theLIA

Guide to Wireless Lighting Systems

January 2019

THE LIGHTING INDUSTRY ASSOCIATION

www.thelia.org.uk

INTRODUCTION

Wireless technologies have revolutionised how we interact with the world in our daily lives. We expect to access the internet wherever we go and we love the convenience of being able to access content wherever we are, or interact with devices remotely.

This guide will illustrate how wireless technology is revolutionising the lighting industry by unlocking additional benefits, and indeed enhancing the overall user experience.

There has been so much confusion within the market regarding wireless technology and we felt that as the Lighting Industry Association (LIA) we should attempt to demystify some of the jargon and expand on the benefits and possible weaknesses of wireless technology.

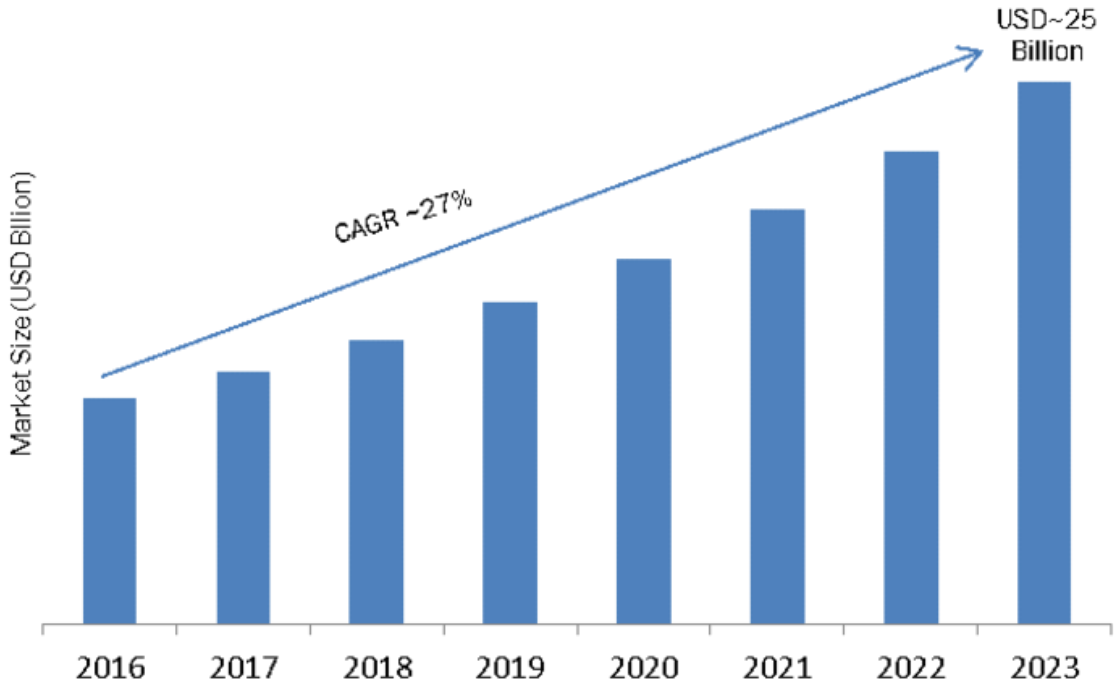
OPPORTUNITIES

Connected devices are everywhere; the demand for them is increasing at an exponential rate and is expected to reach 30 billion devices by 2020.

Lighting has also gone through a transition with many smart wireless devices being offered for the home that allow us to connect to an intelligent light, thermostat or camera. It is worth mentioning that controlling several smart lights in an domestic environment, often a single room, is very different to the connection of multiple wireless points in a commercial building.

This new technological revolution will bring countless benefits, and will create new industries in their own right, which brings us back to lighting. Wherever there are people there is light, and this will open incredible new opportunities for lighting manufacturers, installers, integrators, and all the adjacent industries they service.

