WHITE PAPER

ZIGBEE

TECHNOLOGY FOR DATA CENTERS INFRASTRUCTURE

#LegrandImprovingLives

legrand®

LEGRAND SUPPORTS YOU ON ALL YOUR PROJECTS

This white paper explores the value and relevance of the Zigbee wireless protocol in data center environments, in response to growing challenges such as infrastructure densification, AI-driven workloads, and increasing requirements for reliability and sustainability. It highlights the limitations of traditional wired monitoring architectures and explains why wireless solutions now represent a credible and long-term alternative. The reader will find a detailed overview of the Zigbee protocol, including its mesh network architecture, security mechanisms, and low-power operation. The document also outlines concrete operational benefits such as reduced installation costs, improved deployment flexibility, and minimized risks associated with human intervention. Finally, use cases and a real-world deployment example illustrate how Zigbee can enhance monitoring, performance, and resilience in next-generation data centers.

Contents

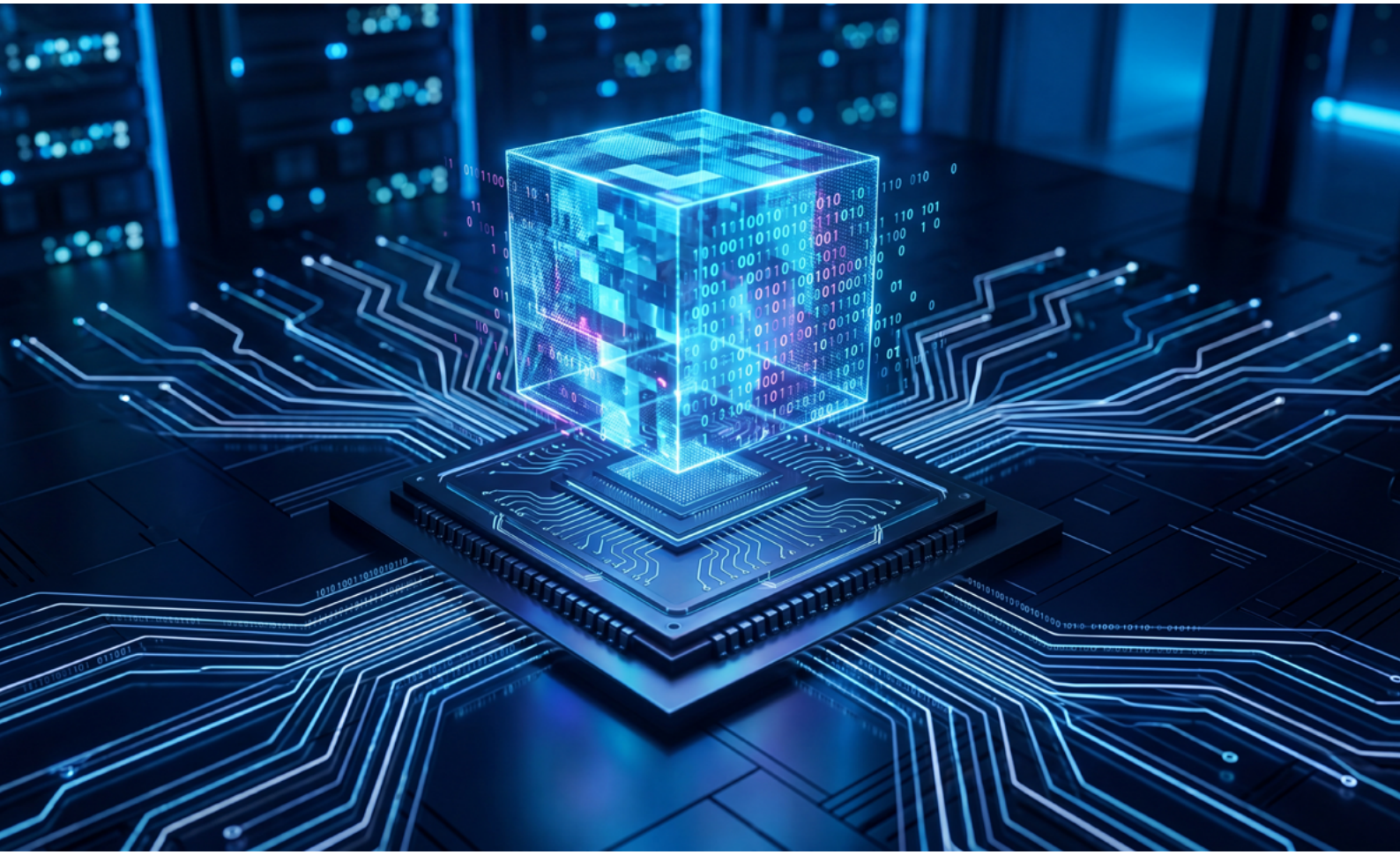
WIRELESS SUPERVISION FOR DATA CENTERS INFRASTRUCURE:

