

Cybersecurity information

Intended environment

This product is intended for use in industrial / OT environments. Where applicable, for products with communication, configuration, or diagnostic interfaces, deploy the product in a segmented OT network and do not expose it directly to the Internet or to uncontrolled IT networks. A common architecture is to place the product behind a PLC or industrial gateway and allow communication only with approved devices and required functions.

Defense-in-depth recommendations

No single control is sufficient. Depending on the installation, apply the following measures as appropriate:

- **Network partitioning / filtering:** Use firewalls or ACLs to restrict traffic to required protocols, ports, and endpoints. Where feasible, use industrial firewalls with OT-aware inspection.
- **Traffic monitoring:** Monitor for anomalous or unexpected traffic where feasible.
- **IP addressing / reachability:** Use private IP address ranges and limit communications to the minimum necessary devices and services.
- **Access controls:** Restrict physical and logical access so that only authorized personnel can access the product and the OT network. Protect commissioning and configuration means, such as tags, configuration cards, and keys, with controlled access.
- **Credentials and services, where applicable:** Change default credentials on password-protected interfaces and disable or restrict unused services.

Failure to apply the above measures may increase cybersecurity risk and reduce the overall security of the installation. The integrator and operator remain responsible for securing the installation environment, including network architecture, access control, monitoring, and physical protection

Security lifecycle, updates, and reporting

- Product cybersecurity information, including the single point of contact for reporting vulnerabilities and the Company's coordinated vulnerability disclosure policy, is available at: <https://www.telemecaniquesensors.com/global/en/support/product-cybersecurity>
- Cybersecurity point of contact: cybersecurity@tesensors.com
- Product-specific cybersecurity support information, including the support end date (**MM/YYYY**), is available on the relevant **product page** or other company-provided purchase information.

Cybersecurity support and vulnerability handling

We provide cybersecurity support for this product until the published support end date shown for the product. During that support period, we assess reported vulnerabilities affecting the product and, as appropriate to the risk and technical feasibility of the product, provide mitigation information and/or security updates. Security updates, where made available, are distributed through appropriate controlled channels. Relevant security information may be communicated through product pages, website notices, advisories, direct email, or other appropriate customer communication channels.