Secure, scalable, redundant, interoperable and reliable wireless network -
THE IoT REVOLUTION FOR COMMERCIAL BUILDINGS and smart city

IP500® > a dual band, asynchron, highly encrypted mesh network which serves as a wireless communication base for ALL sensor and actor communication in an IoT network; from fire detection to access and comfort control up to mobility information and much more; even drone and robot guidance with its "indoor GPS" possibilities!

THE IOT REVOLUTION CAN BEGIN

Of all applications in commercial buildings, the security applications in an IoT network are of supreme importance. Looking at that, a wireless network, one first needs to look at the necessary demands of these sensors and regulations in regards of communication.
But in an ideal case one wants to operate all sensors and communication relevant to a smart building or smart city within ONE wireless network.

This requires full interoperability of all IP500® products, no matter which manufacturer makes such sensing / acting product.

The IP500® Alliance – founded from 2005-2009 from ABI-Sicherheitssystem, Belimo, Bosch Security Systems, JOB Detectomat, Dorma, Gunnebo, Hekatron, Honeywell, LINK, Siemens Building Technologies Division, SimonsVoss, STG-BEIKIRCH, Tyco, UTC Fire & Security, WAGO, Xtralis – has defined and finally delivered a network standard that serves all these necessities.

IP500® has implemented this idea over the last years and has like this defined "best-in-class" Wireless technology with a network layer and IoT infrastructure with the specifications that all these members have defined as "IP500® " standard.

These specifications were then implemented by partners in products that are available today, e.g. Wireless modules with further PIP chips coming very soon.

ENDURANCE AND STRONG PARTNERS

Due to cooperation with the certification bodies TÜV Rheinland and the Association of Property insurance companies (VdS), the focus during development was set on system view and important safety standards.

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.

The IP500® standard is aligned with the security standards which are critical for the system level and was approved by the relevant certification bodies, e.g. the VdS, TÜV Rheinland.
As a result, the IP500® standard is unique worldwide today and 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-compliant with European, American and Japanese norms.

DEMANDS OF USERS AND STANDARDS FOR WIRELESS-BASED SECURITY APPLICATIONS
From the beginning 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, other features where incorporated and coordinated with these requirements and embedded in the IP500® specification to build a "best-in-class" wireless communication IoT technology.

The "top-down" process, from a system perspective, has ensured that the IP500® standard is guaranteed to meet the requirements of all possible target applications from security to comfort and high speed with minimum energy usage.

The main driving factors of these applications in commercial buildings are:

- Highest robustness of the wireless connection in the commercial and industrial environment.
- Maximum security in data transmission, including key management.
- Short response time (latency) between sensors, actuators and the infrastructure (gateways).
- High data rate and at the same time a long wireless range.
- Scalable and robust, asynchron meshed network architecture (mesh topology).
- Intelligent Energy and battery management.
- Interoperability between all OEM products.
- Redundant network topology including gateways with databases that allow change of gateways WITHOUT shutting down the system.

PRE-COMPLIANCE WITH EUROPEAN STANDARDS

The VdS label is a worldwide seal of quality. It is one of the most important quality indicator for those responsible for deciding, purchasing, integrating and installing security & safety technology services - especially in commercial buildings.
In years of cooperation with the VdS, the IP500® Alliance has successfully developed a robust and reliable wireless IoT standard in of pre-conformity - according to EN 50131-5-3 [2].
This pre-conformity allows the members of the IP500® Alliance to pass their products, which are equipped with a IP500® Wireless module (CNX200), without additional development effort and other pre-conformity test for the VdS test. This results in considerable time and cost savings for the manufacturer and makes it easy to invite all OEM to integrate their products in the same IP500® wireless network.

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.

WIRELESS TECHNOLOGY FOR THE HIGHEST DEMANDS

In order to meet all requirements at the same time that conformity and interoperability is achieved, the members and partners of the IP500® Alliance have coordinated and developed the entire IP500® system at all three levels (layers).

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. 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.

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) [3] 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.