IP500 – The IoT Revolution – Interoperability between Comfort- & Security-Applications in Commercial Buildings.

Many of us drive cars and have a good grasp of what functions make sense in a car and when we wouldn't drive a car at all. For example, we wouldn't get into a car if there would be no seat belt or ABS system with disc brakes (instead of drum brakes). In other words, would you use a car without air-conditioning if you work in Dubai? On the other hand, after a few years in Alaska you would have forgotten where to turn the air conditioning on! The "message" is that most cars are built for the whole world and not just for Dubai or Alaska! If we pull this metaphor into the IoT wireless world, a car in a road network can also be seen as a data packet in a wireless network that has to meet certain requirements. As in the road network, the data packet experiences the same problems, it gets stuck in the data congestion (not enough bandwidth) and therefore arrives too late or never at all. The security aspects and robustness in a data network are discussed in detail later when it comes to security requirements or collisions in a robust commercial building IoT infrastructure.

In issue no. 2 of the magazine "Elektronik" 2020, issued on 23rd Jan. 2020, as well as in "Elektronik International – edition embedded world / in English", the title "The IoT Revolution" made it clear that it isn't important for an IoT wireless network for commercial buildings to "only" offer one or two "performance aspects, i.e. "long range and long battery life", but rather has to simultaneously fulfill far more critical performance and security aspects.

Today, no other wireless standard has really succeeded in offering that!

IoT Wireless platform designed from top down

The secret is very simple and makes sense to everyone when you think about it. The solution is that when designing an "embedded system", i.e. a wireless chip, all critical aspects that are important from the regulatory, user's and system level point of view, must be included right from the beginning of the chip-design. Then it depends upon who decides what the critical aspects are ... the car manufacturer or the user!? The car maker, in other words in the wireless IoT world the chip manufacturers, usually incorporates the technology that he already has in his portfolio,using his currently available "implementation know-how"!

The car industry is pretty good in that sense. Right from the beginning of the development they work closely with the authorities for the infrastructure and the technical safety requirements for a car (like TÜV in Germany). They also look at the system and user level to ensure comfort and performance requirements are going to be met. If you do not pay attention to this in the design of any kind of product, then the products (in our case the wireless solutions chip / complete module) gets stuck in few applications and the potential of the global market is going to be limited! In such case, having a limited performance portfolio of a wireless chip/module, you cannot consider it to be an IoT wireless platform at all!

If you talk about a wireless IoT platform for all applications in a commercial building, you need to meet all the critical aspects in such IoT network. This article gives you the answer and explains why specific requirements, like "high data rate and robustness, at the same time very low latency time of data transmission" have an enormous impact on the individual applications, its sensors and actors.

Common wireless IoT platform support planner tools

So, let's start from the system perspective of a planner or system integrator into a planning process of the entire IoT infrastructure and the related applications for a commercial building. The goal is to offer the end user a wireless IoT network which is concurrently secure, scalable and very robust / reliable, and all at a sustainable "cost-of-ownership" ratio.

In the planning process of commercial buildings, planners are nowadays using planning tools like a BIM (Building-Information-Modeling) tool in combination with installation guideline tools such as the VDI installation guideline, which is used in Germany. The reference to the BIM system in this planning phase is described in more detail in a following paragraph. Actually, the planner is going through the same process, when he is planning an IT / WiFi based infrastructure for high data rates applications. In this case he also does not have to care about the end products which are connected to the WiFi infrastructure. So if an IoT sensor network infrastructure fulfills all the requirements for all applications, it will then be easy to connect security and comfort applications in the same IoT network without great effort and interoperability issues.

That means once the wireless IoT infrastructure for all sensors (with full coverage in the entire commercial building) has been completed in the first planning phase, the planner will then usually start to plan the security-relevant applications (sensors & actors). Without any changes or new gateways, he then considers all the other applications into his following plans. We call this "Freedom in Design" at the application level, because the planner is free in his design of all the sensor and actor applications using the same IP500 wireless IoT platform / infrastructure in the entire building. As a result, it lowers system complexity with a shorter design / planning time. Also the installation time is much shorter, because the installation guidelines (i.e. the VDI 3813 for HAVC & Lighting and access control) have pre-defined all the necessary information detailing how to connect and install the IP500 infrastructure with the OEM (Original Equipment Manufacturers) Products (sensor / actor) as well as the communication format to the control unit interface / BMS.