GLOBAL SMART LIGHTING CONTROL MARKET

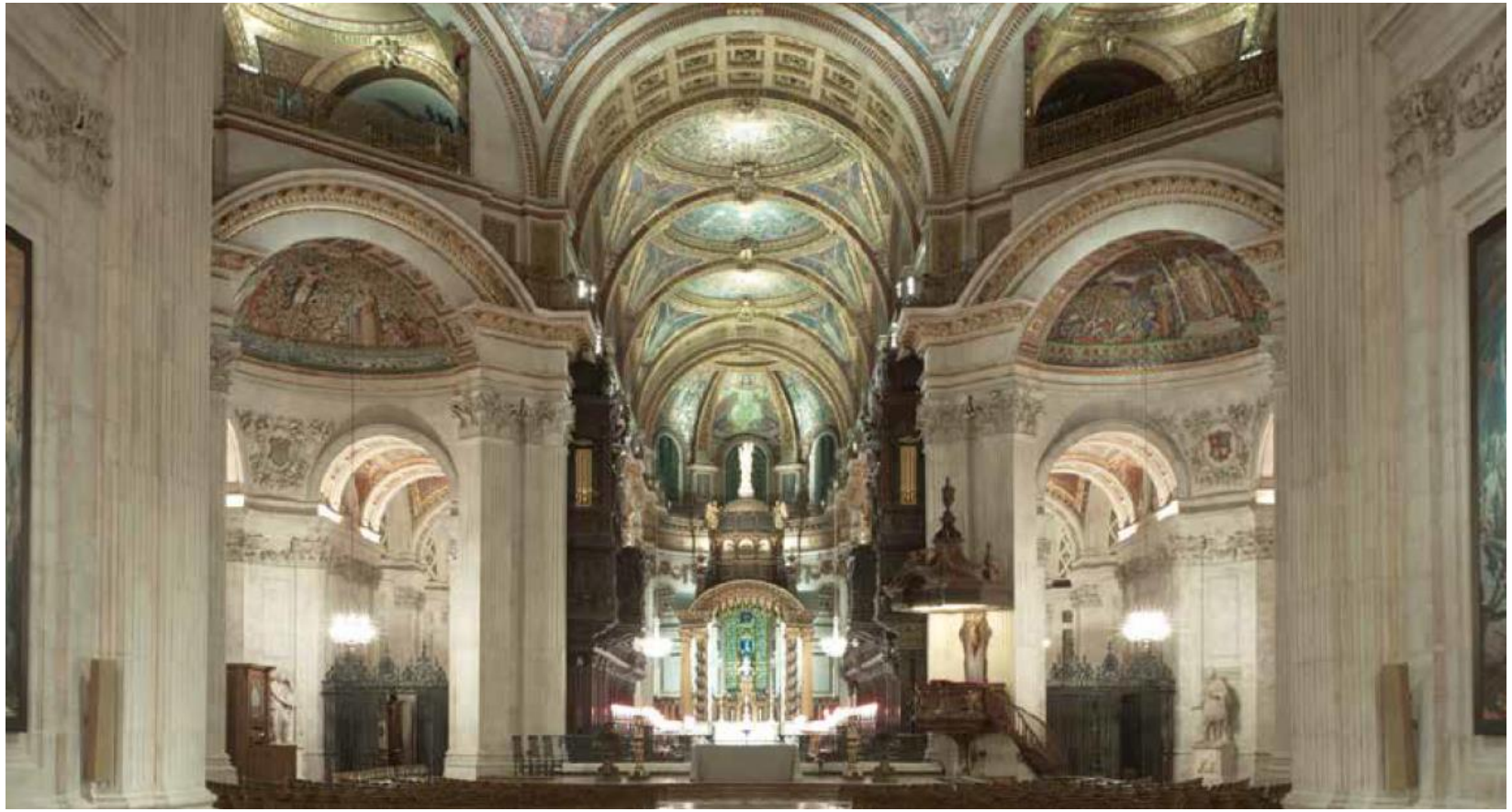


Source: MRFR Analysis

RETROFITS

Finding the right balance of cost, complexity and control has been especially difficult in retrofit scenarios, where existing building infrastructure often gets in the way of installing a lighting control system. Adding wiring is often expensive, unrealistic or even impossible, depending on the type of building and location of the lighting.

Wireless provides an ideal solution for retrofits, allowing the existing infrastructure to remain without unnecessary changes, and enabling new devices such as sensors to be placed where needed, rather than restricted to where they can be wired. This is especially true in challenging environments like high-bay warehouses, large retail and industrial buildings.



ADDED VALUE

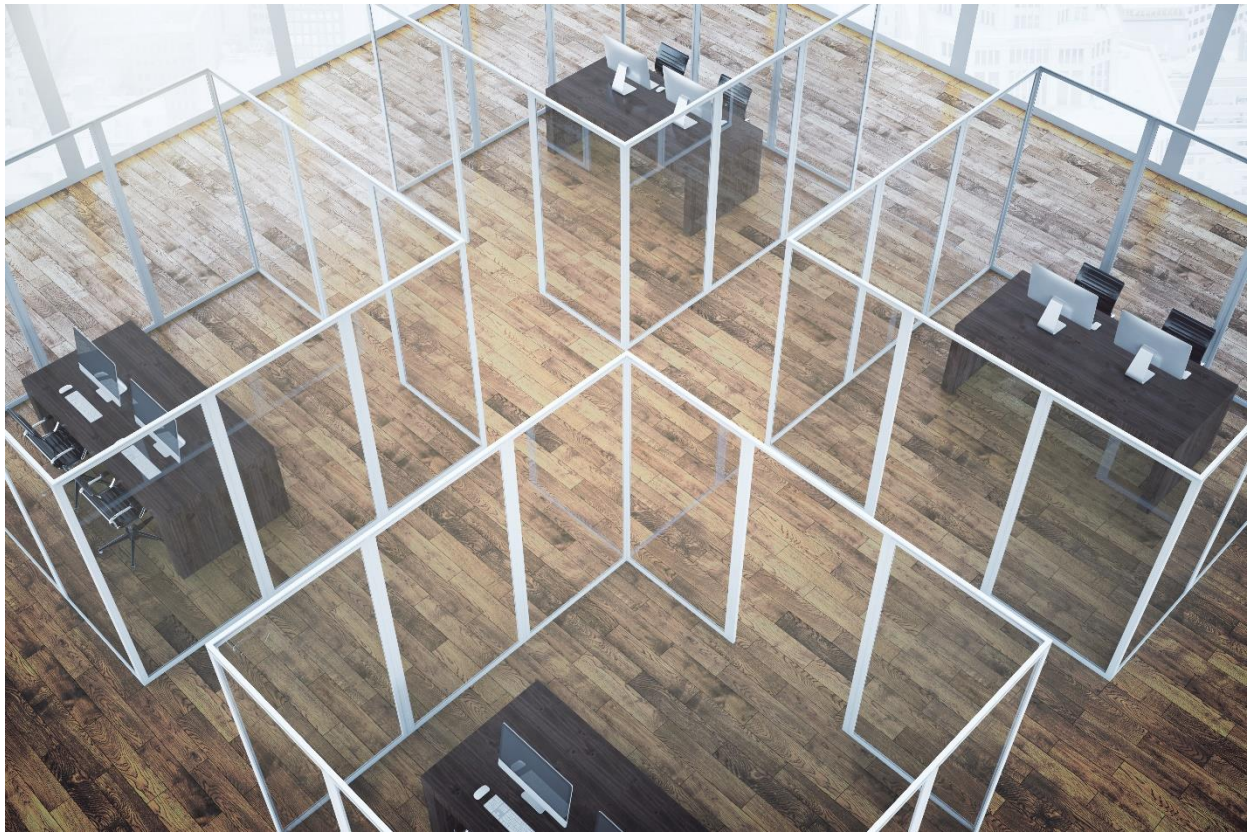
Wireless can provide opportunities to upgrade existing controls without the need for wiring changes.

