SECURE AND RELIABLE WIRELESS NETWORKING

THE IOT REVOLUTION FOR COMMERCIAL BUILDINGS

(photo: Shutterstock)

The IoT standard for wireless communication IP500 was developed to address the toughest demands in commercial buildings. With the EN pre-conformity, certified by the Association of Property Insurers (VdS), the IP500 standard positions itself in the wireless IoT market as a "hidden champion" for IoT applications for commercial buildings.

By Helmut Adamski and Witali Gisbrecht

With the recent successes of the IP500 Alliance [1] a new chapter in the IoT market for commercial buildings has started. Key manufacturers (global players) of security products started writing this chapter about ten years ago.

Just remember: At the time, other wireless IoT standards were trying to win over the IoT market. This has partly succeeded for the smart home market and is currently being tried in the wide area IoT market for smart city applications. Nevertheless, the gap between known wireless IoT systems for end users and the required standards in the commercial sector is enormous. Why? – Because technical challenges must work together in the overall picture of a wireless IoT platform. This means that different requirements must be supported by a wireless IoT platform at the same time; For example, a very low time delay (latency) in the IoT network and at the same time as a high data rate and transmission range, and this must be robust, secure and with a low energy budget for battery powered sensors. At first glance, this does not seem possible – but it is possible if the entire system is repeatedly coordinated between the application and the solution.

If a developer only wants to operate a certain IoT application, it is sufficient to concentrate on a few or maybe even one technical parameter, e.g. long range. However, if additional high data rates and low latency are required at the same time, other suitable wireless standards for this IoT application are not available as an IoT platform. Users experience this with other wireless IoT standards; they find themselves "caught" in a certain application when they want to implement new functions or expand the range of applications in the same IoT network.

IP500 ALLIANCE

The IP500 Alliance started its activities as an interest group with well-known global manufacturers after the IEEE standard 802.15.4 (2006) was ratified in 2007. The goal was to define from the system perspective of the user, regulations and applications for the most robust IoT system for commercial buildings based on the IEEE and IPv6 standards, and to develop and establish them with partners.

In May 2010, the IP500 Alliance formed in the historic VDI house in Berlin as a registered association (e.V.) and started its work.

The previous work was essentially characterized by three phases:

➔ 2005–2009 collaboration on the IEEE 802.15.4 and IPv6 standards and formation of the IP500 specification.

➔ 2010–2013 Presentation of the first IP500 wireless modules (CNX100) in products.

➔ From 2014 expansion of the product portfolio up to EN pre-conformity by VdS.

Today, the IP500 standard has leading manufacturers as members with voting status. Only they are authorized, with one voice per manufacturer, to select the appropriate technologies (wireless, network and infrastructure) which has brought the IP500 standard to fruition.

The IP500 Alliance is represented worldwide in Japan, India, the USA and Colombia by representatives with local technical support. The headquarters of the IP500 Alliance is in Berlin.

Selected partners and global service companies (service providers) have been accepted as "None Voting Members" and form the technical backbone, as well as providing technical support to manufacturers and providing the delivery of IP500 wireless modules worldwide.

The IP500 Alliance has additionally established a certification process in order to guarantee interoperability of the various IP500 networked OEM products.

