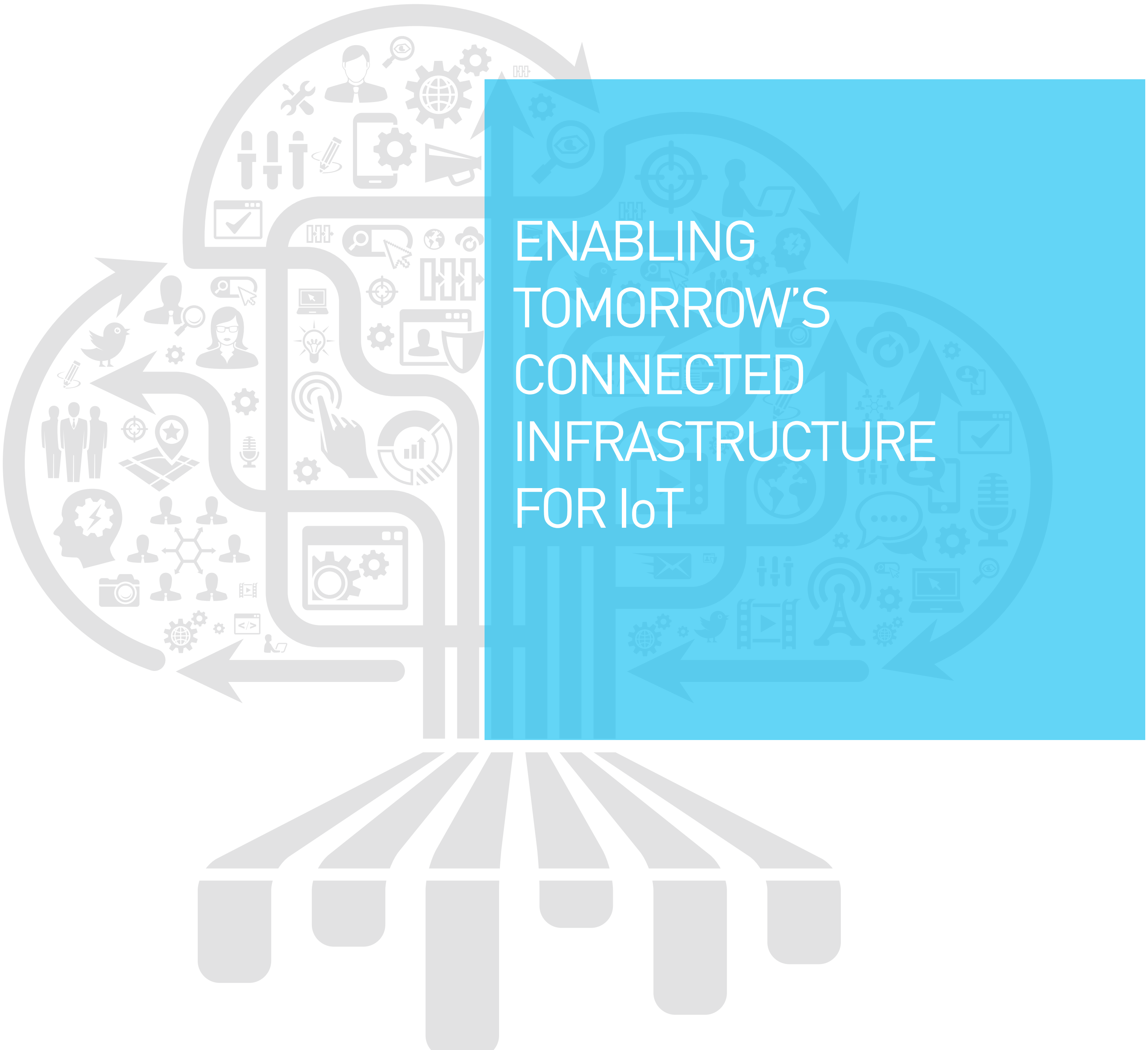
A brand of legrand



ENABLING TOMORROW'S CONNECTED INFRASTRUCTURE FOR IoT

Rudy Montgelas
Sr. Technologist
DATA COMMUNICATIONS
Legrand, North America

ORTRONICS®

INTRODUCTION

The need for the "Connected Infrastructure of Tomorrow" is approaching faster than you think. With the Internet of Things (IoT) there are new and critical considerations to think about as one prepares for what's ahead. Are you ready for it? To start planning and preparing now for tomorrow's network, we have to understand the requirements for power, light and data today. We have to be smart about the future[1]. What will the world we live, play and work in be like 10-15 years from now? One can only guess, but there are some important things to consider today, when we design the infrastructure to support tomorrow's needs being driven by billions of IoT connected devices.