RELIABLE, SECURE AND SCALABLE WITH ZIGBEE

Modern, dynamic data centers are continuously evolving to satisfy not just the ever-growing demands of our digital age, but also to respond to the current, and growing, AI explosion, with its demand for ever higher density computing. At the same time, the data center industry is also responding to the demands of sustainability, with Net Zero as the ultimate objective. In this rapidly evolving data center landscape, many long-held, traditional approaches to data center design, build, operations, maintenance, and support are being questioned.

This white paper aims to:

- examine the benefits that the Zigbee wireless protocol can bring to the data center when it comes to facilitating real-time monitoring and control.
- demonstrate the reliability and robust security of Zigbee
- explain why Zigbee is particularly well-suited radio technology for data center PDU and sensor supervision



FROM EVOLUTION TO REVOLUTION ?

Given their mission-critical status, data centers have tended to evolve relatively slowly over time when it comes to introducing new infrastructure technologies and new approaches to design, construction, operation and maintenance practices.

However, recent drivers—cloud adoption, digital transformation, AI, and sustainability—have accelerated innovation and change across the industry. The rise of hyperscalers has led to widespread adoption of new approaches, such as modular design, liquid cooling, automation, and even unconventional concepts like underwater or timber-built data centers.

Owners and operators now prioritize agility, flexibility, and scalability, often redesigning layouts before construction is complete to meet evolving AI compute demands. As a result, solutions that enable quick, cost-effective adaptation are highly valued. Reducing cable complexity, for example, can significantly improve efficiency in today's high-density environments. **Wireless technologies, once considered risky, have matured and now meet the stringent reliability requirements of modern data centers.**

A DIGITAL AND INCREASINGLY WIRELESS WORLD

Ultimately, it is this resilience and uptime guarantee imperative that decides the type and pace of data center innovation. Risk assessments will be conducted to determine the potential benefits and downsides of introducing new solutions and approaches into the data center. As a rule, there are good reasons as to why data centers are designed, built, operated and maintained in the ways in which they are. Therefore, advocates of change and innovation need to convince others that the benefits of the new outweigh any disadvantages – with any potential compromise in uptime being a non-starter.

One area where the rate of change has been both incredibly fast (quite literally!), but also somewhat cautious, is that of the connectivity solutions which link together the data center facilities' infrastructure and the IT infrastructure within the racks, the cabinets and the overall building, and then beyond to the outside world.

If flexibility were the only consideration, wireless technology would clearly be the preferred option. After all, what could be more flexible than a network which has no wires or cables that need to be plugged in and out, swapped over, changed, upgraded, repaired, or replaced? No bird nests of wires, no poorly installed and insecure cables - potentially compromising cooling efficiency. There is no need for humans to enter the data center aisles to open cabinets, potentially making mistakes. A significant proportion of data center incidents occur following human intervention. The Uptime Institute estimates, based on 25 years of data, that human error plays a role in two-thirds to four fifths of all outages (Annual Outage Analysis - 2025 Report). So, anything that can be done to minimize the presence of humans in and around highly sensitive IT hardware, let alone interaction with cabinets, racks, and cables, makes complete sense.