Perfect for the retrofit market, wireless allows for the gradual update of existing systems through a piece by piece upgrade, offering unparalleled flexibility, scalability and limiting modifications to existing wiring.

The installation of devices is no longer limited by what the wiring permits, and in combination with certain technologies, the lighting industry can now provide analytical information that allows the building or business owner to optimise their services or sales, as well as staff productivity.

FLEXIBILITY

Once a wireless network is established, that network can grow to cover an ever-expanding area at a low additional cost. Additional sensors, switches and luminaires can easily be added, and these elements can use the same wireless control system without requiring a new control infrastructure. Lights are grouped via software rather than hard-wiring. Therefore, changes can be made at any time, or new devices included, by simple reprogramming, which can now be easily achieved by the installer without having to call an engineer to come on site.

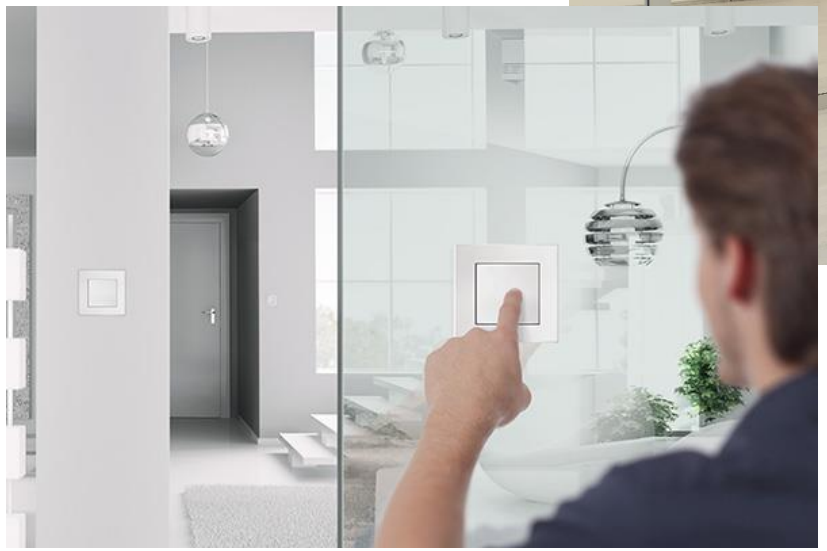


SCALABILITY

Instead of placing controls where wiring permits, building owners can place controls where they are needed to improve building performance. As the needs of a space change, changes can be made at any point, or new devices and control strategies added, simply by reprogramming.

For example, in buildings with glass or concrete walls, installers no longer need to worry about wiring routes – they can simply put the controls where they make the most sense. Flexibility and control are further enhanced by a single switch being able to communicate with multiple devices, and a single device being able to be controlled by multiple switches.

As the needs of a space change, wireless controls can be reconfigured or expanded to accommodate alterations without the cost- and time-intensive process of damaging walls and ceilings for rewiring.



TRAFFIC ENGINEERING

Each different wireless technology has its own traffic capacity limits. For example in a Bluetooth Mesh, each core node retransmits each message that it receives and each node is limited to a sustained message transmission rate of 10 messages per second. A mesh-wide message rate of 10 per second may be suitable for a deployment controlling 100 luminaires but building users are unlikely to be satisfied by the response times for a mesh system controlling 5000 luminaires.

When selecting a wireless technology it is important to understand both its capacity limits and the eventual size of the deployment that is being proposed. Is the system expected to increase in size significantly as devices are added during building fit-out and will that cause a degradation in system reliability or response time? When considering a wireless technology, look for deployments of a similar size to that proposed or for computer simulations that will give an indication of performance.