WHAT IS AN IoT CONNECTED DEVICE?

The Internet of Things is comprised of networks of uniquely identifiable endpoints or "Things" such as smart thermostats, telephones, security cameras, security badges and more. These devices support various applications by collecting useful data with the help of various existing technologies, and then autonomously communicating the data between other devices to make enhancements to the surrounding environment, all without human interaction. Connected devices often leverage internet protocol (IP) and many are Power-over-Ethernet (PoE) ready.

Growth in the IoT marketplace is staggering, and the network bandwidth capacity and data storage demands placed on the connected world infrastructure are expected to be phenomenal because of it. In 2008 the number of things connected to the Internet exceeded the number of people on Earth[2]. By 2012, the number of POE-powered devices was estimated at 100 million. By 2020, about 250 million cars are expected to be connected to the internet, and the number of IoT devices is estimated to exceed 100 billion objects, or about 26 smart objects for every human being on Earth. As another example, Amazon has sold over 3 million Echo wireless speakers and personal digital assistants in the U.S. since its launch in late 2014, including one million during the Christmas shopping season in 2015. More than half of the purchasers use it for more than just a voice controlled music streamer[3].

IoT BENEFITS

The benefits derived through connected devices and supporting systems can be described as an enhancement to the user's environment by:

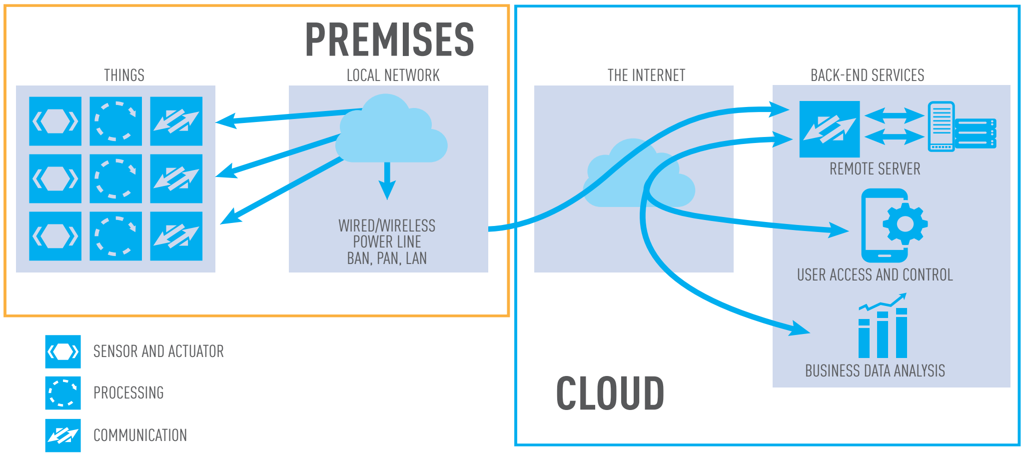
- Creating and delivering new experiences and services for customers
- Improving or customizing products to create new business models
- Automating processes to reduce response times
- Understanding business operations in real time
- Making accurate predictions to take appropriate actions
- Managing assets and assuring security
- Providing automated system monitoring, real time support and maintenance

These benefits also enable a person to manage their day to day lives more effectively and efficiently through better delegation, immediate attention to changes as they arise and improvements in their daily processes. For instance, extremely small size wearable devices today, such as smart watches, can wirelessly communicate, analyze and report the state of the wearer's temperature, heartbeat, physical activity and location for sports and medical applications.[3] Mobile devices such as unmanned aircraft systems (drones) can be used for visual monitoring of oil and gas pipelines, along with the sophisticated lasers and detectors they employ, to report back video surveillance and security information. Implantable devices in a dog's neck or collar can provide information on its whereabouts and health directly to the owner's and veterinarian's cell phone. The IoT applications are many and span across numerous industries.

