ioXt 2021 Network Lighting Controller Profile

Version 1.00

Document C-20-08-20
Date 7/9/21
Document Status: Release
Abstract
Keywords

1. Notice of Use and Disclosure

Elements of ioXt Alliance documentation, specifications, and test plans may be subject to third party property rights, including without limitation copyrights and patents. The ioXt Alliance is not responsible and shall not be held responsible in any manner for identifying or failing to identify any or all such third-party intellectual property rights.

This document and information contained herein are provided on a “AS IS” basis.

THE IOXT ALLIANCE DISCLAIMS ALL WARRANTIES EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OF THIRD-PARTIES, OR ANY IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR USE, TITLE, NON INFRINGEMENT, OR GUARANTEE OF PRODUCT SECURITY. IN NO EVENT WILL THE IOXT ALLIANCE BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OF DATA, INTERRUPTION OF BUSINESS, OR FOR ANY OTHER DIRECT, INDIRECT, SPECIAL OR EXEMPLARY, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, IN CONTRACT OR IN TORT, IN CONNECTION WITH THIS DOCUMENT OR THE INFORMATION CONTAINED HEREIN.

The above notice must be included in all copies of this document.

2. Document Version Information

Version	Date	Author	Description
0.01	8/20/20	Brad Ree (ioXt)	Initial Draft
1.0	7/9/21	Brad Ree (ioXt)	Release

Table of Contents

3. Introductions

3.1. Purpose

This document provides the specifications required to certify a device such that the manufacturer may use the ioXt Compliance mark. This specification defines which devices may be certified under the profile, along with the test plan which must be met. The test cases are defined in the ioXt Test Case Library document.
The Network Lighting Controller profile shall define the devices which may be certified using the profile, a threat model, and test plan.
ioXt approved labs must be explicitly approved to execute this profile and shall be governed with the ioXt Lab Agreement.

3.2. Verbal forms for expressions of provisions

This profile will utilize the definition of terms and usages for Requirements, Recommendations, and Permissions as defined by the ISO/IEC Directives, Part2.

A reference for these definitions can be found here:
https://www.iso.org/sites/directives/current/part2/index.xhtml#_idTextAnchor072

3.3. Acronyms and Abbreviations

Acronym	Definition
VDP	Vulnerability Disclosure Program or Vulnerability Reporting Pledge
AA	Automatically Applied Update Pledge
SE	Security Expiration Date Pledge
VS	Verified Software Pledge
UP	No Universal Password Pledge
PC	Proven Cryptography Pledge
SI	Secured Interface Pledge
CM	Countermeasure

3.4. Definitions

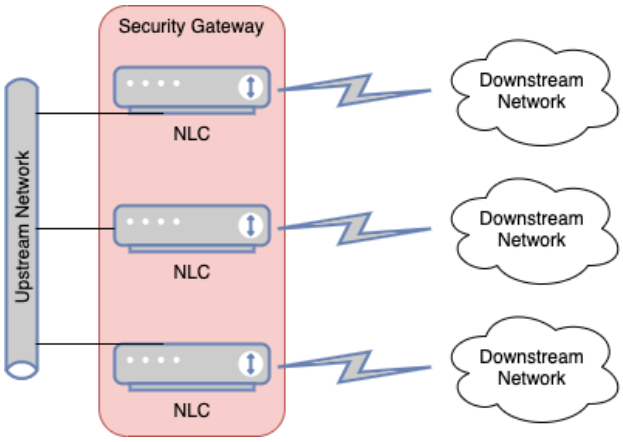
Term	Definition
Constrained	A device that contains sufficient resources only to perform the function for which they were designed. Lacking

