FFP Series Fire Panel 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.

Notice – inclusion of third-party PLCs and associated software

This product includes Programmable Logic Controllers (PLCs) manufactured by Schneider Electric to enable feedback control of the system. As with all software periodically vulnerabilities might be discovered, and the vendor will release patches or updates. Please contact your Xylem sales representative or contact product.security@xylem.com regarding security questions.

Certain industrial protocols (such as Modbus and BACnet) do not offer security protections at protocol-level and may be exposed to additional cybersecurity risks. Customers using such protocols should implement necessary security when using Modbus, including all security recommendations included below.

Security Recommendations for End-User

Xylem-labeled FFP-series fire panel 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
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.	This safeguard supports the ability to limit exposure associated with physical threats to the device such as rogue/malicious device joining the Modbus RTU network over RS485 interface, and limits access to the devices for change passcodes, erasing logs, or changing configurations.	ATT&CK for ICS: M0801 NIST SP 800-53 Rev5: AC-3, PE-3 ISA/IEC 62443-3-3: SR 2.1
Ensure that the device is not exposed to internet at all. For example: https://www.cisa.gov/sites/default/files/publications/Shodan_Technical_508c.pdf) If there is any requirement to expose the device to internet, follow 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. (e.g., set up a demilitarized zone [DMZ] to segment fire system from rest of network.	This safeguard ensures that data and SCADA controls are not exposed to the internet. This also helps in preventing Man-in-the-middle attacks when the device is accessed via internet. We recommend using network segmentation and segregation so that we can minimize 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
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. Ensure engineering change control process at the facility.	This safeguard prevents attacks related to the components with known vulnerabilities. Sometimes vulnerabilities are discovered, and we work with our partners to provide updates. 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
Ensure RBAC should be followed. Ensure that installer and operator roles use different passcodes.	Basic role based access control (RBAC) is set up on this device to separate installer privileges from operator privilege. This safeguard helps in prevention of attacks due to misconfigurations or default configurations.	ATT&CK for ICS: M0937, M0918, M0801 NIST SP 800-53 Rev5: AC-3(7), SC-7(5) ISA/IEC 62443-3-3: SR 2.1, SR 5.1
Ensure default credentials are not used, passwords must be changed periodically. Ensure password change control process at the facility.	This safeguard will help in prevention of passwords and account takeover attacks.	ATT&CK for ICS: M0927 NIST SP 800-53 Rev5: IA-5 ISA/IEC 62443-3-3: SR 1.7

Safeguard	Security Context & Rationale	References
Ensure data backup and restore process is implemented.	This safeguard provides capability to participate in system level backup operations to safeguard the component state.	ATT&CK for ICS: M0953 NIST SP 800-53 Rev5: CP-10 ISA/IEC 62443-3-3: SR 7.4
Ensure periodic log monitoring capability at the facility. 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 Service Italia S.r.l.
Via Vittorio Lombardi 14
36075 – Montecchio Maggiore (VI) - Italy
www.xylem.com

Xylem is a registered trademark of Xylem Inc. or one of its subsidiaries. All other trademarks or registered trademarks are property of their respective owners.
© 2024 Xylem Inc. Cod.001088120EN rev.A 08/2024