The planner can also address end-user requests (i.e. from facility management or security companies) even after completion of the construction. On top of this the adaptation of new innovative application ideas during the lifetime of the building can be easily adapted or extended (retrofit) without great effort and cost.

IoT platforms today and in the future!

Over the past decades many wireless-based IoT solutions, i.e. ZigBee, Z-Wave, Enocean, ULE and many more, have tried to establish themselves as a global wireless IoT standard. LoRa, SigFox, BLE, 5G, NBIoT or others have also made great effort to accomplish the same. The desire of these individual wireless technologies to address a wide range of applications outside of their core technology competence is great, but also understandable.

Today you can buy IoT products in the SmartHome market based on point-to-point (peer-to-peer) or limited mesh wireless network technologies. This is “good enough” for consumer or SmartHome applications. But this is not the case for commercial building installations, where many more IoT devices (1000s) in a much large area must interoperate while being challenged by high interference from other wireless / electrical sources. In addition, many different applications must be interoperable at the RF (Radio Frequency), network (mesh) and functional (Protocol) level, according to regulations and requirements of institutions or insurance companies (VdS) who demand the highest robustness and security with lowest latency time of the wireless IoT network for mission critical applications. Or, to explain it in another way, if a wireless technology simply cannot operate an application, like a door or light control, because of a very high latency time over 6 seconds per transmission, as it is the case with LongRang wireless technologies, the goal of a “IoT wireless platform” can no longer be achieved!

OEMs need a common wireless IoT platform to address WPAN market

On the other hand many OEM’s of single products or complete building automation systems had,at the time, from around the year 2000+, more or less no other choice than using off-the-shelf wireless modules (so a car without air-condition) or even to develop their own proprietary RF solutions (RF module and network). Some OEM’s are focused on security applications, and therefore they must comply with the security-relevant requirements (e.g. like "VdS" in Europe or “UL” in USA). In this case, adding wireless communication to their security products portfolio, they had to use an off-the-shelf RF chip with a lot of additional development work (HW & SW) and additional certification effort. However, some of these OEM’s then continued with a wired solution. It is obvious that this way (proprietary wireless network) is not a long-term solution either. We don't need to discuss an example with the car – it would be like every city having its own street width where only certain cars from a single manufacturer could drive on these streets!

So, these global OEM’s / manufacturers are also very interested in addressing the enormous IoT WPAN market and expending their business opportunities / volume. As it is the case with WiFi or 4G / 5G, that is only possible with common wireless IoT platform providing a robust, secure and powerful technology, included in a common wireless (RF) module / chip.

The certified and turn-key “IP500 / CNX200 Module” provides such a wireless IoT platform for all WPAN applications. The easy integration of the IP500 / CNX200 Module saves the OEM’s a lot of development costs, time and above all a long and expensive certification process for their OEM products according to e.g. RED, or FCC for the related bands (Sub-GHz and 2.4 GHz).

Details of the IP500 / CNX200 Module are described in the 2nd edition of the magazine Elektronik or can be obtained by visiting the IP500 Alliance website (www.ip500alliance.org).

Due to the pre-conformity (highest robustness and performance) certification by official test authorities, the “IP500 / CNX200” wireless module therefore enables the OEM’s to develop any IoT product for a commercial building. This enables the OEM’s to expend into a much wider business scope in the global IoT WPAM market. It also allows the OEM’s to cooperate much easier with complementary OEM solutions in large SmartBuilding projects, due to the interoperability at IP500 RF chip, network and infrastructure level.

This means that the OEM’s can expand their product portfolio and system faster (time to market) at lower cost to address the enormous potential of business opportunity in the rapidly growing global IoT WPAN market. The following graph shows the enormous growth rate and total potential that can be addressed with a secure and high-performance IoT wireless platform.