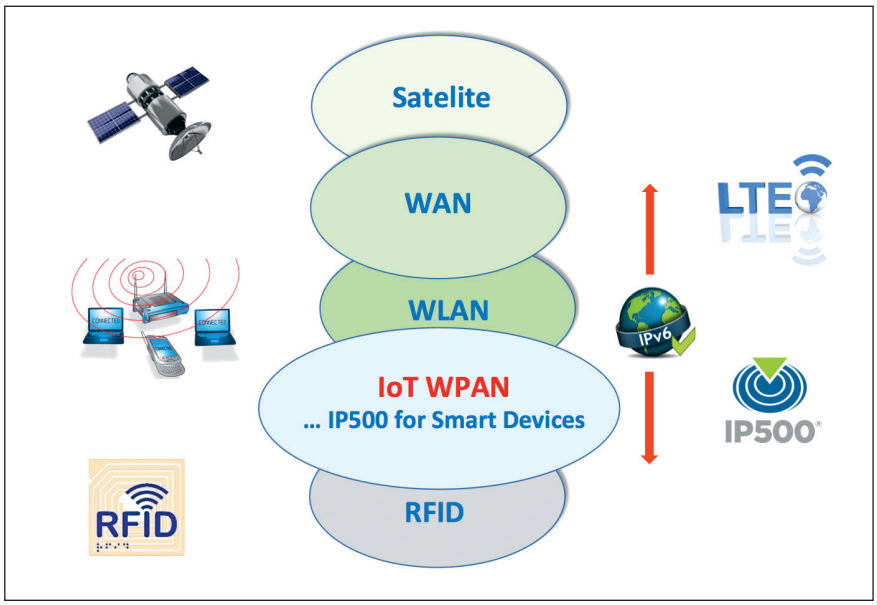

Figure 1. The IP500 Alliance wants to establish the IP500 standard as the dominant infrastructure for wireless IoT applications in commercial buildings. (image: IP500 Alliance)

THE IOT REVOLUTION CAN BEGIN

Since the beginning, the aim of the IP500 Alliance was to establish a wireless IoT platform that can network all smart sensor applications in a building in one and the same infrastructure. Comparable to the WLAN standard, which has established itself as the wireless standard for IT applications (Figure 1).

If you consider all the applications in commercial buildings, the security applications in an IoT network are of supreme importance. This requires interoperability of all IP500 products, no matter which manufacturer makes such sensing / acting devices.

The IP500 Alliance has consistently implemented this idea over the years and has defined the "best-in-class" wireless technology in a clever constellation with the network layer and the IoT

infrastructure into the specifications of the IP500 standard. These specs were then implemented by partners in products that are available today, e.g. wireless modules (CNX200, Figure 2) and gateways (GW260).

ENDURANCE AND STRONG PARTNERS PAY OFF

Through close cooperation with the certification bodies TÜV Rheinland and the Association of Property Insurers (VdS), the system view and important safety standards were kept in focus during the development of the IP500 standard. The result is now revolutionizing the IoT world, with maximum robustness, security, scalability and performance in wireless communication, in IoT network technology and its infrastructure.

Unaffected by other existing wireless IoT standards, which were developed primarily through the bottom-up strategy of the IC and network manufacturers, the IP500 Alliance with its members and partners has created the wireless IoT platform IP500 from the system level point of view. The IP500 standard has been brought into line with the security standards that are decisive for the system level and has been approved by the relevant certification bodies, e.g. the VdS. As a result, the IP500 standard is unique worldwide today in that it is able to provide a wireless IoT standard as a platform that can simultaneously meet the highest performance demands in the IoT network and is pre-

Figure 2. The IP500 wireless module CNX200 contains a microcontroller for the IP500 network stack and also the antenna. It fulfills all requirements for worldwide certification – for Europe (RED), India, Japan, USA (FCC), etc. (photo: IP500 Alliance)

