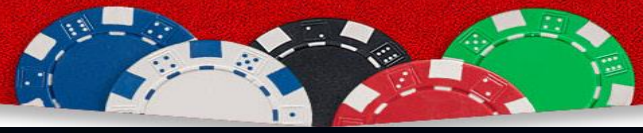


The IoT of Lighting Digital and Wireless Lighting

Chris Yorgey
Lutron Electronics
cyorgey@lutron.com

Tuesday, November 1, 2016 10:00 AM

LUTRON

Overview

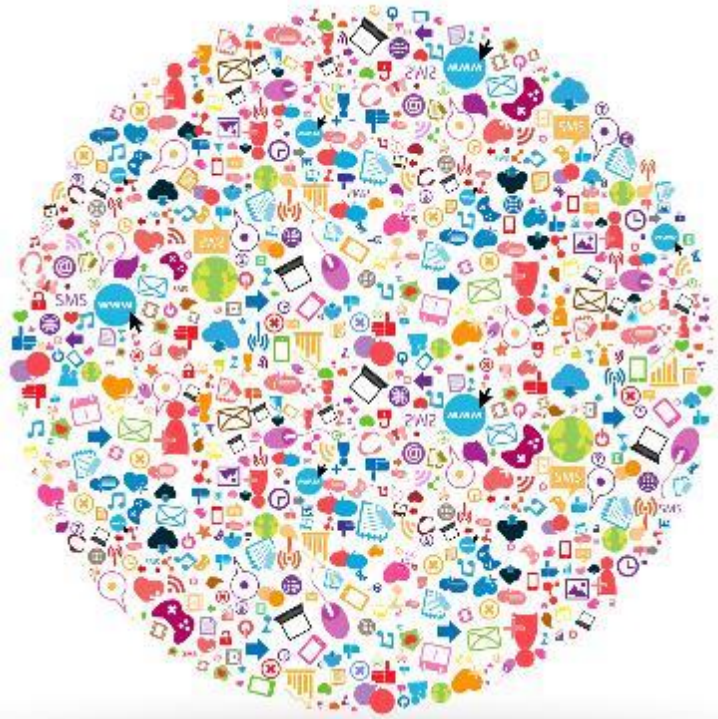
- Growth of the Internet, IoT and Solid State Lighting
- Overview of wired and wireless digital lighting control systems
- Guidelines for selecting a wireless lighting control protocol
- Current and future benefits of IoT lighting control systems
- Cybersecurity risks and best practices

Growth of Internet, IoT And Solid State Lighting

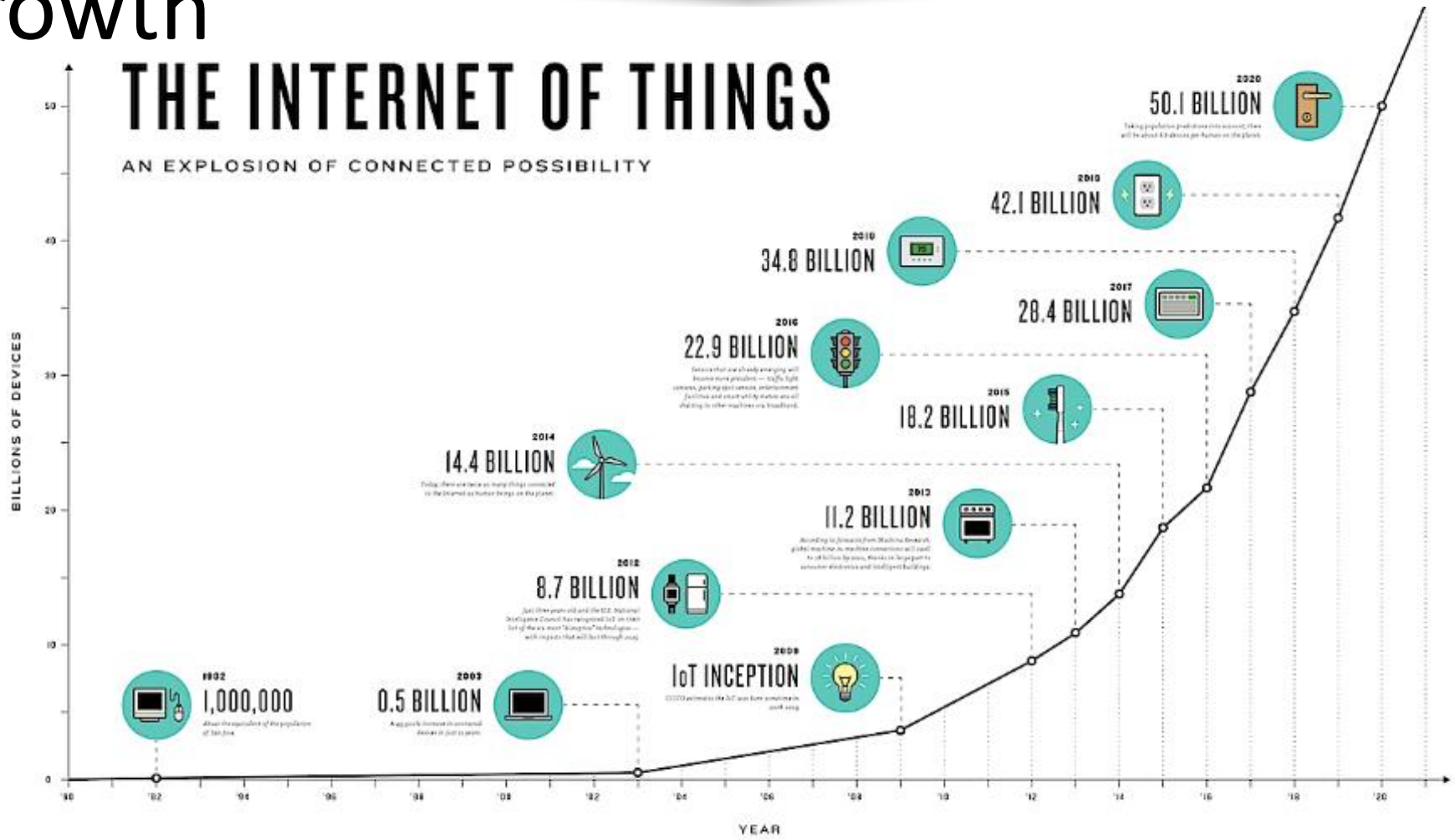
IoT Defined

The internetworking of physical devices, vehicles, buildings and other items embedded with electronics, software, sensors, actuators and network connectivity that enable these objects to collect and exchange data

https://en.wikipedia.org/wiki/Internet_of_things



IoT Growth



https://www.ncta.com/platform/industry-news/infographic-the-growth-of-the-internet-of-things/

IoT Growth

- 2005 - 500 million devices connected to the internet
- 2015 - 8 billion connected devices
- 2035 - Projection is 1 trillion connected devices
- We are 1% of the way into this transformation

Solid State Lighting /LED Growth

- **2003** - started the conversation about a new lighting technology
- **2005** - the first viable architectural LED lighting products
- **2010** - the first viable LED replacement lamps became readily available
- **2020** - DOE projects that 75% of our outdoor lighting will be LED (2014 report)

Digital Wired and Wireless Lighting Control

Digitally Addressable Lighting Control

- Fixture is able to connect to a network
  - "Smart" LED drivers connect directly to the network
  - Interfaces connect "dumb" drivers to the network
- Benefits
  - Control is independent of power
  - Easily reconfigure space
  - Collect data from fixture
    - Energy consumption
    - Lamp outage