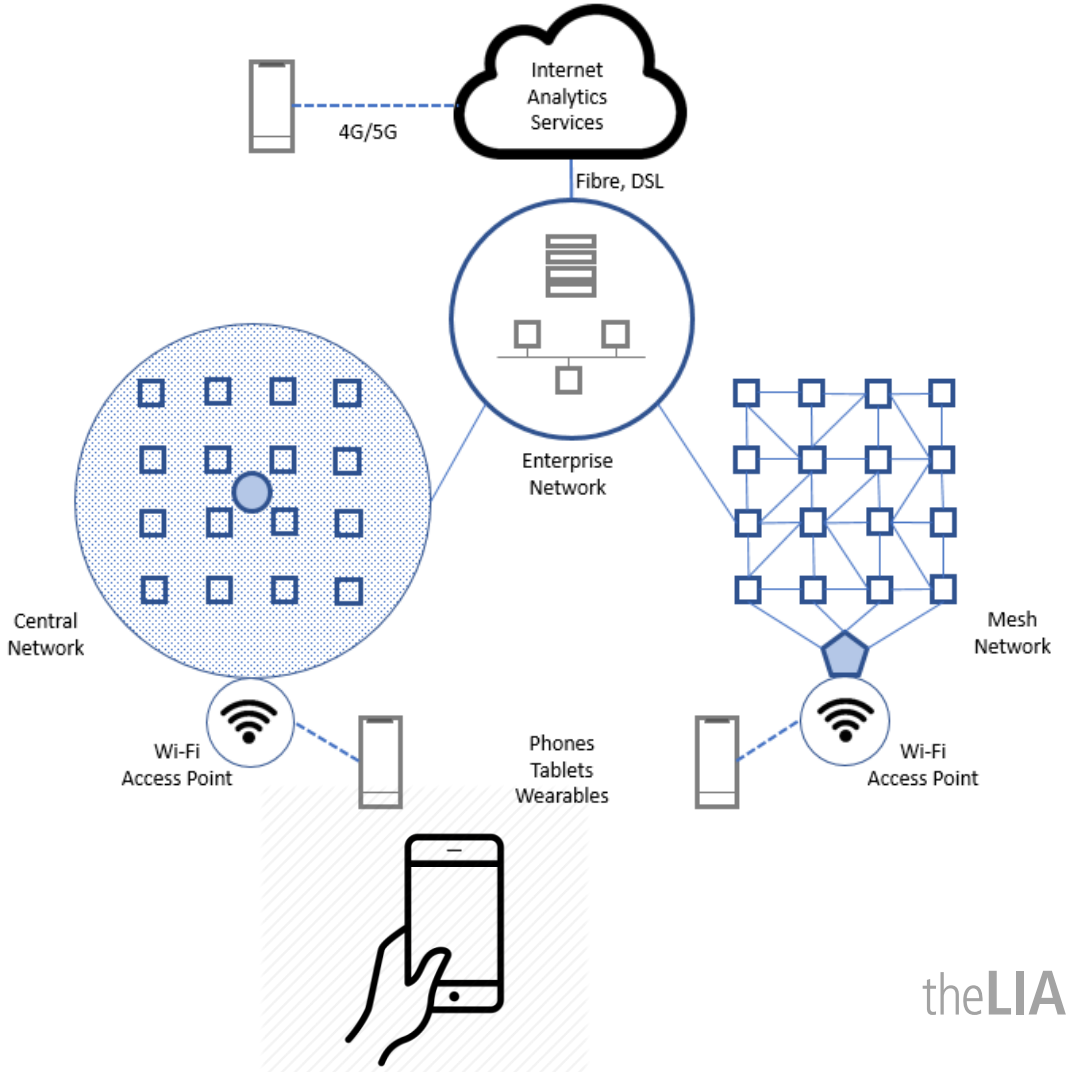
For large deployments, a mixture of wireless and wired communications links may be appropriate – wireless links where they are needed to support user interfaces such as smart phone apps and where wiring is hard to install; wired links for the backbone where most of the traffic flows.

TECHNOLOGY

Following the rapid evolution of wireless networking devices, a large number of networking technologies have emerged.
A common misconception is that there has to be a single wireless technology to do it all. Today we use several wired technologies, each with their own benefits and trade offs.

Wireless is very much the same. It is likely that we will use Wi-Fi and Bluetooth just because our smart devices use them, but that does not mean that you must or should use them for everything.

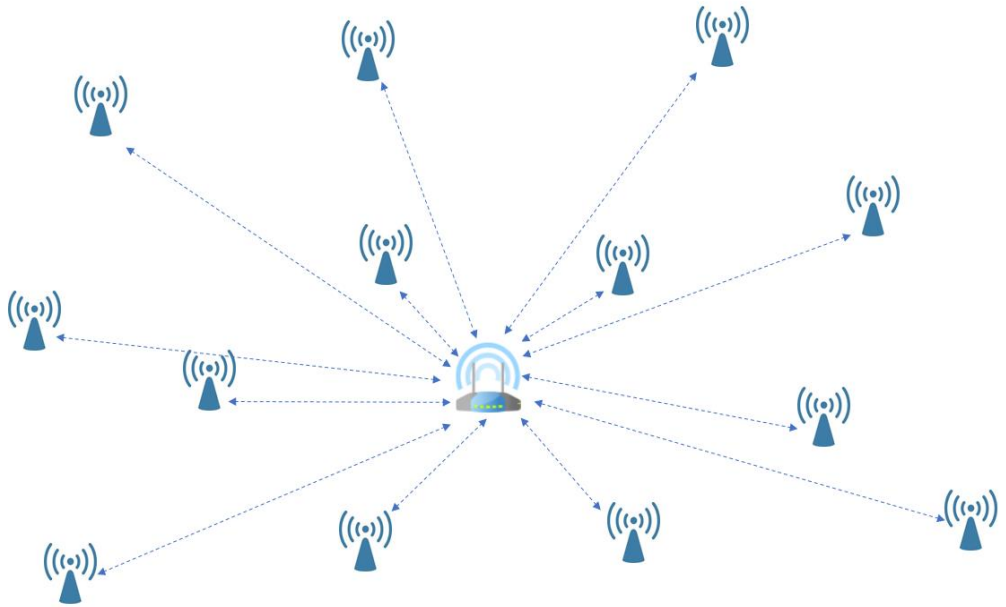
Light is part of the life safety provision of any building, and reaction time is critical. Some technologies have been designed with low latency in mind, others specialize in high bandwidth to transmit lots of data to the cloud for analysis. Some work great with a small number of devices, others are designed for hundreds of nodes. You will find that wireless systems may use more than one wireless technology, particularly in commercial buildings.