	sufficient processing, memory, or power resources to perform additional functions or features.
Threat Modelling	Threat modelling works to understand, identify, and communicate threats to scope security engagements or prioritize mitigations.
Likelihood: Physical Access	The attacker has unrestricted physical access to the device.
Likelihood: Proximity Access	The attacker is able to interact with the NLC via the local network. Examples of this interaction include an attacker within Radio range or has access to the Physical Local Network.
Likelihood: Remote Access	The attacker is remote to the network and device. The attacker does not have access to the cloud service, or the internet routing network.
Likelihood: Easy	Does not require a compromised device. Easily executed by casual adversaries.
Likelihood: Moderate	Requires non-trivial effort/expense per Device or requires a compromised device.
Likelihood: Difficult	Requires intimate knowledge of or access to the victim, or non-trivial effort/expense by motivated or sophisticated adversaries.
Impact: Low sensitivity data or Denial of Service	Some data is compromised but no sensitive data or control is compromised.
Impact: Limited sensitive data or control	Limited sensitive data or some functions of the device are compromised.
Impact: Complete compromise	Significant sensitive data or all effective functions of the device are compromised. By definition, compromise of a controller implicitly implies complete compromise of its downstream devices.
Impact: Single Device	Only a single device is compromised to some degree.
Impact: Local Network	One or more devices within a local network are impacted by the attack.
Impact: Entire Fleet	All fielded devices of the given type are subject to compromise to some extent. The attack can be scaled for the entire fleet.
Vectored Attack	The attacker is seeking to gain access to higher levels of the system or network through constrained devices using physical or proximity access.
OT Network	Operational Technology Networks are those networks that support the operation of devices that have a direct interaction with a physical space or equipment. These

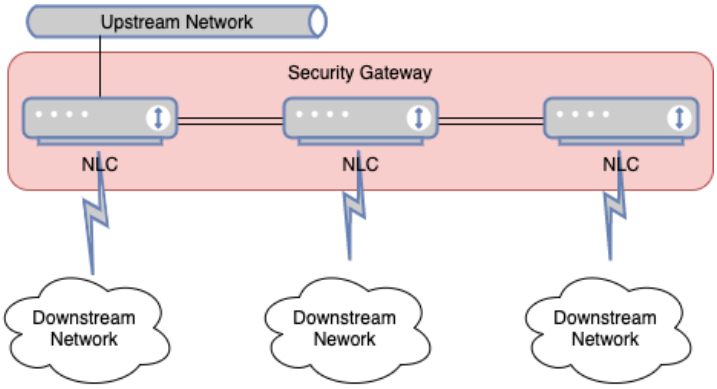
	include aspects that may have an impact on Life and Safety. These networks may consist of legacy as well as modern OT protocol implementations.
Downstream Network	Networks are relative to the Edge or Aggregation device that is responsible for the control of a lighting network. Networks that are Downstream of the NLC consist of OT or lighting control networks that terminate on at the NLC. These networks do not directly communicate with the outside world and rely on the NLC to broker to translate or pass on messages.
Upstream Network	In general, the Upstream Network is any network not included in the Downstream Network definition.
Preconfigured NLC based lighting test system	A network lighting controller with at least two devices connected on the downstream network. One of the downstream devices must be configured to control the other downstream device. The network lighting controller shall have an administrator and user account created.

Generic NLC Network Diagram Examples

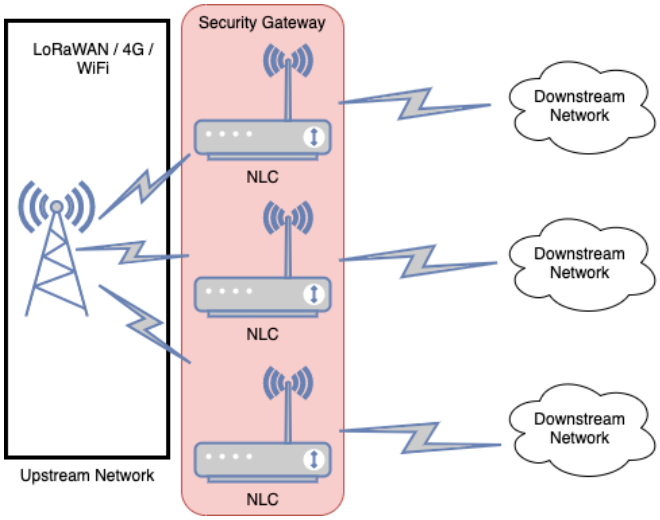
NLC Common Upstream Bus



NLC Chained Upstream Bus



NLC Wireless Upstream Bus



3.5. References

Application Threat Modeling. (n.d.). Retrieved from owasp.org: https://owasp.org/www-community/Application_Threat_Modeling

ioXt 2020 Base Profile. (n.d.). Retrieved from https://ioxtalliancemembers.org/wg/Compliance_wg/document/135

Terminology for Constrained-Node Networks. Retrieved from IETF: https://tools.ietf.org/html/rfc7228

3.6. Profile Methodology

This profile contains a Device Definition that specifies which devices are covered.
The process of threat modeling has been followed to identify potential threats against the device. Known threats have been included in Appendix A: Threat Model. Once all potentially known threats have been identified, the severity of each threat was evaluated. Countermeasures to those threats with High or Medium severity were defined and helped determine the Test Plan.