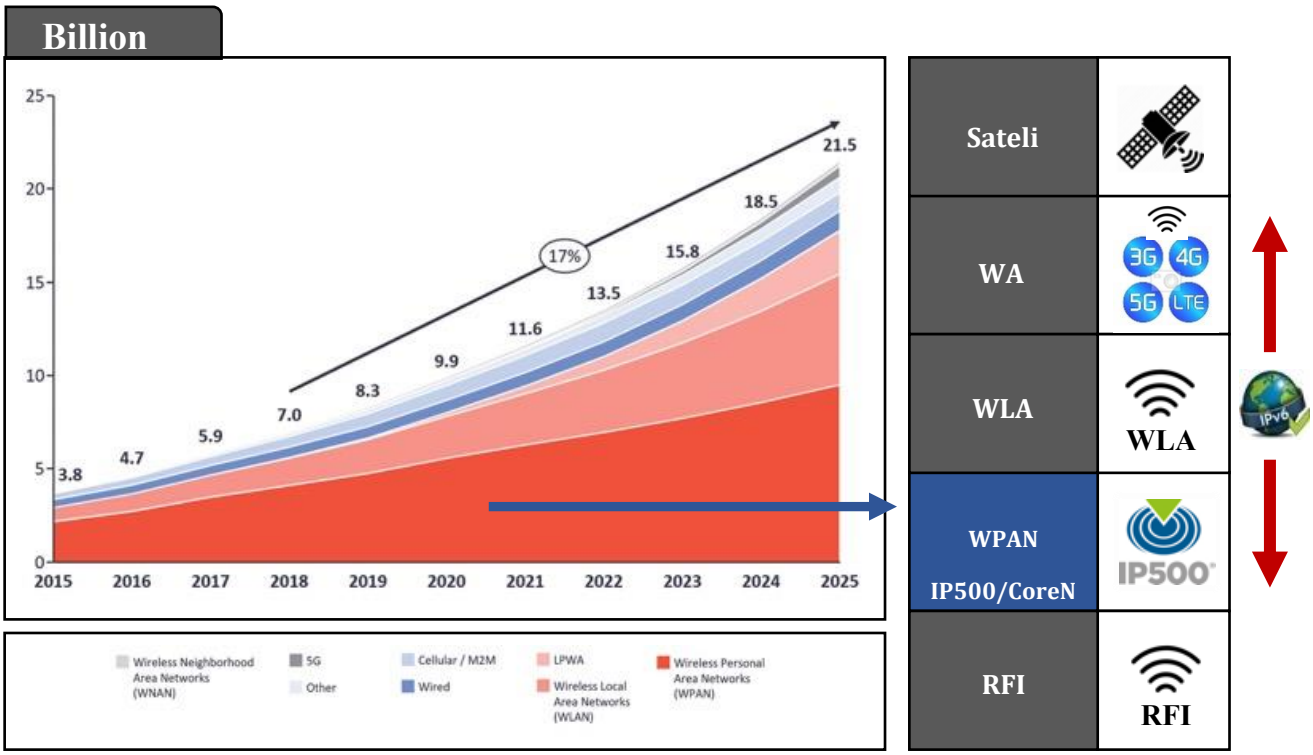


Figure 1: IP500 - the IoT platform for WPAN applications in commercial buildings - IoT 4.0

As already mentioned, from the beginning (that was around the year 2000) some of the IoT Alliances tried to establish themselves as an IoT standard for specific applications. The main target market was the "SmartHome" using the 2.4GHz (or 1.8GHz DECT) band, or Sub-GHz without IPv6. Then the chip manufacturers developed the corresponding RF chips according to IEEE802.15.4 b .. g .. standards, based on mainly FSK modulation. If we go back briefly to our example with the car, it would look like this. The car manufacturers would build an engine (RF chip) that is only designed for the city (SmartHome), can drive 50 km / h and has a range of, let’s say, 50 kilometers. Without spinning this further, it becomes clear that this would not lead to the goal if the car (i.e. the IoT RF solution) were built with such a performance

limitation. It would be as if a car had not been designed for driving on a highway - so had no capability of high speed (data rate), no long range, nor a short braking distances (latency time).

The future of wireless IoT platforms (IoT 4.0)

The IP500 Alliance started to work on the IP500 IoT platform a little more than 10 years ago. The goal was to establish a wireless IoT platform with the most important security and performance aspects for all IoT sensors and actors applications in commercial buildings. The entry hurdle was set very high, to provide a wireless standard that also met the requirements of the "Security" (intrusion) and "Safety" (fire) (as reference - EN norms by VdS pre-conformity for Europe or UL for USA) applications at the same time. These applications have the toughest commercial building installation. So, related to our example with the car or truck, it has to be able to pass under the lowest bridge.

All the hard work of the IP500 members and partners took a lot of time (over 10 years) and effort. But all the effort paid off, because the combination of leading wireless network and newest chip technologies has enabled the IP500 Alliance to provide the "best-in-class" wireless IoT platform today.