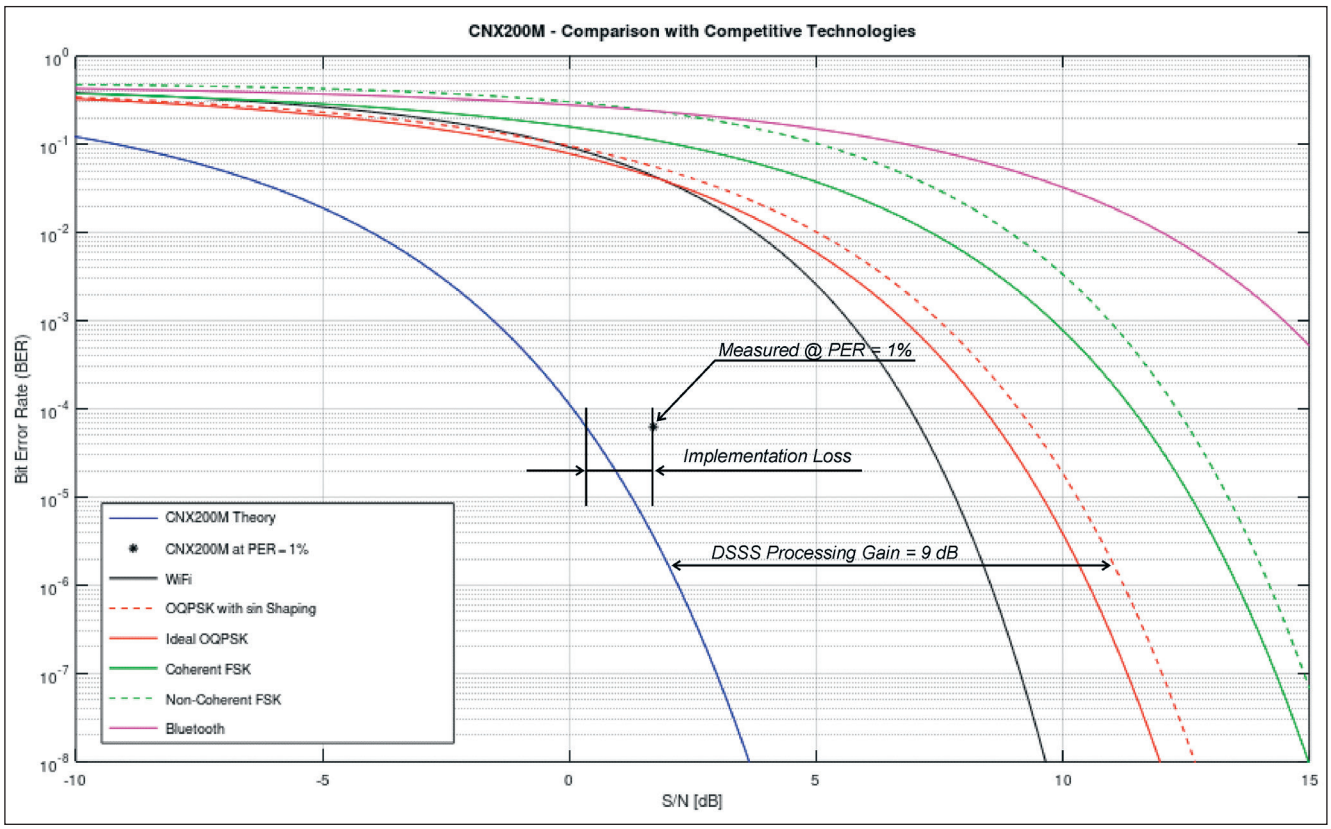

Figure 3. A comparison of the various wireless technologies shows that IP500 uses DNSS (Direct Spread Spectrum Sequence) — measured in the 2.4 GHz band and at 250 kbit/s — a process gain (processing gain) of 9 dB can realize and can work with a smaller signal-to-noise ratio (SNR). (image: IP500 Alliance)

compliant with European norms, e.g. EN 50131-5-3 [2].

DEMANDS OF USERS AND STANDARDS FOR WIRELESS-BASED SECURITY APPLICATIONS

From the beginning of development, the requirements and standards for critical applications in a commercial building – access control, fire detectors, etc. – were given priority in the IP500 standard. At the same time, the best-in-class IoT technologies were correlated with these requirements and embedded in the IP500 specification. This top-down process, from a system perspective, has ensured that the IP500 standard is guaranteed to meet the requirements of target applications. The main driving factors of these applications in commercial buildings are:

➔ Highest robustness of wireless connection in the commercial and industrial environments.

➔ Maximum security in data transmission, including key management.

➔ Short response time (latency) between sensors, actuators and the infrastructure (gateways).

➔ High data rate with a long wireless range.

➔ Scalable and robust meshed network architecture (mesh topology).

➔ Energy and battery management.

➔ Interoperability between all OEM products.

➔ Redundant network topology including gateways with databases.