4. Profile Scope

4.1. Device expected use

4.1.1. Commercial device
4.1.2. Long life deployment (10+ years)
4.1.3. Physical access control can not be guaranteed, but may be limited
4.1.4. Upstream side of NLC is on a LAN with other building/corp devices in which other devices may not be trusted
4.1.5. Legacy protocol security on the Downstream side shall not be addressed in this profile, as legacy devices must still be supported. (Protections for Downstream legacy networks are determined at the NLC)
4.1.6. Device/lighting network must have high availability
4.1.7. End point devices should maintain functionality with loss of internet connectivity or connectivity to the Lighting controller
4.1.8. May be deployed before Internet services are available
4.1.9. May lose Internet connection for long periods of time
4.1.10. Northbound communications may be to both local and remote (cloud) networks
4.1.11. Includes unicast, multicast, and broadcast communications.
4.1.12. Shall communicate with southbound devices or end devices for the purpose of updates, settings adjustments, or control

4.2. Devices which are in scope

4.2.1. Shall contain a Upstream interface which is IP
4.2.2. Shall contain a wired or wireless interface for Upstream communications
4.2.3. The device shall not be constrained
4.2.4. One or more Downstream interfaces to lighting devices
4.2.5. End Devices connecting to the Downstream interface terminates the security in the device before being routed to the Upstream interface.