“The IoT Revolution – IoT 4.0” has begun!

The chip industry, using <20nm silicon structure technology and also cost-effective micro controller designs with parallel processing capability, with an high integration level resulting in a small chip area of less than 1-2 square millimeters, make such competitive and highly integrated RF chip / solutions possible. Understanding how powerful chip technology is today, as an example, just look at how knowing the user requirements and integrating them in the chips right at the beginning of the products design has revolutionized laptops and smartphones. , ,.

The following illustration (Figure 2.) shows the division of the IoT applications into 4 main areas, which are combined under the term "IoT - Internet of Thing 4.0". Each of these 4 application areas has special requirements of the applications for wireless networking, which must also be synchronized at all levels of the IoT wireless module (RF, network and infrastructure).

As already indicated, the IP500 Alliance had these requirements in focus from the start and was the only wireless standard in the world to take safety and security into account.

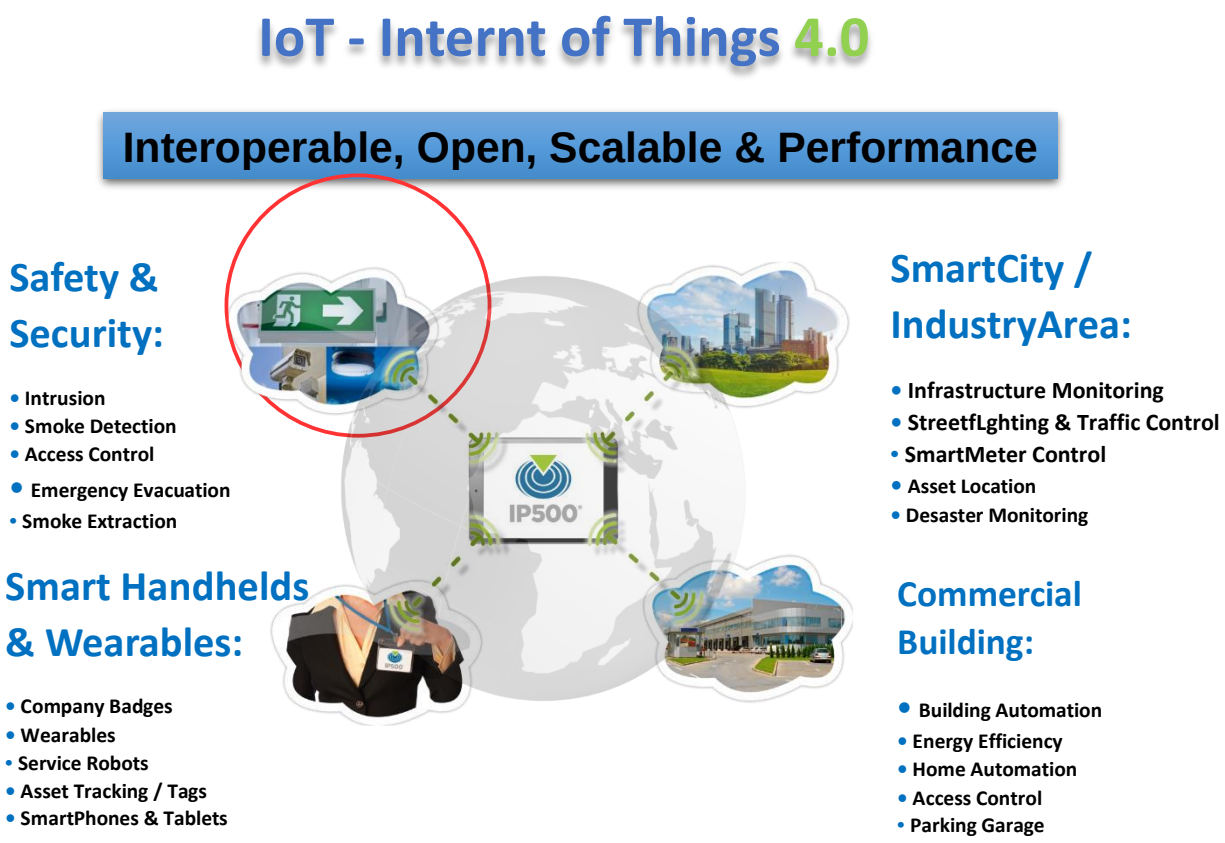


Figure 2: As a wireless platform, IP500 addresses the 4 main application fields - IoT 4.0

If you go into each IoT application area in detail, it becomes clear that many IoT wireless standards only cover specific / imitated limited range of applications and therefore they cannot be used as the "IoT wireless platform 4.0".