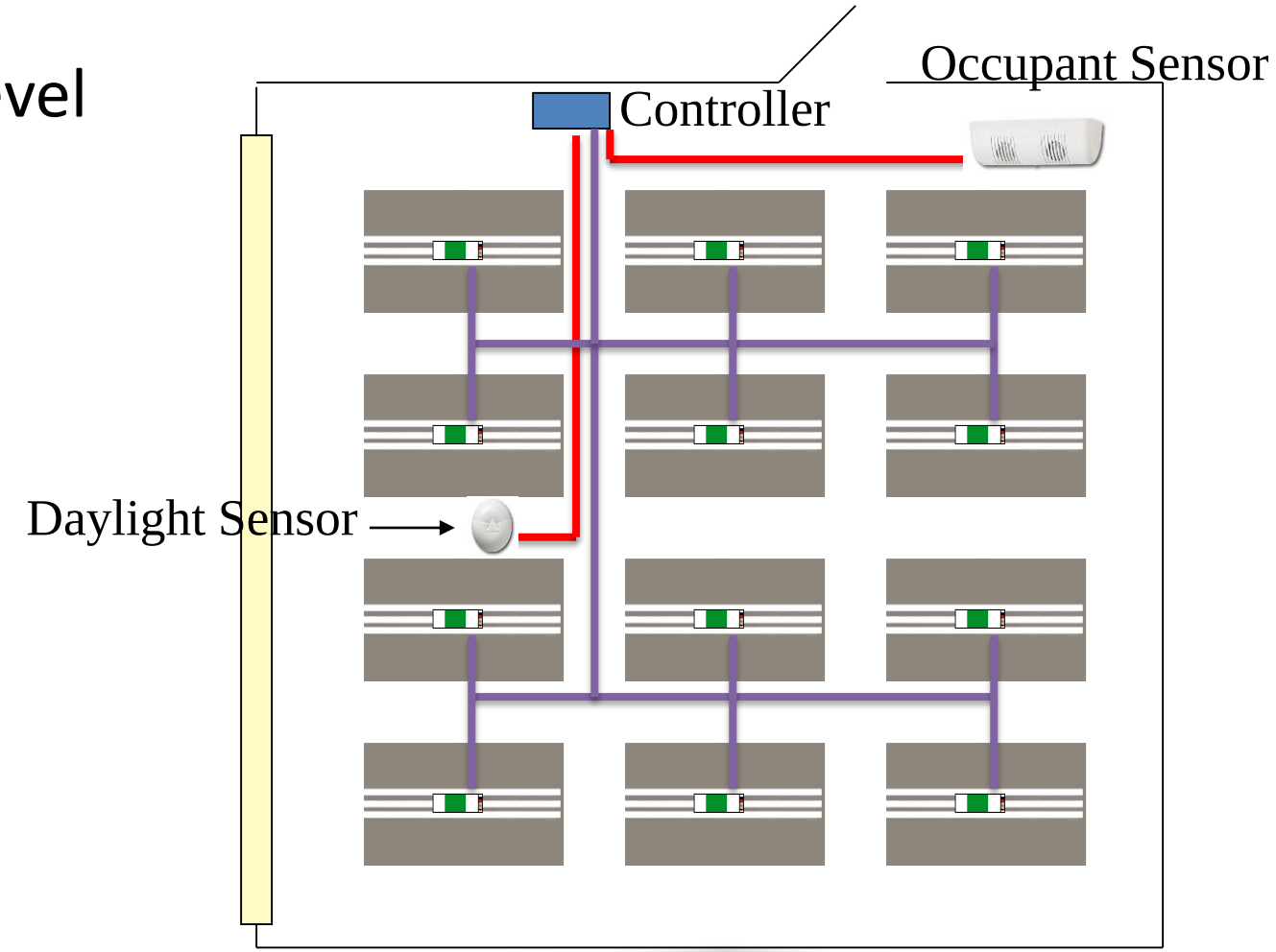
Wired Digital Lighting Control

Digital Addressable Lighting Interface (DALI)

- Networking protocol for digital addressable lighting
- Wiring simplified vs. 0-10V
  - Class 1 or Class 2 wiring
  - Hard-wired zones are eliminated
  - Polarity/topology insensitive
- Original DALI standard for drivers published 2000
- DALI 2 standard in development
  - Defines standards for controls
  - Requires product certification