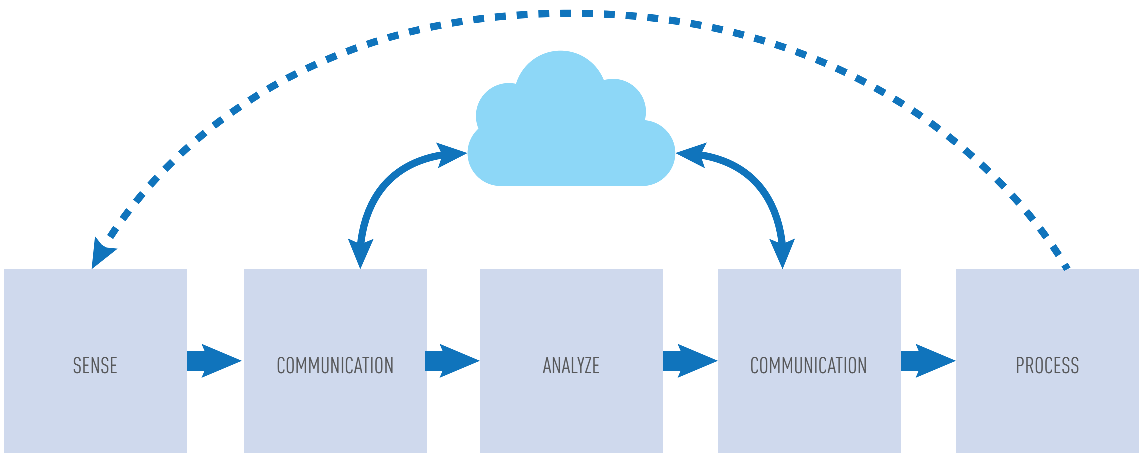
CONSIDERATIONS FOR TOMORROW'S CONNECTED INFRASTRUCTURE

With the mobility offered by connected devices, the idea of Bringing Your Own Devices (BYOD) to work is rapidly catching on, creating a requirement for more sophisticated Power, Light and Data (PLD) converged networks in commercial buildings, offices and data centers. This will enable enhanced user experiences with the added ability to utilize and manage PLD through shared communications. The network infrastructure will be required to support tomorrow's connected devices and application needs.

IoT devices are usually IP addressable end points that can utilize the IoT framework of Edge processing coupled with the intelligence of the Cloud. IoT devices also contain the hardware and software necessary to perform smart functions locally and process that information to create beneficial actions. As we look at what's going to be required for future appliances, mobile devices, computers, wearables, and even the next autonomous vehicle, some common and important elements are necessary no matter the operating space. Whether in your home, at work or travelling, the idea is to drive more value to the end user and their environment through the interaction of software programming, sensors and communicating devices that can all function together intelligently as a system.



IoT devices are designed to provide us a benefit. These devices Sense – Communicate – Analyze – Communicate and Process something usually in a sequential loop. The "communication" element is a common and important part of the loop because it creates or enables a linked backbone for the whole system to communicate to itself and to the Internet.



"Enabling the Infrastructure for IoT" is the effective interconnection of communicating devices, to themselves and to the Internet through the use of structured cabling or twisted-pair cables, to physically wire shared wireless networks such as Wi-Fi, cellular and Bluetooth.

SOME EXAMPLES OF IoT CONNECTED DEVICES ARE:

- Webcams and security cameras
- Web based programmable thermostats
- Remotely controlled power outlets
- Gateway hubs
- Electronic door locks
- Alarm systems
- Internet ready appliances
- Smart soda machines
- Occupancy sensors
- Intercoms and web based speaker systems
- Environmental monitoring devices
- Low Voltage Intelligent LED Lighting
- Wireless Access Points
- Sound masking
- Building Management Systems
- Digital signage
- Visible Communication (e.g. Li-Fi)

IoT BUILDING BLOCKS

A Connected IoT device is one that is able to sense and collect information from locally occupied spaces, or the environment, and process or act on its own accordingly. It can be through a local network supporting Internet based software services and application services, commonly referred as "Apps" running over connected communications networks.

A Gateway is an IoT enabling device for machine to machine (M2M) communications that provides a portal to the communications network connecting appliances in the home, workplace or "Smart City"

The Edge is an IoT concept describing the migration of computing applications, data, and services away from centralized nodes to the logical extremes of a network, thus enabling analytics and knowledge generation to occur at the source of the data.

Fog is an IoT architecture approach that uses a collaborative multitude of end-user clients or near-user edge devices to carry out a substantial amount of temporary storage, communication, control, configuration, measurement and management.

Security is one of the largest challenges to individuals and companies planning to adopt IoT solutions. Since IoT devices can be connected directly to the internet, it is critical to have Information Access Management (IAM) protocols and services in place enabling only individuals authorized to access specific resources at the correct times and for the right reasons.