If we look into the near future of a commercial building (i.e. hotel or hospitals) and the desire to lower cost or improve comfort and serviceability, mobility will become an important feature. The requirements for supporting mobile devices (like a badge for people or robots, or asset tracking of inventory and valuable goods) in buildings is going to be part of the IP500 wireless platform.

The following list shows the most important wireless properties that must be fulfilled in the following application areas:

Smart City / Grid:

This refers to applications such as metering (electricity / gas / water), street lighting, parking station and container tracking, disaster and agricultural monitoring, asset tracking and traffic control.

Important requirements for the wireless part:
Long Range (500 - 1000 meters) and High Security of the communication

Smart Facility / Home:

This refers to applications such as access control / door, air conditioning & HAVC, lighting, asset tracking, and elevator control.

Important requirements for the wireless part:
High robustness, security and high data rate / bandwidth, low latency, scalability / mesh network

Smart handhelds / wearables:

This refers to the applications such as a badge or wearable items for people and robots, asset tracking and access control.

Important requirements for the wireless part:
Low latency, long battery life, high security

Security & Safety:

Applications such as intrusion / access control, fire and smoke extraction and evacuation.

Important requirements for the wireless part:
Safety and Security Regulations / Requirements means high security, performance and robustness at low latency

For whatever reason, some of these IoT sensor applications today have a “hidden champion” for wireless technology. For example:

a.) SmartCity / Industry Area: LoRa or SigFox.
b.) Commercial Building & Home: Z-Wave, and ZigBee, sometimes BLE.
c.) Handhelds / Wearables: BLE.
d.) Safety & Security: proprietary wireless solutions.

If you try to get all these wireless technologies under one roof at RF & protocol module level, a system architect quickly realizes that it is not easy or even not possible! Each solution is so different (at RF and protocol, IPv6, security mechanisms etc.) that networking of the respective interoperability of OEM products is then only possible at the IT (gateway) level. Imagine that with WiFi!

To take another example than just the cars - we will not be able to marry a giraffe to a mouse. As we know, incompatible networks / gateways drive up the complexity, installation and maintenance costs of an IoT infrastructure. If SW updates come into play over lifetime of a building, the handling and maintenance of such IoT system is going to be very costly and requires a huge effort and technical know-how.

The IP500 / CNX200 Module is the only IoT wireless platform which is pre-conforming with security norms (EN 50131-5-3) and is therefore able to addresses comfort **AND** security applications for commercial buildings with the same RF Module. This unique position of the IP500 / CNX200 Module has been confirmed by official test houses (TÜV Rheinland and VdS)!

Image 3: IP500 - The wireless chips can only be used universally from top-down, never bottom-up!

Because of this pre-conformity, the IP500 / CNX200 Module can also be used in simple applications, like temperature, lighting. Of course the module price is driven by volumes. So new combinations and full interoperability between comfort and security applications are now possible.

However, a wireless module without pre-conformity for safety & security applications cannot just be integrated in an OEM solution for safety & security applications for commercial buildings. If an OEM still wants to develop such an “of-the-shelf” wireless module, additional development efforts and lengthy certification and conformity tests are required. Then such OEM product would be automatically pretty much a proprietary solution and would not interoperable with complementary IoT solutions.

Influence of the IoT wireless technology / platform on a BIM system!

Let’s discuss why these key elements of a wireless IoT module, referring to Pre-Conformity (VdS), performance, security and interoperability, have a big influence at the IoT system level and therefore have a major impact on operations cost, security and comfort of a large commercial building for the planners, systems integrators and end-user.

If you take all the mentioned requirements into account, especially looked from the system level or end user (incl. planner and installer) point of view, then there is major requirement for using planning and installation tools for large commercial buildings. Because in a large installation, all the applications comfort (HVAC, lighting) and security (access control, intrusion, fire etc.) should be combined in such a modular planner tool, like a BIM (Building-Information Modeling) tool. A BIM tool is then basically based on the assumption that interoperability between all applications at wireless (RF), network, protocol and infrastructure level is guaranteed. So customized wireless solutions and different network protocols / gateways are basically killing such model, or at least make the planning process much more complicated.

