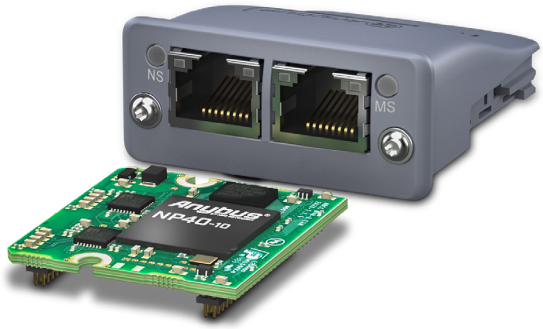
Anybus CompactCom 40 IIoT Secure Security Data Sheet



Document owner: HMS Product Security (PSIRT)
Applies to: Anybus CompactCom 40 IIoT Secure
Version: 1.0
Date: 2025-11-26

This Security Data Sheet provides a condensed overview of the security functions of the Anybus CompactCom 40 IIoT Secure variants. Additional security guidance is also available in the Anybus Embedded Security Guide.
It supplements the product information and user manuals available on the product pages at hms-networks.com.

Application scope

Applies to Anybus CompactCom 40 IIoT Secure variants
Protocols supported: PROFINET (PIR) and EtherNet/IP (EIP)
Formats: Module (M40) and Brick (B40)

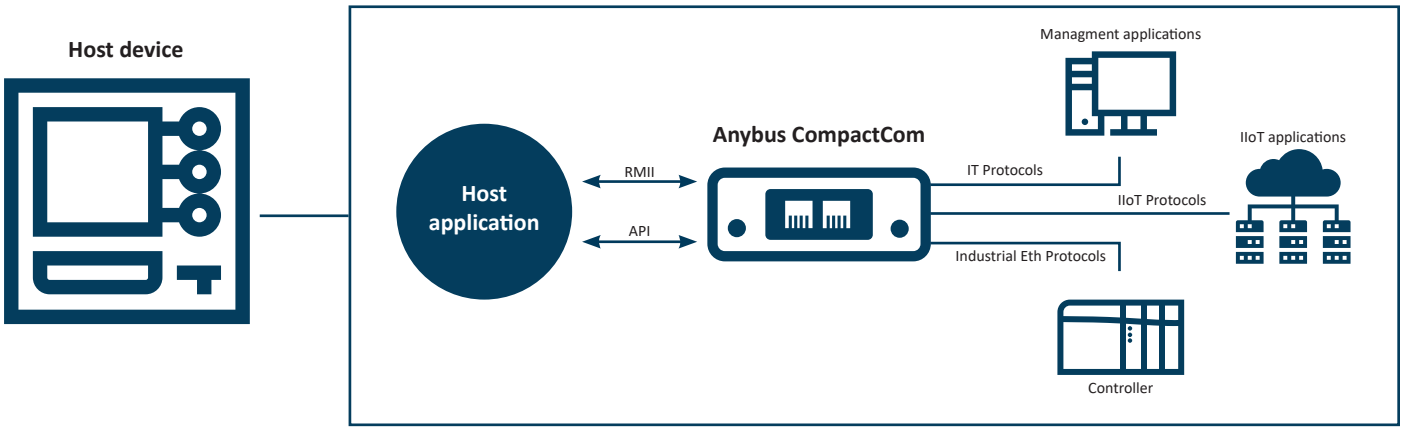
Product Identification

Attribute	Internal
Device type	- Physical label on the device - via Anybus API - via the integrated webserver - through specific protocol object
Product code/network	- Physical label on the device - via Anybus API - via the integrated webserver - through specific protocol object
Software version	- Physical label on the device - via Anybus API - via the integrated webserver - through specific protocol object
Hardware version	- Printed on PCB
MAC address	- Physical label on the device - via Anybus API - via the integrated webserver - through specific protocol object
Serial number	- Physical label on the device - via Anybus API - via the integrated webserver - through specific protocol object

HMS Industrial Networks AB, Box 4126, 300 04 Halmstad, Sweden
Phone: +46 (0) 35 17 29 00
E-mail: info@hms-networks.com

Product Intended Use

Anybus CompactCom 40 IIoT Secure products are components that, once integrated into industrial devices, enable these devices to communicate on an industrial network. Device manufacturers integrating the Anybus CompactCom component are responsible for implementing and maintaining the overall device security strategy and compliance to regulations.



Unless specified by manufacturer integration, Anybus CompactCom 40 IIoT Secure products are intended to be used for communication, in restricted access locations (physical access), and in trusted networks as defined below.

Trusted network: Dedicated and segmented network zones, isolated from untrusted or general purpose networks.

Access limited to authorized personnel: Only personnel with valid security clearance and appropriate access levels are permitted to access or modify the network and its interfaces.

