Communication Interface Exposure & Cybersecurity Controls

Product Name: Enforcer V11

Part code(s): ENF32GB-WE and all relevant kits and assemblies that include this product.

Manufacturer: Pyronix Ltd. Secure House, Braithwell Way, Hellaby, Rotherham, S66 8QY

1. Purpose of This Section

This section outlines the physical and logical communication interfaces of the Enforcer V11 in accordance with the requirements of:

Directive 2014/53/EU (RED) Articles 3(3)(d), (e), and (f)

Delegated Regulation (EU) 2022/30

Standard EN 18031, including exposure risk classification under GEC-4 and compliance decision node DT.GEC-4.DN-2.

The information supports the risk assessment and demonstrates that no interfaces are unintentionally exposed in a way that would compromise network performance, personal data, or privacy.

2. Interface Capability Summary

The Enforcer V11 contains or supports the following communication interfaces:

Interface	Present by Default	Enabled by Default	Requires Auth to Enable	User Removable Hardware	Use Case
Wi-Fi	Yes	No	Yes	No	App comms via cloud/ARC comms
Cellular	No	No	Yes	Yes	App comms via cloud/ARC comms
Ethernet	No	No	Yes	Yes	App comms via cloud/ARC comms

3. Wi-Fi Interface (Integrated)

- **Interface Type:** IEEE 802.11 b/g/n 2.4GHz
- **Hardware Capability:** Integrated on all Enforcer V11 units
- **Enabled by Default:** No
- **Enablement Method:** Installer menu; authentication required
- **Security Measures:** WPA2 encryption, PyronixCloud pairing authentication, no broadcast without configuration
- **Purpose:** Remote communication with PyronixCloud platform and mobile app; and/or signalling to an ARC
- **Exposure Risk:** Controlled - not exposed until activated by authenticated installer
- **Standard Relevance:** EN 18031 GEC-4 compliant

4 Optional Interfaces (User-Installed Modules)

4.1 Cellular

- **Interface Type:** 4G/GPRS via expansion module
- **Hardware Capability:** Requires DIGI-4G or DIGI-GPRS module (not present by default)
- **Enabled by Default:** No
- **Enablement Method:** Requires physical installation and configuration
- **Security Measures:** VPN/APN segregation; authenticated access; encrypted signalling
- **Purpose:** Remote communication with PyronixCloud platform and mobile app; and/or signalling to an ARC
- **Exposure Risk:** Moderate - mitigated by hardware separation and encryption
- **Standard Relevance:** EN 18031 GEC-4 compliant

4.2 Ethernet

- **Interface Type:** RJ45 Ethernet (10/100 Mbps)
- **Hardware Capability:** Requires optional DIGI-LAN module
- **Enabled by Default:** No
- **Enablement Method:** Engineer menu configuration
- **Security Measures:** Outbound-only communication to PyronixCloud; no open ports; encrypted signalling; engineer-level authentication required for enablement.
- **Purpose:** Remote communication with PyronixCloud platform and mobile app; and/or signalling to an ARC
- **Exposure Risk:** Moderate – mitigated via access control and outbound-only configuration
- **Standard Relevance:** EN 18031 GEC-4 compliant

5. Disabled or Inactive Interfaces

- No interfaces are enabled unless explicitly activated by an authenticated user.
- Hardware interfaces (Cellular, Ethernet) are not active unless installed.
- No undocumented or hidden interfaces are present.

6. Risk Mitigation Summary (EN 18031 Decision Compliance)

The table summarises the compliance status of the Enforcer V11 against each section of the EN 18031 standard with a Pass or Fail designation. This overview highlights the key evaluation criteria met by the product. Detailed decision trees and full compliance documentation can be provided upon request for comprehensive technical review.

EN 18031 Section	Pass/Fail	Description
ACM Access Control Mechanism	✓	Governs the policies and mechanisms controlling user and system access rights to protect against unauthorised access.
AUM Authentication Mechanism	✓	Specifies authentication requirements for network and user interfaces, including password policies, authenticator validation, change management, and brute force protection.
SUM Security Update Mechanism	✓	Ensures the device supports secure software updates with integrity and authenticity verification, including options for automated or user-approved installations.
SSM Secure Software Mechanism	N/A	Requires secure storage of sensitive and network-related data persistently stored on the device to protect against unauthorised access or tampering.
SCM Secure Communication Mechanism	✓	Requires secure communication protocols with integrity, authenticity, confidentiality, and replay protection to safeguard data transmission.
RLM Resilience Mechanism	✓	Ensures devices can mitigate and recover from Denial of Service (DoS) attacks and other failures affecting network interfaces.
NMM Network Monitoring Mechanism	✓	For network devices, mandates monitoring of network traffic to detect anomalies such as DoS attacks.
TCM Traffic Control Management	✓	For network devices, requires mechanisms to control and prioritise network traffic to prevent overload or delays.
CCK Confidential Cryptographic Keys	✓	Specifies secure generation, storage, and uniqueness of cryptographic keys with minimum security strength standards.
GEC General Engineering Controls 1	✓	Tracks hardware/software components and known vulnerabilities; ensures re-mediation or acceptance.
CRY Cryptography	✓	Requires the use of recommended, secure cryptographic algorithms and practices to protect secure and network assets.

7. Supporting Documents & References

- Enforcer V11 Declaration of Conformity - *view here*
- Enforcer V11 EN 18031-1 Decision Tree Reference Guide - *view here*

Author	Daniel Mills
Position	Technical Product Marketer
Date	31/07/25
Document reference	RED-001
Revision	01
Approved by	John Walker
Position	Compliance Engineer
Signature