If the interoperability and the requested performance of the IP500 OEM products and infrastructure are integrated in the BIM data base, the BIM tool is then able to place the IP500 gateways in an optimal location for full coverage in the entire building. Then the planner can is able to create a 3D BIM Model of the entire building with all the requested IoT applications connected to the same IP500 infrastructure.

The 3D BIM Model has the huge advantage for a planner, system integrator, the installer and end-user because they can simulate all the IoT applications and the interoperability at an early stage of the planning and construction process. Making changes or adding new applications is very easy at that planning stage.

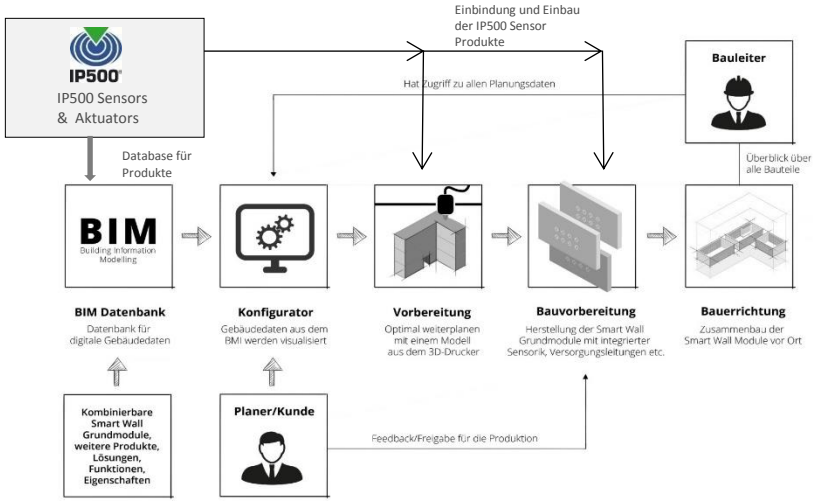
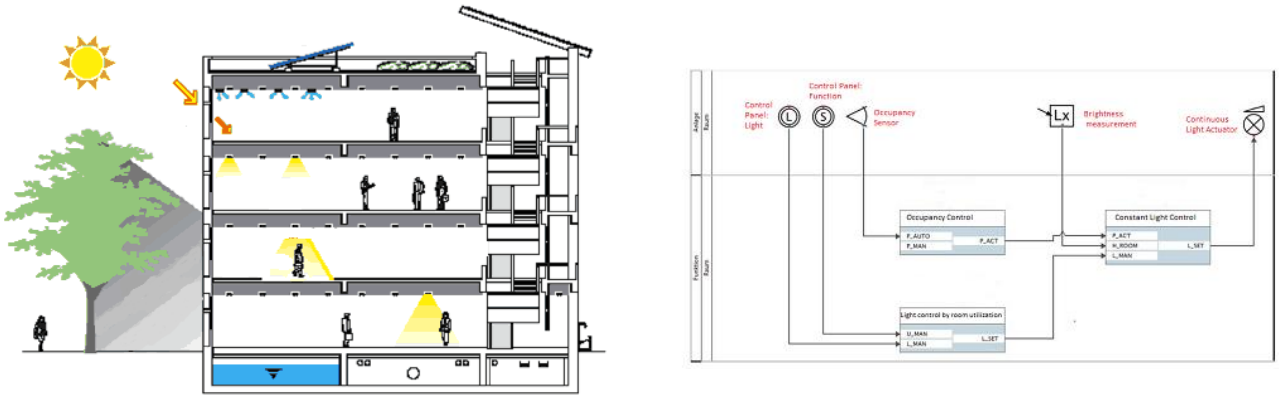


Image 4: BIM modeling tool for planning a commercial building

Integration of the IP500 IoT networks in installation guideline (VDI)!

As soon as the planner has the appropriate BIM model ready, then he synchronizes all the IoT system and product information with the installation guidelines. This transmission in the installation guideline requires a fully interoperability and scalability at the sensor, actor and infrastructure level. Therefore, the IP500 Alliance has worked closely with the planners, system integrators and installers to make sure, that the IP500 wireless platform provides this important base.