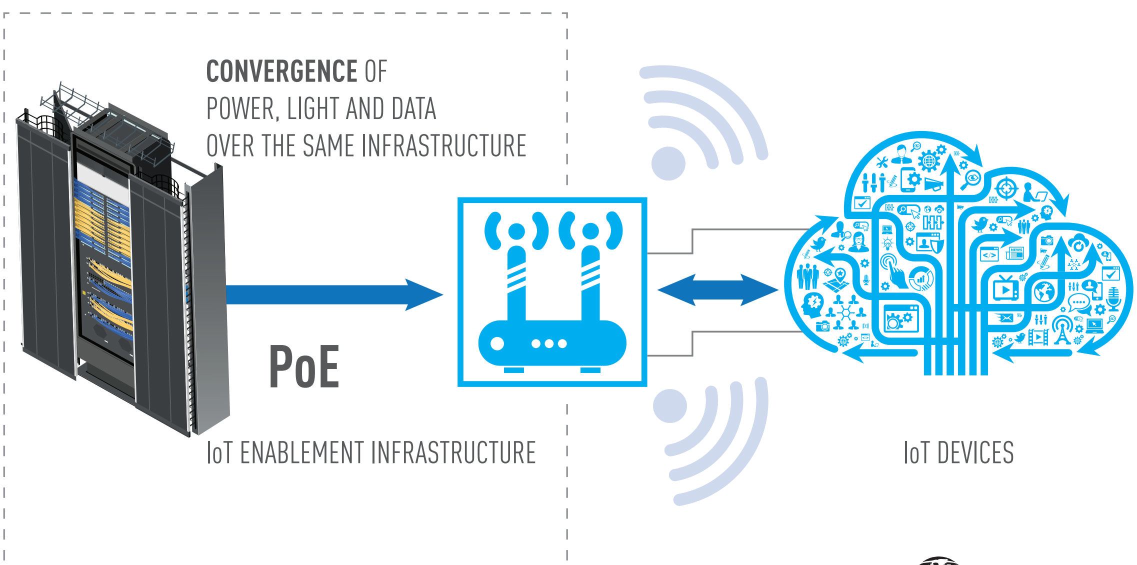
THE EVOLVING TECHNOLOGICAL LANDSCAPE

Since the dawn of the internet, our interactions have traditionally been Human to Human (H2H) or Human to Machine (H2M and M2H) for storing and processing digital voice, video and data information. The IoT connected world is pushing this evolution toward intelligent Machine to Machine interfaces (M2M) as we embed that intelligence into everything around us. It seems logical that, along with rapid advancements in computing combined with more advanced algorithms, we are setting the stage for the next wave of artificial intelligence that brings machines closer to humans (M+H). As these devices become more intelligent and prolific, Machine to Machine interfaces, and the direct human interaction with them in a more natural manner, will be more prevalent.

H2H RISE OF AVAILABILITY	H2M RISE OF REACH	M2H RISE OF MOBILITY	M2M RISE OF INFORMATION	M+H RISE OF INTELLIGENCE
HUMAN TO HUMAN ACCESS TO EVERYONE ▪ Voice communication ▪ SMS	**HUMAN TO MACHINE** ACCESS TO INFORMATION ▪ e-Commerce ▪ World Wide Web ▪ Social media	**MACHINE TO HUMAN** ACCESS TO RELEVANCE ▪ TV and radio ▪ e-Magazines ▪ e-Billboards ▪ Websites	**MACHINE TO MACHINE** ACCESS TO INTELLIGENCE ▪ Networked sensors ▪ Networked computers ▪ Connected devices IoT	**MACHINE AND HUMAN** ACCESS TO AUTOMATION ▪ Artificial intelligence

CONVERGENCE

Convergence can actually mean many different things. Historically, the term had been applied to communication networks where the convergence of Internet Protocol (IP) based devices had allowed the use of the Internet to digitally connect voice and data services such as public switched telephones and computer networks. Today, it means more than that, especially when we think of all the lighting, sensors, devices and computers connected to the public network through secure interfaces. All of these things require not only links to provide conduits for data, computation analysis and control, but also power to allow them to function effectively and efficiently.



Trade Convergence is a result of the reduction in the overlap of the trades that will be required to install IoT "things" and the new trades that will be able to implement them. An example of trade convergence is the low voltage cabling contractor's ability to install the overhead PoE intelligent LED lighting and cabling without the need for costly high voltage AC cabling or a building inspector to perform a final AC wiring inspection.

