

Cybersecurity in a New Light: IT Considerations for Connected Lighting Systems

Dan Kuhl, Evergreen Consulting Group
Levin Nock, Design Lights Consortium
Maurice Karagiorgos, Lutron Electronics



Today's Session

- Use the chat feature to ask questions!
- We will have time at the end for Q&A
- Our presenters will be referencing various technologies today. We do not endorse any specific manufacturers; references are for educational purposes



Today's Panelists



Dan Kuhl
Sr. Lighting Specialist
Evergreen Consulting
Group



Maurice Karagiorgos
Regional Manager/
Systems Application
Engineer
Lutron Electronics



Levin Nock
Sr. Technical
Manager
Design Lights
Consortium

Who is NEEA?

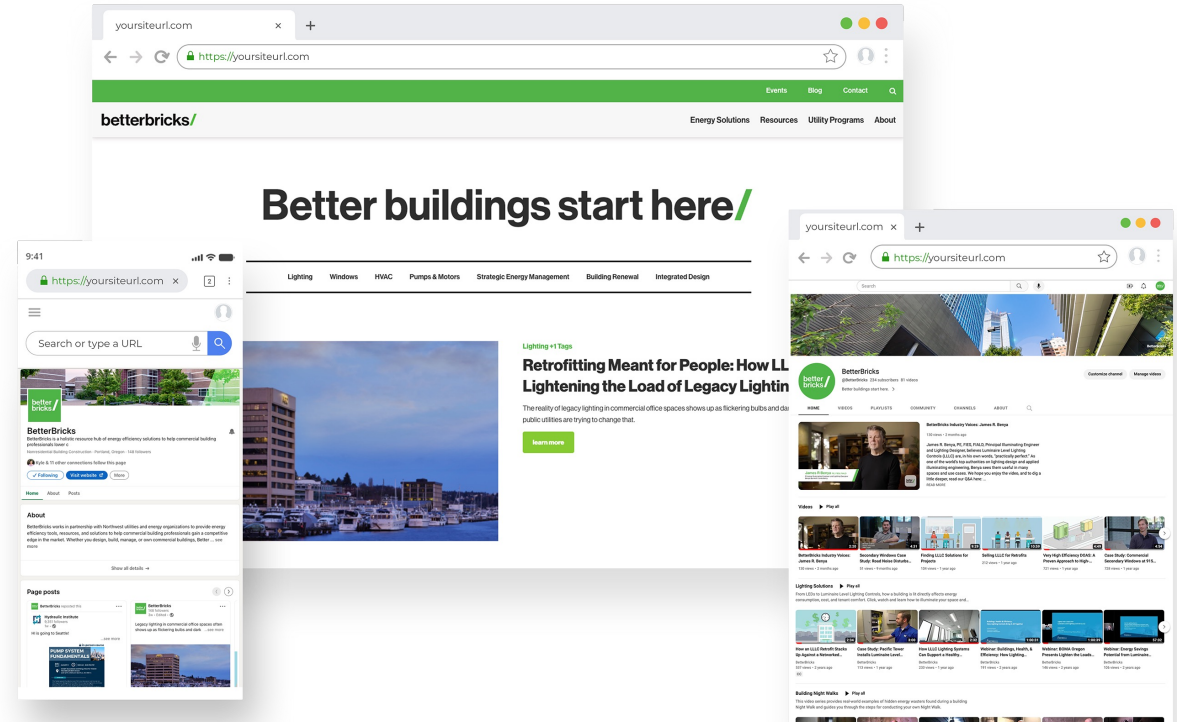


What is BetterBricks?

Working in partnership with Northwest utilities and energy organizations to provide energy efficiency tools, resources, and solutions to help commercial building professionals gain a competitive edge in the market.

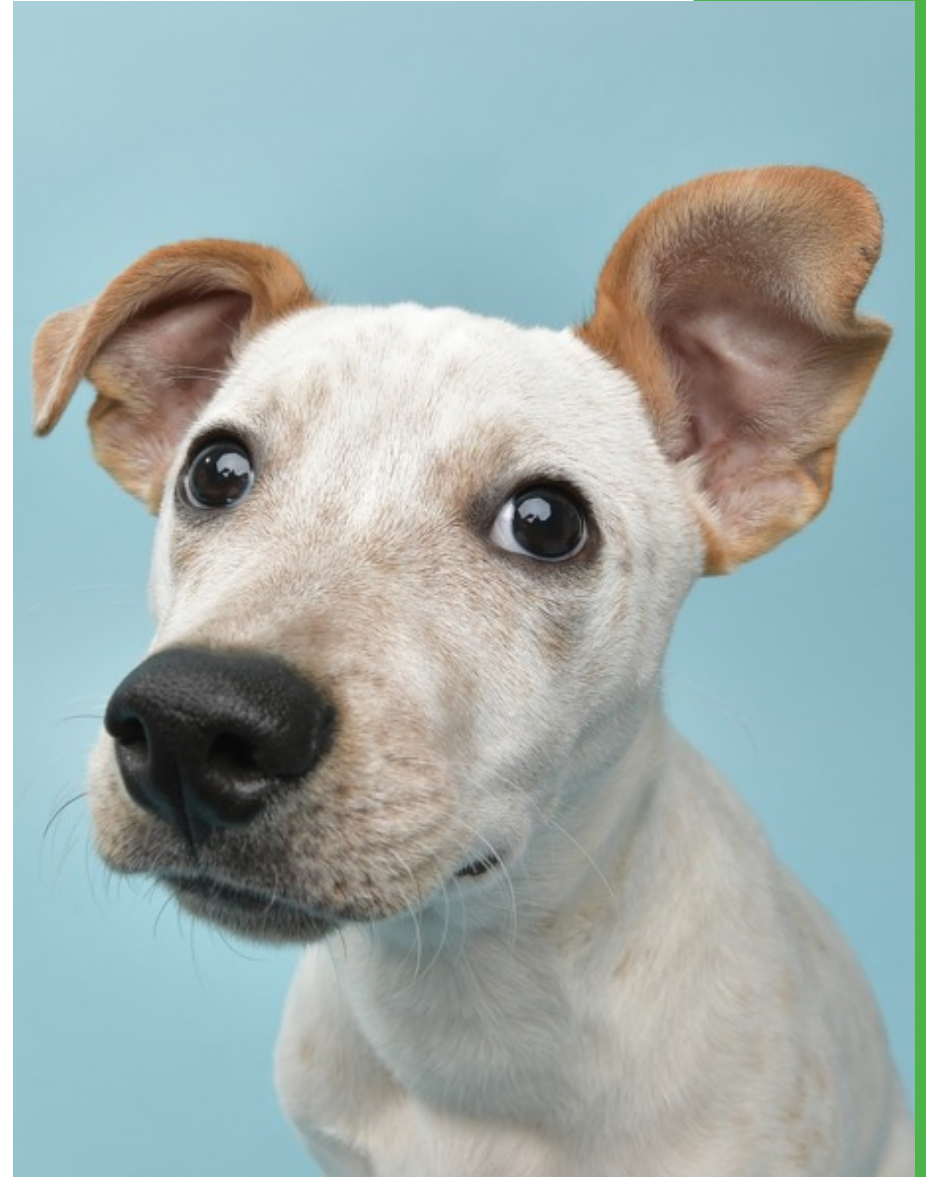
betterbricks.com

LinkedIn/YouTube: @BetterBricks



Cybersecurity

“Someone cracked my password. Now I need to rename my puppy” - Unknown



Cybersecurity & Lighting

- Cybersecurity is the practice of defending networked systems and data from malicious attacks
- Currently there is no one-size-fits-all solution, but multiple 3rd party standards exist
- To determine which security standards will best mitigate risk, end-users need to identify and provide us with the specific criteria that matters



The World of Networked Controls & Cybersecurity

- Cybersecurity for networked lighting controls is of fundamental importance to NLC market adoption
- Hacking of an NLC system could become a headline and cause potential users to question/delay utilizing the technology
- Lost energy savings from canceled or delayed NLC deployment is significant



Why We Need To Know More: The Risks

The Risks Are Rising

- 5,400 cyber attacks daily across all IoT devices
- Attacks are increasing
- 7 million data points compromised daily

The Stakes Are High

- Average payout for successful cyber attack is \$330,000
- Estimated that global cybercrime damages will be 10 trillion by 2025
- Company reputation can be damaged, thereby losing business

Why We Need To Know More: US Department of Energy (DOE)

- DOE has set a national goal of tripling the energy efficiency and demand flexibility of the buildings sector by 2030, relative to 2020 level
- DOE forecasts that connected lighting systems can contribute to that goal by delivering 125 T Wh of annual energy savings by 2035, equivalent to the annual output of 50 typical (500 MW) power plants



IT Standards & Best Practices



Section 1: How to communicate IT considerations to both customers and manufacturers for a seamless installation



Section 2: A review of Design Lights Consortium (DLC) IT requirements and protocols, designed to remove the uncertainty around IT concerns

**Maurice
Karagiorgos –
Lutron Electronics**



Luminaire Level Lighting Controls Capabilities

Simple Systems

- Occupancy Sensing
- Daylight Sensing
- Personal Tuning
- High-End Trim

Advanced Capabilities

- Demand response or off-site control
- Data collection and monitoring
- 3rd party programming and troubleshooting
- Integration with other building systems

Can the systems that we are considering meet the functional needs and provide the security and protection that we need?



What Functions Do I Want?

Many of today's new systems offer some interesting new options that might affect our IT department.

- Some of those include:
- Off site control of the system
- Data collection and monitoring
- 3rd party programming and troubleshooting
- Integration with other systems



Off Site Control Of The Lighting Control System

This option allows for control of the lighting control system from outside the building or campus

One example would be a school facilities engineer being able to override normal school hours for a snow day or an unscheduled event

This requires that the system be able to be connected to via an app or website that has a connection to the lighting controls system. This can be done through the existing building structure, or a building may ask that the system be kept separate from its current IT structure

Time Commitment From Onsite IT Staff

- Most time commitment occurs before onsite implementation
- Some manufacturers have IT Security Questionnaires that help lay the groundwork
- Keep in mind the time, depending on the project & manufacturer it can take some significant time before it's finalized with the customer



Common IT Department Needs:



Verify presence of Personally Identifiable Information (PII), Electronic Protected Health Information (ePHI), or financial data in the LLLC system.



Assess participation in Generative Artificial Intelligence (Generative AI) within the LLLC system.



Confirm manufacturer's dedicated cybersecurity staff support for the product and/or services.