Having the comfort and security applications in the same installation guideline (like VDI 3813 for HVAC, lighting and security) offers an enormous advantage for the planner and installer right from the beginning of the process. Since the planners no longer have to deal with various gateways for different IoT wireless networks nor with non-compatible protocols and performance issue, he can use pre-specified symbols and combined functions for both “comfort and security” in the same installation and process, based on the building structure and the user requirements (see below in Figure 5). Even outdoor system sensors are then integrated into the same IP500 network and the BMS, since the key technology aspects of these out-door applications can also be covered.



Specified and combined symbols and user functions for IoT installation included in the VDI Guideline:

- Actuator and sensor have specific symbol like: “occupancy sensor”
- Utilization of specific function blocs like “occupancy control”
- The input & output information and optional parameter are designed as follows:
  - **P_** people presence, **U_** Room utilization, **L_** Light; **H_** illumination level
  - **AUTO**: automatically, **MAN**: manually, **ACT**: actual**, SET**: set value
  - **P-AUTO**: presence in the room, automatically detected by a sensor
  - **L_MAN**: light control coming from the manual control unit

Figure 5: Planning an entire building automation structure with the help of the VDI Installation Guild Line

Such an efficient and scalable planning / installation process, based on the interoperability across all the IP500 applications (comfort / security) connected to one common IoT infrastructure, saves time and cost and allows the acting parties to add new applications and combinations from different OEM’s, that were not previously possible.

Combine “comfort & security” applications, example "lighting" in office buildings and parking garages – based on the IP500 wireless IoT platform

General lighting is a central and important (comfort) application in every building; commercial, public or private. Most lighting systems in a commercial building are controlled by a protocol called DALI. In addition to the 230 / 110V supply voltage, the luminaire is supplied with data via a 2-core DALI bus cable, e.g. Switch on and off or to dim. DALI 2 also created the option of transmitting the power consumption of the lights.

This installation technology has been around for a long time and can therefore easily operate simple lighting functions with "on-off and dimming".

If a user wants to expand the functionality of the lighting system to make it "smarter" by new and innovative sensing solutions, this is only possible with a relatively high amount of effort in the classic wired installation and is associated with high installation costs. Should functions can be expanded using mobile applications or combine it with security applications in commercial or industrial building, i.e. for:

- Identifying the presence or number of people in a room, in combination with HVAC
- security guard control walk, in combination with access control end elevators
- evacuation of people in an alarm situation
- delivery of food, good or supplies by robots in combination with access control end elevators

The traditionally wired lighting solutions quickly reach their limits. The extension of such mobile based functions is only possible with the support of a secure and high performance wireless IoT platform / network!

The use of wireless connectivity in luminaires based on ZigBee or BLE (Bluetooth Low Energy) is available in the consumer environment, because of popularity of some wireless standards and because of the wireless connection to a smartphone, voice guidance systems or tablets is possible directly via BLE.

But these wireless technologies do have limit if you want to combine such lighting system with security and mobility applications (see background in the previous paragraph).

The future of Smart Building with a common wireless IoT platform:

If you now look at the trends in the planning and installation world and the opportunities for end-users to have comfort and security applications supported by one IoT wireless platform in their building, planners, system integrators and construction companies have realized the opportunity and have started to integrated the IP500 infrastructure with IP500 OEM products in large commercial building projects around the world (see one example in figure 6. below) – reference to specific projects are available on request, contact IP500 Alliance.

Due to the high robustness of the IP500 Dual Frequency & Mesh technology, the IP500 wireless network can cover large areas in commercial buildings safely and robustly. As already mentioned, the latency time, data rate, security and scalability play a critical role in the decision of such applications. Switching on processes of large-area lighting systems, such as in a larger office room or parking garage, a low latency time of less than approximately 200ms is very important because the switch-on process is visible to the human eye after a delay of approximately <200ms. So, a “light organ” effect, which is caused by interference-prone, with high latency, wireless networks, will quickly lead to dissatisfaction with the user.

The following system drawing shows an installation of a lighting system, in combination with the traditional DALI protocol, a WiFi connection to the GUI / control unit (laptop, smartphone or PC) and the connection of comfort and security OEM products to the IP500 Gateway.