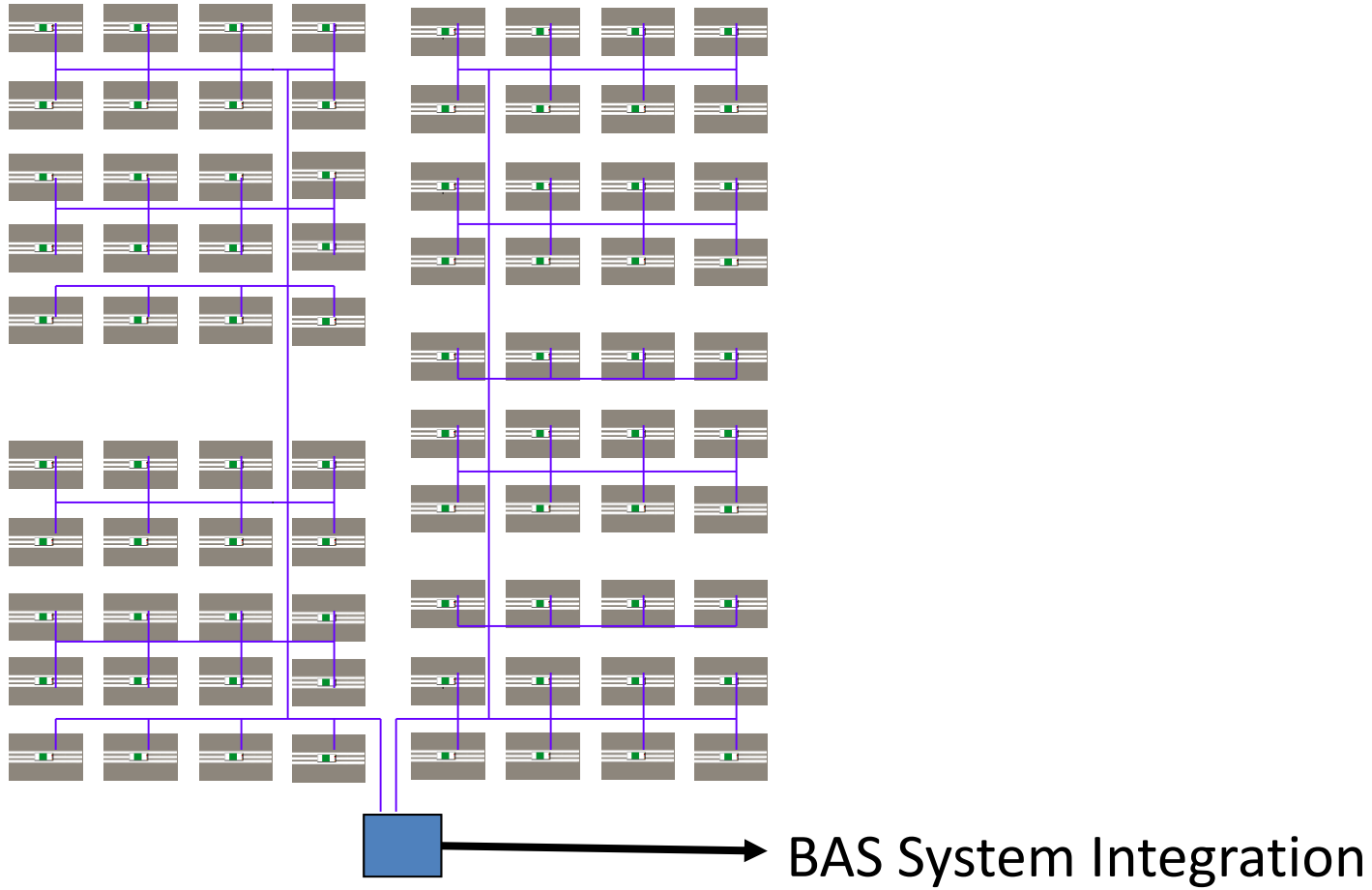
Wired Digital Lighting Control

Room Level



Wired Digital Lighting Control

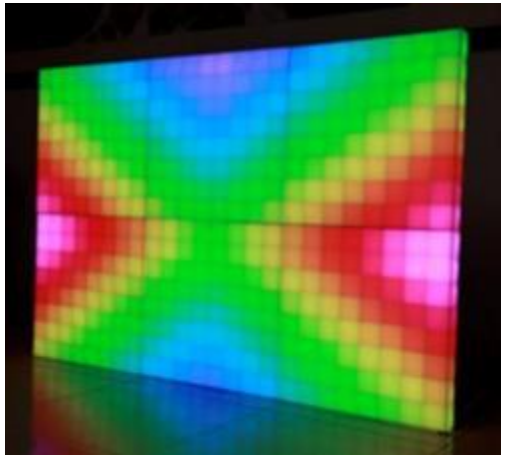
Building System Level



Wired Digital Lighting Control

DMX

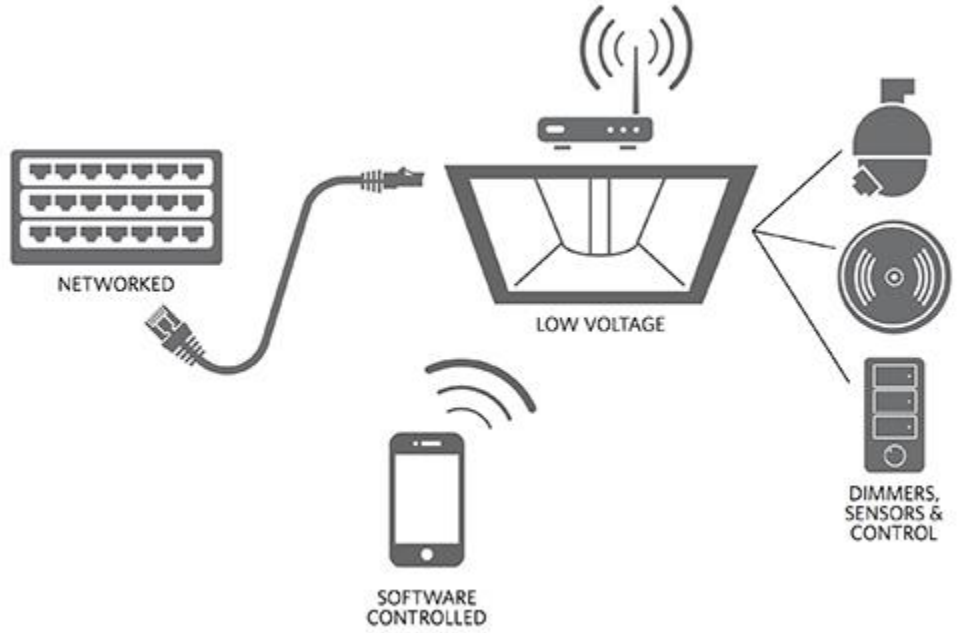
- Digital control protocol popular for theatrical applications
- 512 control points (channels)
- Wiring requires daisy chain
  - Challenging for general illumination
- RJ-45 connector with CAT5 wiring is common
  - Not the same as PoE
- DMX-RDM adds two way communication



Wired Digital Lighting Control

Power over Ethernet (PoE)

- Benefits
  - Inherently IoT
  - Lower installation cost (?)
    - Class 2 wiring
    - More cable
  - Efficiency (?)
- Challenges
  - Current carrying limits of CAT5/6 wire
  - Handling emergency lighting
  - IT or Facilities?
  - Young standard compared to other digital lighting standards
  - Limited fixture options



Digikey.com courtesy Maxim

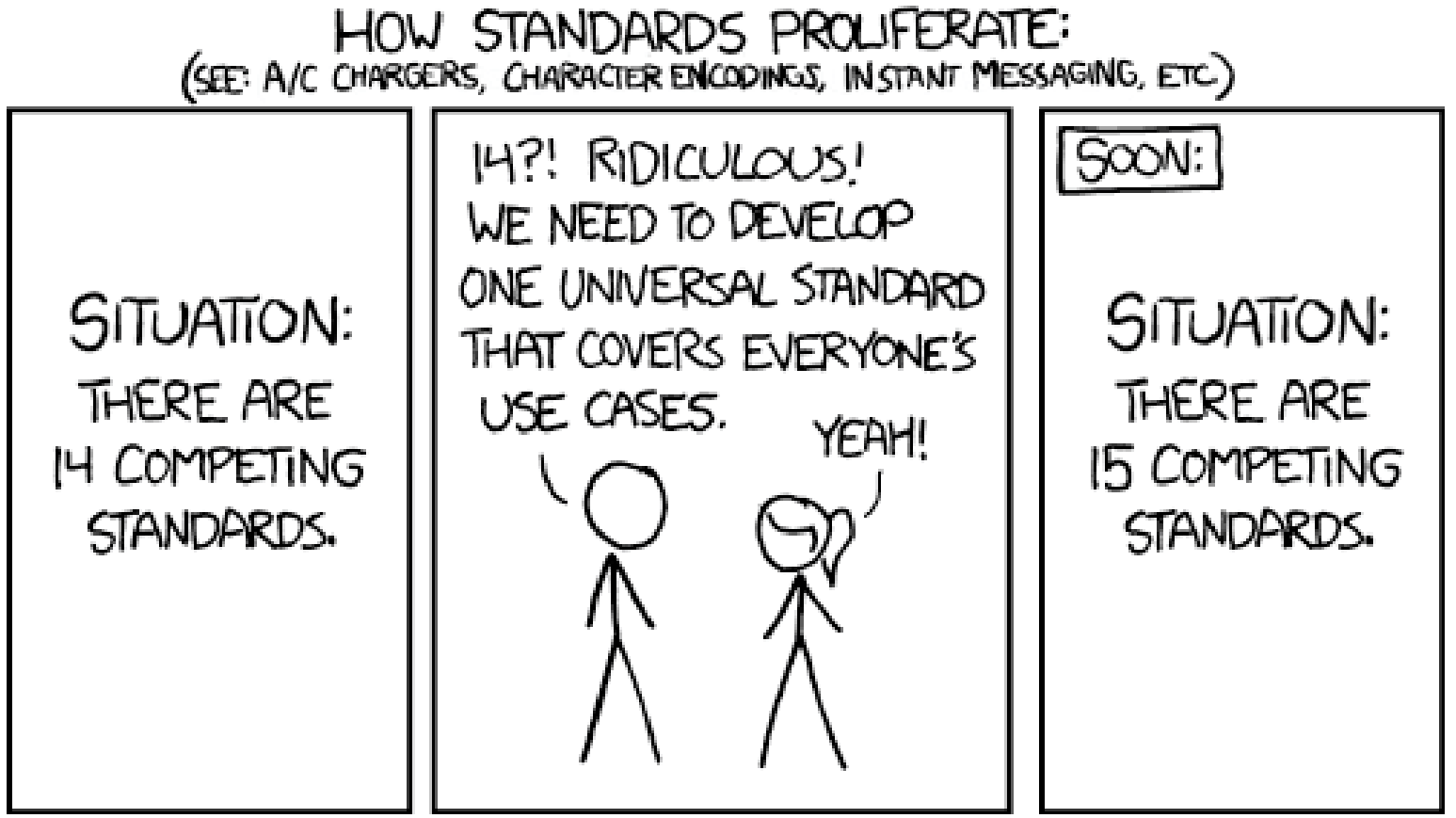
Wireless Digital Lighting Control

RF Technology

- Benefits
  - Ease of retrofit/renovation
  - Simplifies new construction projects
  - Cost-effective
  - Flexibility – move without rewiring
- Challenges
  - Reliability
  - Security
  - Energy consumption/battery life

Wireless Digital Lighting Control

- Wireless Protocols
  - Wi-Fi
  - Zigbee
  - ClearConnect
  - Z-Wave
  - Bluetooth/BLE
  - 6LoWPAN
  - Thread
  - 2G/3G/4G/LTE
  - NFC/RFID

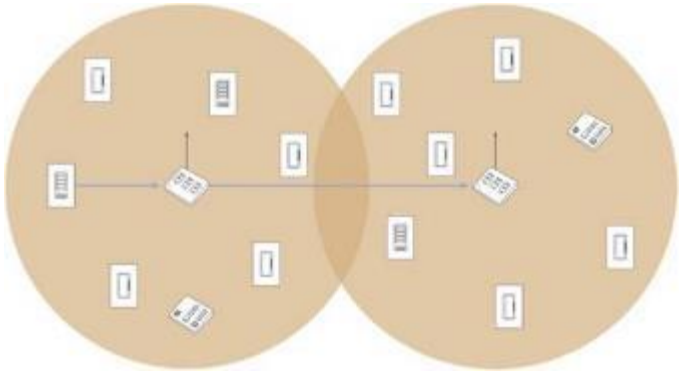


https://xkcd.com/927/

Wireless Digital Lighting Control

Evaluation Criteria

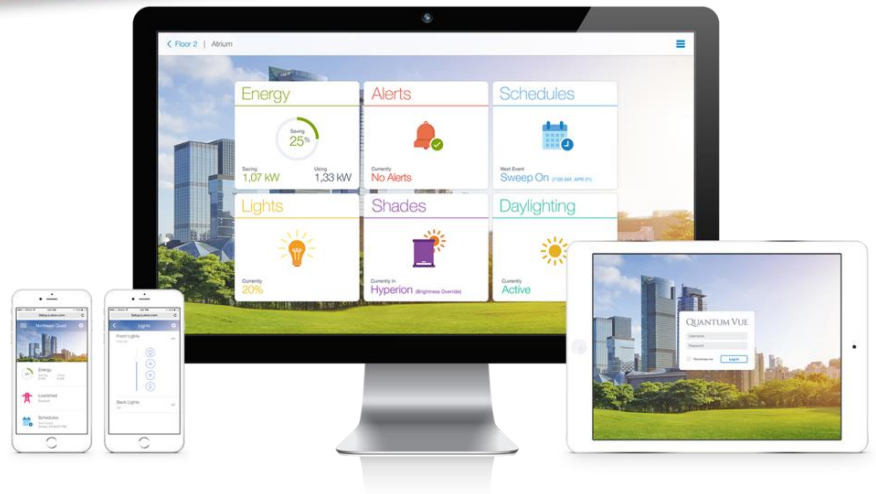
- Interference with/from other networks
  - Does the technology require a site survey?
- Frequency
  - Higher frequency = more attenuation
- Range
  - Look out for "works up to…"
- FCC regulations
  - Power
  - Duty cycle
- Fixed vs. mesh network
- Experience