4.3. Device MAY include the following

4.3.1. May contain additional interfaces for communications to BMS network technologies

4.3.2. May include a secondary interface to configure the NLC

4.3.3. May include a means to allow an administrator roll back of the NLC firmware

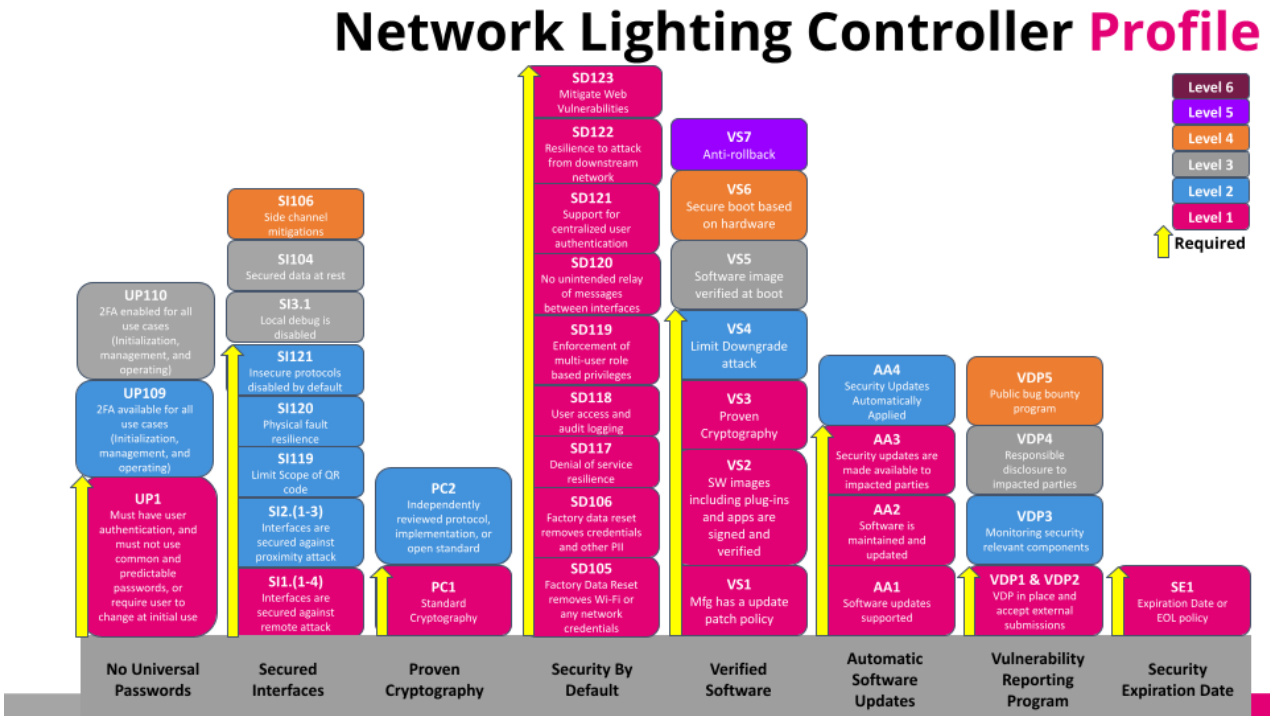
5. Requirements

5.1. Test Case Library Version

The profile requirement document only describes the test cases needed for certification by test case ID. The actual text of the test cases are located in the ioXt Test Case Library. As the test case library is a shared document used by all profiles, there may be newer versions of the library than was approved when this profile was created.

The NLC profile version 1.0 shall only use ioXt Test Case Library version 5.01. Further, this profile includes threats from the Common Commercial Ethernet Threat Model version 1.00.

5.2. Profile Summary



5.3. Proven Cryptography

5.3.1. Requirements

ID	Test Case
PC1	Standard cryptography
PC2	Independently reviewed protocol, implementation, or open standard

5.3.2. Security Levels

Security Level	Test Cases	Required For Certification
1	PC1	Yes
2	PC2	

5.4. No Universal Password

5.4.1. Requirements

ID	Test Case
UP1	User credentials shall not be common or predictable, or the credentials must be required to change at initial use.
UP109	2FA available for all use cases (Initialization, management, and operating)
UP110	2FA enabled for all use cases (Initialization, management, and operating)

5.4.2. Security Levels

Security Level	Test Cases	Required for Certification
1	UP1	Yes
2	UP109	
3	UP110	

5.5. Verified Software

5.5.1. Requirements

ID	Test Case
VS1	Manufacturer has an update patch policy
VS2	Software images including plug-ins and apps are signed and verified
VS3	Proven Cryptography

VS4	Limit Downgrade attack
VS5	Software image verified at boot
VS6	Secure boot based on hardware
VS7	Anti-rollback

5.5.2. Security Levels

Security Level	Test Cases	Required for Certification
1	VS1 VS2 VS3	Yes
2	VS4	Yes
3	VS5	
4	VS6	
5	VS7	

5.6. Security by Default

5.6.1. Requirements

ID	Test Case
SD105	Factory Data Reset removes Wi-Fi or any network credentials
SD106	Factory Data Reset removes account token, credentials and other PII
SD117	Denial of service resilience
SD118	User access and audit logging
SD119	Enforcement of multi-user role based privileges
SD120	No unintended relay of messages between interfaces

SD121	Support for centralized user authentication
SD122	Resilience to attack from downstream network
SD123	Mitigate web vulnerabilities

5.6.2. Security Levels

Security Level	Test Cases	Required for Certification
1	SD105 SD106 SD117 SD118 SD119 SD120 SD121 SD122 SD123	Yes

5.7. Secured Interfaces

5.7.1. Requirements

ID	Test Case
SI1.1	Remote Attack: All certifiable protocols used on the interfaces contained in the device shall be Certified
SI1.2	Remote Attack: Unused Services are disabled
SI1.3	Remote Attack: Authentication
SI1.4	Remote Attack: Secured Communications
SI2.1	Proximity Attack: Unused Services are disabled

SI2.2	Proximity Attack: Authentication
SI2.3	Proximity Attack: Secured Communications
SI119	Limit Scope of QR code
SI120	Physical fault resilience
SI121	Insecure protocols disabled by default
SI3.1	Local debug is disabled
SI104	Secured data at rest
SI106	Side channel mitigations

5.7.2.Security Levels

Security Level	Test Cases	Required for Certification
1	SI1.1 SI1.2 SI1.3 SI1.4	Yes
2	SI2.1 SI2.2 SI2.3 SI119 SI120 SI121	Yes
	SI3.1 SI104	
	SI106	