Most standardization committees for wireless IoT systems have started from the perspective of RF (radio frequency) transceiver ICs (integrated chip), that is, "bottom up". This means that the IC manufacturers have followed the IEEE 802.15.4 (x) standard and developed the corresponding IoT ICs, as have the network manufacturers and the software developers. However, the layers for bit transmission (PHY – Physical) and security (MAC – Media Access Control) are only roughly described in the IEEE standard – and they have no relation to the application and its requirements.

Developers and users must observe and also comply with the legal requirements regarding frequency usage in the respective countries. However, these rules pose enormous challenges for wireless IoT systems.

If you look at the 2.4 GHz range, for example, it is very busy, especially through streaming applications with Wi-Fi and Bluetooth. In comparison, the sub-GHz range only offers narrow channels and the usable frequency bands differ from region to region.

To meet these challenges, the IP500 Alliance has specified a dual-band process that offers high data rates in the 2.4 GHz band and a long range in the sub-GHz range.

Due to the asynchronous, meshed dual-band network, additional robustness and redundancy for the transmission of sensor data is achieved even in a very difficult environments. The data packets are cryptographically encrypted so that the IP500 standard combines performance and security in a wireless IoT network.

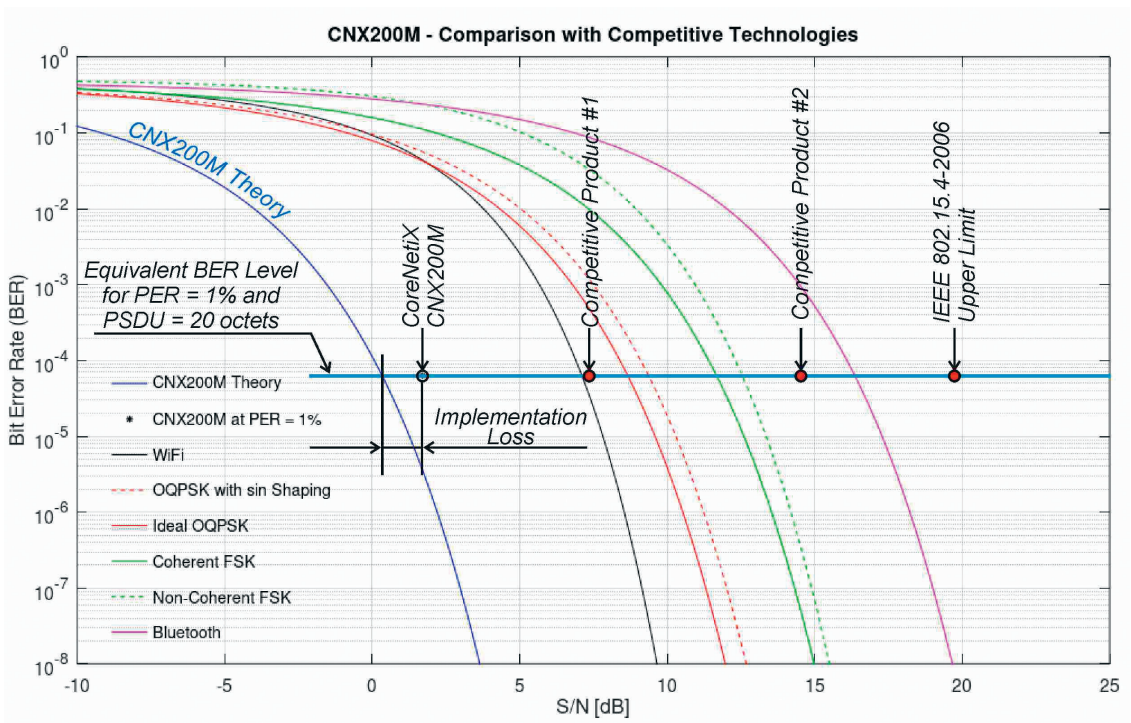

Figure 4. Comparison of the different wireless technologies – theoretical values and values of real implementations. The further left a technology, a product, can be placed on a horizontal, the better the signal-to-noise ratio. (image: IP500 Alliance)

