

Manufacturer's Statement on Cybersecurity PLC Tecomat

Manufacturer: **Teco a.s.**

Registered office: Průmyslová zóna Štáralka 984, 280 02 Kolín, Czech Republic

Document: Manufacturer's Statement on Cybersecurity

Version: 1.0

Date: 20 January 2026

1. Purpose of the Document

This document represents the official statement of the manufacturer Teco a.s. regarding the cybersecurity of programmable logic controllers (PLCs) used in industrial and infrastructure applications. It is intended primarily for:

- system integrators
- operators of technological units and infrastructure
- security, IT, and technical departments of customers
- supplier documentation, internal audits, and security assessments

The purpose of this document is to:

- describe the security characteristics of the products,
- define the assumptions for their secure use,
- clearly distinguish the responsibilities of the manufacturer, integrator, and operator.

This document does not replace project documentation, the operator's security policy, or a system risk analysis.

2. Scope of Validity

This statement applies to programmable logic controllers manufactured by Teco a.s., in particular the Tecomat TC800 / Foxtrot 2 product line, including their standard firmware and built-in communication functions.

3. PLC Characteristics from a Cybersecurity Perspective

- Tecomat PLCs are embedded industrial control devices intended for controlling technological processes.
- PLCs are not general-purpose computing systems (such as personal computers or servers).
- PLCs are designed to operate in a separated technological network and are not intended for direct connection to the public internet.
- The PLC architecture limits communication interfaces and services to the necessary minimum.
- Firmware is managed by the manufacturer and is not intended to be modified by third parties.
- The device does not allow general remote administration of the operating system. Any configuration is performed via a secured service interface available exclusively to the manufacturer.

- This approach corresponds to common practice in industrial automation and the principle of defense in depth, where system security is not based on a single measure but on a combination of technical and organizational elements.

4. Security Features Relevant for Operation in IP Networks

Depending on the specific configuration and usage, Tecomat PLCs provide in particular the following security features:

- Authentication of access to configuration and service interfaces using a username and password.
- Possibility of using encrypted communication for selected functions (e.g., secure access to the device's web interface), if enabled by configuration.
- Separation of communication interfaces and support for designing separated network segments (e.g., technological part and service access).
- Controlled firmware updates performed by authorized personnel in accordance with manufacturer and operator procedures.
- Support for operation in non-public communication modes (e.g., via private mobile connectivity or secured access channels), so that the device is not directly accessible from the public internet.

This document intentionally does not contain technical details of the internal architecture, operating system description, or detailed security mechanisms, which are not commonly disclosed even by other PLC manufacturers.

5. Assumptions for Secure Use

The declared security features of Tecomat PLCs assume that the integrator and operator ensure in particular:

- Operation of the PLC in a separated technological network or in a network segment with controlled access.
- Indirect connection to external networks exclusively through appropriate protective elements (e.g., firewall, VPN, controlled access).
- Secure management of access credentials and user authorizations.
- Limitation or disabling of unused communication services.
- Controlled firmware update and service intervention processes.
- Ensuring monitoring, event logging, and incident response within the operator's security management system.

6. Relationship to Standards and Regulation

IEC 62443

Tecomat PLCs can be integrated into a system designed according to IEC 62443, particularly within the concept of separating technological parts of the system and controlled communication between

them.

This document does not represent product certification according to IEC 62443.

ISO/IEC 27001

ISO/IEC 27001 applies to organizations and their processes. This statement serves as input for evaluating the PLC as a technical component within asset and supplier management.

NIS2 / Cybersecurity Act

Obligations arising from regulation typically apply to operators of regulated services. Teco a.s. acts as a component manufacturer and provides information about product characteristics and its secure use.

7. Sanctions and Export Restrictions

Teco a.s. complies with applicable European Union sanctions regimes.

Deliveries, re-export, provision of technical support, or access to products may be restricted or prohibited especially in relation to:

- - Russian Federation
- - Belarus

The integrator and end user are obliged to ensure that the intended use of the products complies with applicable sanctions and export legislation.

8. Definition of Responsibilities

- Teco a.s. is responsible for the design and manufacture of PLCs, controlled firmware releases, and providing information for secure product use.
- The integrator is responsible for the secure design of the entire system architecture in which any configuration of Tecomat PLCs is used, including network structure, connection methods, and access control.
- The operator is responsible for secure system operation, access management, network protection, monitoring, and compliance with regulatory obligations.

9. Conclusion

PLCs manufactured by Teco a.s. are designed for secure operation in technological applications when the stated assumptions are met. This document serves as a concise and official security statement of the manufacturer for the purposes of integrators and operators.

On behalf of Teco a.s.
Ing. Jaromír Klaban
Managing Director