Check manufacturer's participation in relevant certifications or assessments related to information security.



Evaluate the manufacturer's security program for Risk Measurement, Risk Mitigation, Risk Monitoring, and Risk Reporting.



Examine wired and wireless protocols, security practices, and cryptography securing communication in the LLLC system.



Ensure products within the LLLC system adhere to well-known security standards, with signed and secured firmware, industry best practice cryptography, no universal passwords, and implementation of NIST best practices for passwords and secure communication connections.

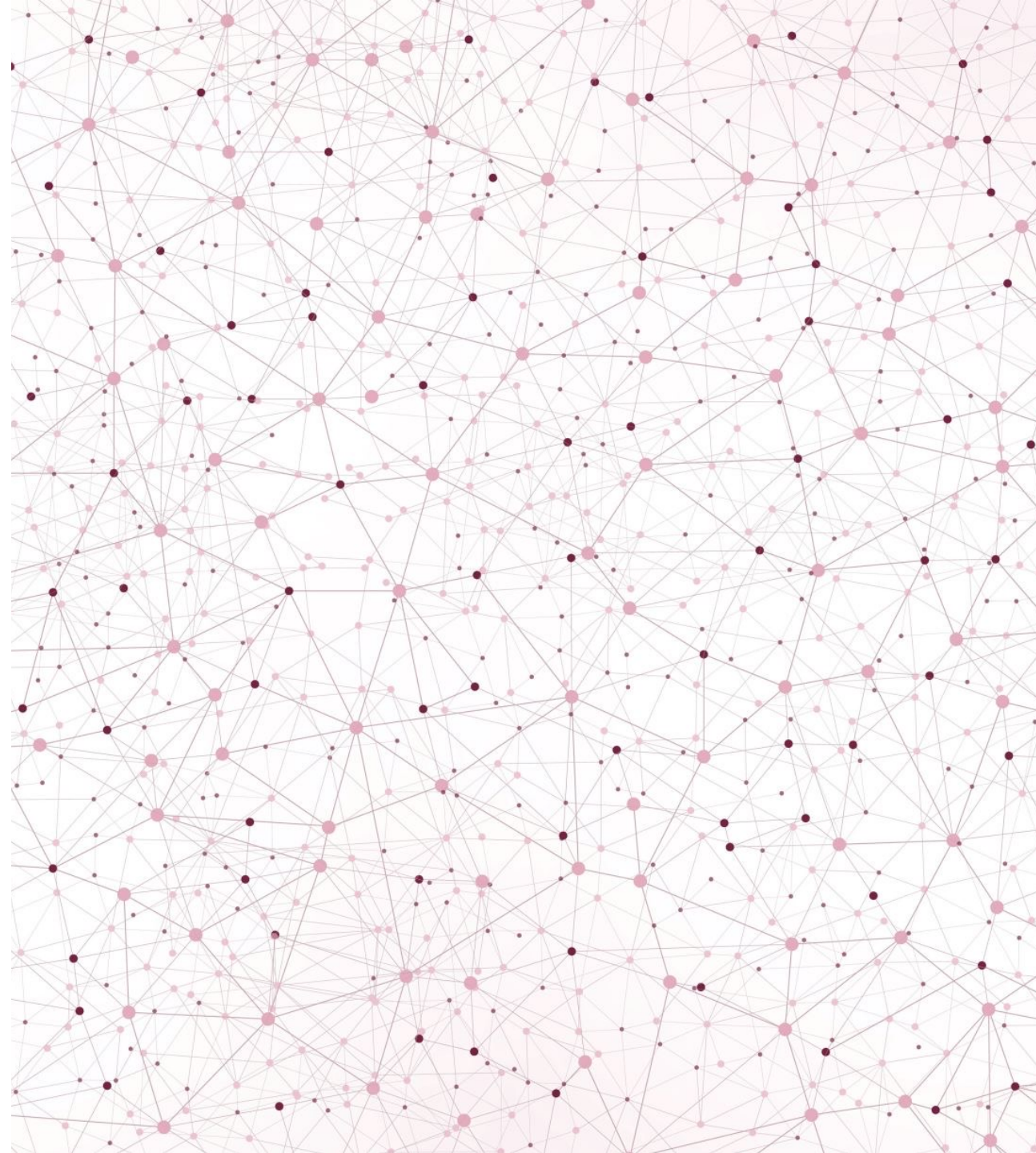
Data Collection and Monitoring

Many lighting controls systems are able to give data back to the building operators to better understand the use and energy consumption in their buildings.

- Data collection would include:
- Total energy savings for a building and individual spaces
- Areas that are heavily used and areas that are scarcely used (allows for reallocation)
- Hours of operation for spaces
- Identification of problem areas and spaces – devices being left on or spaces with the lights on with no employee's present
- Some data collection may be required by the local PUD to receive funding

3rd Party Programming and Troubleshooting

- Often times, manufacturers will offer programming and troubleshooting from an offsite location. While this often is a cost savings versus on-site services, it has to be managed from an IT perspective
- If 3rd party programming is wanted or required, generally two options exist – access to the lighting control system by allowing access to the lighting controls through the IT or a direct connection via a wireless device (such as a laptop brought onto the site)
- A third option exists where a laptop or device is brought on-site and is physically hooked to the building internet and then removed after programming is completed. This needs to be done with cooperation of the IT department to ensure security of the building



Integration With Other Systems

This has become a very common option used with lighting controls systems and other systems within a building – mostly commonly HVAC. Other systems will use the occupancy controls of the lighting controls system to determine whether to turn on and off HVAC inside an area.

- Traditionally, this is done using BACnet or similar communication protocol and done using the existing IT system to bring communication to the two systems
- Additionally, buildings may want to have a single scheduling system that will send commands to the lighting system
- Each of these systems and connections need to be communicated and reviewed with the IT Department



Does This System Reside On My Current IT?

- Current lighting controls systems can reside completely outside and separate from a building's IT system, reside as part of a building's IT, and/or can be a hybrid of the two options
- Many systems do not need to reside on a building's IT and either had a stand along programming interface or do not need of at all. These systems stand completely alone, can be programmed and adjusted without accessing building IT and often do not or cannot integrate to other building systems or be accessed from outside the building. These systems tend be used for smaller buildings or areas, not be able to communicate across areas and tend to have less options that systems that need a programming front end or front ends that do not communicate via IT or other means

Options and building needs should be discussed with IT

Does This System Reside On My Current IT?

- Systems that use front ends that need access to an IT system come in two options – those that use IT to communicate internally and those that use IT to speak externally of the building
- Systems that use IT to communicate internally use the IT wiring as the communication conduit across the building and will need the IT department to route the devices to each other
- Those systems that reside within a building's existing IT systems are often separated by placing them onto their own virtual server to separate the controls from their normal IT systems



Does This System Reside On My Current IT?

- Systems that reside on a building's IT network **MUST BE** discussed with IT Departments prior to the system's installations
- Complete sets of specifications for the lighting controls system, including the system's Security Statement and IT Implementation Guides should be provided for review – one such example can be found at:
<https://assets.lutron.com/a/documents/040437.pdf>



Levin Nock – Design Lights Consortium



What is the DLC?

- Non-profit
- Promotes high-quality, energy-efficient lighting products
- US and Canada



All NEEA Member Programs are DLC Member Programs





APPLICATION PORTAL ↗

Welcome to The MyDLC Dashboard



Dashboard

QPL Search

Connect with DLC

News & Updates

Events & Webinars

Application Pre-submission

Tools

Resources & Tools

Find Qualified Products

By Model or Manufacturer | Select a QPL | Search

Quick Links

- Request DLC Data Access Subscription →
- Product Submission Instructions →
- DLC Resource Hub →

News & Updates



Upcoming Events

Feb 21, 2024

Submitting Product Images to the SSL QPL

SSL WEBINAR





DLC Qualified Product Lists (QPLs)



	SSL (Solid State Lighting)	NLC	Horticulture	Luna
Launched	2010	2016	2019	2022
Products	C&I LED Luminaires, Lamps, Retrofit Kits	Networked Lighting Control Systems	Horticultural LED Luminaires, Lamps, Retrofit Kits	Outdoor LED Products meeting DLC night sky guidelines
Products Listed	313,056	67	1,610	251
QPL Activity	3,800 Product Views/ Day	1,000 Product Views/Month	4,000 Product Views/Month	200 Product Views/Month



What the DLC does

- Is a nonprofit
- Maintains lists of qualified products
- Lists are used for rebates & incentives
- Creates policies
- Refers to standards

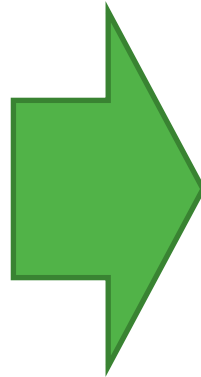
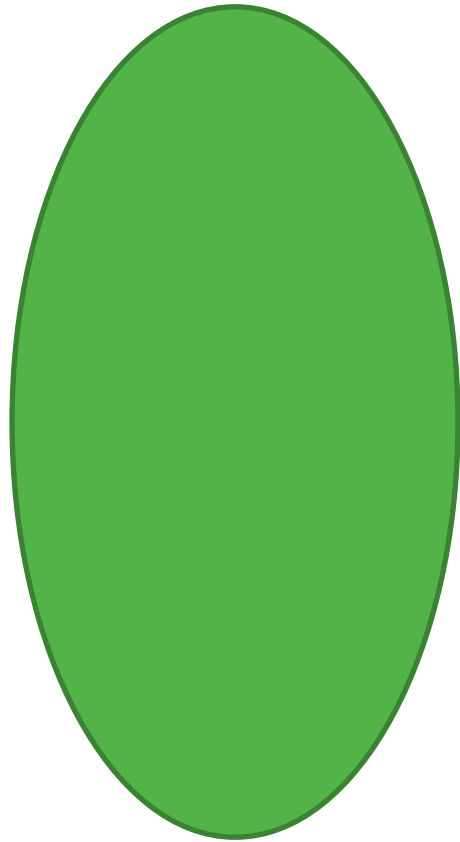


and does not do

- Does not create standards
- Does not test products
- Does not offer direct rebates or incentives
- Does not sell lighting products



All Lighting Controls



**Networked Lighting Control System
Technical Requirements**
Version NLCS
January 25, 2021

Note: Changes from Version 4.0 are highlighted in yellow.

This version of the Technical Requirements document contains corrections and clarifications made to the originally released document, which are displayed as Policy Clarifications and Updates at the end of this document.