After all, **wireless offers several key benefits for the data center environment**. The mobility and convenience of the infrastructure – the ability to connect freely and easily without the plugging in and out of cables is a major advantage (as previously highlighted, removing the need for humans to interact with racks and cabinets) – means that wireless networks provide significant flexibility and agility, and speed of connection, when compared to cables. Similarly, the **ease of installation** of a wireless network, as well as subsequent expansion, is a much less complicated and labor-intensive task than managing cables. The simple absence of the 'clutter' of cables, however well managed, not only creates a cleaner and potentially safer environment, but it also **saves space**, space which is often at a premium in a data center environment. **Scalability** is another big advantage – a wireless network can generally accommodate new connections with minimal infrastructure changes or time spent in the data center aisles and halls.

It's also worth reemphasizing the potential disadvantages of wired networks at this point. Wired networks tie devices to specific locations and moving a device generally requires the unplugging and re-routing of cables, with the attendant disruption this creates within the data center. The installation of a wired network tends to involve more time and expense than a wireless equivalent. Indeed, it is likely to require professional installation and maintenance, and upgrades will also involve physical work. Cable management issues within the data center are well-documented, but that doesn't lessen the potential problem of a tangled mess of cables, which can pose a safety hazard and complicate troubleshooting and maintenance. Scalability-wise, adding new devices to a wired network may require new cabling, as well as possibly new switches and routers – a time-consuming and costly process compared to wireless scaling.

	WIRELESS	WIRED
INSTALLATION	▪ Fast and easy ▪ Flexible location of hardware ▪ Save space	▪ Labor-intensive ▪ Fixed location
MAINTENANCE	▪ Scalable with minimal infrastructure change	▪ Generally require new cabling and possibly additional IT equipment
	► Reduce manual intervention and thus risk	**► Prone to human errors**

While the completely wireless data center may be a long way into the future, the growing use of wireless in this environment must at least be considered. A hybrid approach would seem to be the best fit. Consider how wireless networks have 'encroached' into areas where wires and cables were once considered compulsory – for example, many an office LAN has been transformed into a wireless LAN. Any reduction of cables within the data center, without compromising resilience, should be considered. While IT hardware will continue to be hardwired, **the idea of enabling the data center infrastructure to communicate wirelessly bears close examination**.

Firstly, this means the identification of the wireless communications protocol most suited to the demands of the data center. Step forward Zigbee .

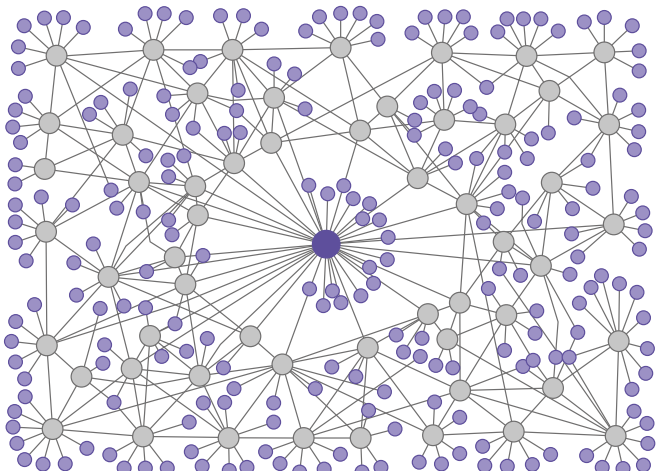
ZIGBEE – THE WIRELESS PROTOCOL OF CHOICE FOR MISSION CRITICAL IOT APPLICATIONS

Zigbee is a **wireless communications protocol**, which is designed for low-power and relatively low-data rate applications related to the Internet of Things (IoT). It is used to create self-healing mesh networks – where devices can communicate with each other – which delivers extended network range and reliability. As a result, Zigbee is increasingly used as the wireless protocol of choice for industrial automation applications, as well as in smart homes.

