hydrovar X Series
Cybersecurity Reference Guide

Xylem values system security and resilience. Defending against cybersecurity threats is a shared responsibility. Xylem builds products that are secure by design. Our customers have a responsibility to understand the risks inherent in their processes and take steps to operate and maintain their solutions securely. This section reviews security features and provides guidance to help securely operate this product. For details and updates on Xylem product cybersecurity visit https://www.xylem.com/en-us/about-xylem/cybersecurity/.

Xylem Product Cybersecurity

Xylem performs appropriate due care in building security and resilience into products. Xylem performs the following security activities for defense-in-depth:

- Security engineers perform **threat modeling** to identify **testable controls**
- Code is scanned for flaws with **static analysis** tools and hardened
- **Product components are analyzed** and hardened
- Security controls are verified through **automated and manual tests**
- Xylem maintains relationships with customers, integrators, and the cybersecurity research community and the **Product Security Incident Response Team (PSIRT)** coordinates the collection, analysis, remediation, and responsible disclosure of vulnerability and remediation information to keep products secure
- Cloud connections, data flows, and cloud infrastructure are continuously monitored by the **Product Security Operations Center (PSOC)**
- Product security is **governed through a three lines of defense** model that includes: product developers, product security engineers, and audit staff.

Security Recommendations for End-User

Hydrovar X is developed considering security best practices. The following guidance provides recommendation for secure operations, hardening and account management. In the table below: *Safeguard* describes the security guidance, *Security Context & Rationale* provides overview of security features and value of the security safeguard, and *References* provide additional resources for further investigation for implementing the recommended safeguards.

Safeguard	Security Context & Rationale	References
Ensure that the device is not exposed to internet, using below recommendations: • Implement firewall & define rules to protect device from Denial-of-service attempts. • Protect the network address information of device using Network Address Translation (NAT) technique.	This safeguard ensures that data and SCADA controls are not exposed to internet. This also helps in preventing Man-in-the-middle attacks when the device is accessed connecting the RS485 port to a device routing the intranet. We recommend using network segmentation and segregation which minimizes access to sensitive information for those systems and people who do not need it, while ensuring that the organization can continue to operate effectively.	ATT&CK for ICS: M0930 NIST SP 800-95 NIST SP 800-44 v2 ISA/IEC 62443-3-3: SR 5.1, SR 7.1

Safeguard	Security Context & Rationale	References
Restrict physical access. • Ensure physical access to assets is limited. Include physical isolation to protect the environment and equipment therein. • Ensure strict control over physical access in and out of the facility.	The communication ports have been hardened to restrict access and ensure integrity of device operations. This safeguard supports the ability to further limit exposure associated with physical threats to the device such as rogue/malicious device joining the Modbus RTU network or the BACNet BMS network over RS485 interface.	ATT&CK for ICS: M0801 NIST SP 800-53 Rev5: AC-3, PE-3 ISA/IEC 62443-3-3: SR 2.1
Ensure cybersecurity policies, awareness, and training to the operators, administra- tors and other personnel.	This safeguard prevents Social Engineering attacks and promotes awareness related to cybersecurity.	ATT&CK for ICS: M0917 NIST SP 800-53 Rev5: AT-2 ISA/IEC 62443-2-4: SP.01
Ensure patch management is done regularly and updated appropriately.	This safeguard prevents attacks related using components with known vulnerabilities. Sometimes vulnerabilities are discovered, and we work with our partners to deploy updates to security and resilience. This safeguard mitigates exploitation risks and ensures security patching.	ATT&CK for ICS: M0951 NIST SP 800-53 Rev5: MA-2 ISA/IEC 62443-2-3
Create and exercise disaster recovery plans.	Hydrovar X has no way to perform a back-up of the current system configuration but can revert to factory settings via Display or via Modbus. Moreover, a copy of the current configuration can be downloaded using the app. The configuration can be restored manually from this copy. Defining this process provides systems resilience, including against ransomware.	ATT&CK for ICS: M0953 NIST SP 800-53 Rev5: CP-10 ISA/IEC 62443-3-3: SR 7.4
Implement specific inventory, logging and monitoring of hardware and report security-related incidents to Xylem at product.security@xylem.com. These might include unexpected operations, confirmed tampering, or theft of the device.	Devices are hardened and Xylem provides PSIRT to help customers investigate potential security incidents. This safeguard supports the ability to track assets and recognize potential security events.	ATT&CK for ICS: M0947 NIST SP 800-53 Rev5: SM-8 ISA/IEC 62443-3-3: SR 1.11, SR 2.8, SR 3.4

For additional information see references:

- ATT&CK for ICS available online: https://attack.mitre.org/mitigations/ics/
- NIST SP 800-53 Rev 5 available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- ISA/IEC 62443 standards available for purchase from ISA, IEC, or ANSI.

xylem
Let's Solve Water

Xylem Service Italia S.r.l.
Via Vittorio Lombardi 14
36075 – Montecchio Maggiore (VI) - Italy
www.xylem.com