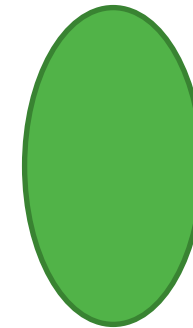
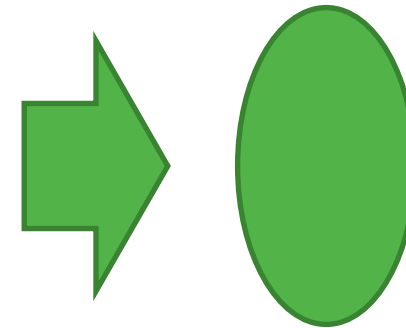
Schedule of Revisions

Revision No.	Date	Description
1.0	Apr 21, 2016	• Initial Technical Requirements published.
1.01	May 7, 2016	• Clarified that the Technical Requirements are for interior control systems. Systems designed and marketed exclusively for exterior applications are not eligible to be qualified.
1.02	Feb 24, 2017	• Clarified that the Technical Requirements do not cover DC or PoE systems.
2.0	Jun 1, 2017	• Version 2.0 published, with addition of exterior control systems.
3.0	Jun 1, 2018	• Version 3.0 published, with addition of DC/PoE systems, scenes, and multi-year plans for energy monitoring and cybersecurity.
4.0	Jun 10, 2019	• Version 4.0 published, with addition of energy monitoring requirement, criteria for cybersecurity certifications, and building management systems capable of networked lighting control.
5.0	June 23, 2020	• NLCS published, with addition of cybersecurity requirement. Energy monitoring definition aligned with ASHRAE 90.1-2016. Three capabilities labeled as supporting Interoperability.

Released June 23, 2020; Updated December 18, 2020

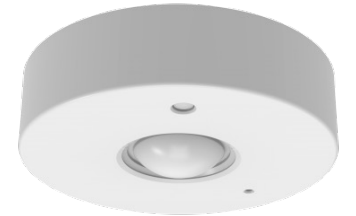
Page 1 of 21

DLC-qualified Networked Lighting Controls



The DLC's Requirements for Networked Lighting Controls

- Networking of Luminaires and Devices
- Occupancy Sensing
- Daylight Harvesting
- High-End Trim
- Zoning
- Individual Luminaire Addressability
- Continuous Dimming
- Energy Monitoring (except room-level)
- **Cybersecurity (as of 2/28/2022)**





You have 0 saved items

Save Search Criteria View Saved Searches

Listed Products

Manufacturer filter this list

Brand filter this list

Ease of Implementation

Technical Requirements Version 5.0 (67)

Interior Scope

Exterior Scope

Advanced Capabilities

User Interface

Integral Controls

Wired/Wireless Communication

Search by system name, manufacturer, brand, or product ID

Search Tip: For an exact search, use quotes around the search term (ex. "PV05LXDK").

Prev 1 2 3 Next

Viewing 1-25 of 67 results

Add All Results to My List

LiteLogic

Add to my list

Manufacturer: Barron Lighting Group Inc. Brand: Trace-Lite

Exterior Scope: Structured Parking,Area/Building Exterior/Parking,Streetlight (residential streets) Technical Requirements Version: 5.0

LiteLogic

Add to my list

Manufacturer: Barron Lighting Group Inc. Brand: Trace-Lite

Interior Scope: Room or Zone,Structured Parking Technical Requirements Version: 5.0

GEBC

Add to my list

Manufacturer: Homewell Inc Brand: GEBC

Interior Scope: Portfolio/Enterprise,Whole Building,Room or Zone,Structured Parking Technical Requirements Version: 5.0

Keilton + autani

Add to my list

Manufacturer: Litetrace Brand: Keilton + autani

Exterior Scope: Structured Parking,Area/Building Exterior/Parking,Streetlight (residential streets) Technical Requirements Version: 5.0

Why does the DLC care about cybersecurity?



Why does the DLC care about cybersecurity?



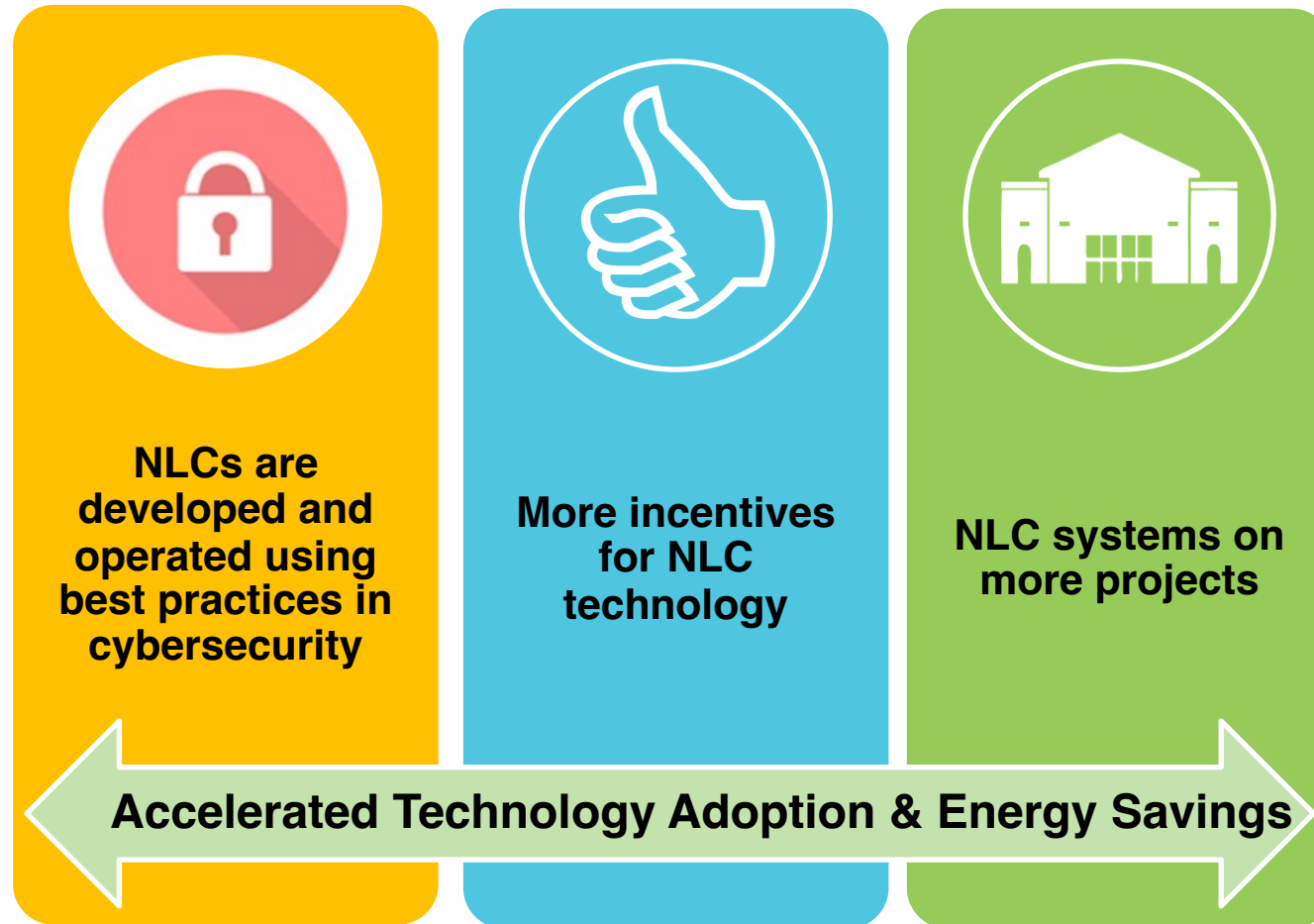
Example hacks	Date
Target, 40M credit cards thru RTUs	2013
Mirai botnet (IoT)	2016
JBS meat processing	2021
Kaseya IT \$70M supermarkets	
MGM Resorts and Caesars	2023
23and Me	2024

DLC Cybersecurity Initiative Intent

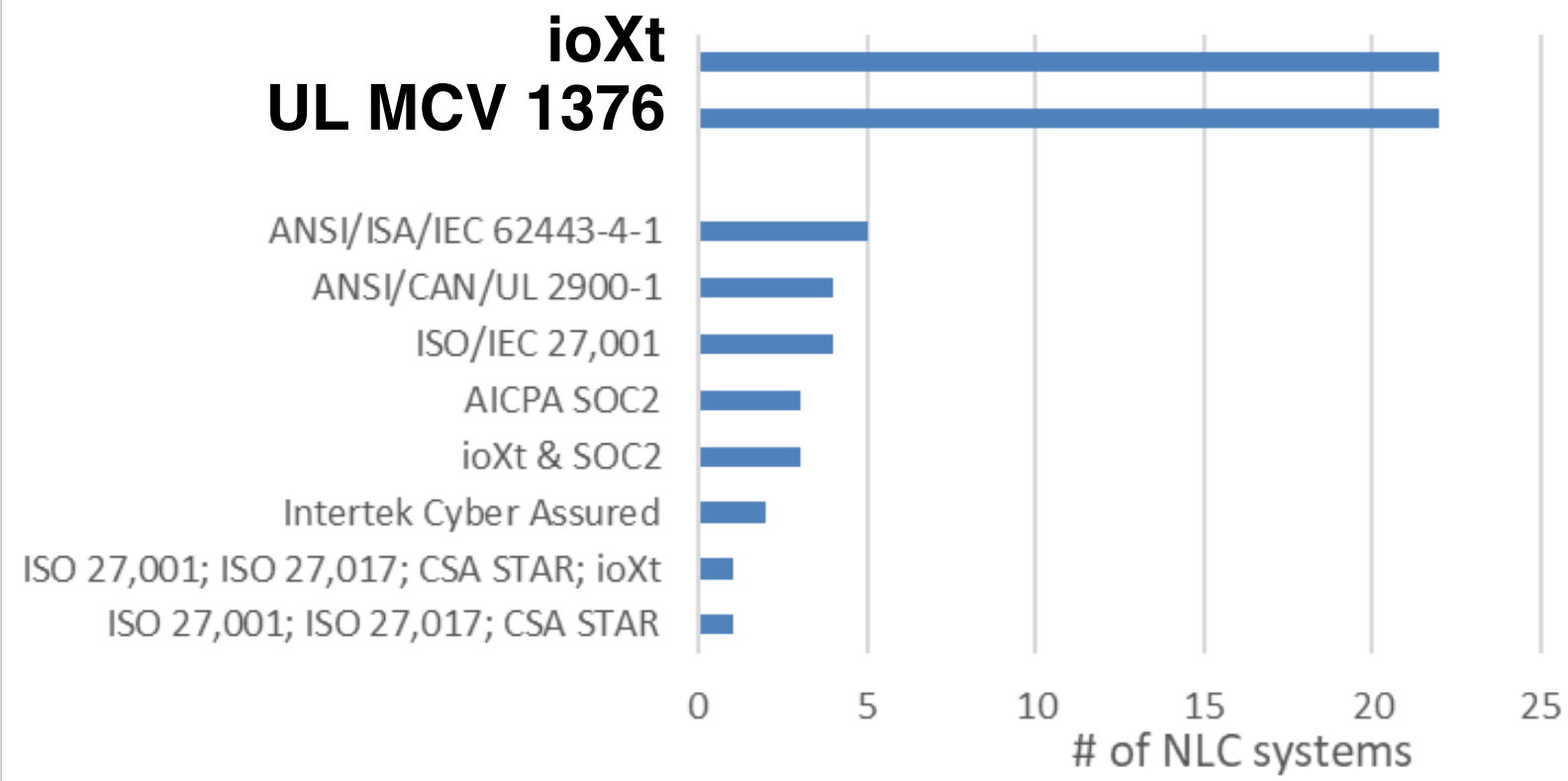
- Ensure listed NLC systems address cybersecurity
- 3rd party certifications
- Disclose those efforts for users of the QPL (Qualified Products List)