HOW DO WE POWER ALL OF THESE THINGS?

More and more, connected devices such as sensors, computers and robots, are becoming part of the spaces that we live, work, travel and play in. To operate these electronic IoT devices, they ultimately need to be powered. In order to achieve a reduction in energy consumption and an increase in efficiency compared with traditional high voltage AC systems, DC power is increasingly becoming the power of choice. Power has traditionally been supplied to a connected device through the local power mains grid, where AC power had to be converted to DC. DC power, directly from batteries and/or solar cells could also provide the power or be combined as a backup for the AC Power.

Hybrid power and data communications cabling, containing separate conductors for the data and power within the same sheath has often been used to remotely power long distance surveillance video cameras.

Power can also be delivered remotely through low voltage Power-over-Ethernet cabling from PoE-based switches. A significant benefit of the connected infrastructure is that it not only provides the communication links, but also the power to the connected devices and/or their supporting gateway devices using converged data with low voltage direct current (DC) power. Converging the power and data over the same cabling infrastructure is a more cost-effective and simplified option than running high voltage and communication cabling separately. It also facilitates the capability for energy consumption monitoring and environmental sensors, as well as remote security and software control.

POWER-OVER-ETHERNET

Power-over-Ethernet, or PoE, consists of several standardized systems which enable the transfer of data and power through a single Ethernet cable, from the power source equipment (PSE) to several low voltage powered devices (PD), such as cameras, VoIP phones, Wi-Fi routers and others.

For true local converged power and data using PoE, DC power is injected by the PSE into the same copper conductors that carry the digital communications signals. PoE-enabled PDs separate the power from the digital data stream. Depending on the application requirements, DC power can be injected either End span by the PoE enabled switch in the data center or Mid span by a device located in the wiring closet.[4] Data center switches, that have the PoE capabilities built right in to the copper ports, are becoming more common in data center telcom room (TR) and wiring closets.

DC power, delivered through PoE converged cabling systems, is a critical building block for IoT devices and applications. PoE power from data centers is an important enabler to IoT in all of our spaces, especially for new builds, since building control systems are becoming more intelligent and are proactive rather than reactive. Low voltage DC powered devices eliminate the need for bulky wall outlets and AC to DC adapter cables, thereby reducing heat dissipation, energy usage and component costs. Easier maintenance and installation is a direct result, along with the potential for less system downtime. Power can also be provided more effectively to remote locations using PoE. Additionally, power backup and redundancy can easily be supplied by an uninterruptible power supply (UPS) or other battery backup system.

Worldwide standards are also being developed for PoE based systems under the auspices of the IEEE and the TIA. The PoE based standards, which define PD operating powers, are currently governed by the IEEE which has ratified the standards for Type 1 PoE and Type 2 PoE+ devices as shown in the tables on the following page. Type 3 PoE++ and type 4PoE++ device standards are expected to be ratified in 2017.