The Anybus CompactCom 40 IIoT Secure includes security features for IT and IoT communications beyond automation networks. In a fully secured installation, the network may be connected to the IT level to access IIoT data, but this connection must be protected—typically via a Firewall. Since the IT protocols are secure there are no requirement to have a physically secure IT network. Individual servers on the IT network, however, need to be secure.

Product Interfaces

Type	No. of ports	Default mode	Can be changed	Comment
Network interfaces				
Ethernet Ports	2	Active	Yes	Disable unused Ethernet port
Host interfaces				
Anybus Host API	1	Active	Yes	Anybus Host API is an internal device interface and is either on SPI, Serial or Parallel interfaces
Other interfaces				
JTAG	1	Inactive	No	

HMS Industrial Networks AB, Box 4126, 300 04 Halmstad, Sweden
Phone: +46 (0) 35 17 29 00
E-mail: info@hms-networks.com

Network services and ports

Function	Port	Protocol	Default	Secure channel	Can be changed	Comment
Industrial protocols						
PROFINET	34962 Ethertype layer2		Active	No	No	Cyclic I/O data
PROFINET	34962 34963 34964 34980 161	UDP	Active	No	No	RPC Alarm DCP LLDP SNMP Client
EtherNet/IP	2222	UDP	Active	No	No	Cyclic I/O data
EtherNet/IP	44818	TCP/UDP	Active	No	No	Common services CIP
IT protocols						
HTTPS server	443	TCP	Active	Yes	No	Webserver for device configuration, web pages and monitoring.
Web access over TLS 1.2	4443	TCP	Active	Yes, TLS	Yes	Secure file transfer
WebDAV	4443	TCP	Active	Yes	Yes	Secure Firmware upload and access to the local file system.
SHICP	3250	UDP	Active	No	Yes	Used for communication with the HMS IP Config tool.
BOOTP/DHCP	67/68	UDP	Active	No	Yes	IP address setting.
NTP Server	123	UDP	Inactive	No	Yes	Network Time Protocol
IIoT protocols						
OPC UA	4840 443	TCP	Inactive	No Yes	Yes	Secure OPC UA over HTTPS, Port 443. Authentication through name and password or CA Certificates
MQTT	1883 8883	TCP	Inactive	No Yes	Yes	Secure MQTT over TLS/SSL 1.2 on port 8883. Authentication through CA and Device Certificates

Component access functions

Type:	No. of ports	Default mode	Can be changed
Login & Password	Active	Yes	Admin account must be setup at the first access. Robust password rules, possibility to configure password requirements. Hashed password storage.
User Management	Active	Yes	Central User and Role management. 3 default roles (administrator, operator, and user) and possibility to add personalized roles. Access permissions (Webserver, WebDAV, OPC UA, firmware update, handling of certificates)

Software and data

Function	Default mode	Comment
Firmware update	By request	FW update via WebDAV is supported, or through the Firmware Manager Tool.
Syslog	Not supported	Functionality planned for future versions.

HMS Industrial Networks AB, Box 4126, 300 04 Halmstad, Sweden
Phone: +46 (0) 35 17 29 00
E-mail: info@hms-networks.com

Product Specific Security functionalities

The Anybus CompactCom 40 IIoT Secure is designed with security as its primary focus, and includes the following additional security measures:

- **Compliance with 802.1AR: Secure Device Identity**
  The Anybus CompactCom 40 IIoT Secure complies with the IEEE 802.1AR standard, which focuses on Secure Device Identity (DevID) for the purpose of enhancing device authentication and trust within network environmen

- **Security Chip**
  The Anybus CompactCom 40 IIoT Secure includes a security chip for storing certificate private keys.

- **Secure boot**
  As with all products in the Anybus CompactCom 40 series, the Anybus CompactCom IIoT Secure only accepts firmware that has been digitally signed by HMS Networks. To add another layer of security, the Anybus CompactCom IIoT Secure also verifies that the firmware hasn't changed each time it is booted. This dual approach fortifies the product's security, further safeguarding against unauthorized modifications or tampering

- **Encryption**
  The Anybus CompactCom 40 IIoT Secure uses secure protocols to encrypt data exchanges over IT and IIoT services, safeguarding against interception or tampering by third parties.

Software Update Policy

Firmware updates are available on requests from HMS Networks directly.
Firmware updates via File Transfer Protocol is supported, or through the Firmware Manager Tool. WebDAV needs to be enabled. The Anybus CompactCom 40 IIoT Secure can also be updated via the application interface from the device, or via the Anybus CompactCom 40 StarterKit.
To prevent unauthorized or malicious code from being downloaded, the Anybus CompactCom 40 IIoT Secure only accepts firmware that has been digitally signed by HMS Networks. Firmware integrity is verified at system boot.

Revision history

Version	Date	Description
1.0	2025-11-06	

HMS Industrial Networks AB, Box 4126, 300 04 Halmstad, Sweden
Phone: +46 (0) 35 17 29 00
E-mail: info@hms-networks.com