5.8. Automatically Applied Updates

5.8.1.Requirements

ID	Test Case

AA1	Software updates supported
AA2	Software is Maintained and Updated
AA3	Software updates are made available to impacted parties
AA4	Security Updates Automatically Applied

5.8.2. Security Levels

Security Level	Test Cases	Required for Certification
1	AA1 AA2 AA3	Yes
	AA4	

5.9. Vulnerability Reporting Program

5.9.1. Requirements

ID		Test Case
VDP1		Vulnerability Disclosure Program (VDP) in place
VDP2		Accept external submissions
VDP3		Monitoring security relevant components
VDP4		Responsible disclosure to impacted parties
VDP5		Public bug bounty program

5.9.2. Security Levels

Security Level	Test Cases	Required for Certification
1	VDP1 VDP2	Yes

	VDP3	
	VDP4	
	VDP5	

5.10. Security Expiration Date

5.10.1. Requirements

ID		Test Case
SE1.1		End of life notification policy is published
SE1.2		Expiration Date is published

5.10.2. Security Levels

Security Level	Test Cases	Required for Certification
1	SE1.1 or SE1.2	Yes

6. Threat Model

6.1. Threat Evaluation

6.1.1. Likelihood (Difficulty x Access)

Difficulty ↓ Access →	Physical Access	Proximity Access	Remote Access
Difficult	Low	Medium	Medium
Moderate	Low	Medium	High
Easy	Medium	High	High

6.1.2. Impact (Scope x Data access/control)

Scope ↓ Data Access/Control →	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device	Low	Medium	Medium
Local Network	Low	Medium	High
Entire Fleet	Medium	High	High

6.1.3. Severity (Likelihood x Impact)

Likelihood↓Impact→	Low	Medium	High
Low	Low	Medium	Medium
Medium	Low	Medium	High
High	Medium	High	High

6.2. Provisioning

6.2.1. Re-provision from user account to attackers account

Threat Description	Attacker forces deprovisioning of device through factory reset, legitimate re-provisioning mechanism, or existing vulnerability.
Threat Agent	Attacker with physical access to machine (factory reset) or in proximity or remote access.
Resulting Impact	Complete compromise of device. If factory reset or other memory wipe technique not used for attack, sensitive user data may also be exposed.

6.2.1.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult	**X**		
Medium			
Easy			

6.2.1.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			**X**
Local Network			
Entire Fleet			

6.2.1.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low		**X**	
Medium			
High			

6.2.1.4. Countermeasure

Test Case	UP2.1, SI1.3, SI2.2, SI103
Comments/Guidance	

6.3. Normal Operation – Physical Attacks

6.3.1. Attacker reads flash memory for security parameters or sensitive user data

Threat Description	An attacker attempts to extract security parameters or sensitive user data from the flash memory in the device.
Threat Agent	Attacker with physical access to device.
Resulting Impact	Compromise of sensitive user or security data (e.g. encryption keys).

6.3.1.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Medium	**X**		
Easy			

6.3.1.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device		**X**	
Local Network			
Entire Fleet			

6.3.1.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low		**X**	
Medium			
High			

6.3.1.4. Countermeasure

Test Case	SI104
Comments/Guidance	

6.3.2. Attacker monitors external upstream radio interface to steal sensitive data

Threat Description	Attacker makes an electrical connection to an external radio interface component within the device and extracts a session key. Key may be used to break encrypted traffic or perform following man-in-the-middle attack
Threat Agent	Attacker with physical access to a device who has disassembled unit.
Resulting Impact	Compromise of sensitive user data. Further device and data compromise depending on success of a following man-in-the-middle attack. Vulnerability ends when session key rotation period expires.

6.3.2.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult	**X**		
Medium			
Easy			

6.3.2.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device		**X**	
Local Network			
Entire Fleet			

6.3.2.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low		**X**	
Medium			
High			

6.3.2.4. Countermeasure

Test Case	SI1.3, SI1.4, SI2.2, SI2.3
Comments/Guidance	

6.4. Normal Operation - Network-based Attacks

6.5. Normal Operation - Functional Attacks

6.5.1. Attacker pairs Network Lighting Controller to their device

Threat Description	Attacker pairs with device over phone, tablet, or other device controlled by attacker.
Threat Agent	Attacker in physical proximity to the device.
Resulting Impact	The attacker can control the device and may be able to retrieve sensitive user data.

