


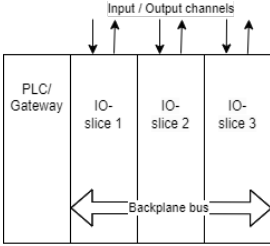

## XN-322... I/O Series

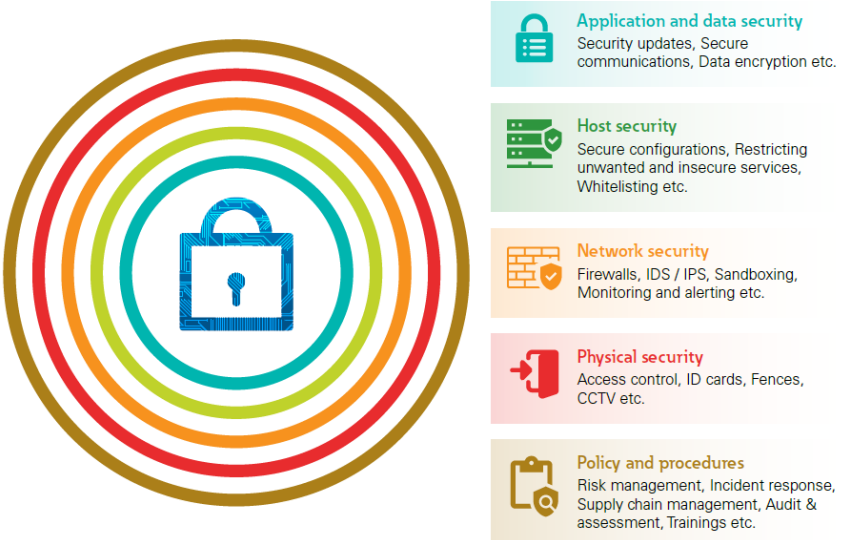
# EATON PRODUCT SECURE CONFIGURATION GUIDELINES

## Documentation to securely deploy and configure Eaton products

**XN-322-IO-Series** have been designed with cybersecurity as an important consideration. A number of features are offered in the product to address cybersecurity risks. These Cybersecurity Recommendations provide information to help users to deploy and maintain the product in a manner that minimizes the cybersecurity risks. These Cybersecurity Recommendations are not intended to provide a comprehensive guide to cybersecurity, but rather to complement customers' existing cybersecurity programs.

Eaton is committed to minimizing the cybersecurity risk in its products and deploying cybersecurity best practices in its products and solutions, making them more secure, reliable, competitive for customers.

Category	Description
<p><b>[1] Intended Use &amp; Deployment Context</b></p>	<p>Our ultra-compact, slice-based XN300 I/O system with push-in connectors and high connection density can be used as a local I/O level for the Eaton XC300 PLC or, via gateways, as a remote I/O level in CAN and Ether CAT networks. In combination with our HMI/PLC products, it enables modern automation solutions for the production of standard machines. Various models and the application-oriented functions of the I/O modules increase flexibility, reduce equipment costs and enable customized system solutions while keeping the footprint to a minimum. The user-friendly installation of the cutting-edge I/O slices simplifies handling and enables the I/O block and the sensors and actuators to be pre-assembled. The plug-in connections and the clear signal assignment simplify commissioning and extend the functionality of the system, enabling it to meet the specific requirements of the machine-building sector.</p> <div style="display: flex; justify-content: space-around; align-items: center;">   </div>
<p><b>[2] Asset Management</b></p>	<p>Keeping track of software and hardware assets in your environment is a prerequisite for effectively managing cybersecurity. Eaton recommends that you maintain an asset inventory that uniquely identifies each important component. To facilitate this, <b>XN-322-IO-Series</b> supports the following identifying information:</p> <p>Hardware:</p> <p>The following information can be found <i>printed on the right side of the housing</i>.</p> <div style="display: flex;"> <div style="flex: 1;"> <p>Vendor →</p> <p>Type name →</p> <p>Part-No →</p> <p>Version →</p> <p>Serial-No →</p> <p>Production Date →</p> </div> <div style="flex: 2; border: 1px solid gray; padding: 5px;">  </div> </div>
<p><b>[3] Defense in Depth</b></p>	<p>Defense in Depth basically means applying multiple counter-measures for mitigating risks, in a layered or step wise manner. A layered approach to security as shown in the below diagram is what is recommended. Defense in Depth is the responsibility of both the manufacturer and the customer.</p>

Category	Description
	
<p><b>[4] Physical Security</b></p>	<p>An attacker with unauthorized physical access can cause serious disruption to system/device functionality. Additionally, Industrial Control Protocols don't offer cryptographic protections, making ICS and SCADA communications especially vulnerable to threats to their confidentiality. Physical security is an important layer of defense in such cases. <b>XN-322-IO-Series</b> are designed to be deployed and operated in a physically secure location. Followings are some best practices that Eaton recommends to physically secure your system/device:</p> <ul style="list-style-type: none"> <li>• Secure the facility and equipment rooms or closets with access control mechanisms such as locks, entry card readers, guards, man traps, CCTV, etc. as appropriate.</li> <li>• Restrict physical access to cabinets and/or enclosures containing <b>XN-322-IO-Series</b> and the associated system. Monitor and log the access at all times.</li> </ul>
<p><b>[5] Malware Defenses</b></p>	<p>Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.</p>
<p><b>[6] Business Continuity / Cybersecurity Disaster Recovery</b></p>	<p><b>Plan for Business Continuity / Cybersecurity Disaster Recovery</b></p> <p>Eaton recommends incorporating <b>XN-322-IO-Series</b> into the organization's business continuity and disaster recovery plans. Organizations should establish a Business Continuity Plan and a Disaster Recovery Plan and should periodically review and, where possible, exercise these plans. As part of the plan, important system   device data should be backed up and securely stored, including:</p> <ul style="list-style-type: none"> <li>• The current configuration.</li> <li>• Documentation of the current permissions / access controls, if not backed up as part of the configuration.</li> </ul>

## References

[R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):

[http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct\\_1603172.pdf](http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf)

[R2] Cybersecurity Best Practices Checklist Reminder (WP910003EN):

<https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf>

[R3] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>

[R4] National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41", October 2009: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf>

[R5] NIST SP 800-88, Guidelines for Media Sanitization, September 2006:

[http://ws680.nist.gov/publication/get\\_pdf.cfm?pub\\_id=50819](http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819)

[R6] A Summary of Cybersecurity Best Practices - Homeland Security

<https://www.hsdl.org/?view&did=806518>

[R7] Cybersecurity Best Practices for Modern Vehicles - NHTSA

[https://www.nhtsa.gov/staticfiles/nvs/pdf/812333\\_CybersecurityForModernVehicles.pdf](https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf)

[R8] Characterization of Potential Security Threats in Modern Automobiles - NHTSA

[https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074\\_Characterization\\_PotentialThreatsAutos\(1\).pdf](https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074_Characterization_PotentialThreatsAutos(1).pdf)

[R9] Threat Modeling for Automotive Security Analysis

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf>