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.

Cybersecurity Standards Recognized by the DLC

This table describes the primary application and timeline for certification of the cybersecurity standards listed in Table CS-1 of the DLC NLC5 Technical Requirements.

Standard	Primary Application	Timeline for Certification
ANSI/UL 2900-1	Network-connectable products, including NLC	Dependent on system complexity (contact provider for more information)
CSA/ANSI T-200	Maturity level evaluation of software development or product connected to a network and cybersecurity programs	Dependent on the time it takes to meet the required maturity level for all associated cybersecurity controls
IEC 62443	Securing operational technology (OT) that is used in automation and control systems, including industrial, building automation, energy sector, water/wastewater, and others.	ISASecure certifications include: • Supplier development processes to ISA/IEC 62443-4-1 • Component security capabilities to ISA/IEC 62443-4-2 • System security capabilities to ISA/IEC 62443-3-3
SOC 2	Internal corporate governance and vendor management regarding data integrity, confidentiality, and privacy	8 to 24 months to start, then annual audits
ISO/IEC 27001	Internal corporate governance and vendor management to manage data and risk	Details not available (contact provider for more information)
ISO/IEC 27017	Cloud security addition to ISO 27001	Details not available (contact provider for more information)

FedRAMP	Cloud applications for federal installations	2 to 9 months, then annual assessments
CSA STAR	Assessment of appropriate level of cloud security	STAR Attestation varies based on project complexity, type of report (Type I or Type II) and level of maturity. STAR Certification varies based on scope size and complexity. Attestation valid for 1 year, certification valid for 3 years.
ioXt	Internet gateway basic profile, plus extension profiles for specific residential and commercial devices; commercial NLC-specific profile planned 2021	Details not available (contact provider for more information)
PSA Certified	Primary Application	Timeline for Certification

ANSI/UL 2900-1

The ANSI/UL 2900 series of standards was developed as part of UL's Cybersecurity Assurance Program (UL CAP), which provides manufacturers testable and measurable criteria to assess product weaknesses, vulnerabilities, and security risk controls.

ANSI/UL 2900-1 applies to network-connectable products that shall be evaluated and tested for vulnerabilities, software weaknesses, and malware. This standard describes:

- Requirements for the software developer (vendor or other supply chain member) and risk management process for their product.
- Methods by which a product shall be evaluated and tested for the presence of vulnerabilities, software weaknesses, and malware.
- Requirements for the presence of security risk controls in the architecture and design of a product.

ANSI/UL 2900-1 applies to general network-connectable products, including networked lighting controls. The UL 2900-2 family has specific standards for healthcare, industrial control, and building and life safety.

CSA/ANSI T200

CSA/ANSI T200 is a Bi National (Canada & USA) Cybersecurity Standard published by CSA Group. This Standard describes a methodology for assessing the product software and cybersecurity control maturity of an organization. This Standard provides the evaluators and vendors a method to determine the control maturity of the organization and products/solutions being developed regardless of solution vertical. It covers the entire product system life cycle from conception to full commissioning and until the end of life. This Standard is applicable to all IoT and related products/solutions.

The maturity level of each cybersecurity activity is assessed so that an organization can assert their security maturity in relationship to best practices. The maturity levels of the CVP range from Level 0 to Level 3, where Level 0 means no evidence exists of the basic controls needed to protect the organization or its products, while Level 3 affirms a well-established process for security implementation with continuous support and security enhancements.

IEC 62443

The IEC 62443 series of standards was originally developed for automation and control systems. Today, the IEC 62443 standards are being analyzed for use as a technology horizontal standard with formal applicability to multiple industry sectors. Each document in the series covers an aspect of cybersecurity and is updated independently. Various documents cover component technical requirements, system technical requirements, product supplier development lifecycle practices, integrator practices, and end user management and operation of a cybersecurity program at a site.

- **Part 4-1: Product security development life cycle** requirements describe the requirements for a product developer's security development lifecycle. The principal audience includes suppliers of control system and component products.
- **Part 4-2: Technical security requirement for IACS (Industrial Automation and Control System) components** describes the requirements for IACS components based on security level. Components include embedded devices, host devices, network devices, and software applications. The principal audience includes suppliers of Component products that are used in control systems.
- **Part 3-3: System security requirements and security levels** describes the requirements for an IACS system based on security level. The principal audience includes suppliers of control systems, system integrators, and asset owners.