Zigbee operates on the physical layer and media access control (MAC) layer defined by the **IEEE 802.15.4 standard**. This technical standard is intended to offer the fundamental lower network layers of a low-rate wireless personal area network (LR-WPAN), which focuses on **low-cost, low-latency communication** between devices. As the protocol is designed to be low-power and energy-efficient, the battery-powered devices typically consume very little power, allowing them to run for years on a single battery. Unlike Wi-Fi, which offers higher bandwidth but higher power consumption, Zigbee focuses on energy efficiency.

Zigbee offers three main device types – a **coordinator** which, as the name suggests, is the central device responsible for establishing and managing the network (assigning device addresses and security aspects); a **router**, which helps relay data and expands the network's range; and **end devices** (none routing device)– typically battery-powered and communicate with a parent router or coordinator. The typical data rate is up to 250 Kbps, which is suitable for applications that do not require high throughput. Devices in a Zigbee network communicate using short-range communication, typically with a range of up to 200 meters in open space, but this can be extended through the mesh network.

In essence, the Zigbee **mesh wireless networking topology** means that devices within the network can act as both transmitters and receivers, allowing them to relay data across multiple hops. As data can be passed through multiple intermediate nodes until it reaches its destination, the network range is increased. Furthermore, unlike point-to-point communications, mesh networks ensure that, should a device fail or be temporarily out of range/unavailable, the network still function without complete disruption (an alternative route across the mesh is followed).



Zigbee network topology, dense, self mesh structure:

- Zigbee trust center (central coordinator),
- Zigbee router, 100+: meshed nodes formed a robust multipath network
- Zigbee end devices 200+: sensors using one relays node at a time

The Zigbee protocol stands out for its many advantages, which can be summarized as follows:

- ## Interoperability and Cost-effectiveness

  Zigbee was designed with interoperability in mind, ensuring that devices from different manufacturers can work together seamlessly. This cross-platform compatibility is essential for growing IoT markets, where users expect devices from multiple vendors to work together without compatibility issues.

  Being **open-source** and supported by a range of manufacturers leads to competitive pricing for Zigbee-enabled devices. Additionally, because Zigbee devices utilize low-power technology and have longer lifespans, the total **cost of ownership** over the long term is very favorable when compared to other wireless solutions that require more frequent battery replacements and/ or higher energy consumption.

- ## Mesh networking for scalability and reliability

  Zigbee supports mesh networking, which enhances the scalability and reliability of IoT systems. In a mesh network, devices can communicate with each other through intermediate devices, or routers, which can extend the network's range far beyond the capabilities of a single point-to-point communication link. This mesh topology allows Zigbee networks to **scale easily**, with the potential to support hundreds of devices (and technically thousands), depending on network configuration.

  If one device fails or moves out of range, the data can be rerouted through other devices, which makes Zigbee networks **self-healing** and more resilient. Zigbee offers fast self-healing mesh (and without any controller intervention) compared to Z-wave.

- ## Scalability

  Zigbee supports hundreds of devices (and technically thousands) in a single network, making it ideal for industrial setups. This capability far exceeds Bluetooth's practical limits and even Z-Wave, which is limited to approximately 232 devices. This, combined with the fact that adding or removing devices from the network is simple and secure, makes Zigbee ideal for industrial setups.

- ## Low latency

  Zigbee offers relatively fast communication (e.g. lower latency than Z-Wave), suitable for real-time control. In addition, Zigbee devices support over-the-air firmware updates, allowing devices to receive software updates without the need for manual intervention.

- ## Low power consumption

  One of the biggest advantages of Zigbee is its low power consumption. Devices in a Zigbee network are designed to be energy efficient, which is especially important for battery-operated. Zigbee devices use a sleeping mode, where they remain inactive for most of the time and only "wake up" when they need to send or receive data. This means that battery-powered Zigbee devices can last up to 10 years without needing a recharge or battery replacement.

- ## Security

  Zigbee features built-in security measures to ensure the privacy and integrity of data within the network. The protocol uses **AES-128 encryption** for secure communication between devices.

  Additionally, Zigbee includes **secure device pairing**, ensuring that only authorized devices can join the network, and support for secure key management.