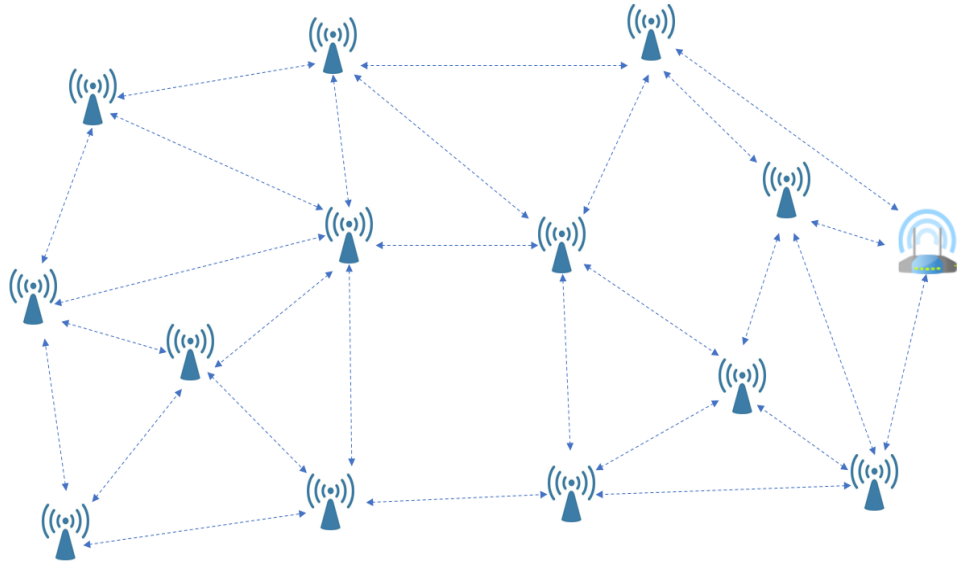
NETWORKS

Fixed Networks

These networks require routing devices to be in a fixed location during installation and commissioning to ensure appropriate coverage. Their components are addressed in a rigid way without allowing automatic reconfiguration of the network. The network hierarchy can be different, but it will remain the same when the nodes are being moved to another location. These types of networks are commonly optimised for systems where reaction time is critical.



Fixed Network



Mesh Network

Mesh Networks

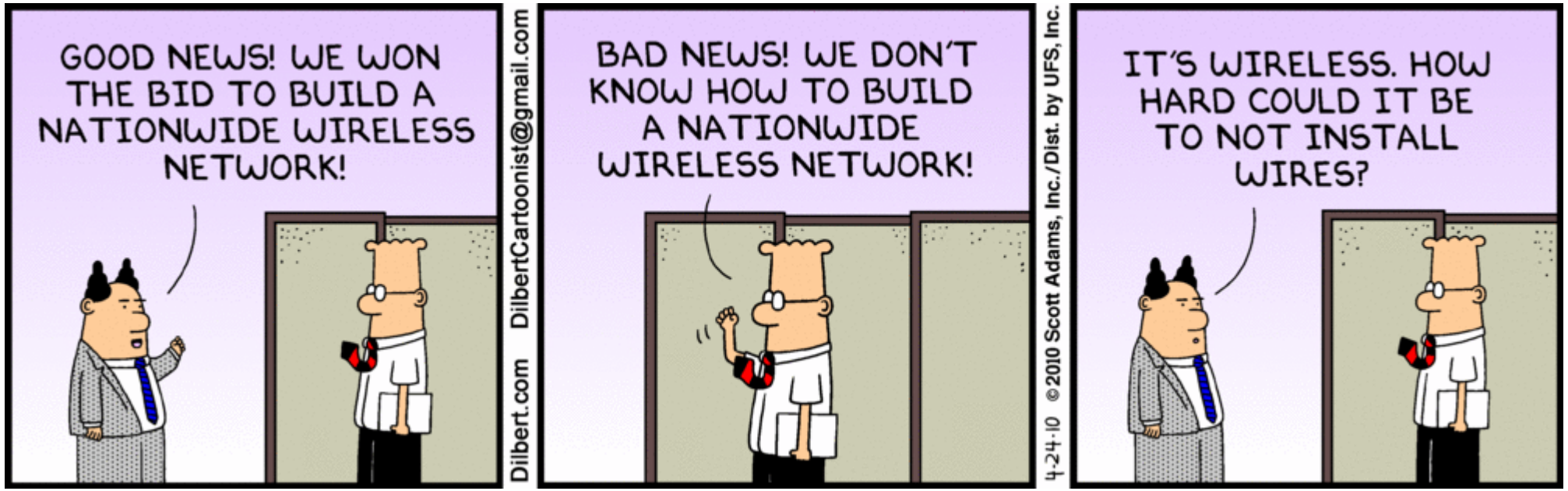
The main characteristic of a mesh network is the communication between the nodes is in a non-hierarchical way. All the network members establish communication with their neighbours, typically during the initialisation of the system. It is usually a dynamic process, which can allow the system to overcome random node failures. This is commonly referred to as “self-healing” and a mesh network provides a large degree of resilience against such failures.

PROTOCOLS

Protocols are the language that devices use to communicate with each other. Several different protocols have been developed over the years. Powered by new components provided at an ever decreasing cost, this is one of the most dynamic markets in the controls industry. Naturally, this has led to a plethora of systems with proprietary protocols, in parallel with others that use open protocols.

Proprietary protocols can give a quite efficient and fast system and are typically quick to be developed, as they largely depend on a single developer. They may be focused to specific markets or applications and can be supported by one or more manufacturers that adopt the specific technology. There are many proprietary systems that have been widely adopted while others have practically disappeared.