DLC Goals



Certifications of Systems on the NLC QPL



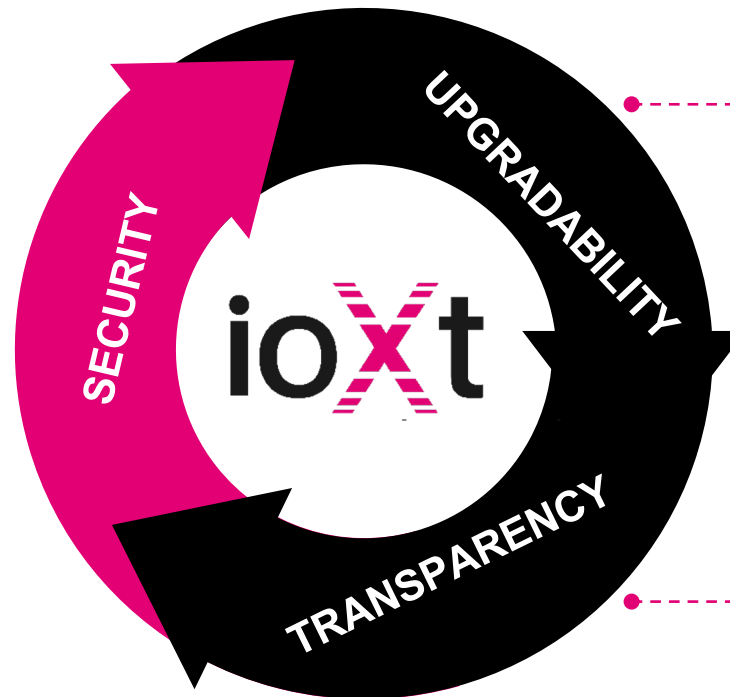
Popular

ioXt Security Pledge



SECURITY

- No Universal Passwords
- Secured Interfaces
- Proven Cryptography
- Security by Default



UPGRADABILITY

- Automatic Security Updates
- Verified Software



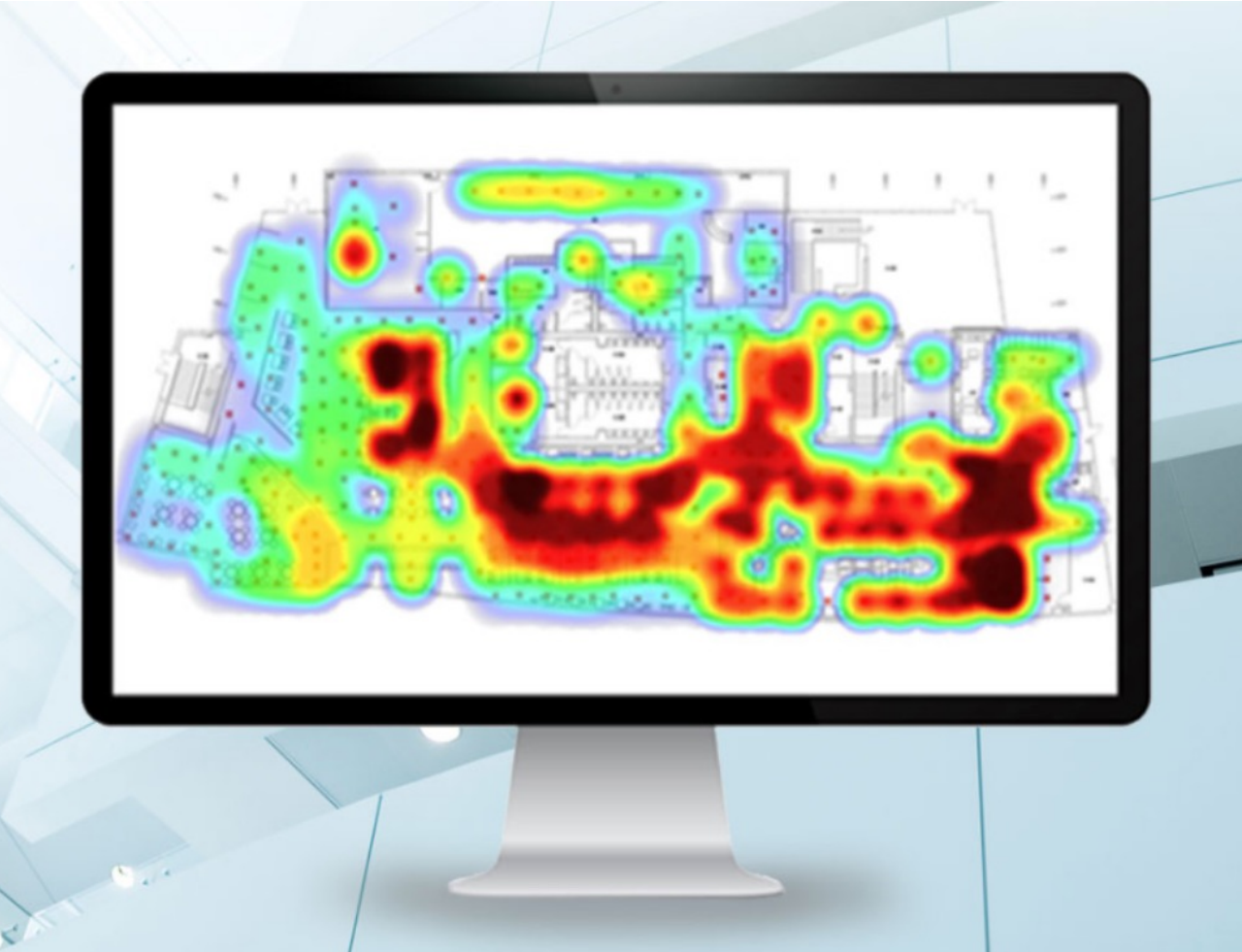
TRANSPARENCY

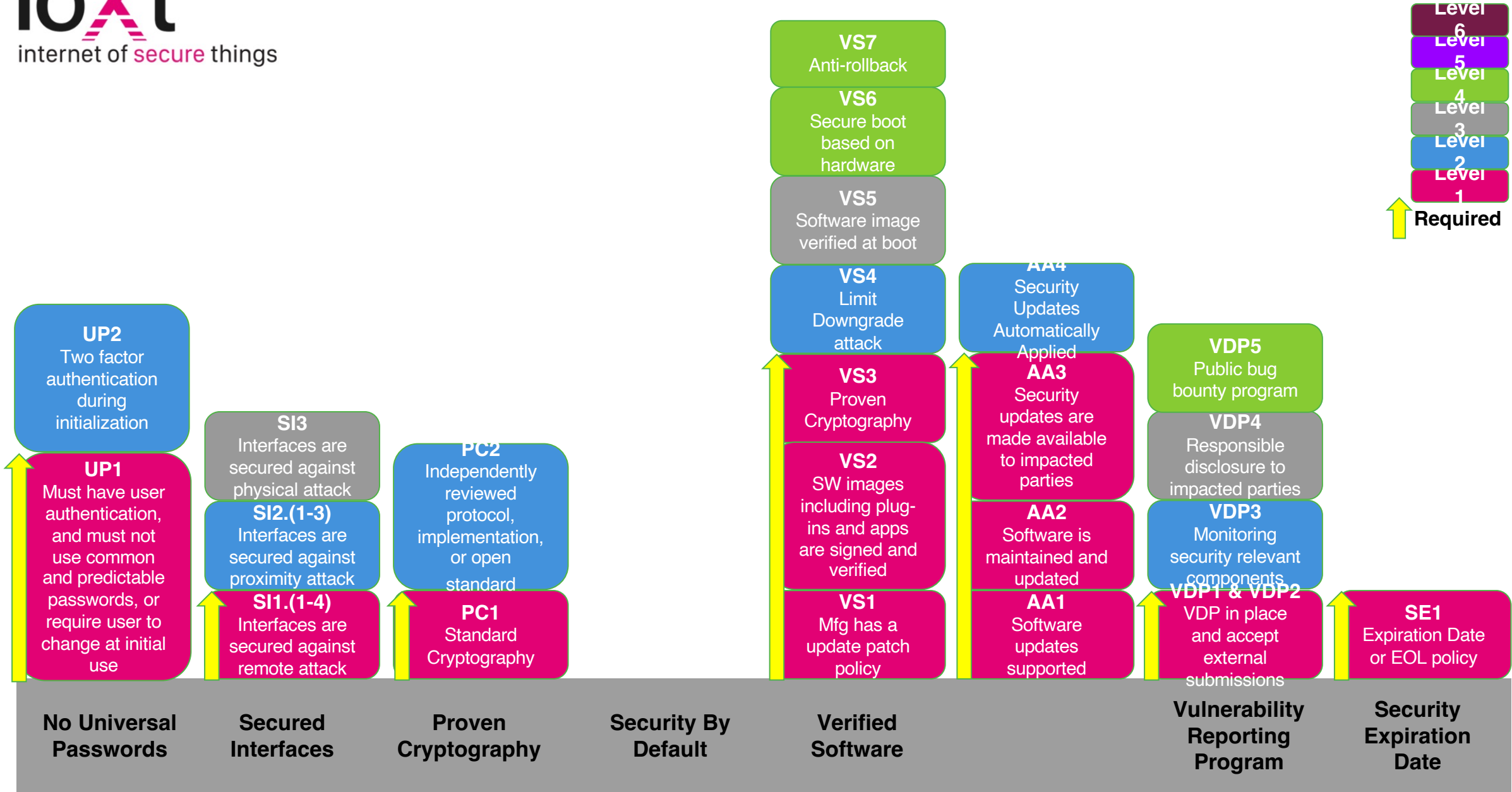
- Security Expiration Date
- Vulnerability Reporting Program