ZIGBEE – THE WIRELESS PROTOCOL OF CHOICE FOR MISSION CRITICAL IOT APPLICATIONS (continued)

FOCUS ON SECURE DEVICE PAIRING

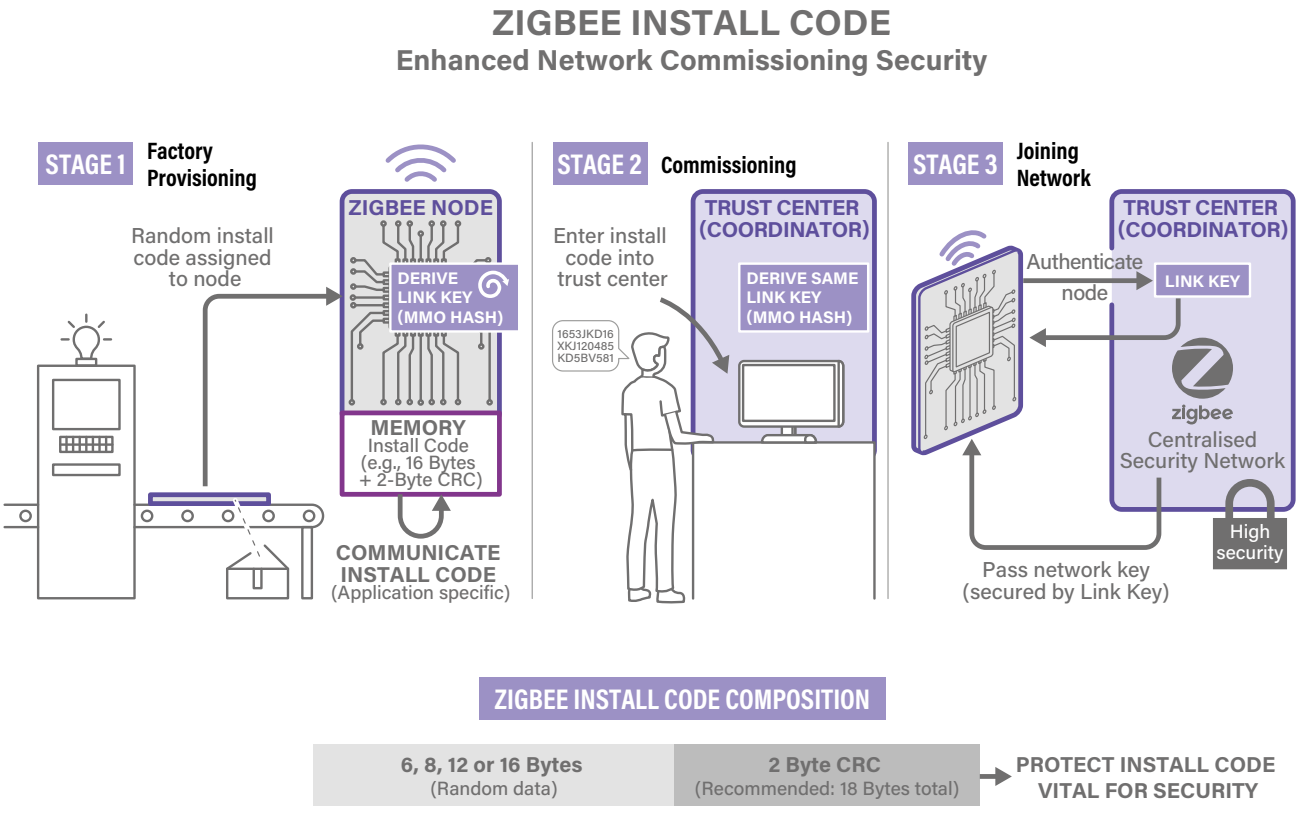
- In Zigbee, devices are required to support installation codes as part of the security model. These codes are used during the initial joining of a device to a Zigbee network, under the control of a central security authority called the trust center.