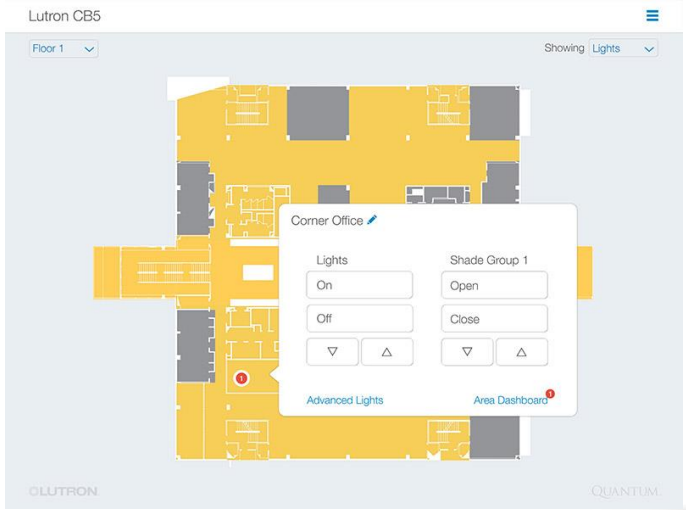


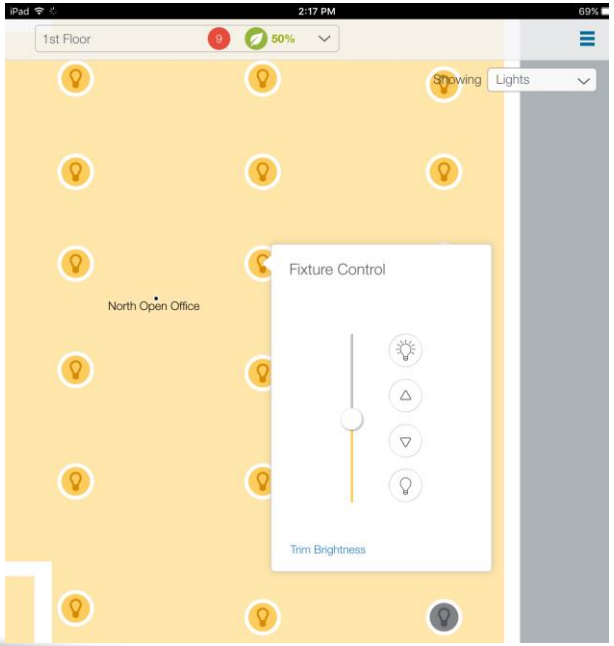
Benefits of an IoT Lighting Control System

Real-time Control

- Control lights in an area
- Individual fixture modifications
  - Dim light up or down
  - Task tune a single fixture

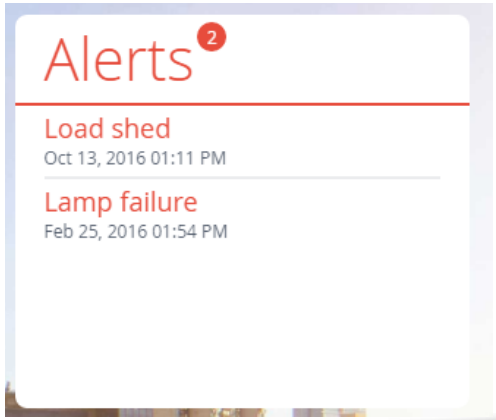


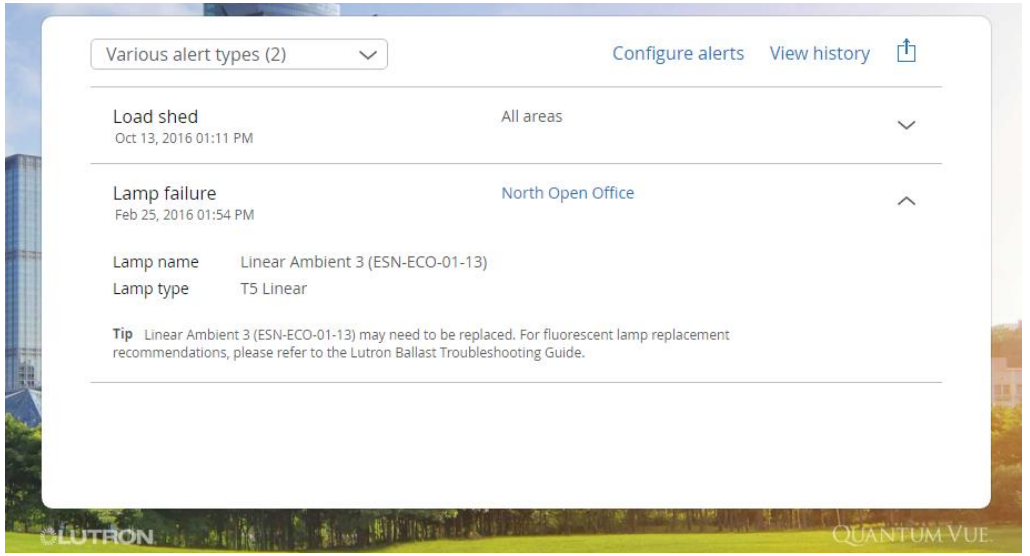


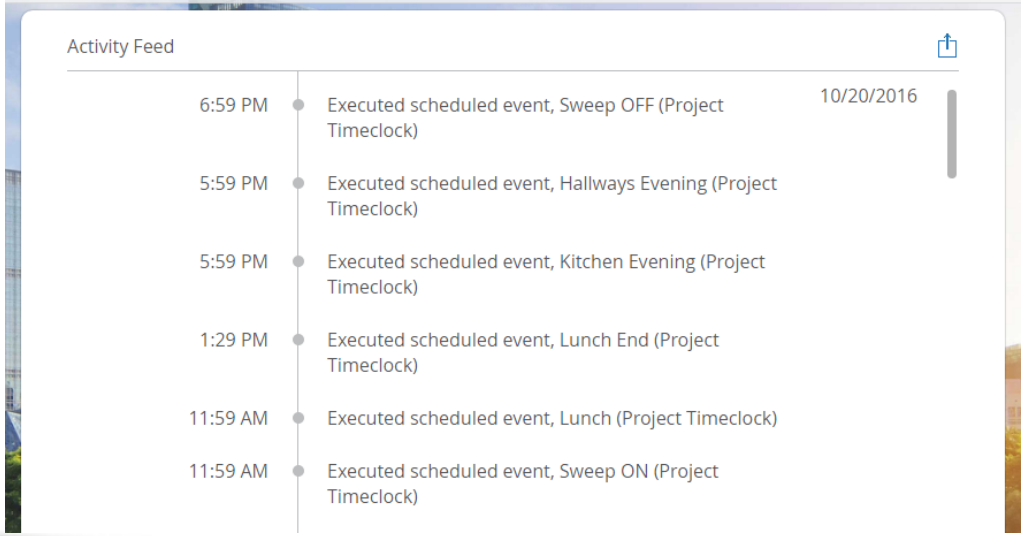


Diagnostics

- Dashboard of system status
- Email alerts of issues
  - Lamp nearing end of life
  - Lamp failure
  - Device not communicating
- System activity reports