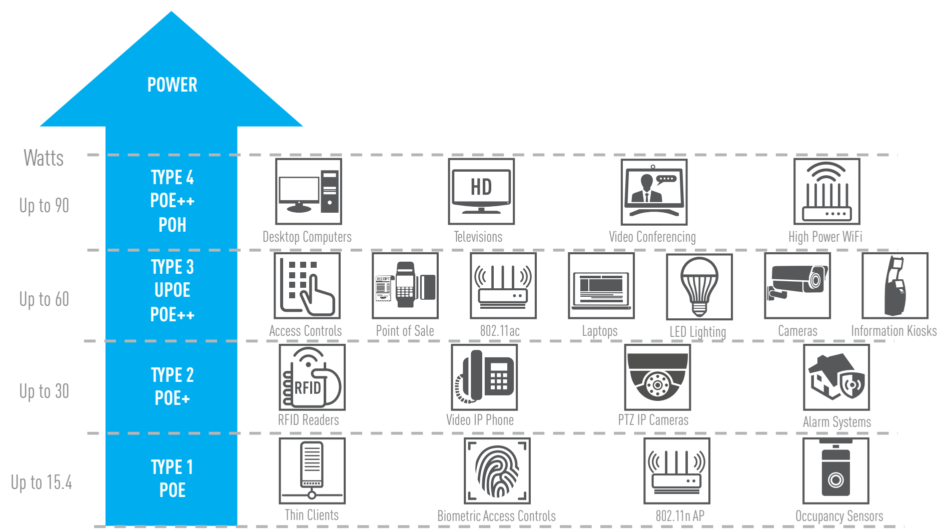
POE – POWER OVER ETHERNET

STANDARDS AND APPLICATIONS

ORGANIZATION/STANDARD	WATTS FROM POWER SOURCE EQUIPMENT	APPLICATIONS
IEEE 802.3AF 2-Pair PoE	Up to 15.4W	802.11n WAPs, Access Control, Thin Clients, IP Phones,
IEEE 802.3AT 2-Pair PoE+	Up to 30W	IP Cameras, Alarms, Video IP Phones, RFID Readers
IEEE 802.3BT 4-Pair* PoE++ Type 3	Up to 60W	Access Control, IP Cameras, 802.11ac WAPs, Point-of-Sale Readers
Cisco UPOE	Up to 60W	Access Control, IP Cameras, 802.11ac WAPs, Point-of-Sale Readers
IEEE 802.3BT 4-Pair* PoE++ Type 4	Up to 100W	Televisions, Desktop Computers
HDBaseT Draft IEEE 1911 Standard**	Up to 100W	Televisions, Computers, Projectors

Notes: *Proposed standards, not yet ratified. **Active IEEE working group on ratification of HDBaseT as an approved IEEE standard. See the full working group and active projects regarding HDBaseT on IEEE website under "HDBT5 - HDBaseT 5Play Working Group".

Power over HDBaseT (POH), is a version of PoE specifically for multimedia applications, enabling up to 10.2 Gbps of uncompressed video and audio, 100BaseT Ethernet, control signals and power sharing over the same cable, across distances of up to 100 meters using RJ45 connectors. Other commercial



PoE solutions are also emerging, such as the 60W Universal PoE (UPOE) from Cisco.

When considering a connected infrastructure design, it is important to start by determining the type of IoT applications that will be implemented, now and for the future, and then determine the power supply requirements needed to power the connected devices.

INTELLIGENT LED LIGHTING: PROOF OF PLD CONVERGENCE

PLD convergence is Power, Light and Data supplied all over low-voltage Ethernet cabling in commercial buildings and office spaces. Intelligent LED lighting in office or residential architectural spaces has automated and functional capabilities beyond those of traditional incandescent or fluorescent lighting systems. Cisco's Digital Ceiling Framework is an example of such an intelligent LED lighting system.DC power and control signals for the lights are delivered by Cisco 3850 PoE switches through the Ethernet structured cabling system, which significantly reduces energy usage and allows tailoring of the user's lighting experience. PoE power is delivered centrally from the switches to the LED lights and to other PoE powered PD connected devices. Software controls the lighting's intensity and color through Apps on mobile devices such as smart phones and personal computers.

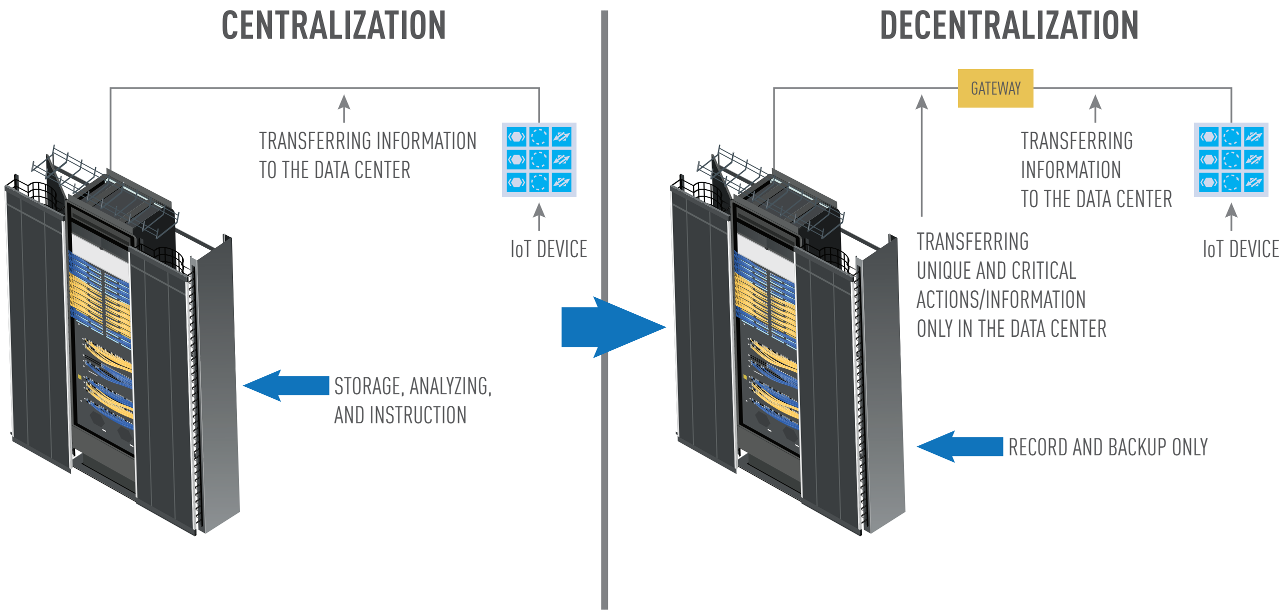
Intelligent LED lighting systems generally require higher operating powers than traditional PoE systems. This places increased current handling demands on the connected cabling infrastructure. So, one must evaluate the properties of the overall cabling system. The lower resistance and higher current rating of Superior Essex's PowerWise® Ethernet copper cabling provides higher power efficiency and better heat dissipation. Ortronics' RJ-45 High Density Jack (HDJ) design locates the spark gap erosion away from the jack's data contact area, and provides headroom above the IEEE requirement for current carrying capacity.This complete cabling system then extends the performance and long-term reliability of the link to the LED lighting fixtures.

