Anybus CompactCom 30 Security Data Sheet

Document owner: HMS Product Security (PSIRT)
Applies to: Anybus CompactCom 30 (Standard variants)
Version: 1.0
Date: 2025-11-06

This Security Data Sheet provides a condensed overview of the security functions of the Anybus CompactCom 30 standard 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 30 Standard variants and included protocols
Formats: Module (M30), Brick (B30)

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

Product Intended Use

Anybus CompactCom 30 standard 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 30 standard products are intended to be used for communication with OT controllers, in restricted access locations (physical access), and in secured networks.

Product Interfaces

Type	No. of ports	Default mode	Can be changed	Comment
Network interfaces				
Ethernet Ports (PRT, EIP, EIT, ECT, BIP, SRC3)	2	Active	No	
RS485 (DPV1, CCL, RTU, BMP)	1	Active	No	
CAN (DEV, COP)	1	Active	No	
Coax (CNT)	2		No	
Host interfaces				
Anybus Host API	1	Active	Yes	Anybus Host API is an internal device interface and is either on Serial or Parallel interfaces
Other interfaces				
JTAG	1	Inactive	No	Internal HMS use

Network services and ports

Function	Port	Protocol	Default	Can be changed	Comment
Industrial protocols					
PROFINET	34962	Ethertype layer2	Active	No	Cyclic I/O data
PROFINET	34962/ 34963/ 34964/ 34980	UDP	Active	No	RPC/Alarm/DCP/LLDP
EtherNet/IP	2222	UDP	Active	No	Cyclic I/O data
EtherNet/IP	44818	TCP/UDP	Active	No	Common services CIP
Modbus-TCP	502	TCP/UDP	Active	No	Cyclic I/O data
EtherCAT	34980	Ethertype layer2	Active	No	Cyclic I/O data
BACnet/IP	47808	UDP	Active	No	Cyclic I/O data
Sercos 3	35021	Ethertype	Active	No	Cyclic I/O data
HTTP server	80	TCP	Active	Yes	Unsecure web access. Disable if unused.
FTP Server	20/21	TCP	Active	Yes	Unsecure File Transfer Protocol. Disable if unused. Must be enabled for firmware update
SMTP client	25	TCP	Inactive	Yes	Unsecure Email
SNMP client	161	UDP	Active	No	Simple Network Man-agement Protocol. Only valid on PROFINET.
HICP	3250	UDP	Active	Yes	HMS IP Config tool. Create password
BOOTP/DHCP	67/68	UDP	Active	Yes	Inactive by default on PROFINET

Component access functions

Type:	No. of ports	Default mode	Can be changed
Login & Password	Inactive	Yes	Admin account should be setup at the first access. Password can be configured for different users.

Software and data

Function	Default mode	Comment
Firmware update	By request	FW update via FTP is supported, or through the Firmware Manager Tool.
Syslog	Not supported	

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. FTP needs to be enabled. The Anybus CompactCom 30 can also be updated via the application interface from the device, or via the Anybus CompactCom StarterKit.

Security Posture Summary

The Anybus CompactCom 30 is available as standard variants with the focus on OT communication. For applications with higher security requirements, the use of the Anybus CompactCom 40 IIoT Secure variant is suggested and our Anybus Common Interface makes the transition easy. For more information please refer to the security datasheet of the Anybus CompactCom IIoT Secure.

Recommended device hardening:

- Disable unused Ethernet ports on supported variants.
- Close or restrict services not used by the host application (e.g., SNMP, FTP, HTTP).
- If active, make sure the authentication (users and passwords) is defined.
- Keep firmware up to date.

For further guidance, please refer to the Anybus Embedded Security Guide.

Revision history

Version	Date	Description
1.0	2025-11-06	