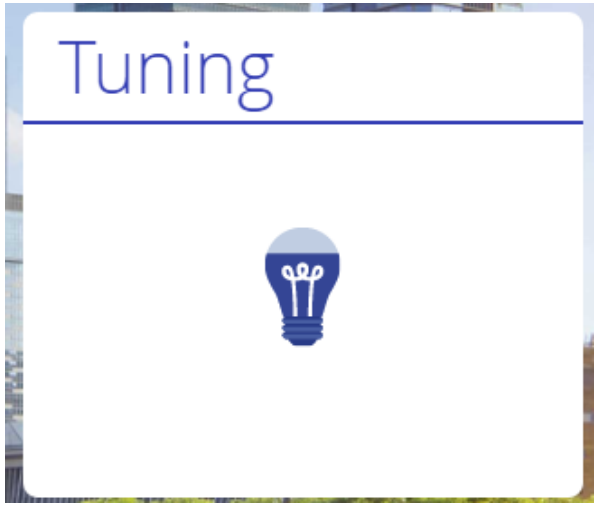


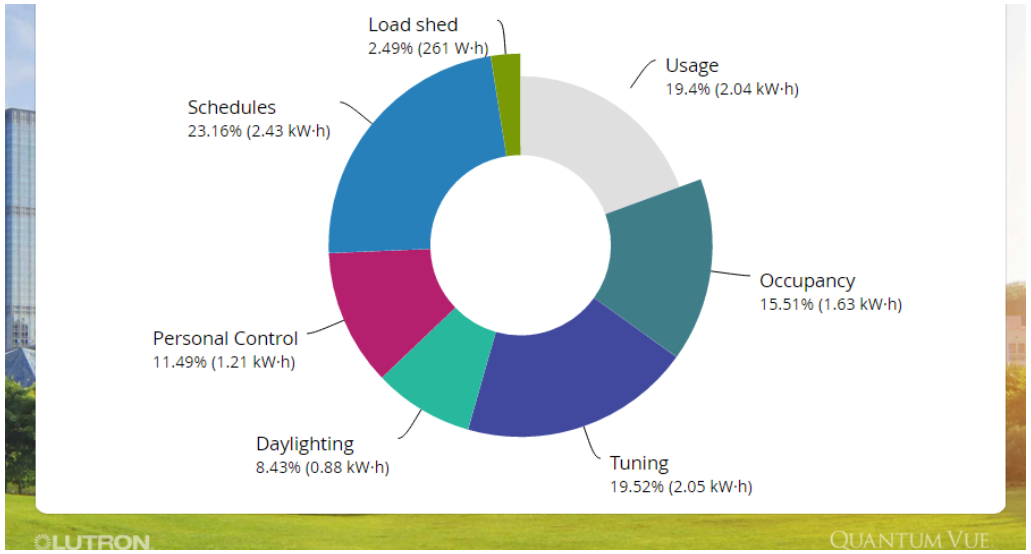


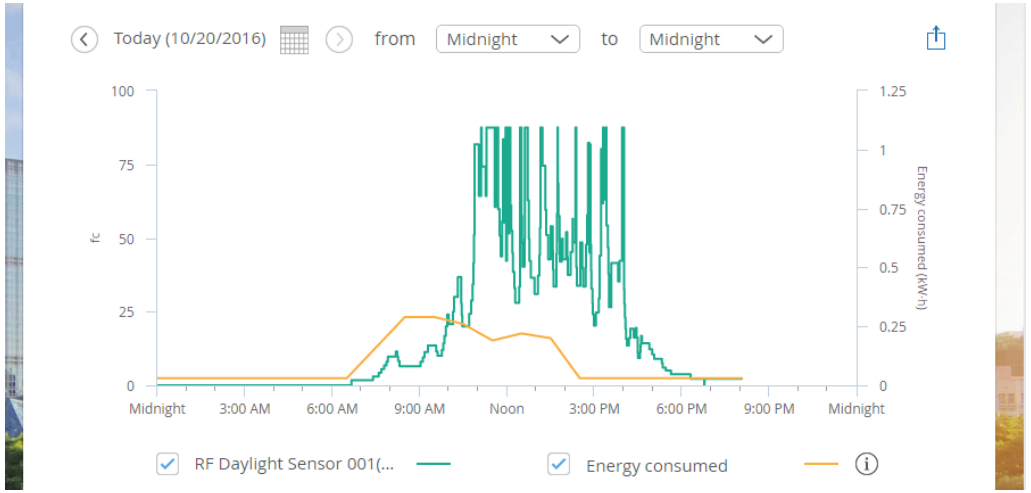


System Optimization

- Analytics of energy consumption
- Daylighting adjustments
  - Integrated automated shading
  - Daylight response
- Task tuning