Along with PLD convergence, LiFi (Light Fidelity) wireless networking is a relatively new technology. It utilizes visible light communications by modulating the overhead LED lighting fixtures with the network communications data to provide a localized, line-of-sight free-space optical data link. Some of the advantages of LiFi over WiFi are a reduced susceptibility to interference from multiple RF sources and the wider operating spectrum of the visible LED lights. However, the need for line-of-sight operation with LiFi restricts, at this point, the area coverage and the mobility of connected devices.

CENTRALIZED VERSUS DECENTRALIZED ARCHITECTURES

In centralized architectures, IoT connected devices transfer their sensor data information and computing requests directly back to the data center where the processing and storage of information is performed by servers running specific Apps through switches. Requests for action and processed data are in turn sent back to the connected devices from these centralized applications.

In the decentralized (or zone) approach, edge computing is enabled by Apps running on embedded micro-processors in the connected devices and the gateways, which pushes the responsibility for computing and information processing out to the local devices. Instead of IoT devices such as security cameras, smart thermostats and building automation systems communicating back to the data center for instructions or data analysis, the information is processed locally so that network latency does not affect IoT device performance. Only the transfer of unique and critical information is required to be sent back to the data center. This allows for faster processing of streaming data and communications with other devices to accomplish tasks and allow systems to work autonomously by delivering information to the decision-making points faster and more efficiently. The decentralized approach also reduces the "Big Data" communications impact since data can be scrutinized and processed at the edge first, so that only the useful data need be stored in a data center SANs.



It is expected that a rapid adoption of the decentralized architecture design approach will occur through the increased use of gateways to support applications such as security, occupancy, LED lights or LAN and Wi-Fi. This design approach may also help to consolidate telecom rooms (TR), where less rack space will be required and also create the need for higher performance backbone cabling such as CAT6A or fiber to run from the TRs to the gateways.

With decentralized architectures, simpler, smaller, and cheaper IoT devices can run Apps on embedded micro-processing devices, and they don't need to be directly addressable from the data center. This closed loop zone security can reduce vulnerability to outside security attacks. In addition, it is easier to assure Data Governance (i.e. that the data remains local – which is supported by many global governmental data governance policies). Also, evolution of the presently installed IoT base infrastructure will make it easier to meet the future demands for new subscribers and applications based on a changing connected world market.

A Passive Optical LANs (POLs) or Ethernet Passive Optical Networks (EPONs) are an example of a hybrid type of LAN architecture using a single mode fiber and single mode SC/APC splitters from a centralized Optical Line Terminal (OLT). Decentralized power is sourced at the connected devices and provided by a local ONT (Optical Network Terminal).

DENSITY AND SPACE OPTIMIZATION

The ability to easily and effectively manage multimedia copper and fiber connections will be necessary because of the convergence of data, video, and security and AV in the telecom room. The HDJ series connection solutions from Ortronics provides flexible multimedia modular connectivity for up to forty-eight RJ-45 or F-Connector copper modules or up to 576 fiber connections with MTP®/MPO adapter modules in a 1U rack space.