6.5.1.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Medium			
Easy		X	

6.5.1.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			X
Local Network			
Entire Fleet			

6.5.1.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium			
High		X	

6.5.1.4. Countermeasure

Test Case	SD105, SD106
Comments/Guidance	

6.6. Device Upgrade

6.6.1. Image Rollback

Threat Description	The attacker has compromised the cloud upgrade service and attempts to roll back the version of code running on the device.
Threat Agent	Firmware error or attacker inside network.
Resulting Impact	Security patches may be lost.

6.6.1.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			**X**
Moderate			
Easy			

6.6.1.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			**X**
Local Network			
Entire Fleet			

6.6.1.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium		**X**	
High			

6.6.1.4. Countermeasure

Test Case	VS2, VS3, VS4
Comments/Guidance	

6.6.2. Firmware Update Service is spoofed and invalid image sent to the device

Threat Description	Cloud service is spoofed, device receives update from that a malicious update service .
Threat Agent	Man in the middle with poisoned DNS records
Resulting Impact	Device received compromised firmware - may be used to attack other devices.

6.6.2.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			**X**
Medium			
Easy			

6.6.2.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			
Local Network			
Entire Fleet			**X**

6.6.2.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium			**X**
High			

6.6.2.4. Countermeasure

Test Case	VS2, VS3
Comments/Guidance	

6.6.3. Attacker attempts to modify the bootloader to bypass secured image

Threat Description	The attacker modifies the bootloader image on the device with the goal of loading a corrupt image.
Threat Agent	Malware with limited security privileges.
Resulting Impact	Malware has increased security privileges, completely compromising device.

6.6.3.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult	X		
Medium			
Easy			

6.6.3.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			X
Local Network			
Entire Fleet			

6.6.3.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low		X	
Medium			
High			

6.6.3.4. Countermeasure

Test Case	VS2, VS3, VS6
Comments/Guidance	

6.6.4. Update Blocked

Threat Description	Denial of service attack prevents upgrade of target device.
Threat Agent	Attacker inside network or attacker outside network but within RF transmitter range.
Resulting Impact	Security patches could be blocked.

6.6.4.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Medium		X	
Easy			

6.6.4.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			
Local Network	X		
Entire Fleet			

6.6.4.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium	X		
High			

6.6.4.4. Countermeasure

Test Case	Low severity, thus no mitigation required per process.
Comments/Guidance	

6.6.5. Open API Ports

Threat Description	Devices that expose API / JSON ports without authentication or authorization.
Threat Agent	Unauthorized users interacting with the lighting infrastructure.
Resulting Impact	

6.6.5.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Medium			
Easy		X	

6.6.5.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			
Local Network		X	
Entire Fleet			

6.6.5.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium			
High		X	

6.6.5.4. Countermeasure

Test Case	SI1.2, SI1.3, SI1.4, SI2.1, SI2.2, SI2.3, SD118, SI121
Comments/Guidance	

6.6.6. Management Protocols

Threat Description	Device management protocols such as SNMP or SYSLOG are not securely configured. Ex. SNMPv2 or Clear channel syslog.
Threat Agent	Unauthorized user gains access through PUBLIC or shared PRIVATE SNMP channels Gaining complete access of the device.
Resulting Impact	

6.6.6.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Medium		X	
Easy			

6.6.6.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device		X	
Local Network			
Entire Fleet			

6.6.6.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium		X	
High			

6.6.7. Countermeasure

Test Case	SI1.3, SI1.4, SI2.2, SI2.3, SI121
Comments/Guidance	Ensure that SNMPv3 is in use or Syslog over TLS.