Open protocols, on the other hand, may take more time to be developed as they are typically the result of efforts by several companies working together. This can provide the longevity of the support and most likely, interoperability between different suppliers, at the cost of slower development.



INTEROPERABILITY

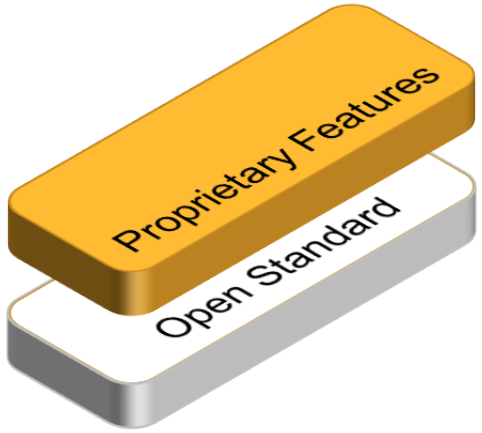
Interoperability is largely a manufacturer's choice, and it is important to differentiate between devices and systems, even when using open protocols.

Devices: Interoperability between devices requires the use of a common protocol. An open protocol is more likely to be supported by more suppliers, although there have been proprietary ones that have been so widely adopted they have become a de-facto standard in their own right.

Systems: Interoperability between systems is usually easier to achieve, if the systems support some of the common industry protocols. This is typically done using interfacing devices or directly on the central controller level, should there be one.

DEPLOYMENT

In reality, most control systems are based on a combination of open and proprietary protocols or features, and indeed open protocols are designed to allow manufacturers to expand them with proprietary features. This is true for both wired (e.g. DALI-2) and wireless (e.g. Bluetooth) protocols.
You can think of it as layers:



Always verify compatibility before mixing and matching components from different manufacturers, if in doubt carry out trials.

SECURITY

OVERVIEW

Security is a risk to any system and with our increased reliance on smart technology we need to ensure we keep our data and systems safe.

In all wireless applications we need to consider the security of the complete system and therefore prevent any unauthorised access or damage to the connected devices or data using wireless networks.

Use products and systems from reputable manufacturers (such as LIA members) that take your security and data privacy seriously.

IMPLEMENTATION

Security is a process. It is never finished, and requires continued updates and evaluation, it is only as good as the weakest link.

It does not matter how secure a door is if others have the key, so always use protocols with the right level of security by design.

And to continue with our door parallel, it certainly does not matter how secure your door is if you do not lock it, which is why commissioning is so important. Security minded manufacturers will not let you commission the system without setting up a minimum level of security.

Software, and especially the user interface, will define the ease with which a system can be configured and if the security is in place then a key or certificate needs to be provided to allow the system to recognise a connecting wireless device.

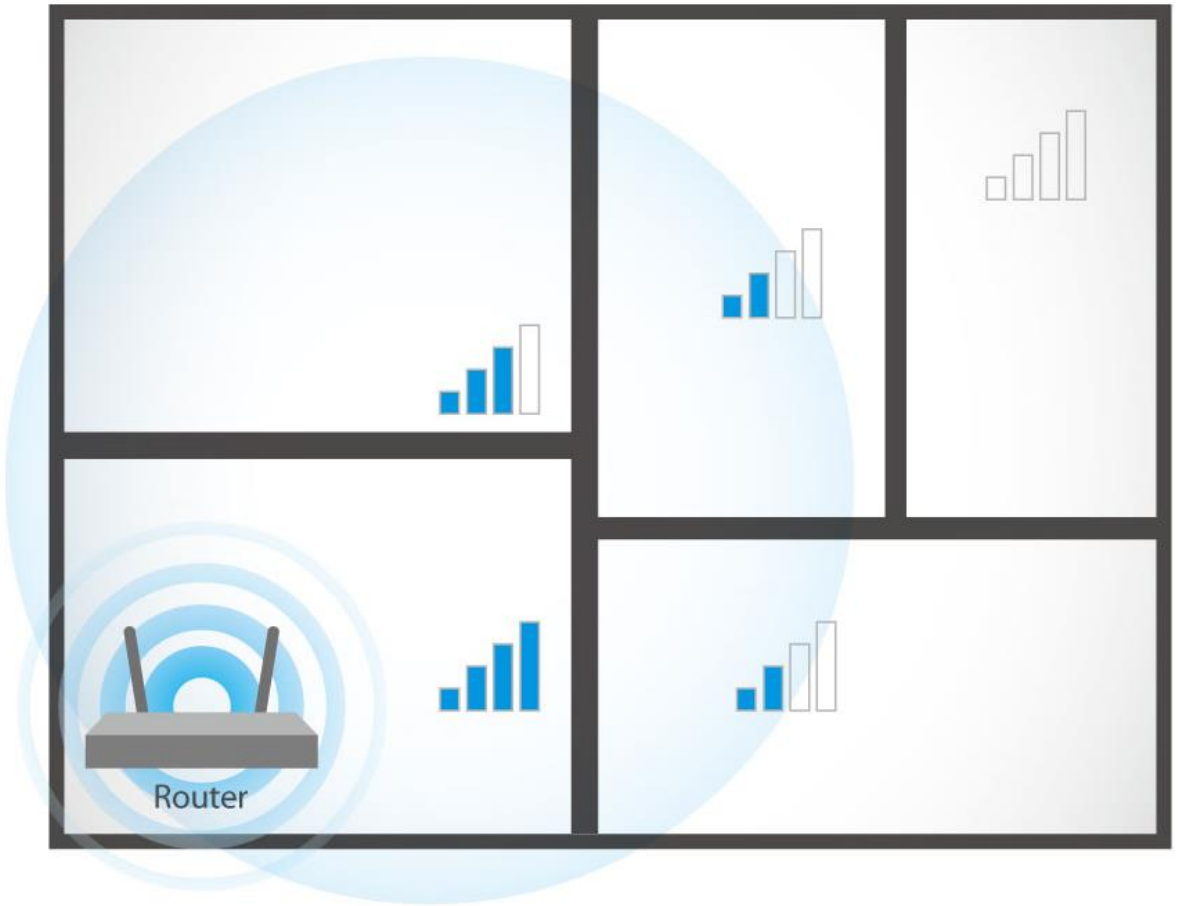
Always understand your application. Sometimes just because you can connect your system to everything it does not mean you should, especially when it comes to security and data privacy.