Certifications to the IEC 62443 standards are offered by the International Society of Automation (ISA), the authors of the 62443 series of standards, under the ISASecure® brand. ISASecure certifications are delivered via a global network of ISO 17065 accredited certification bodies accredited to ISASecure CB requirements by ISO 17011 accreditation bodies.

SOC 2 (Service Organization Control 2)

The SOC 2 report is intended to meet the needs of a broad range of users and is tailored to each service organization's needs (different principles, controls, and tests of controls). These reports can play an important role in the oversight of the organization, vendor management programs, internal corporate governance and risk management processes, and regulatory oversight.

SOC 2 reports are administered by certified public accountants and provide a description of the service organization's system. This report contains detailed information about whether:

- The description of the service organization's system was presented in accordance with the description criteria, and

- The controls stated in the description were suitably designed and operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria (security, availability, and processing integrity of the systems used to process users' data and the confidentiality and privacy of the information processed by these systems).

ISO/IEC 27001

This international standard provides requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). It includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

The ISO/IEC 27001 certification usually involves a three-stage external audit process defined by the ISO/IEC 17021 and ISO/IEC 27006 standards:

- **Stage 1** is a preliminary, informal review of the ISMS; for example, checking for the existence and completeness of key documentation, such as the organization's information security policy, Statement of Applicability (SoA) and Risk Treatment Plan (RTP). This stage serves to familiarize the auditors with the organization and vice versa.
- **Stage 2** is a more detailed and formal compliance audit that independently tests the ISMS against the requirements specified in ISO/IEC 27001. The auditors will seek evidence to confirm that the management system has been properly designed and implemented, and is currently in operation. Certification audits are usually conducted by ISO/IEC 27001 Lead Auditors. Passing this stage results in the ISMS being certified compliant with ISO/IEC 27001.
- **Ongoing** involves follow-up reviews or audits to confirm that the organization remains in compliance with the standard. Certification maintenance requires periodic reassessment audits to confirm that the ISMS continues to operate as specified and intended. These audits should happen at least annually, but are often conducted more frequently (by agreement with management), particularly while the ISMS is still maturing.

ISO/IEC 27017

This international standard provides guidelines supporting the implementation of information security controls for cloud service customers and cloud service providers. Some guidelines are for cloud service customers who implement the controls, and others are for cloud service providers to support the implementation of those controls. The selection of appropriate information security controls and the application of the implementation guidance provided will depend on a risk assessment and any legal, contractual, regulatory, or other cloud-sector specific information security requirements.

This standard gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

- Additional implementation guidance for relevant controls specified in ISO/IEC 27002, and
- Additional controls with implementation guidance that specifically relate to cloud services.

FedRAMP (The Federal Risk and Authorization Management Program)

The FedRAMP program provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by the US government. FedRAMP is mandatory for federal agency cloud deployments and service models at the low, moderate, and high risk impact levels. The FedRAMP security controls are based on NIST SP 800-53 Revision 4 baselines and contain controls above the NIST baseline that address the unique elements of cloud computing.

The purpose of FedRAMP is to:

- Ensure that cloud systems used by government entities have adequate safeguards,
- Eliminate duplication of effort and reduce risk management costs, and
- Enable rapid and cost-effective Government procurement of information systems/services.

CSA STAR™ (Cloud Security Alliance Security Trust, Assurance and Risk)

CSA STAR addresses security assurance in the cloud, with principles of transparency, rigorous auditing, and harmonization of standards. The CSA Cloud Controls Matrix (CCM) tool provides a meta-framework of cloud-specific security controls; mapped to leading standards, best practices, and regulations for information security tailored to cloud computing.

STAR enables cloud service solution providers to validate their cloud security and offer proof to current and future customers of the controls in place. STAR lets cloud customers assess which organizations meet the level of assurance they require and gain insight into the controls in place to protect their data.

ioXt

The mission of the ioXt Alliance is to build confidence in Internet of Things (IoT) products through multi-stakeholder, international, harmonized, and standardized security and privacy requirements, product compliance programs, and public transparency of those requirements and programs. Alliance members provide products and services for markets ranging from consumer electronics, mobile, automotive, and commercial building controls. Multiple labs provide testing.

The program is based on eight principles, which map back to US and EU regulations. These principles are further broken into multiple levels per principle, with over 60 test cases covering topics such as security, upgradability, and transparency. Device profiles are being developed to capture the unique security requirements for specific devices and markets. Process, components, and systems are covered, and future expansion will cover cloud services.

The ioXt Base Profile has been available since mid-2020. A profile tailored for networked lighting control gateway devices in commercial buildings is in development, with additional requirements beyond the Base Profile, with expected release mid-2021.

PSA Certified

- PSA Certified offers a framework for securing connected devices, from analysis through to security assessment and certification. The framework provides standardized resources to help resolve the growing fragmentation of IoT requirements and ensure security is no longer a barrier to product development.

Cybersecurity Services Recognized by the DLC

This table describes an overview and timeline for the cybersecurity services listed in Table CS-2 of the DLC NLC5 Technical Requirements.

Service	Overview	Timeline
UL IoT Security Rating (UL MCV 1376)	5-tiered approach to right-size assessment. Commercial NLC-specific profile launched 2020.	2-3 weeks
CSA Cybersecurity Verification Program (CVP) (CSA T200)	Recently standardized, see "Standards" above.	
Intertek Cyber Assured	For internet-connected consumer products.	Approximately 3-5 weeks

UL MCV (UL Marketing Claim Verification) 1376

UL MCV 1376 addresses device security capabilities plus product management, software update, and vulnerability management processes (including for cloud services). Seven different categories are assessed: secure software updates, data and cryptography, secure communications, document/process requirements, privacy requirements, system management, and logical security. Each of the seven categories is rated in five levels of maturity. In each category, the minimum acceptable maturity level is based on a risk analysis of the particular application. The requirements have been developed in alignment with global industry frameworks, including US NIST (United States National Institute of Standards and Technology), ETSI (European Telecommunications Standards Institute), CSDE (Council to Secure the Digital Economy), and UK DCMS (United Kingdom Digital, Culture, Media and Sport Code of Practice). An application-specific profile for networked lighting controls was launched in 2020.

CSA CVP (CSA Group Cybersecurity Verification Program)

This three-step program allows manufacturers to identify security activities employed for their IoT solutions, understand their existing maturity level, and develop specific test programs supporting an effective security culture for their connected solutions. The three steps include:

- **Step 1**: A self-assessment of security activities using a structured template developed by CSA Group.
- **Step 2**: CSA Group conducts an audit of the information presented in the self-assessment template and provides feedback on any gaps, which helps to

affirm a current level of cybersecurity maturity within the organization and product.

- **Step 3**: CSA Group can also perform product security testing using either voluntary international standards or a custom test plan appropriate for the IoT solution.

The maturity level of each cybersecurity activity is assessed so that an organization can assert their security maturity in relationship to best practices. The maturity levels of the CVP range from Level 0 to Level 3, where Level 0 means no evidence exists of the basic controls needed to protect the organization or its products, while Level 3 affirms a well-established process for security implementation with continuous support and security enhancements. This service is expected to become a standard.

Intertek Cyber Assured

Intertek's program was designed to protect the Internet of Things and provides comprehensive, risk appropriate cybersecurity testing for connected products. Its features include continuous vulnerability monitoring and a dedicated certification mark to add to products, with a listing on the Cyber Assured online directory. It incorporates testing of the three corners of the IoT 'triangle': the product itself, its mobile or web app, and the server 'back end'.

The DLC's Networked Lighting Controls Technical Requirements outline a need for testing in many areas of cybersecurity from process, components/embedded devices, system, and cloud services. Cyber Assured addresses all of these categories within one certification and is tailored to offer robust security with a fast-paced test and certification process.

Once the product has passed testing, it is enrolled in Cyber Assured's Continuous Vulnerability Monitoring program; this process detects new vulnerabilities affecting the product and provides the manufacturer with information to 'patch' the product to ensure continued security.