- An installation code acts as a shared secret between a new device and the trust center. Before the device ever connects to the network, this code is used on both sides to generate a temporary security key. This key allows the device to prove its identity when it joins the network.

- Technically, the installation code is a short sequence of bytes (with an integrity check) that is transformed using a standardized cryptographic function into a 128 bit key. This derived key is then used to securely exchange the Zigbee network key, which is required for all further communications.

- To make this process possible, the installation code and the unique identifier of the device (EUI 64) must be provided to the trust center in advance, through an out of band method such as a QR code or a printed label. This happens outside the Zigbee network itself, since the device is not yet connected.

- By using installation codes, Zigbee ensures that only authorized devices can join a network and that the network key is delivered in a secure and controlled manner, even during the very first connection.



But what if a product leaves the network? Could this be a Trojan horse for the future? This is where the Trust Centre concept, implemented in Zigbee, comes in, which prevents any compromise of the Zigbee network

FOCUS ON TRUST CENTER

- To maintain security and ensure the old device can no longer eavesdrop or interact with the network, the Trust Center initiates a key roll.

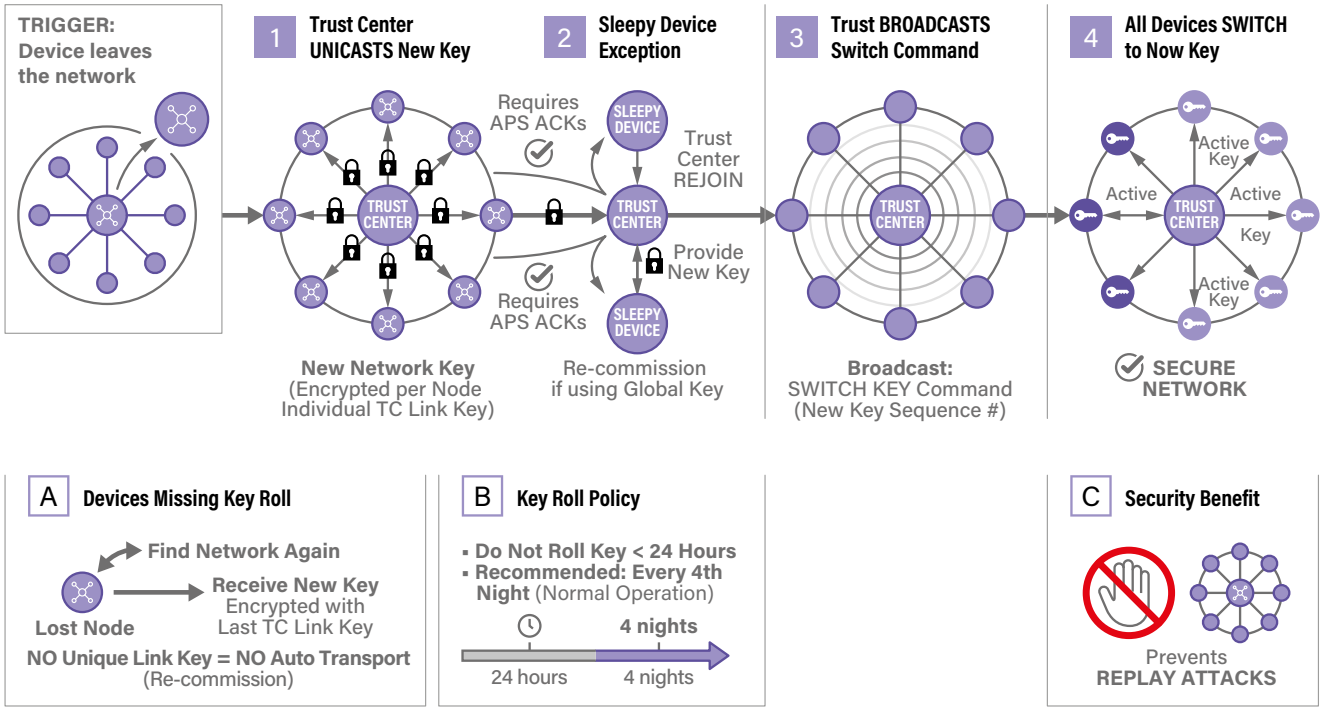
- The Trust Center (TC) generates a new Network Key. And sends this key to every active device in the network via Unicast, it is encrypted using each node's Individual Trust Center Link Key.