BEST PRACTICES - RANGE

Wireless equipment must meet the RED (Radio Equipment Directive), this will ensure they will withstand interference and avoid interfering with other compliant products.

Metal inhibits radio frequency performance. Structures, ceilings, luminaire and equipment housings, ductwork, reinforcement within concrete and even foil covered plasterboard may all inhibit range.

Highly populated areas can also do this, particularly when using frequencies of 2.4GHz and above. Old vaulted basements and building cores are potentially less penetrable, as with Wi-Fi in your home, and transmission through combinations of these, especially at glancing angles, can be problematic. Consider an RF friendly “line of sight” approach for equipment locations when planning your system. Your simple “ceiling void” is actually a complex habitat for equipment and services often unknown to someone trying to plan lighting.



BEST PRACTICES – SYSTEM DESIGN AND INSTALLATION

Never design to your limits! Think spare capacity; you may need “get out of jail free” options to allow more input devices (i.e. detectors, other devices, human or system interfaces) in future. For example you may want to integrate more luminaires within the building (such as task or emergency lighting in future phases). A simple rule of thumb has been to allow 25% spare capacity, but due to the constant developments possible within the IoT arena nowadays, perhaps more might now be prudent.

Always consider how many people might be using your space (i.e. pedestrians entering a stadium or rush hour station, a multi-use business conference centre). Ensure your system can robustly cope with peak demand, now and in the future.

Select and design your system and its components to work autonomously in a professional environment, then add interoperability only where needed. Finally, reporting between systems should be at a higher or system level, which cascades to and from devices or control nodes, when needed. Sending / receiving individual messages about everything from every sensor and device all the time, not only increases complexity and traffic but it slows the system, potentially wastes power, reduces visibility of key issues and distracts you from your core needs.

BEST PRACTICES – COMMISSIONING

Always set up your system to your client specifications, and consider:

- Control strategy
- Integration
- Access and Security
- Maintenance Schedule
- Back up and recovery systems
- Documentation
- Proving and sign-off process

Commissioning and Maintenance are major considerations. You need to be able to link all the devices together, set all functionality, update software and set up the security. Practical methods should be proven in previous applications. They must allow easy location, identification, addressing (if applicable) and selection of individual devices and groups.

These need to be proven against the specification and functionality. Reporting and interoperability needs to be checked and performance proven before handover. These should be checked against your list and specification as well as the control philosophy.

Always back up any software and configuration files, and keep a copy of warranty/software support terms. Completion certification should be provided and performance testing should be witnessed, and signed off by all relevant parties.

BEST PRACTICES – CONTINUAL REVIEW

It is important that at least an annual review is made of the current use, requirements, energy consumption, maintenance and security.

A client feedback group and update loop which includes the user is essential to maximise savings and performance of the system and the building's users. The increasing demand for on-going contractual service performance and cost, plus future proofing must also be reviewed.

To ensure secure operation, maintenance, software (including patches and bug fixes), potential threat, resilience and system security must also form part of your reviews.

Most companies offer service agreements to keep systems current with the latest standards – make sure you have one!

It is important that at least an annual review is made of the current use, requirements, energy consumption, maintenance and security.

A client feedback group and update loop which includes the user is essential to maximise savings and performance of the system and the building's users. The increasing demand for on-going contractual service performance and cost, plus future proofing must also be reviewed.

To ensure secure operation, maintenance, software (including patches and bug fixes), potential threat, resilience and system security must also form part of your reviews.