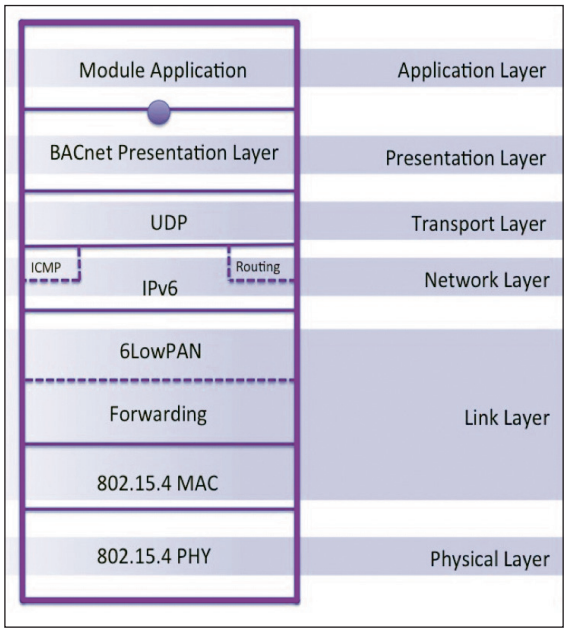

Figure 5. IP500 uses a finer subdivision of the data link layer than the previously known OSI model. (image: IP500 Alliance)

PRE-COMPLIANCE WITH EUROPEAN STANDARDS

The VdS label is a seal of quality and is the most important quality indicator for those responsible for safety security systems when deciding, purchasing, integrating and installing security technology and security services – especially in commercial buildings. Organized in association with other European countries, the Association of Property Insurers is also recognized worldwide in its sphere of activity. A VdS certificate allows security-relevant systems to be approved after they have been checked for security, reliability and more. The aim is to use the tested techniques to reduce the risk of damage and ultimately to prevent damage prematurely. The technical hurdles are enormous in order to obtain a VdS certified product and system. If a manufacturer is interested in having a product certified with a wireless link, this manufacturer must make large investments in order to ultimately develop its proprietary wireless technology for safety-critical applications. As it is important that there is no interference with safety-related applications, this wireless technology still has to pass lengthy.

In years of cooperation with the VdS, the IP500 Alliance has successfully developed a robust and reliable wireless IoT standard in a first step of pre-conformity – according to EN 50131-5-3 [2] – for some important applications required to establish IoT platform. This pre-conformity allows the members of the IP500 Alliance tocertify their products, which are equipped with an IP500 wireless module (CNX200), without additional development effort and other pre-conformity testing for the VdS. This results in considerable time and cost savings for the manufacturer.

WIRELESS TECHNOLOGY FOR THE HIGHEST DEMANDS

In order to meet all requirements to achieve conformity and interoperability, the members and partners of the IP500 Alliance have coordinated and developed the entire IP500 system at all three levels (layers). The three levels are:

➔ 1. Wireless transmission (PHY / MAC).

➔ 2. Network stack and application.

➔ 3. Protocol, infrastructure, gateway and database.

The first two levels – wireless transmission and network stack – are closely coordinated and essentially form a unit, as the example of true dual-band technology with mesh topology shows. In this case, the PHY level provides both frequencies simultaneously and the network stack level automatically routes the data packets depending on the interference in one of the bands to the target node, a gateway or a terminal device.

ADVANTAGES OF THE IP500 STANDARD ON THE WIRELESS LEVEL

Due to the requirements from the system level, OQPSK (Offset Quadrature Phase-Shift Keying) was chosen for modulation. The basis for this is the IEEE standard 802.15.4 (2006), which provides OQSPK for higher data rates in the 2.4 GHz band. Due to the system requirements of the security applications, the simultaneous use of both bands – Sub-GHz and 2.4 GHz – was specified in the IP500 standard. This created a very high level of robustness against interference.

Combined with the asynchronous meshing process of the network stack, the IP500-PHY and network stack can avoid different interferences – both in the case of interference on the frequency level and in the event of interference on the routing path.

The measurement results in Figures 3 and 4, measured in a real environment with high interference, as are typical for buildings, tunnels or metallic environments (aircraft and ships), provide an insight into the robustness of the IP500 standard compared to other wireless standards that are used worldwide.