- For the Battery-powered devices that spend most of their time asleep won't hear the Unicast. These devices check in periodically with a "Data Poll.". When a sleepy node wakes up, the TC delivers the pending key during that brief window of activity. If a device stays asleep too long and misses the window entirely, it will eventually have to perform a Secure Rejoin to get the update.

- Once the TC is confident that the node of the network has the new key in "standby," it triggers the changeover. The TC sends a Broadcast Switch Key command to the entire network. This command includes the New Key Sequence Number, telling all devices it is time to stop using the old key and start using the new one.

- All devices simultaneously switch to the new key. The network is now secured with the rotated key, and the old key is discarded. Devices can join a network and that the network key is delivered in a secure and controlled manner, even during the very first connection.

ZIGBEE SECURITY: ROLLING THE NETWORK KEY



This makes Zigbee a reliable option for sensitive applications.

ZIGBEE – THE WIRELESS PROTOCOL OF CHOICE FOR MISSION CRITICAL IOT APPLICATIONS (continued)

If we take the main radio technologies available on the market and compare their main features point by point, Zigbee's overall capabilities are comfortably ahead of other available wireless technologies. For example, where Zigbee's power efficiency is excellent, Wi-Fi and Z-Wave suffer by comparison. In terms of interoperability, Zigbee again leads the way with high interoperability compared to Wi-Fi, Bluetooth Low Energy (BLE) and Z-Wave. Zigbee matches, if not exceeds, rival protocols in terms of range, interference, and security, but perhaps the most compelling strength of the Zigbee protocol is the combination of its mesh self-organizing topology and the number of devices which can be connected.

In summary, Zigbee offers several compelling benefits, including low power consumption, mesh networking for scalability and reliability, robust security, interoperability across hundreds of companies around the world, cost-effectiveness, standardized technology, market proven and global support. Its ability to support large-scale networks of devices while maintaining energy efficiency makes it an excellent choice for industrial automation, including many potential data center applications.

WHAT ABOUT WIRELESS DEVICES IN THE DATA CENTER?

Having made the case for Zigbee as the preferred wireless communications protocol for use in industrial and commercial building automation, proven by decade in real world applications, we now need to consider the types of IoT and wireless devices which could be deployed to achieve significant operational advantages in a data center environment.

Currently, there are a variety of wireless devices and overall solutions which can be deployed in the data center, providing a range of benefits in this mission-critical environment. Environmental sensors provide real-time monitoring of data center metrics such as temperature, humidity, airflow, leaks, and smoke detection. Simple asset tracking devices, typically RFID, Bluethooth channel sounding, can track the location of servers, racks, and other high-value assets. Wireless surveillance cameras provide security monitoring and intrusion detection. Wireless access points provide staff, customers and subcontractors access to management consoles, diagnostic tools and handheld devices whilst inside the data center. Wireless smart locks and access control systems are becoming increasingly popular – ensuring controlled access to racks or sensitive areas alongside auditability – tracking who accessed what and when. There is also limited adoption, but noticeable growing interest in the use of drones and robots to carry out inspection, thermal imaging and inventory scanning tasks, for example. Drones can provide frequent inspection of large-scale data halls and overhead cables quickly – certainly much faster than the manual equivalent.

Right now, all of these wireless devices and systems described above could best be described as single-point solutions. They perform a single task much more efficiently than a wired, more manual approach, but multiple such solutions are required to provide all of the necessary management and control of the many different parameters which matter inside the data center.

But **what if there was a solution which could provide smart, real-time, and remote wireless monitoring of all the intelligent devices, at pod level, in a data hall?** Busways and PDUs for power distribution, environmental sensors, access control, cooling units… What would be the key component of such a solution?