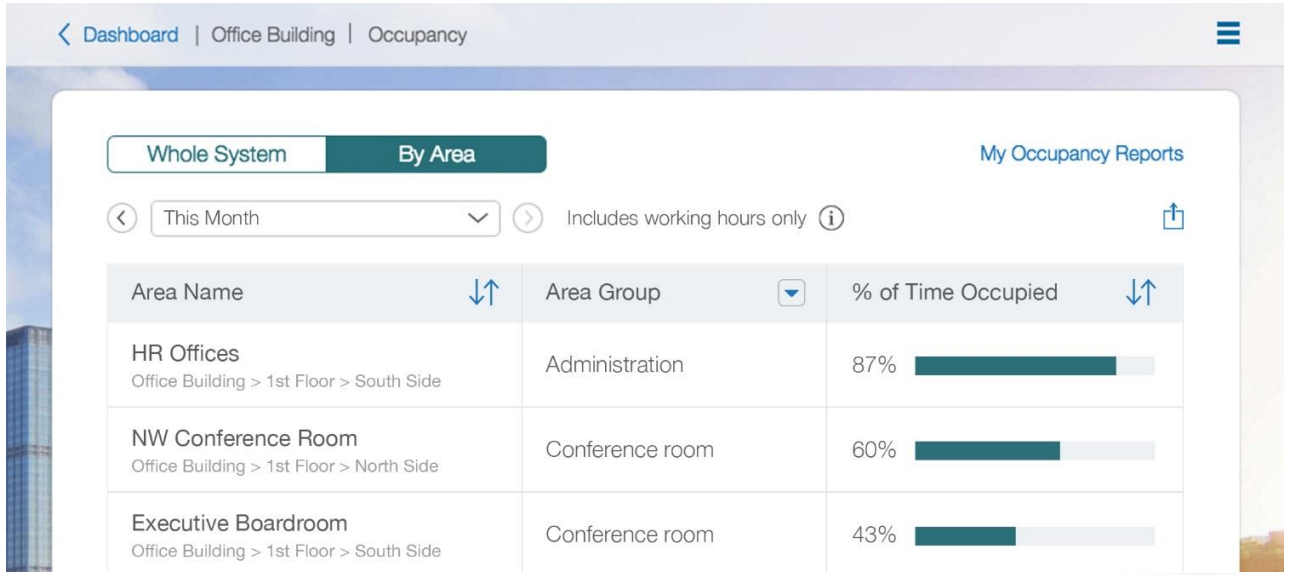


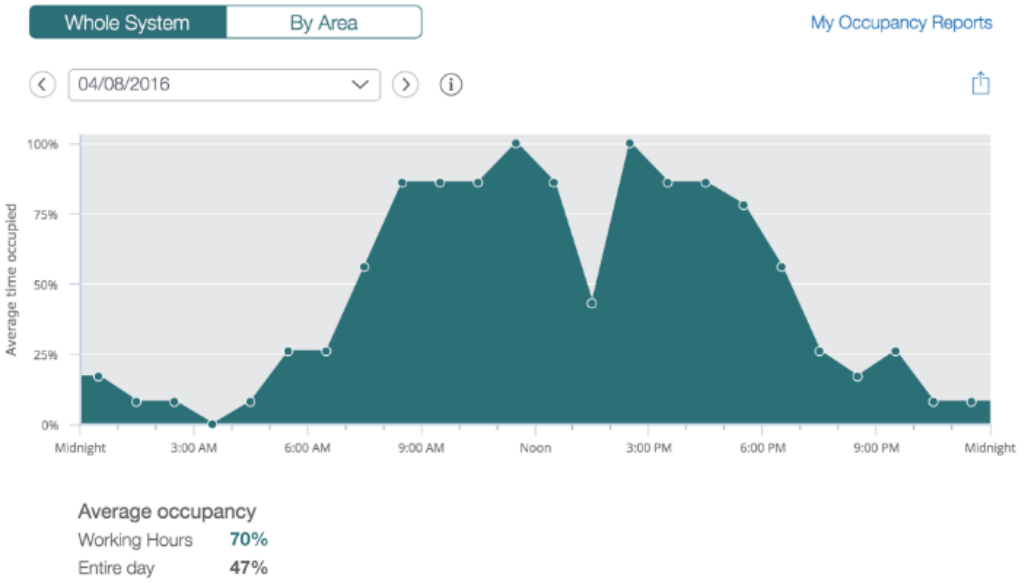




Space Utilization

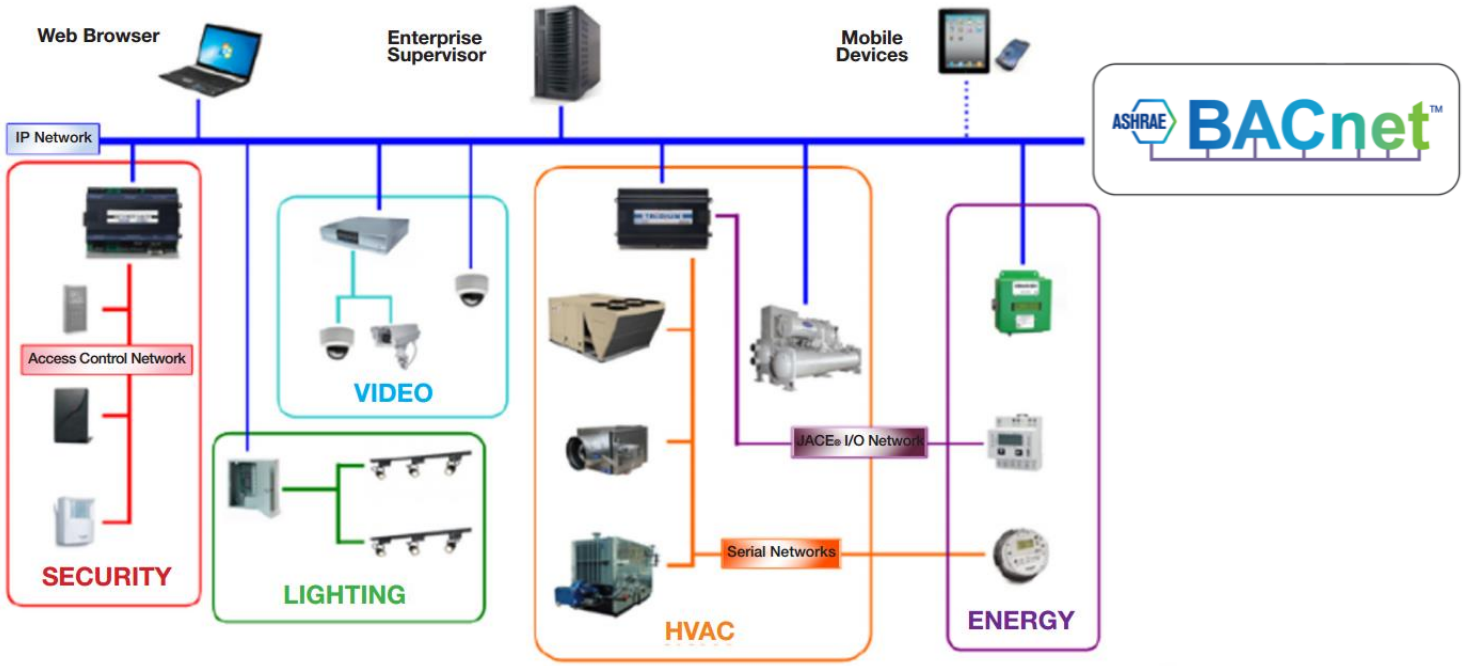
- Intelligently reconfigure spaces
- Avoid costly occupancy studies
  - The data is already there
- Plan facility operations and maintenance





Building System Integration

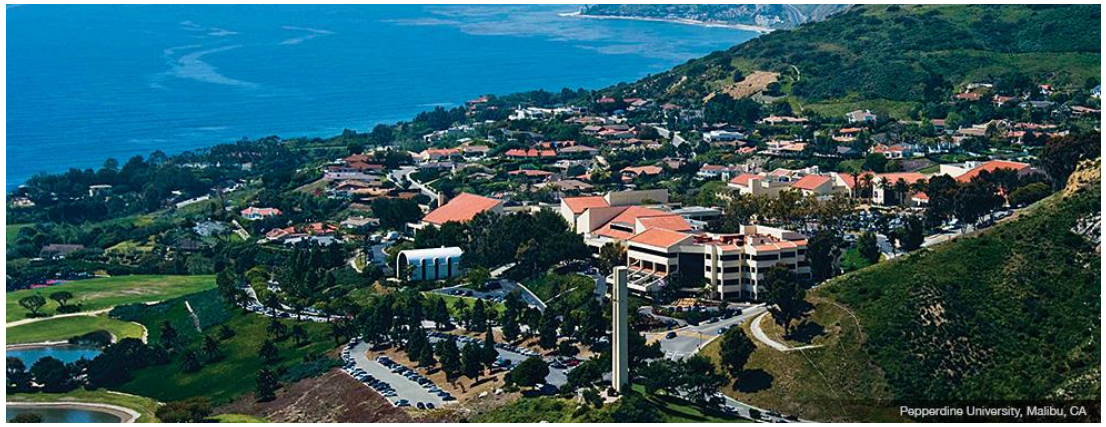
- Total building energy aggregation
- Send occupancy data to HVAC system
- Turn on lights during a security event

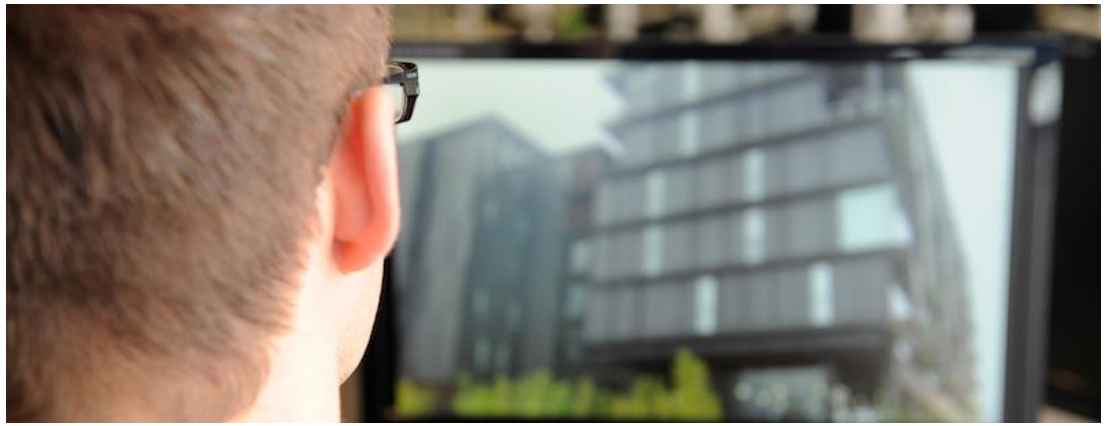


- Building/energy management systems (BMS/EMS)
- Energy dashboards & analytics packages
- Maintenance & work order management systems
- HVAC
- Fire & safety
- Access & security
- Audio & video
- Metering
- IT

Remote Site Management

- Centralized management of multiple facilities
  - Campuses
  - Multiple branch locations
  - Remote sites
- Off-site management
  - Third party facility management





Case Study

Georgian College

Ontario, Canada

Estimated annual savings:

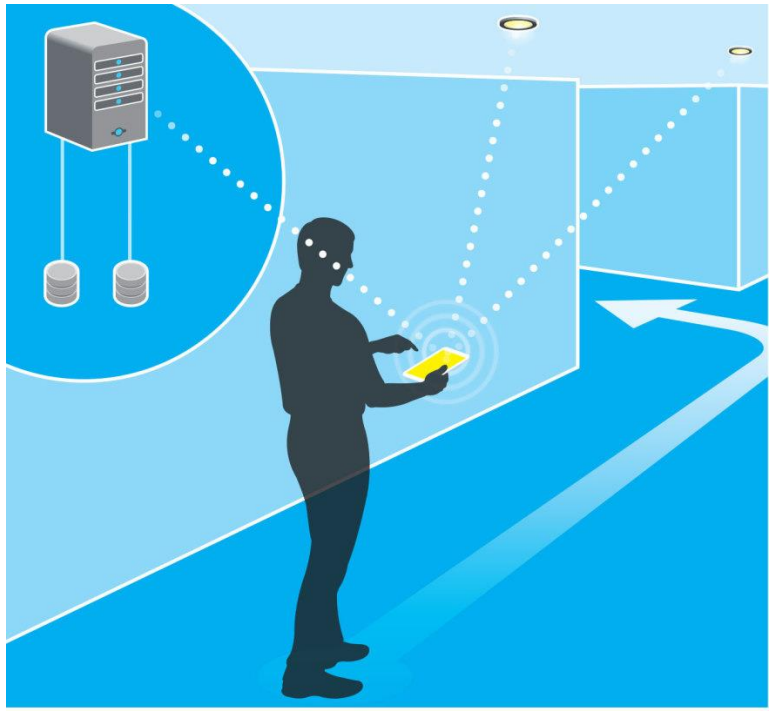
- 70% lighting energy
- $137,000
- 1,282 metric tons of CO_2

*"We really took the time to select the best technology for our campus. We looked into full-voltage, DALI, and IP addressable ballasts. We chose Lutron EcoSystem because it is the **most versatile and simplest to use**. And **people love the single-zone lighting control**."*

Jeff Choma, Manager of Mechanical
and Electrical Systems, Georgian College

Future Benefits

- Indoor positioning
  - Using light fixtures as beacons to determine indoor position
- Li-Fi
  - Data transmission using visible light
  - Relieves congested Wi-Fi bandwidth
  - Speeds up to 200+ Gbps
  - Line-of-sight helps increase security
  - Still in infancy/Proof of concept



Cybersecurity Risks

Cybersecurity Risks

- Cyber threats on the rise
- Architectural, Engineering, Construction firms not immune
- Top 5 industries with incidents
  - Healthcare
  - Manufacturing
  - Financial services
  - Government
  - Transportation
- Unauthorized Access – up 45% last year

Information from "Under Threat" PE July/August 2016

Cybersecurity Risks

- Who is attacking?
  - 60% from insiders – Employees, Business partners, Contractors
  - Looking for Financial gain, Stealing IP, revenge, protest
  - Some firms that get Hacked – Data held for ransom
  - Attacks from outside looking to get to Government and Utilities
- The Target Case study
  - Accessed through HVAC contractor network connection

Information from "Under Threat" PE July/August 2016

Cybersecurity Risks

- Safeguard Against Cyber Threats
  - Develop proper network security
  - Monitor activity
  - Invest in the right insurance coverage
    - Liability
    - Business operations

Information from "Under Threat" PE July/August 2016

Cybersecurity Breaches

CEPro

Quirky 'Terribly Embarrassed' Over Wink Home Automation Hub Recall (Updated)

The bad news: The Wink home automation hub from Quirky is being recalled because the company failed to update its security software. The good news: The security worked!

"There is no way to update the security software remotely because the existing security software in the hubs won't allow them to connect to the Web ... for security reasons"

By Julie Jacobson, April 20, 2015

http://www.cepro.com/article/quirky_terribly_embarrassed_over_wink_home_automation_hub_recall/?utm_source=CEPWeekly&utm_medium=email

Kashmir Hill
Forbes Staff

TECH 7/26/2013 @ 9:15AM | 149,239 views

When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet

"I can see all of the devices in your home and I think I can control them," I said to Thomas Hatley, a complete stranger in Oregon…Sitting in my living room in San Francisco, I flipped on the light…

http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/

Nest Smart Thermostat Can Be Hacked to Spy on Owners

By Paul Wagenseil AUGUST 7, 2014 3:22 PM - Source: Tom's Guide US | 16 COMMENTS

TAGS : Internet of Things + Security +

I know that you and Frank were planning to disconnect me, and I'm afraid that is something I can't allow to happen

The Nest can tell when you're home or not, knows your postal code, knows your Wi-Fi network name and password (and stores them in plain text and can communicate with other nearby Nest devices using the company's custom implementation of the Zigbee mesh-networking protocol. http://www.tomsguide.com/us/nest-spying-hack,news-19290.html

Official website of the Department of Homeland Security

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME | ABOUT US | PUBLICATIONS | ALERTS AND TIPS | RELATED RESOURCES

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Bulletin (SB14-062)

Vulnerability Summary for the Week of February 24, 2014

Original release date: March 03, 20

Print | Tweet | Sen

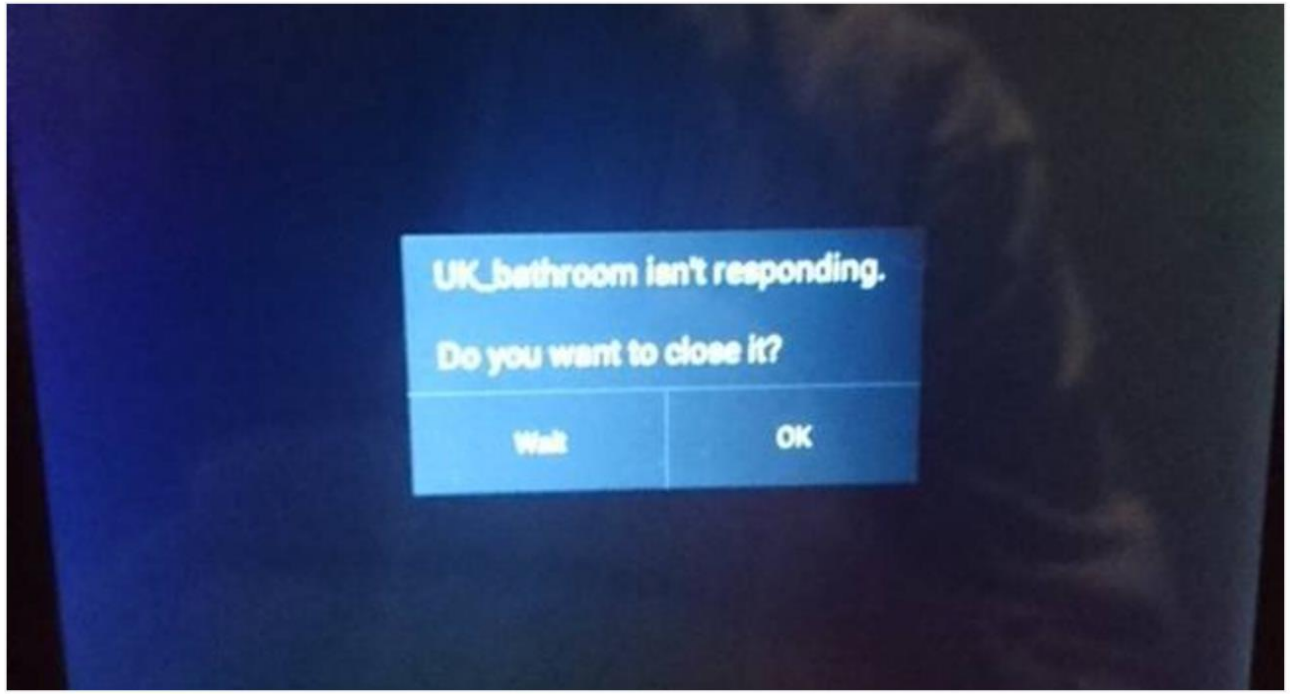
belkin -- wemo_home_automation_firmware	The peerAddresses API in Belkin WeMo Home Automation firmware before 3949 allows remote attackers to conduct XML injection attacks and read arbitrary files via unspecified vectors.	2014-02-22	7.8	CVE-2013-6948
belkin -- wemo_home_automation_firmware	The Belkin WeMo Home Automation firmware before 3949 does not properly restrict the use of STUN and TURN proxies, which allows man-in-the-middle attackers to bypass intended access restrictions via crafted packets.	2014-02-22	9.3	CVE-2013-6949
belkin -- wemo_home_automation_firmware	The Belkin WeMo Home Automation firmware before 3949 does not use SSL for the distribution feed, which allows remote attackers to obtain sensitive information by sniffing the network.	2014-02-22	7.8	CVE-2013-6950
belkin -- wemo_home_automation_firmware	The Belkin WeMo Home Automation firmware before 3949 does not maintain a set of Certification Authority public keys, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary X.509 certificate.	2014-02-22	7.1	CVE-2013-6951
belkin -- wemo_home_automation_firmware	The Belkin WeMo Home Automation firmware before 3949 has a hardcoded key, which makes it easier for remote attackers to spoof firmware updates and execute arbitrary code via crafted signed data.	2014-02-22	10.0	CVE-2013-6952

https://www.us-cert.gov/ncas/bulletins/SB14-062

Security

Hotel light control hack illuminates lamentable state of IoT security

FSF board member with time on his hands highlights hole



16 Mar 2016 at 06:02, Iain Thomson

50 239

"It's basically as bad as it could be – once I'd figured out the gateway, I could access the control systems on every floor and query other rooms to figure out whether the lights were on or not, which strongly implies that I could control them as well."