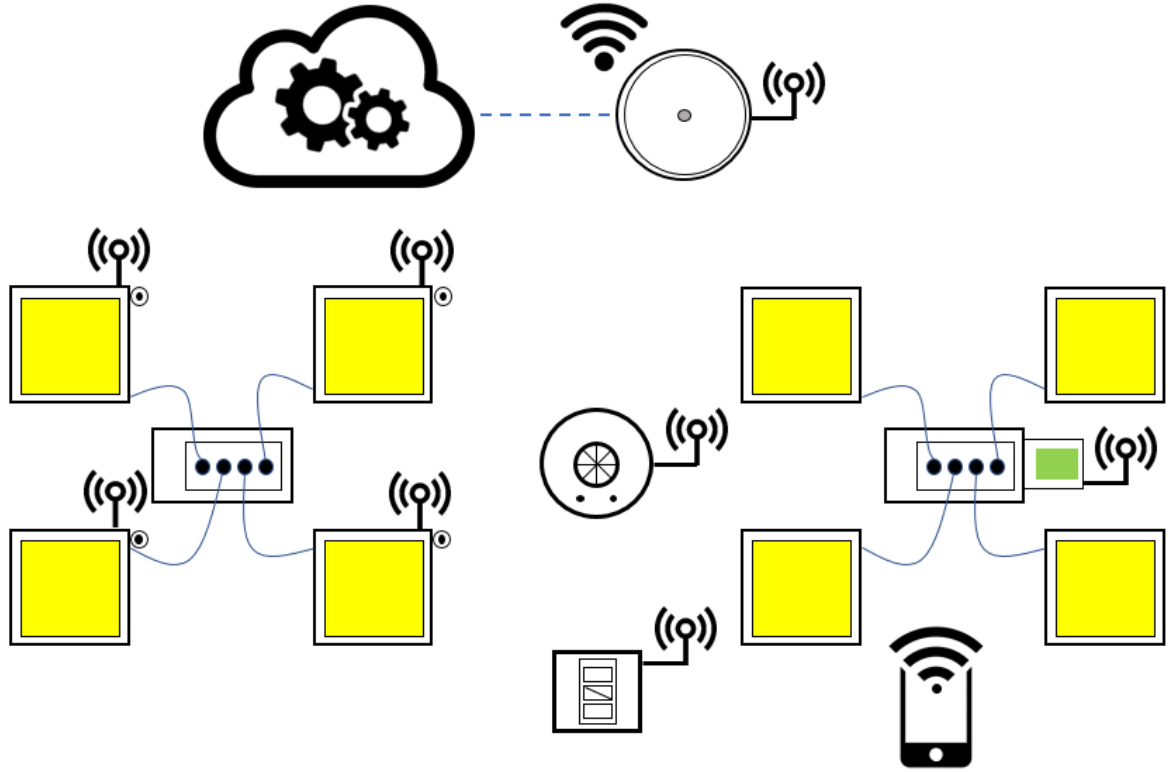
Most companies offer service agreements to keep systems current with the latest standards – make sure you have one!

WIRELESS CONTROL SYSTEMS

If you are providing lighting products today, there is a good chance that they are already being used in combination with wireless technologies. Most systems today offer a combination of wireless and wired topologies so they can add value to the occupants, while still being integrated into the backbone of the building.

The first devices that went wireless were user interfaces (i.e. switches, keypads and sensors), which were combined with more traditional control technologies, such as DALI and more recently DALI-2.

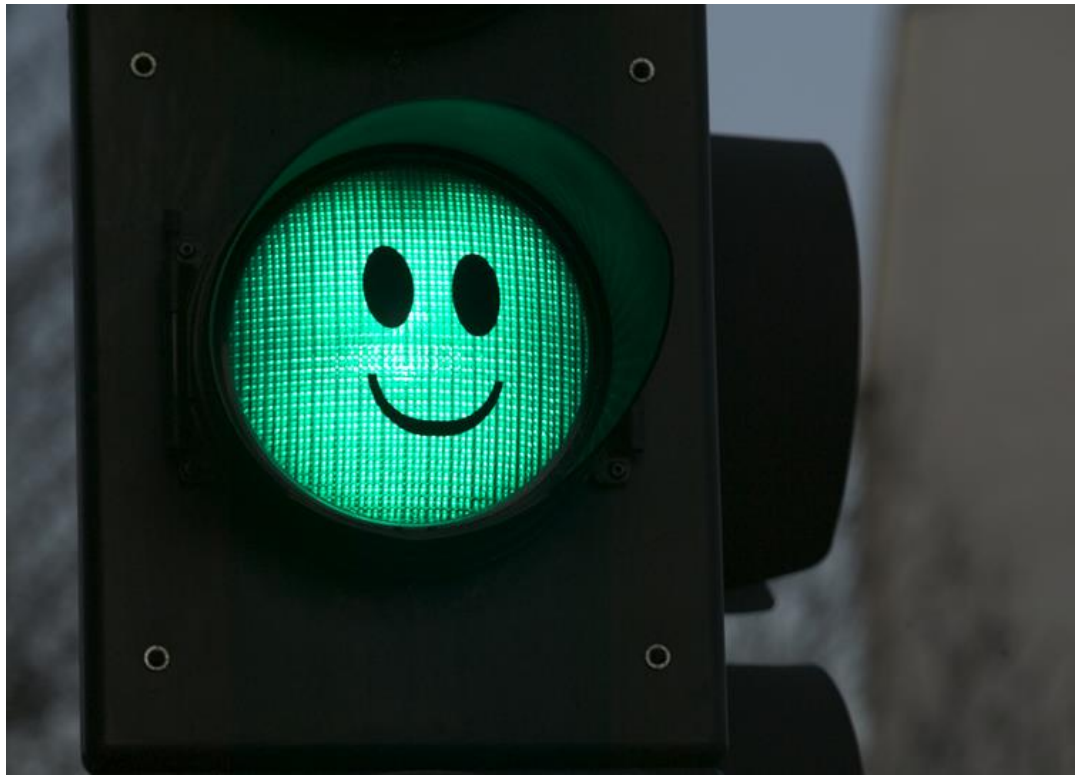
Depending on the application you may want to add a wireless sensor to a luminaire, or you could add a wireless lighting control module to a marshalling box, or maybe both.



CONCLUSION

Work with reputable manufacturers that understand your applications and use certified products.
Design your system with your application in mind, and follow simple common sense practices when designing your installation.
Set up your system to meet your customer needs, and always test it.
Security and maintenance are now processes, do not let anyone tell you otherwise.

Wireless opens up a world of opportunity for the lighting industry, so do not be left behind as we move towards the Internet of Things.



theLIA

This mini guide has set out what can be achieved by wireless lighting control systems. To find out more detail on the design, specification, procurement and installation of a control system, as well as the practical issues and technologies available, please contact the Lighting Industry Association or go to **www.thelia.org.uk** to find out about further guides and training courses.

THE LIGHTING INDUSTRY ASSOCIATION