Residential/Consumer

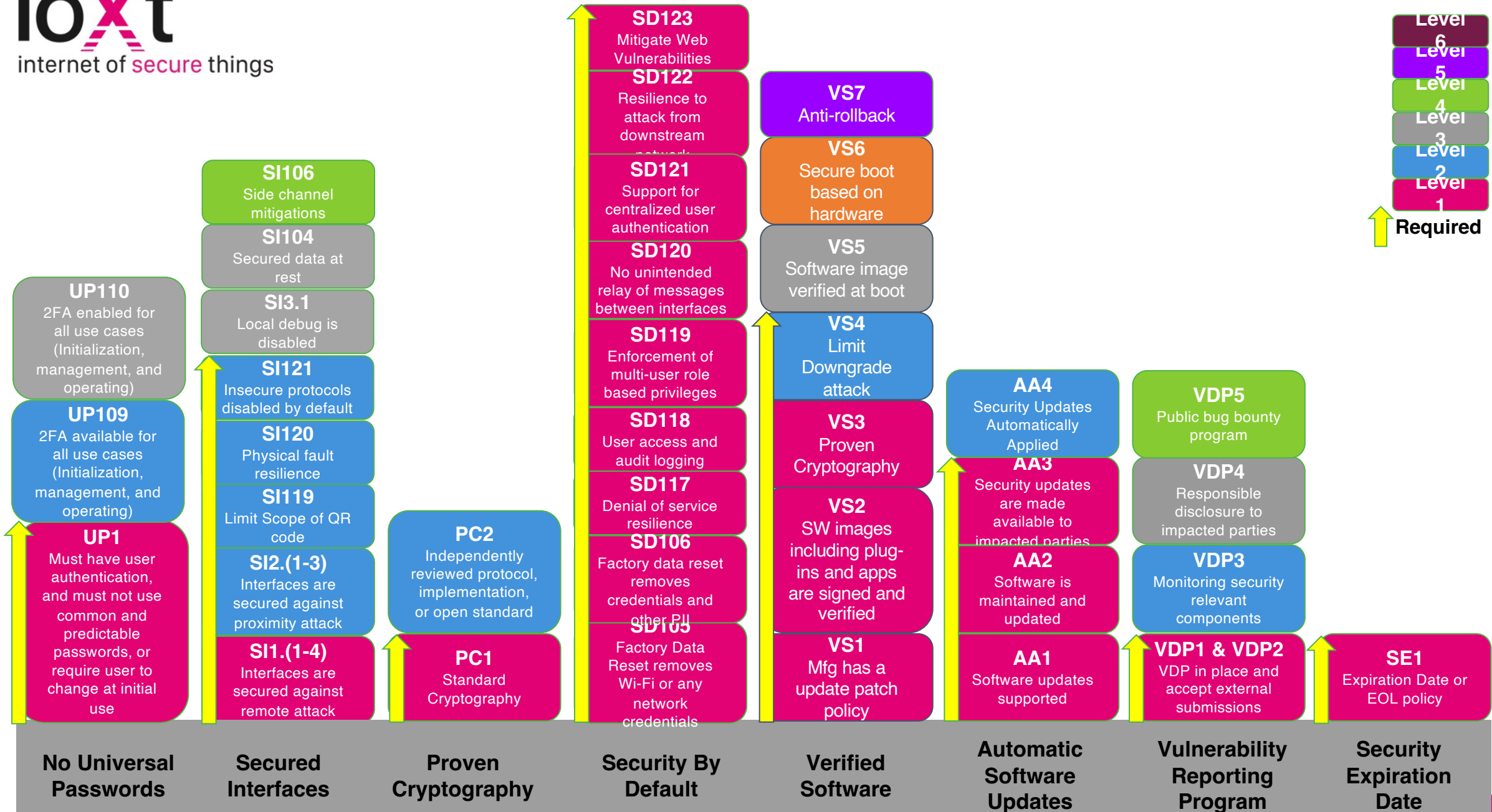
vs.

Commercial





Network Lighting Controller Profile

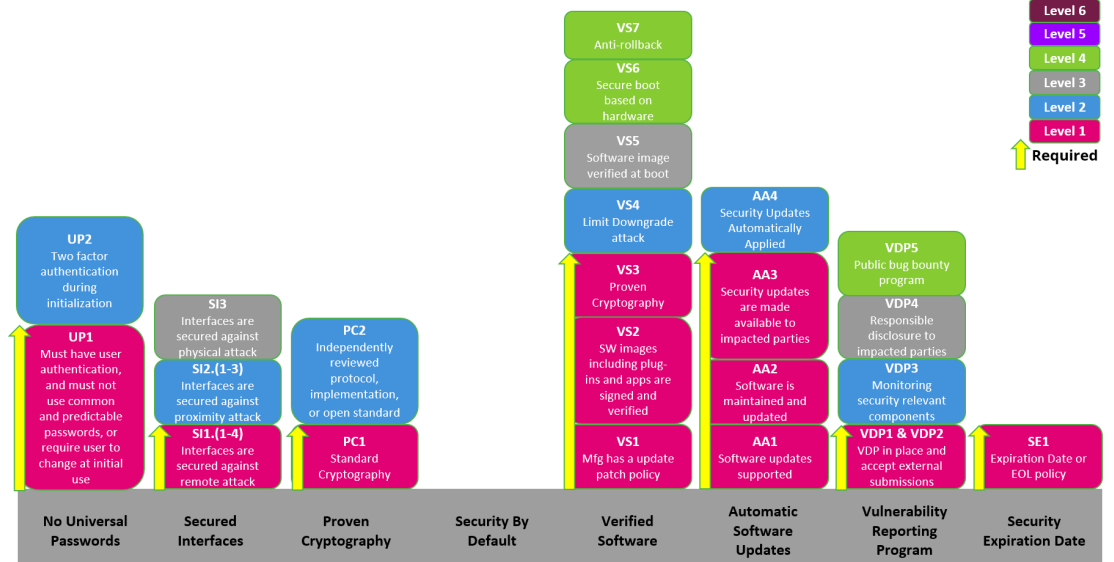


Commercial

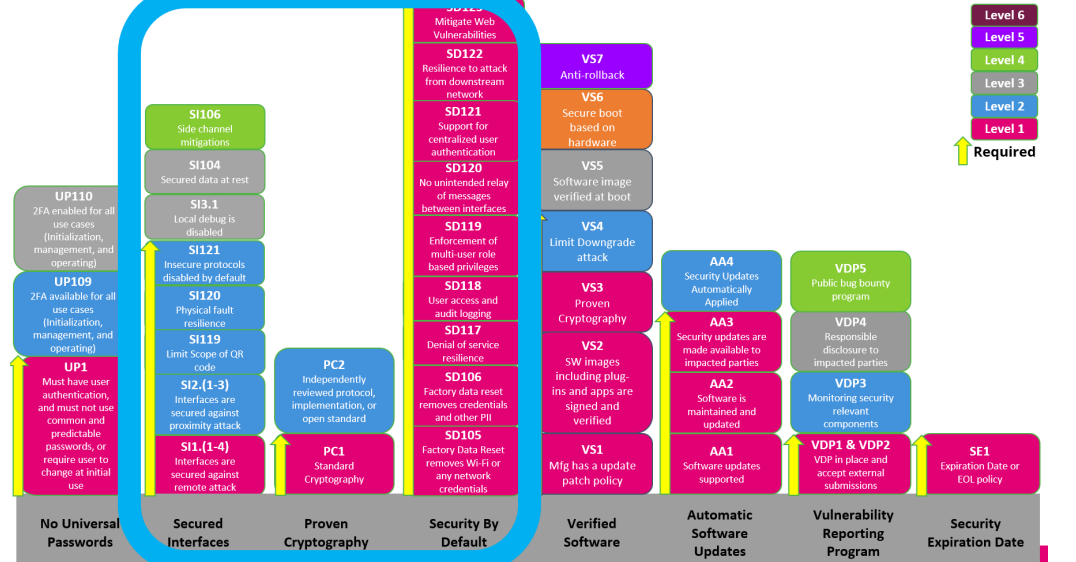
Residential/Consumer

vs. Commercial

Base Profile



Network Lighting Controller Profile



Additional Requirements for Commercial NLC

Secured Interfaces

SI106

Side channel mitigations

SI104

Secured data at rest

SI3.1

Local debug is disabled

SI121

Insecure protocols disabled by default

SI120

Physical fault resilience

SI119

Limit Scope of QR code

Security By Default

SD123

Mitigate Web Vulnerabilities

SD122

Resilience to attack from downstream network

SD121

Support for centralized user authentication

SD120

No unintended relay of messages between interfaces

SD119

Enforcement of multi-user role based privileges

SD118

User access and audit logging

SD117

Denial of service resilience

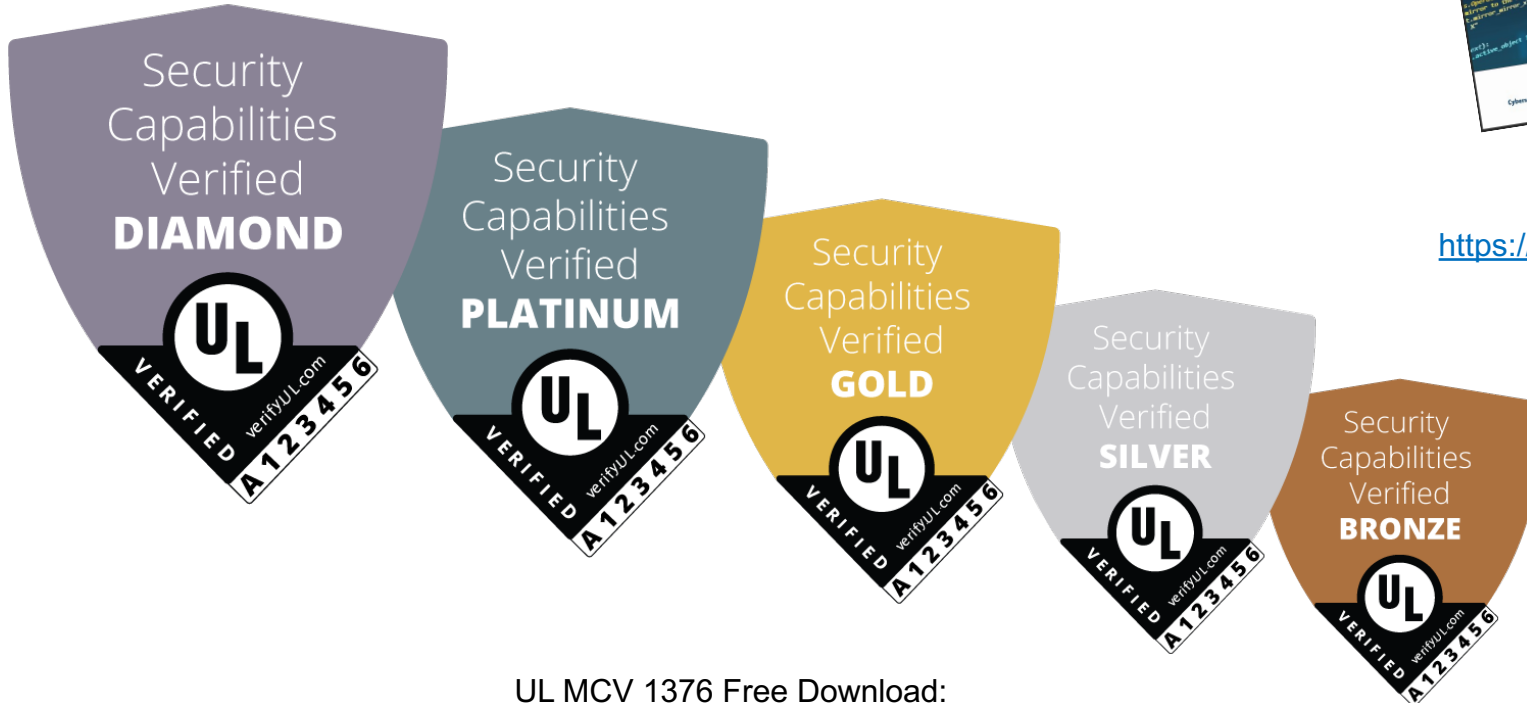
SD106

Factory data reset removes credentials and other PII

SD105

Factory Data Reset removes Wi-Fi or any network credentials

UL MCV 1376

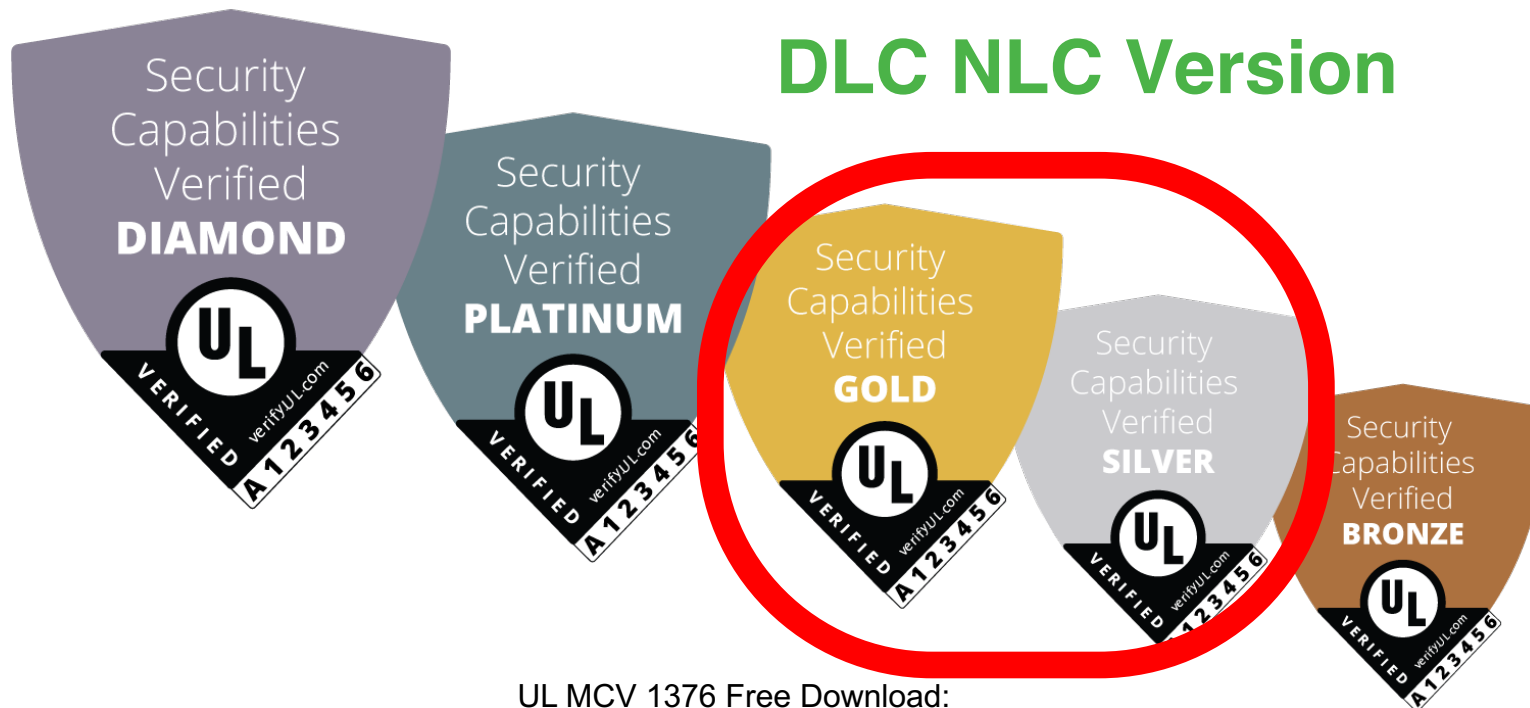


<https://ims.ul.com/loTSecurityTop20>

UL MCV 1376 Free Download:
<https://www.shopulstandards.com/ProductDetail.aspx?UniqueKey=35953>

UL MCV 1376

DLC NLC Version



UL MCV 1376 Free Download:
<https://www.shopulstandards.com/ProductDetail.aspx?UniqueKey=35953>

UL MCV 1376

Alignment Key



FULLY
ALIGNED



PARTIALLY
ALIGNED

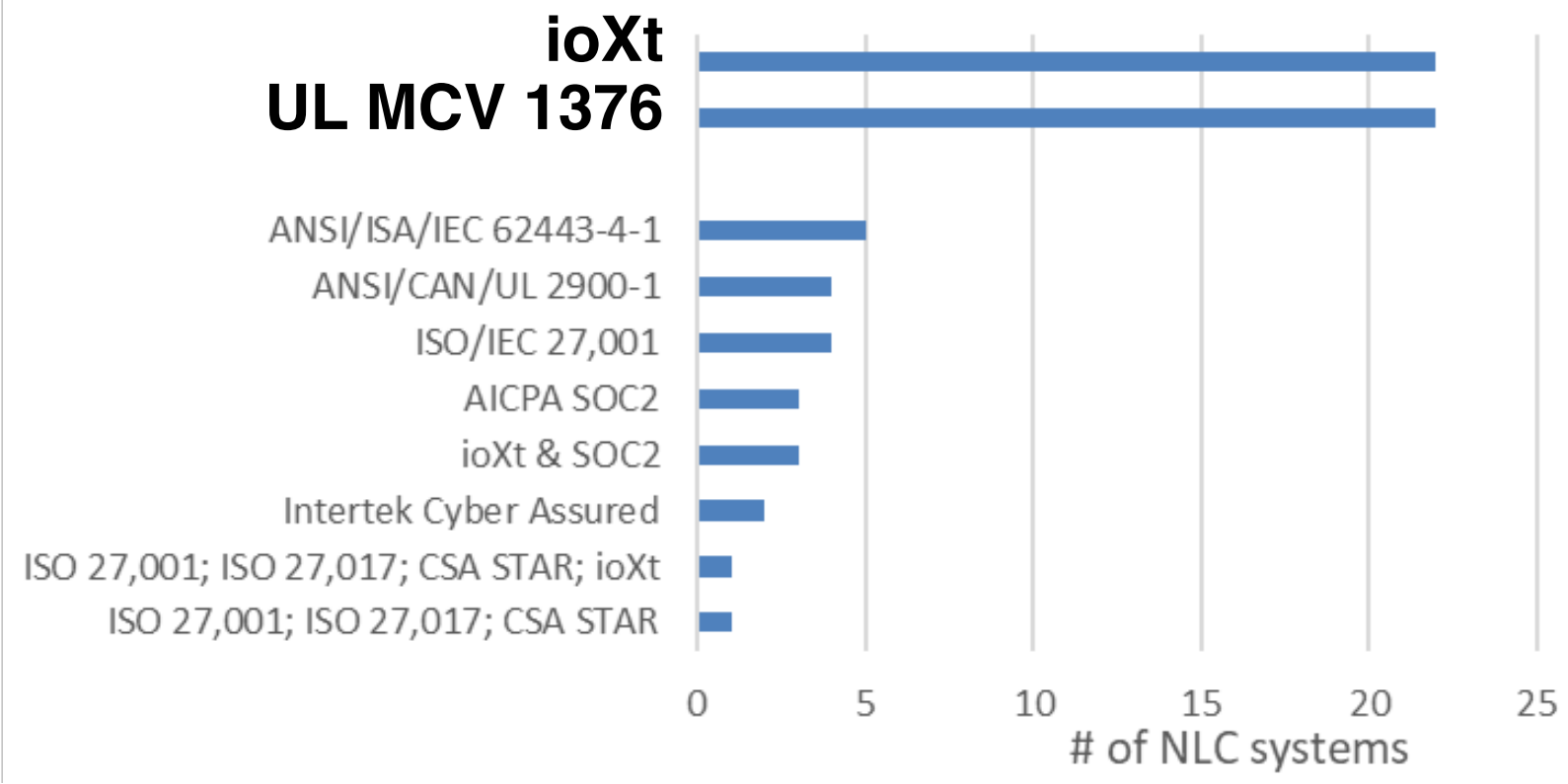


MINIMALLY
ALIGNED

UL IoT Security Rating (UL MCV 1376)	UK DCMS	NIST	ETSI	CSDE
Software Updates				
Data & Cryptography				
Logical Security				
System Management				
User Identifiable Data				
Protocol Security				
Process & Documentation Requirement				

<https://www.ul.com/resources/ul-and-dlc-cyber-program-qualified-products>

Certifications of Systems on the NLC QPL



Popular

Less Popular

Why so many certifications?