6.6.8. PAN/Low-Power Networks

Threat Description	malformed traffic from downstream PAN network
Threat Agent	Attacker introduces malformed traffic via RF on downstream PAN network
Resulting Impact	Device becomes unstable / DoS condition

6.6.8.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Medium		X	
Easy			

6.6.8.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device		X	
Local Network			
Entire Fleet			

6.6.8.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium		X	
High			

6.6.8.4. Countermeasure

Test Case	SD117
Comments/Guidance	

6.6.9. Downstream Network - Physical

Threat Description	Attacker introduces a deliberate fault on the downstream physical network
Threat Agent	Local attacker with physical access to the downstream network introduces a physical fault to disrupt network
Resulting Impact	Device becomes unstable / DoS condition

6.6.9.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Medium	**X**		
Easy			

6.6.9.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device		**X**	
Local Network			
Entire Fleet			

6.6.9.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low		**X**	
Medium			
High			

6.6.9.4. Countermeasure

Test Case	SI120
Comments/Guidance	A fault on one network should not impact the other network. This threat was focused on recovery of the impacted network, thus the impact was a single device. However, it is critical that faults on a network do not propagate beyond the faulted network. Thus, this countermeasure shall be mandatory.

6.6.10. Common Web Vulnerability Attack

Threat Description	Attacker exploits a common web vulnerability such as OWASP top ten vulnerability against the embedded web server of the NLC
Threat Agent	An attacker who has access to the US network interface of the NLC.
Resulting Impact	The attacker may raise access rights, perform denial of service, or other data manipulations through the web interface.

6.6.10.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Medium			
Easy		X	

6.6.10.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device		X	
Local Network			
Entire Fleet			

6.6.10.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium			
High		X	

6.6.10.4. Countermeasure

Test Case	SD123
Comments/Guidance	

6.6.11. Downstream network - Replay attacks

Threat Description	Spoofed or replayed packets on the downstream network influence configuration of NLC
Threat Agent	Attacker introduces spoofed or replayed traffic on downstream network
Resulting Impact	Downstream network influences configuration of NLC

6.6.11.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Medium	**X**		
Easy			

6.6.11.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device		**X**	
Local Network			
Entire Fleet			

6.6.11.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low		**X**	
Medium			
High			

6.6.11.4. Countermeasure

Test Case	SD122
Comments/Guidance	

6.6.12. Default Protocols

Threat Description	Attacker is able to leverage unused default protocols to influence the configuration or operation of the NLC
Threat Agent	Attacker introduces unexpected traffic onto downstream network via unused but available default protocols
Resulting Impact	Device becomes unstable / DoS condition

6.6.12.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Medium	X		
Easy			

6.6.12.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device		X	
Local Network			
Entire Fleet			

6.6.12.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low		X	
Medium			
High			

6.6.12.4. Countermeasure

Test Case	SI121
Comments/Guidance	

6.6.13. Unrestricted Relay of Messages between interfaces

Threat Description	Unintended Relay of Messages between interfaces
Threat Agent	Attacker sends Message to unprovisioned interface that is relayed to provisioned interfaces
Resulting Impact	Three interface devices performing Bacnet/IP routing across two interfaces. Attacker submits Backnet/IP Message to upstream interface which should not ever receive such traffic. Traffic is relayed to interfaces provisioned with Backnet/IP.

6.6.13.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Medium			
Easy		X	

6.6.13.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			
Local Network		X	
Entire Fleet			

6.6.13.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium			
High		X	

6.6.13.4. Countermeasure

Test Case	SD120
Comments/Guidance	

6.6.14. Lack of Multi-User Role Based privilege assignment

Threat Description	Lack of Multi-User Role Based privilege assignment
Threat Agent	Any authenticated user can make changes to the configuration and operation of the device.

Resulting Impact	Only a single privilege level for the device in question, Admin/root.

6.6.14.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Medium			
Easy			**X**

6.6.14.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			**X**
Local Network			
Entire Fleet			

6.6.14.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium			
High		**X**	

6.6.14.4. Countermeasure

Test Case	SD119
Comments/Guidance	

6.6.15. Lack of Centralized AAA Source

Threat Description	Device does not utilize a centrally managed authentication source, resulting in outdated or forgotten users.
Threat Agent	Terminated employee leverages known credentials to access NLC and make unauthorized changes
Resulting Impact	Unauthorized changes made to device pool by malicious actor

6.6.15.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Medium			**X**
Easy			

6.6.15.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			**X**
Local Network			
Entire Fleet			

6.6.15.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium			
High		**X**	

6.6.15.4. Countermeasure

Test Case	SD121
Comments/Guidance	