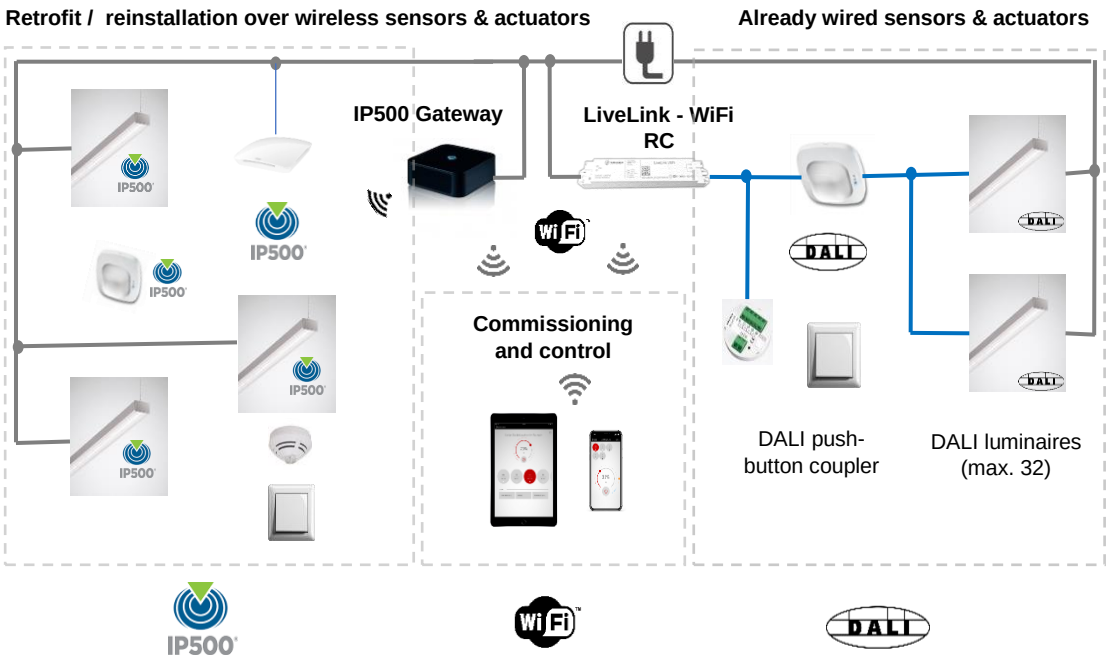


Figure 6: Illustration of the lighting system with DALI (wired) and IP500 network control & back-bone

Since the IP500 network supports the IPv6 protocol and therefore the IP500 gateway is directly connected to the IT network of the commercial building, all data from and to IP500 connected sensors and actors are available via the IT infrastructure. This allows the provision of additional valuable sensing data from IP500 sensors to already wired IT installed building automation systems (e.g. HVAC, access control or elevators).

That allows owners to lower operations cost (heating or lighting) or to improve the security level of their entire existing buildings, without huge installation cost.

Planners and system integrators of large commercial buildings have realized this advantage and opportunity to combine lighting systems with security applications. This also enables leading providers (OEM's) of lighting and sensing solution to integrate the IP500 / CNX200 wireless module into their products.

One of the target projects the "World Trade Center" in New Delhi, India, is one of the largest commercial building worldwide, where an IP500 infrastructure will be the IoT back-Bone for all the IoT applications, incl. lighting, access control (incl. elevators), HAVC and many more.

Figure 7: The World Trade Center in New Delhi, India with IP500 infrastructure and IoT OEM applications

In this case, the planner and system integrator has called for the tender of all the related applications connected to the IP500 infrastructure across the entire building. The lighting solution has implemented the IP500 / CNX200 Module in each lighting luminary and can gather security-relevant applications to provide higher value to the user.

One important part of this building is the large underground parking garages for more than 7000 cars. In this garage all lighting and parking of each car will be part of the IP500 wireless platform. The combination of lighting (comfort) and security applications improves the safety-critical measurement of air / CO_2 and status of the car movements in this large garage. This data will be then sent via the IP500 infrastructure to the control unit / BMS (Building Management System). Such a large installation requires a very robust, high performance (data rate and latency time) and secure and certified wireless IoT network. Therefore the IP500 wireless IoT standard and its members / partners were selected to supply the related IP500 connected products and systems.

Figure 8: System planning of a parking guidance solution for parking garages

The combination of comfort and security related applications in a parking garage improves the security level.

In summary:

The IP500 standard has created an IoT wireless platform that is available today and fulfills all the most important application aspects. It thus offers high scalability, security and performance for convenience and security applications in one and the same IoT infrastructure for commercial buildings, similar as WiFi has been offering us for a long time for high data rate applications!