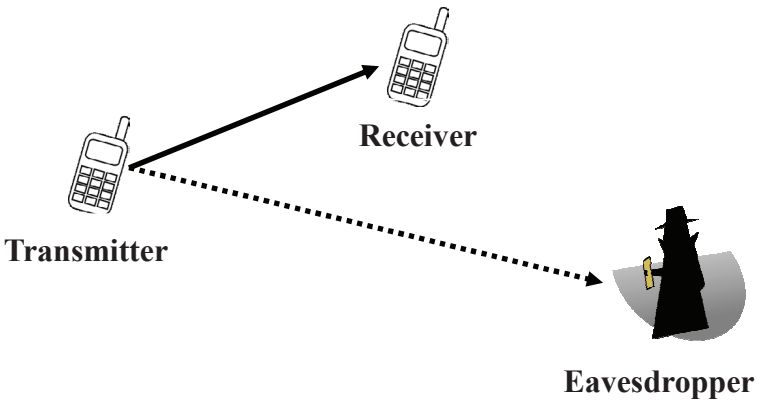


Figure 3: Physical Layer Security

In information theory, especially with respect to the requirement for low latencies of transmission systems, physical layer security is currently [9] under reinforced discus-

sion. The advantages publicized with this technology are that neither key exchange nor key management is necessary and no latency is introduced by enciphering or deciphering. Security solely bases upon channel state information. At this point, however, the deficits of physical layer security appear. First of all, physical layer security up to now produced just theoretical results. It remains blurry how to get information about channel states (particularly the state of the channel from the transmitter to the eavesdropper). What is known is that the channel from the transmitter to the (authorized) receiver has to have a higher capacity than that from the transmitter to the eavesdropper (c.f. figure 3). Here, we should recognize that there is a striking interrelationship to the methods discussed for transmission security (i.e. spread spectrum, trunked radio, absorption walls).

CONCLUSION

Radio communications should be applied in production facilities only if this is absolutely necessary, e.g. for connection of autonomous acting robots or of sensor-actor arrays that are mobile or must be reconfigured fast or frequently.

Different radio technologies are available for different transmission tasks (time critical/not time critical, low/high data volume …). At the top of the automation pyramid, well known technologies (e.g. WLAN) in ISM (industrial, scientific, medical) bands may be employed. Towards the bottom of the pyramid, customized radio technologies (with respect to latency, special formats …) and exclusively usable resources (frequencies) are demanded. Whether 5G is an option for radio communication in production lines is an open issue and has to be investigated.

If transmission and data security are important, the employment of jamming resistant transmission modes (spread spectrum technologies), trunked radio, and possibly mechanical protection by absorption walls or reflectors should be taken into consideration.

If crypto methods are applied, a precise strategy (hazard analysis, threat hierarchy, responsibilities etc.) becomes necessary. Moreover, the relevance of external consulting as well as expertise within the own organization gets paramount importance.

REFERENCES

[1] acatech: "Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0." White Paper, April 2013, gefördert vom Bundesministerium für Bildung und Forschung

[2] Jondral, F.K.: Nachrichtensysteme, 4. Auflage. J. Schlembach Fachverlag, Wilburgstetten 2011

[3] Deng, C. J.; Slezak, G. R.; MacCartney , Jr.; T. S. Rappaport: "Small wavelengths - big potential: millimeter wave propagation measurements for 5G." Microwave Journal, vol. 57, no. 11, 2014, pp. 4-12

[4] Andrews, J.G.; Buzzi, S.; Choi, W.; Hanly, S.V.; Lozano, A.; Soong, A.C.K.; Zhang, J.C.: "What Will 5G Be?" IEEE Journal on Selected Areas in Communications, Vol. 32, No. 6, June 2014, pp. 1065-1082

[5] Torrieri, D.J.: Principles of Secure Communication Systems. Artech House, Boston (MA) 1992
[6] Karpfinger, C.; Kiechle, H: Kryptologie. Vieweg + Teubner, Wiesbaden 2010
[7] Paar, C.; Pelzl, J.: Understanding Cryptography. Springer Verlag, Berlin Heidelberg 2010
[8] Baumslag,G.; Fine, B.; Kreuzer, M.: A Course in Mathematical Cryptography. Walter de Gruyter, Berlin Boston (MA) 2015
[9] Yener, A.; Ulukus, S.: "Wireless Physical Layer Security: Lessons Learned from Information Theory." Proceedings of the IEEE, Vol. 103, No. 10, October 2015, pp. 1814-1825