**ANSI/SA/IEC
62443**

ANSI/ISA/IEC 62443



International Society of Automation

www.ISA.org



**International
Electrotechnical
Commission**

www.IEC.ch



American National Standards Institute

www.ANSI.org

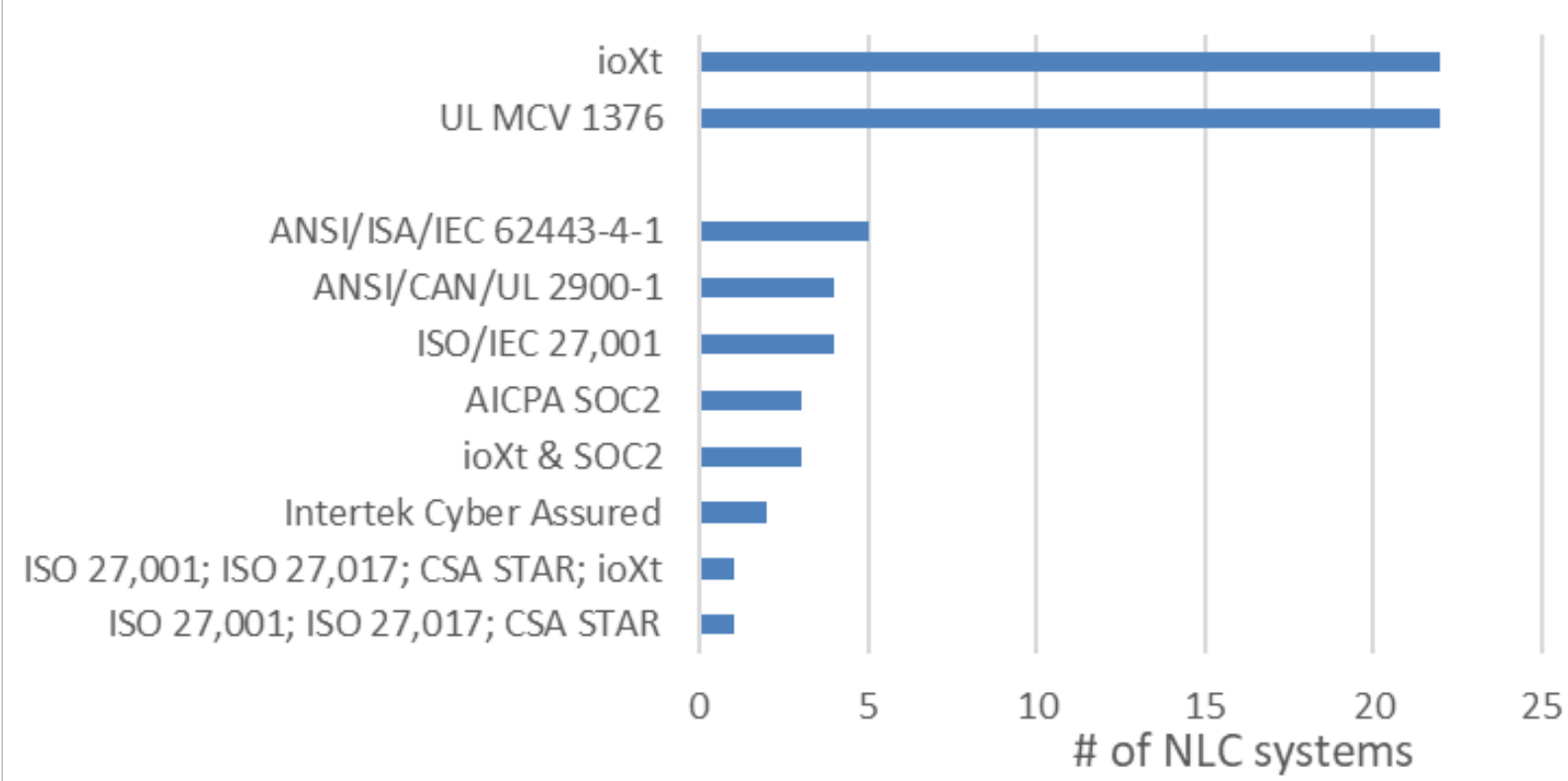
ANSI/CAN/UL 2900-1

The screenshot shows the UL Standards Sales Site interface. The browser address bar displays the URL: `standardscatalog.ul.com/ProductDetail.aspx?productId=UL2900-1`. The site header is red and features the UL logo, the text "UL Standards Sales Site", and navigation links for "Help", "My Cart", and "Sign In". Below the header, there are dropdown menus for "English" and "US Dollar". A navigation bar contains four main categories: "Browse & Buy UL Standards", "UL Resources", "Other Products", and "Sales Site Info".

The main content area is divided into two columns. The left column contains a "Return To Search" link and five buttons: "Complete List of UL Documents", "View Top Sellers", "What's New", "Request a Quote", and "UL Certification Customer". The right column features a product card for "ANSI/CAN/UL Standard for Software Cybersecurity for Network-Connectable Products, Part1: General Requirements". The card includes a UL Standard icon, the product title, and the following details:

- UL Standard
- [Scope](#)
- [Summary of Topics](#)
- Standard 2900-1, Edition 1
- Edition Date: July 05, 2017
- SCC Approved: June 05, 2020
- ANSI Approved: June 05, 2020

Certifications of Systems on the NLC QPL





Less Popular

ISO/IEC 27001 for Information Security Management Systems



iso.org/isoiec-27001-information-security.html

Standards About us News Taking part Store Q Shopping cart EN



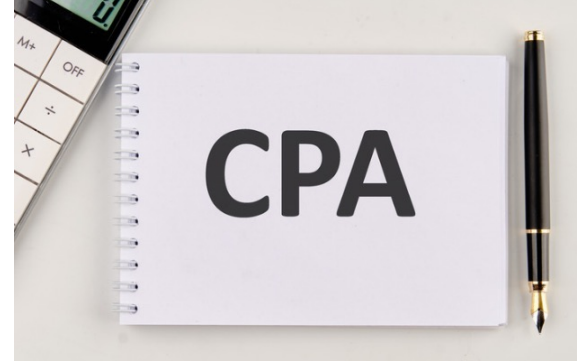
POPULAR STANDARDS

ISO/IEC 27001

INFORMATION SECURITY MANAGEMENT

<https://www.iso.org/isoiec-27001-information-security.html>

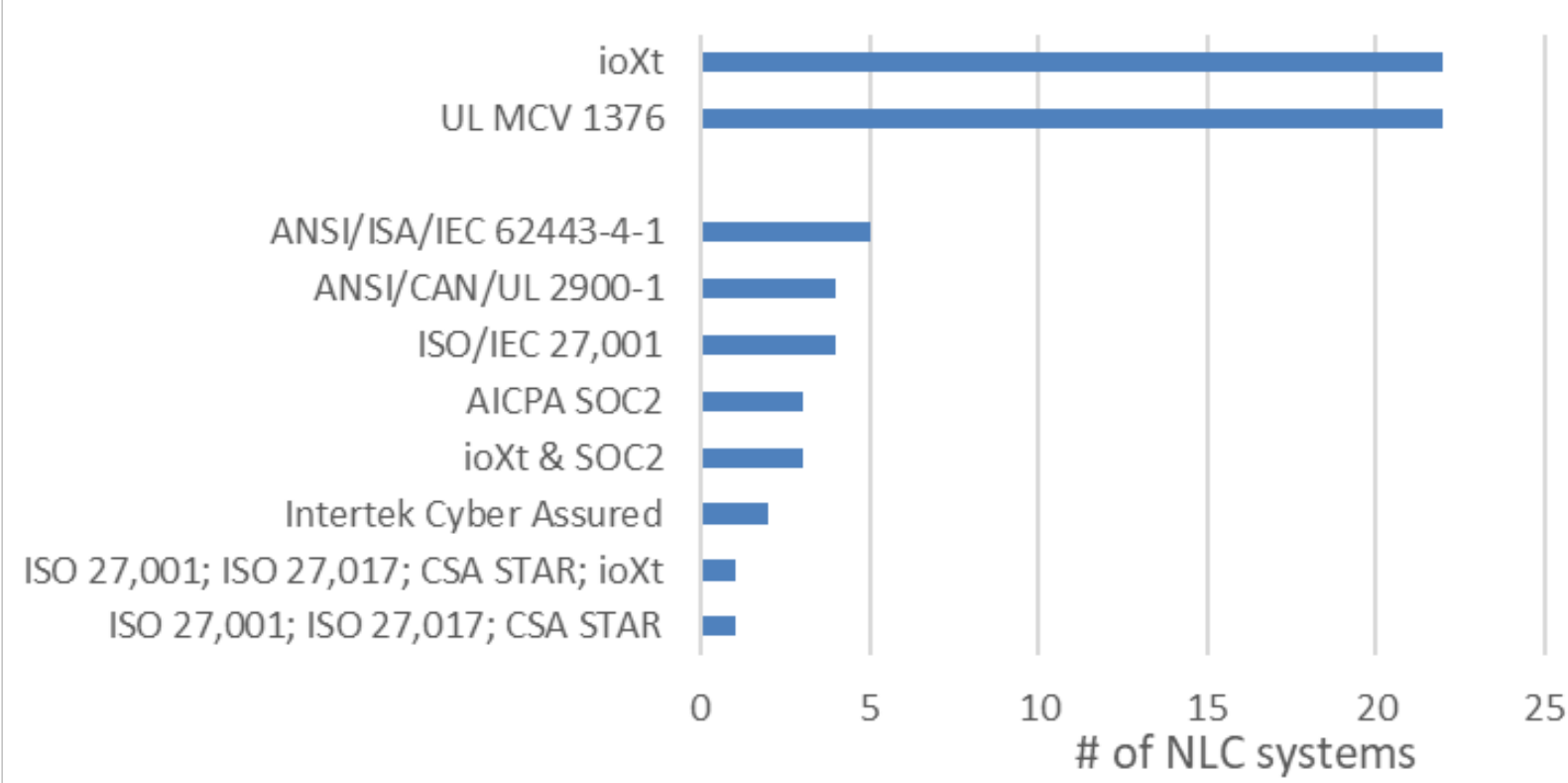
AICPA SOC 2



The screenshot shows the AICPA website page for SOC for Service Organizations. The URL in the browser is [aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html](https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html). The page features the AICPA logo, navigation menus for Topics, Career Guidance, CPE & Learning, Certifications, News & Advocacy, and Membership. The breadcrumb trail is: AICPA > Topics of Interest Overview > Financial Reporting Center (FRC) > Assurance and Advisory > SOC for Service Organizations. The main heading is "SOC for Service Organizations" with a font size adjustment icon (Aa). Below the heading are social media sharing icons for Facebook, Twitter, LinkedIn, Email, and Print. A paragraph explains: "SOC for Service Organizations are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service." Below this text are three columns, each with an AICPA SOC logo and a title: "CPAs", "Users & User Entities" (with a photo of a woman working on a laptop), and "Service Organizations".