Increased needs for port density and space optimization in both the telecom room and the data center will drive the need to support the growth of the number of connected devices, data storage, and computing speeds necessary to keep up with the IoT demands. The ability to migrate from 10 gigabit connections today, to 40 and 100 gigabit optical connections tomorrow, is often necessary in the data center today and will become more prevalent in the telecom room environment. These parallel optical fiber transmission systems employ eight and twelve fiber MTP/MPO parallel fiber optic array connections, optimizing connector space while also providing increased data center transmission speeds*.

Notes: *MTP is a registered trademark of US Conec.

BANDWIDTH AND LATENCY

With the vast growth of connected IoT devices, more and more systems will be collecting information and acting through the Internet. Processing this information will require a network with the necessary performance to transfer both information and power without significant delays or interruptions. Not only is the bandwidth, or information transmission capacity of a connected infrastructure important, but so is the latency, or delay in transmitting critical information from the network core to the Edge. Bandwidth and latency are two distinct performance parameters that are important to many IoT device applications. For instance, time critical functions such as heart rate monitoring, or precisely timed mechanical actuations based on a sensor's response, may not be able to handle significant transmission delays through the network.

SUSTAINABILITY

Infrastructure improvement or expansion projects required to support the adoption in IoT in commercial buildings can also be an opportunity to select solutions with environmental product declarations (EPDs) or health product declarations (HPDs) – which contribute points to a LEED project. Ortronics and Superior Essex have produced the Product Environmental Profiles (PEPs, an industry specific version of EPDs) which are available online for the entire range of cabling systems and associated physical infrastructure solutions. LEED points may be available when these products are used in qualified cabling installations. Superior has also attained the first "Zero Waste to Landfill" certification ever achieved by a communications cable manufacturer.

SUMMARY AND CONCLUSIONS

The Internet of Things, through connected devices, is placing significant demands on networks to the point where a connected infrastructure is becoming more critical than ever when designing tomorrow's networks.

The Ortronics approach to a Connected Infrastructure delivers maximum network performance, time savings in installation and moves, adds or changes, space optimization for faster return-on-investment, superior customer experience as well as sustainability by design.

Planning for the future when designing your converged power, light and data infrastructure is going to require careful consideration of many key design aspects such as:

- Centralized vs. decentralized architectures depending on the IoT application requirements
- Floor-to-ceiling data and PoE connectivity options to support PLD
- High performance cabling systems to handle the necessary power, bandwidth and latency
- Sustainability and energy savings
- Proper cable management and pathways to support migration and ease of maintenance
- Scalable Telecom Rooms and data centers for flexibility and growth
- Increased physical and software-based security

Ortronics offers a broad breadth of end to-end solutions for the building network and the data center. Through our Connected Infrastructure approach, we combine multiple applications, industry leading customer advocacy, design and support teamwork, to comprehensively address the challenges of the IoT world for today and tomorrow.

REFERENCES:

1. Future Smart: Managing the Game-Changing Trends that Will Transform Your World, by James Canton, Da Capo Press, January 27, 2015.
2. Cisco, GE, Google, IEEE Spectrum.
3. Consumer Intelligence Research Partners (CIRP) report.
4. Lighting the Way for Innovation at Launch Fishers with Digital Ceiling PoE LED Solutions, Legrand Data Communications Case Study, July 2016

A brand of legrand®

Europe/Middle East/Africa
Great King Street North
Birmingham, B19 2LF
United Kingdom
Phone: +44(0).796.730.9227

Latin America
Montes Urales NO. 715 3er Piso
Col. Lomas de Chapultepec
MEXICO D.F. - C.P. 11000
Phone: +52.55.5201.6450

Asia Pacific
3rd Floor Hang Seng Building, No. 200
Hennessy Road, Wanchai, Hong Kong
Phone (HKG): +852.9401.1885
Phone (China): +86.1392.4848.222

Level 2, OVAL Building, Hi-tech City,
Madhapur, Hyderabad - 500081, India
Phone: +91.40.4433.4234

ORTRONICS®

Global Headquarters
125 Eugene O'Neill Drive
New London, CT 06320
Phone: +1.800.934.5432
or +1.860.445.3900
Fax: +1.860.405.2992
www.ortronics.com

Follow Us