The open, remote monitoring application could be hosted on any IT device, which would be connected, via the LAN, to the master data collection device which would, in turn, be connected to the intelligent devices via the Zigbee wireless protocol.

Let's take the example of 60 PDUs and 240 sensors connected in this way.

The sensors could be positioned exactly as required and deployed quickly and easily. And, of course, there would be no need for any cables (and cables running through cabinets are far from ideal), between the PDUs or the sensors.

Furthermore, with such a smart, real-time, and remote wireless monitoring solution, there would be no more need for PDU displays, for example. Saving space and avoiding potential installation and display reading issues – cabinets often must be opened to access the screens. No display screens would mean less materials used for the monitoring solution, alongside the many cables which no longer need to be used. So, not just a smart, real-time and remote wireless monitoring solution, but also a sustainable one. Especially when one considers that Zigbee–connected devices – the PDUs and sensors – can be powered by low-power batteries, which could last up to 10 years.

At this stage, it is worth re-stating the benefits that such a wireless solution would provide:

- Fast and flexible deployment
- Redundancy thanks to mesh networking (if one PDU is faulty, all other components of the network are still alive)
- Savings (Capex, Opex)
- Sustainability

WHAT ABOUT WIRELESS DEVICES IN THE DATA CENTER? (continued)

The key to the expanded use of wireless monitoring and, over time, management solutions within the data center lies in multi-parameter solutions. A solution that combines rack power and environmental condition monitoring makes complete sense. But what if some of the other existing data center wireless applications – access and surveillance for example were added to such a solution? **Over time, one single, integrated intelligent, real-time and remote wireless monitoring (and management) solution, with one master control device linking the local Zigbee connected data center devices to the NoC-located application, could replace several single-point wireless solutions.** No elimination of wires in this case(!), but a much more efficient, scalable, and cost-effective single monitoring and control console, nevertheless.

CASE STUDY

The first application of this concept in a data center in the United Arab Emirates enabled the commissioning of a complete Pod, i.e., an installation with 38 PDUs and 76 environmental sensors, in two hours.

WIRELESS DEVICES IN THE DATA CENTER – NO LONGER UNTHINKABLE

So far in this white paper, we have discussed the rapidly changing data center ecosystem, the industry's growing appetite for innovation, some thoughts as to wired and wireless connectivity, why the Zigbee protocol should be the preferred choice for wireless connectivity in the data center and how more and more wireless devices are likely to make their way into this environment in the future.

There are some compelling reasons as to why wireless connectivity will have an increasingly significant role to play when it comes to monitoring, control, and management of more and more data center infrastructure devices. The main one is the way in which AI is changing the data center rules, and as a result, placing an ever-higher premium on the combination of infrastructure flexibility, speed, security, and easy scalability. Wireless connectivity is perfectly placed to deliver these benefits, as well as eliminating many manual tasks, such as reconfiguring cables on a regular basis, hence eliminating a major cause of data center infrastructure errors.

Set against this background, the use of wireless IoT-connected data center infrastructure – such as PDUs, environmental sensors, and the like – is highly relevant. **A Zigbee mesh wireless network, and the various data center infrastructure solutions it connects to DCIM and/or BMS platforms, offers flexibility, agility, scalability, and speed that traditional wired, cabled solutions simply can't match**. This approach not only enhances operational performance but also delivers significant cost savings and reduces manual intervention—minimizing the risk of human error from unplugging, re-routing, and reconnecting cables.

As the data center industry transitions from technology evolution to revolution – remember, the one megawatt rack is rapidly approaching – the benefits of deploying intelligent wireless technology solutions, based on the Zigbee protocol, deserve careful consideration to ensure that the monitoring, control and management of key data center infrastructure is enabling optimized IT asset performance and not becoming a potential bottleneck to operational efficiency.

NOTE

legrandgroup.com | youtube.com/user/legrand | linkedin.com/company/legrand | x.com/Legrand

World Headquarters
and International Department
87045 Limoges Cedex - France
Tel: +33(0)5 55 06 87 87

legrand®