It is advantageous to have a smaller signal-to-noise ratio (SNR) (position of the

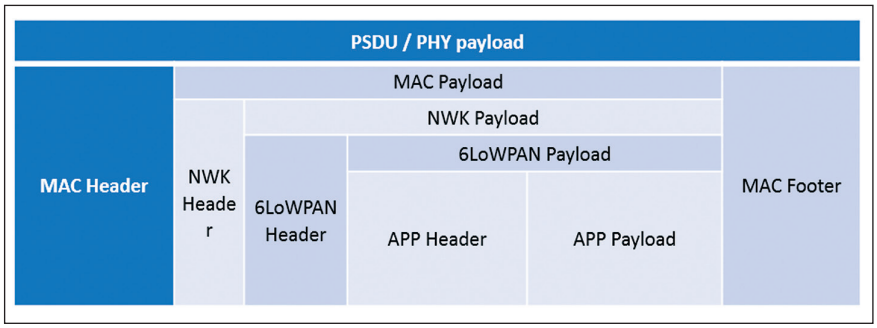

Figure 6. The application data is nested several times in packets in the higher levels of the IP500 protocol before it is sent out by wireless. (image: IP500 Alliance)

MAC Header					MAC Payload	MAC Footer
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source Address	Nutzdaten	Prüfsumme
2 Byte	1 Byte	2 Byte	2 Byte	2 Byte	variabel	2 Byte

Figure 7. IP500 uses the MAC frame of the IEEE 802.15.4 standard (2006). (Image: IP500 Alliance)

NWK Header						
Protocol ID	Header Length	Hop List	Payload Type	Payload Length	Sequence Number	CRC16
1 Byte	1 Byte	12 Byte	1 Byte	1 Byte	4 Byte	2 Byte

Figure 8. The header of the network data packet for IP500 (NWK header) contains the information for the routing (hop list). (Image: IP500 Alliance)

Hop List						
Type	Length	Destination	Source	Hop 1	Hop 2	Hop 3
1 Byte	1 Byte	2 Byte	2 Byte	2 Byte	2 Byte	2 Byte

Figure 9. The hop list specifies the routing of a wireless data packet through the IP500 network. It is generated by the source node by considering the shortest connection to the target node. (source: IP500 Alliance)

product further to the left in Figure 4) for several reasons:

➔ Higher link budget

Given the signal-to-noise ratio, the number of bits received incorrectly is reduced. For example: for SNR = 4 dB, the received messages from the IP500 wireless module CNX200M are error-free in practice.

A bit error rate BER = 10^{-6} means one bad bit per million received bits. In comparison, for the same SNR = 4 dB, the BER for Wi-Fi = 0.01, that is one bad bit per 100 bits received.

Under such conditions (SNR = 4 dB), wireless standards such as Wi-Fi, Bluetooth or LoRa cannot be used practically.

➔ Reduce energy consumption – reliable transmission requires less RF transmission power with a small SNR.

A closer look at the test results shows that the known wireless standards cannot be used extensively as a wireless IoT platform in a commercial or industrial environment, because lack of performance, robustness or security can