<https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html>

Certifications of Systems on the NLC QPL



Less Popular

Intertek Cyber Assured

WHY DID INTERTEK DEVELOP CYBER ASSURED?

- **Cyber Assured** developed from the ground up specifically for consumer IoT products
 - Security requirements for Medical or Industrial Control devices do not always translate to a light bulb or a smart plug.
- **Cyber Assured** provides reasonable security that is appropriate for relatively low cost consumer products.
- **Cyber Assured** incorporates end-to-end security, includes:
 - The IoT Device
 - Mobile App
 - Cloud Service



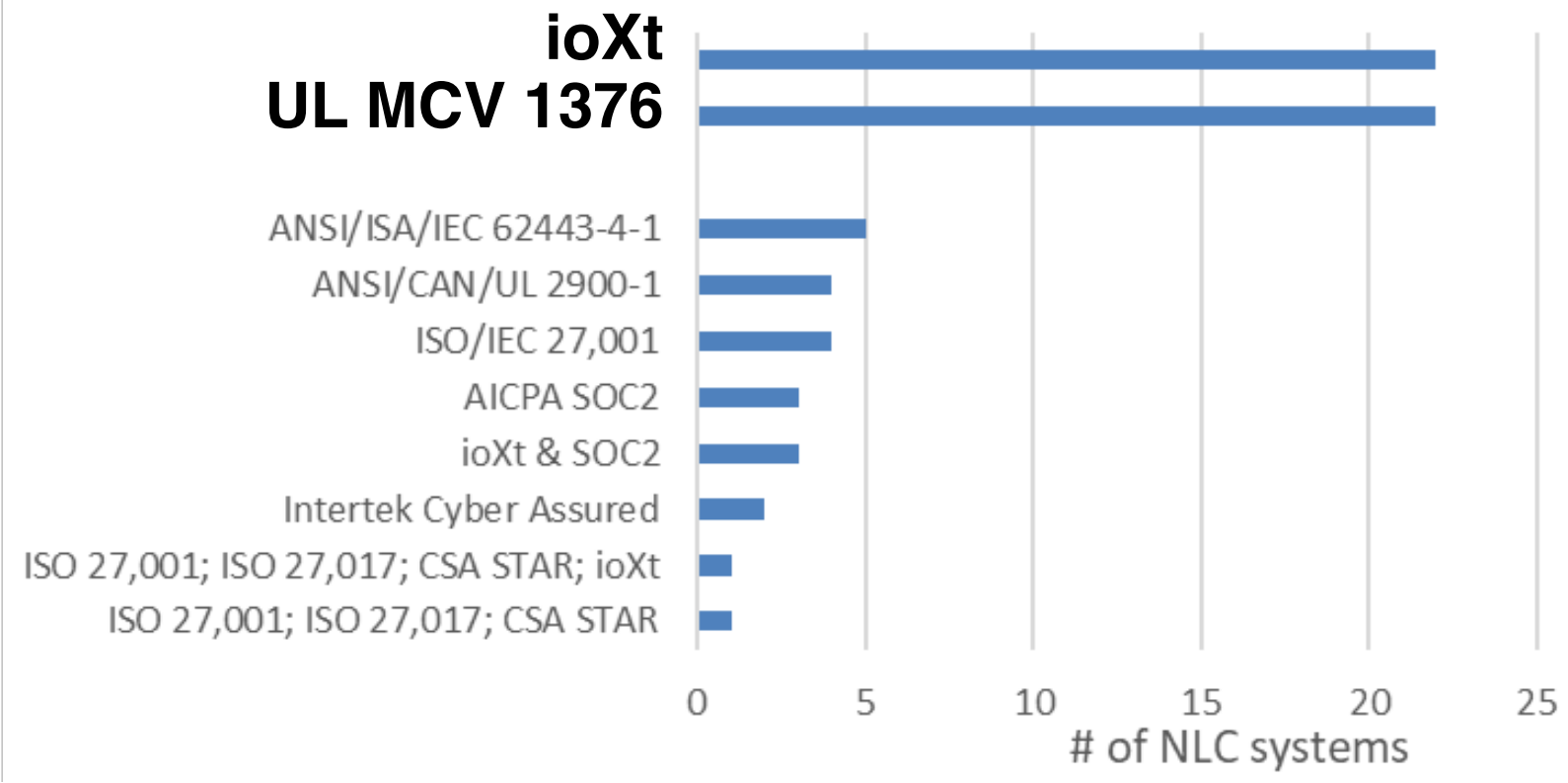
CSA STAR™

Cloud Security Alliance Security, Trust and Assurance Registry



<https://cloudsecurityalliance.org/star/registry/>

Certifications of Systems on the NLC QPL



Popular

For More Details



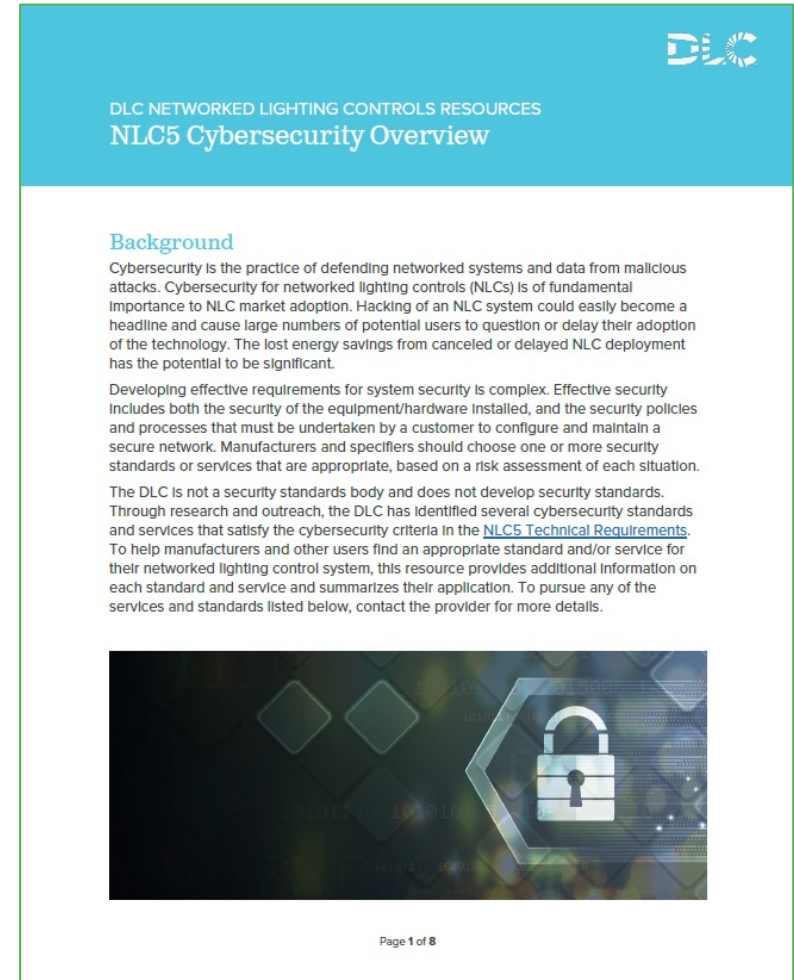
DLC
Energy · Quality · Controllability™

Cybersecurity Webinar

Levin Nock, PhD
Senior Technical Manager

2021.07.20

<https://www.designlights.org/news-events/events/webinar-whats-next-for-cybersecurity-at-the-dlc/>



DLC

DLC NETWORKED LIGHTING CONTROLS RESOURCES
NLC5 Cybersecurity Overview

Background

Cybersecurity is the practice of defending networked systems and data from malicious attacks. Cybersecurity for networked lighting controls (NLCs) is of fundamental importance to NLC market adoption. Hacking of an NLC system could easily become a headline and cause large numbers of potential users to question or delay their adoption of the technology. The lost energy savings from canceled or delayed NLC deployment has the potential to be significant.

Developing effective requirements for system security is complex. Effective security includes both the security of the equipment/hardware installed, and the security policies and processes that must be undertaken by a customer to configure and maintain a secure network. Manufacturers and specifiers should choose one or more security standards or services that are appropriate, based on a risk assessment of each situation.

The DLC is not a security standards body and does not develop security standards. Through research and outreach, the DLC has identified several cybersecurity standards and services that satisfy the cybersecurity criteria in the [NLC5 Technical Requirements](#). To help manufacturers and other users find an appropriate standard and/or service for their networked lighting control system, this resource provides additional information on each standard and service and summarizes their application. To pursue any of the services and standards listed below, contact the provider for more details.

Page 1 of 8

<https://www.designlights.org/dlc-report/nlc5-cybersecurity-overview/>

Resources



Resources

- [DLC Cybersecurity Standards Guide](#)
- [Lighting Controls Association – 8 Tips for Lighting Cybersecurity](#)
- [BetterBricks.com – Wireless Guides & Sequence of Operations](#)





Questions





Thank You!

Levin Nock – Design Lights Consortium

Maurice Karagiorgos – Lutron Electronics

Additional information provided by:

Acuity

Avi-On Lighting

Cooper Lighting

Fernhill Shopworks

Illuminating Engineering Society

Lighting Controls Association

RAB Lighting

Contact Us

Dan Kuhl

Evergreen

[dan.kuhl@evergreen-
efficiency.com](mailto:dan.kuhl@evergreen-efficiency.com)

[www.evergreen-
efficiency.com/](http://www.evergreen-efficiency.com/)

Maurice Karagiorgos

Lutron

Electronics

[mkaragiorgos@
lutron.com](mailto:mkaragiorgos@lutron.com)

www.lutron.com

Levin Nock

Design Lights

Consortium

lnock@designlights.org

g

www.designlights.org