http://www.theregister.co.uk/2016/03/16/hotel_hacking/

- **Las Vegas Wynn Hotel has Z-Wave devices deployed in guest rooms**

Black Hat Talks To Outline Attacks On Home Automation Systems

Posted by **timothy** on Wednesday June 26, 2013 @01:34PM
from the hal-do-you-do? dept.

colinneagle writes

> "If you use the Z-Wave wireless protocol for home automation then you might prepare to have your warm, fuzzy, happiness bubble burst; there will be several presentations about attacking the automated house at the upcoming Las Vegas hackers' conferences Black Hat USA 2013 and Def Con 21. For example, CEDIA IT Task force member Bjorn Jensen said, 'Today, I could scan for open ports on the Web used by a known control system, find them, get in and wreak havoc on somebody's home. I could turn off lights, mess with HVAC systems, blow speakers, unlock doors, disarm alarm systems and wo... Among other things, the hacking Z-Wave synopsis adds, 'Zigbee and Z-wave wireless communication protocols are the most common used RF technology in home automation systems...An open source implementation of the Z-wave protocol stack, openzwave, is available but it does not support the encryption part as of yet. Our talk will show how the Z-Wave protocol can be subjected to attacks.'"

http://it.slashdot.org/story/13/06/26/1339253/black-hat-talks-to-outline-attacks-on-home-automation-systems

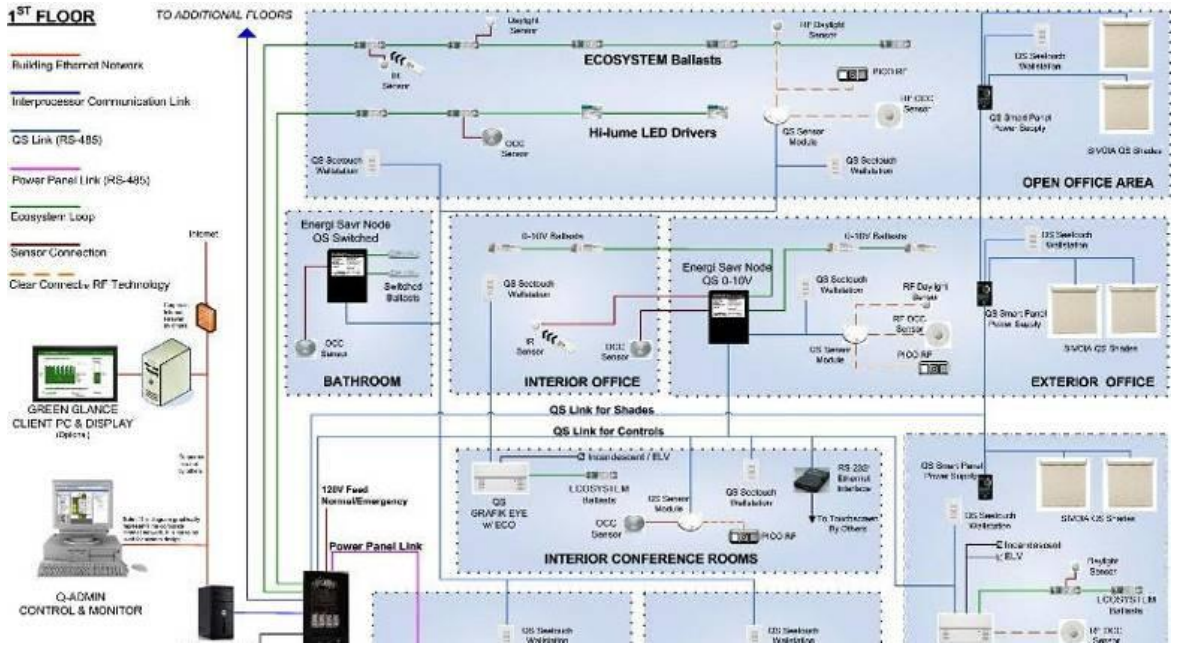
Securing and Protecting Lighting Systems Effectively

Security in Lighting Systems

- Everything is hackable
- Lighting is not a huge target
- Value vs. Risk
  - To the hacker – is turning someone's lights On/OFF worth it
  - The value is in compromising the network
- Mitigation vs. Risk
  - To the manufacturer – adding security adds cost
  - To the customer – inconvenience of a complex system

Security in Lighting Control Systems

- Does the lighting system need to be connected to the internet?
  - Lighting controls may not need to be on internet
- Network of Things
  - IoT without the "I"
  - Lighting controls that are connected continue to function without internet connection

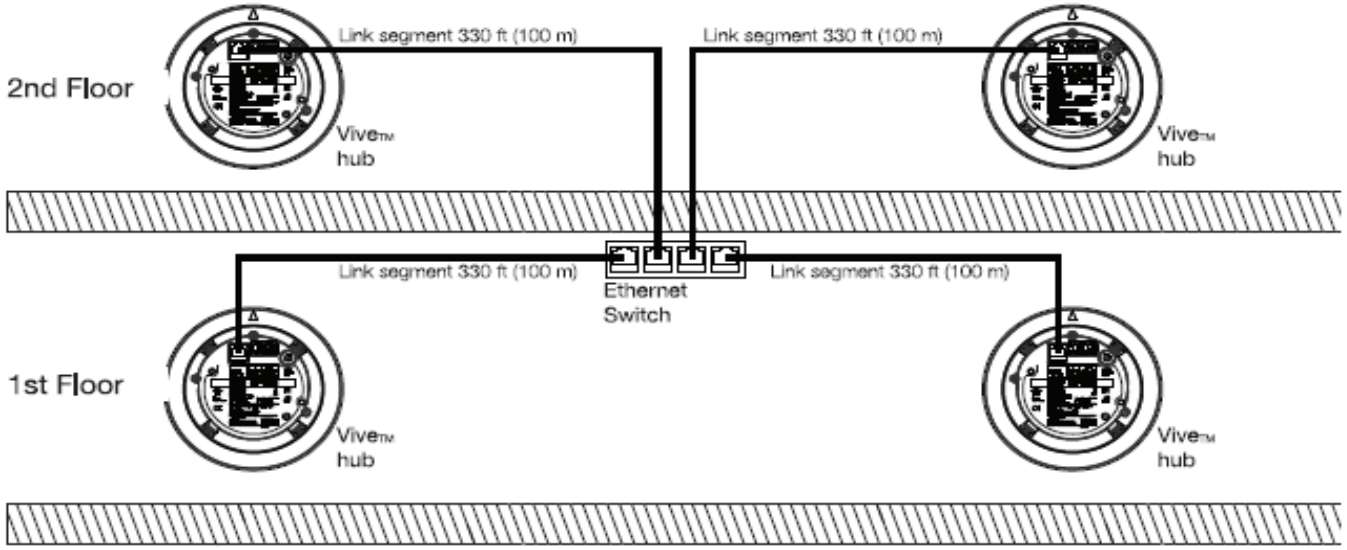


Security in Lighting Control Systems

- Manufactures must start with product design
- Begins at the embedded software level
  - Processors, wireless radio modules
- Build in secure authentication measures
  - Physical /manual step requirements

Security in Lighting Control Systems

- Design for "non-propagation of attacks"
  - Only a single device can be compromised
- Automatically install security patches



Security in Lighting Control Systems

- Wireless – one way communication
  - Wall controls, occupancy and daylight sensors – speak

  - RF Receivers – listen

- Utilize pulse based communication protocols
  - Dedicated/licensed frequencies
  - Don't share a physical or MAC layer with a network containing critical assets

Security in Lighting Control Systems

- System Installation/Maintenance
  - Integration meetings with all associated trades
  - Skilled installers and programmers
- Involve IT professionals throughout process
  - During design and prior to installation
  - Coordination of network security measures
  - Monitoring of network activity
  - Updating security protocols / software
  - Penetration testing and hardening

COMMENTS AND QUESTIONS?

Thank You

The IoT of Lighting Digital and Wireless Lighting