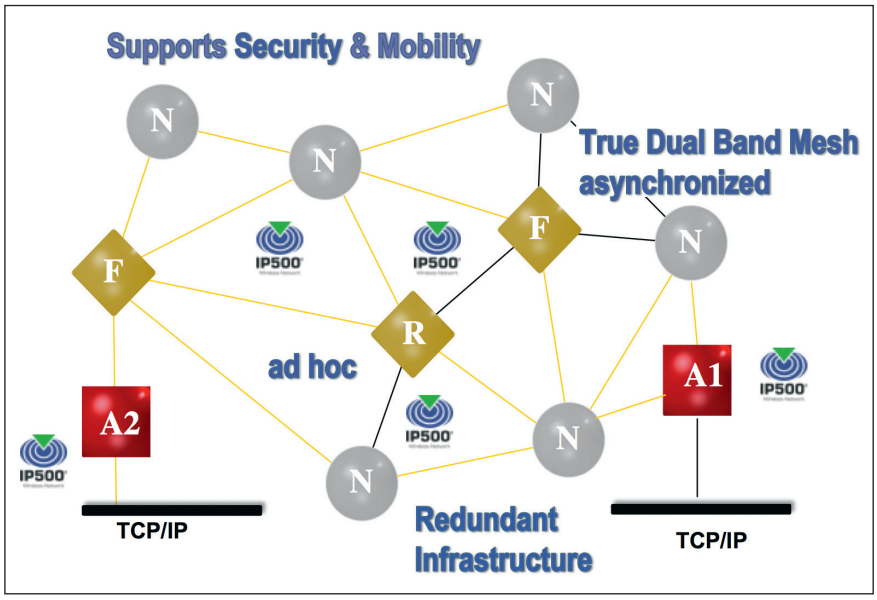

Figure 10: The IP500 network offers security, reliability and robustness through redundancy – with two gateways and operation in two independent frequency bands. (Image: IP500 Alliance)

significantly disrupt the IoT business processes.

THE NETWORK LEVEL OF THE IP500 STANDARD

The construction of the IP500 network stack is responsible for the topology of the network, the scalability, the latency and the encryption of the data – and thus for the robustness and security in the entire IP500 network. Figure 5 shows the IP500 structure based on the well-known OSI model.

The asynchronous transmission method was selected in accordance with the IEEE 802.15.4 standard. Figure 6 shows the structure of a complete IP500 wireless data packet.

The main functions of the network are:

➔ Structure of the data packets (frames) and file headers (headers).

➔ Forwarding of the packets through the asynchronous mesh network using the routing table.

➔ Securing and encryption of data packets.

ROUTING BY HOP LIST

The NWK header (Figure 8) defines the "Hop List", a given route through the network (Figure 9). The message from the application is organized in the packet and routed through the network according to the hop list – in dual band and via the switching nodes of the meshed network. The hop list delivers the next hop thanks to the asynchronous meshed network with minimal computing effort – an important skill that ensures low latency and low energy consumption of the individual network nodes (sensors). The node sending a message determines the hop list for the data packet from its routing table by forming the shortest route. This process offers the end user a self-healing, self-configuring mesh network with the lowest latency.

All messages of the IP500 application layer are sent in both directions between the nodes and the gateway, which is why each node and the gateway knows the route without any computing effort. Additionally the most recently received messages are also stored in the gateway. The use of alternative routes in the meshed network, together with the redundancy at the frequency level, ensures high reliability and low latency when interference occurs, which has been confirmed by VdS as the basis for preconformity with the European standards [2].

SECURITY AND ENCRYPTION IN THE IP500 NETWORK

The calculation of the AES128 key for symmetrical encryption and decryption of the message is based on the sequence number of the message and a master key, which is carried out by an asymmetric ECDH method (Elliptic-curve Diffie-Hellman) between each individual node and the Gateway. End-to-end encryption ensures that the messages cannot be intercepted or forged by forwarding nodes. Using the AES128 key once for a single message increases the security of the IP500 network. HS

Literature

[1] IP500 Alliance, www.IP500alliance.org

[2] DIN EN 50131-5-3: 2017-09; VDE 0830-2-5-3: 2017-09: Alarm systems - Intrusion and hold-up systems - Part 5-3: Requirements for transmission devices, wireless frequency technologies use; German version EN 50131-5-3: 2017.

HELMUT ADAMSKI

is an IoT pioneer and currently leads the IP500 Alliance e.V. as CEO and chairman. He has more than 25 years of experience in the high-tech industry, with a focus on IoT and IT network applications, radio ICs and security applications for buildings and premises. Adamski holds an engineering degree in electronics and attended Executive/MBA programs at the Institute of Excellence, San Diego, and Stanford University, California, USA.

helmut.adamski@ip500alliance.org

WITALI GISBRECHT

is a specialist in the development of embedded software for network stacks, security methods and gateway architectures. He graduated from the University of Paderborn in 2007 with a Bachelor of Science degree in Computer Science.