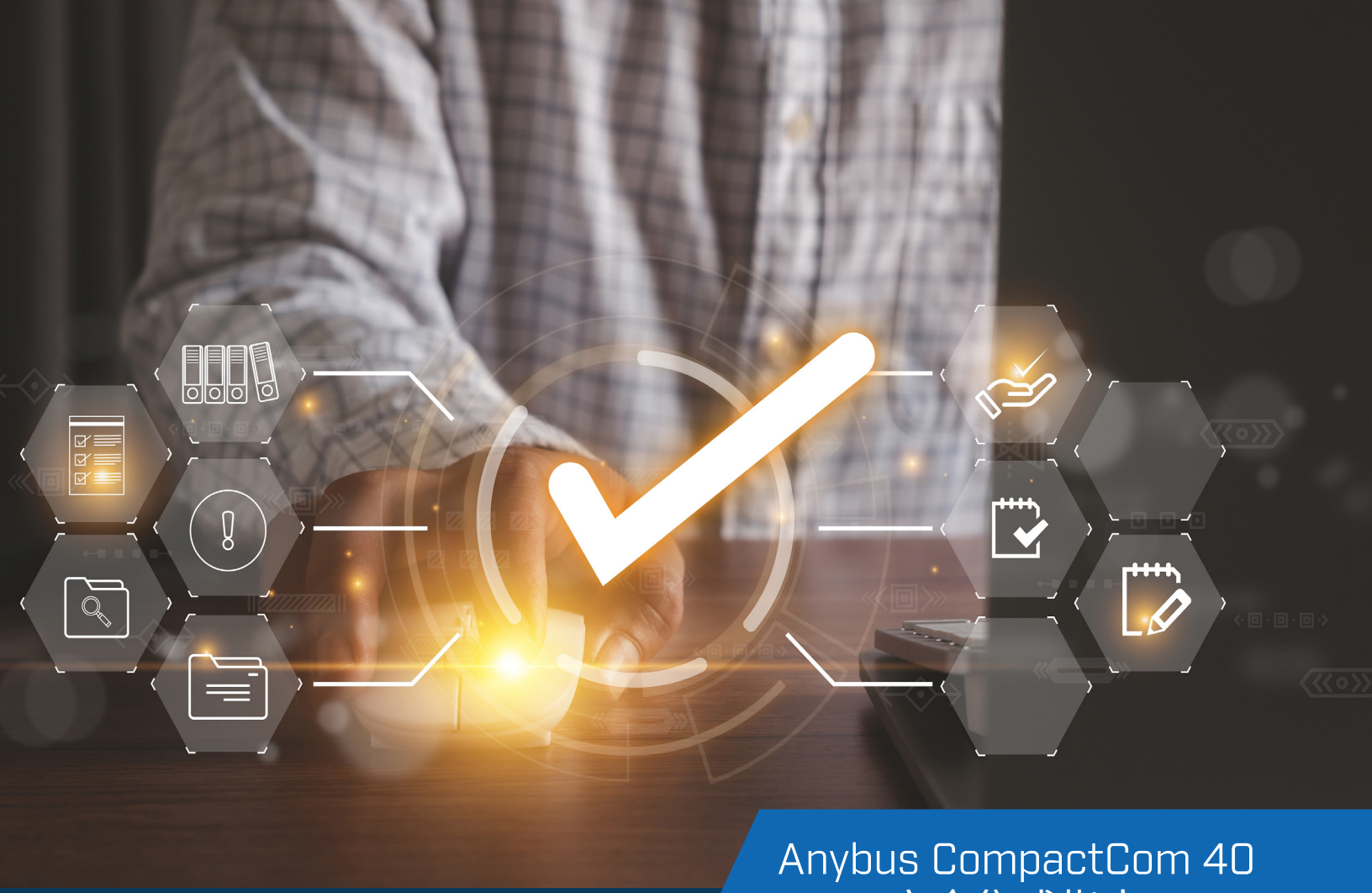


Anybus CompactCom 40
安全集成指南

Anybus CompactCom 40
安全集成指南

确保安全和合规的设备集成

目录

1. 前言

1.1 背景

在持续的工业数字化背景下，工业网络现在连接的机器远远超出了工厂的四面墙壁。因此，网络安全已成为工业通信接口开发过程中的一个关键考虑因素，确保可靠的运行以及遵守当前和未来的安全法规至关重要。

多年来，HMS 工业网络一直密切关注对增强网络安全日益增长的需求，并通过加强公司流程和提高产品稳健性来应对。这种主动的方法使客户更容易实现安全的通信接口。

1.2 文件目的

本文档可作为制造商将 Anybus CompactCom 40 集成到其产品中的指南。它解释了 HMS 工业网络如何在 Anybus CompactCom 40 系列中实施网络安全措施，并提供了解决当前安全期望的最佳方法指南。此外，本文档还帮助制造商回答生产工厂内 IT 专家的网络安全合规询问。

1.3 文件结构

本文档分为两部分：

第 1 部分概述了 HMS 工业网络如何确保将安全性内置到所有 Anybus Compact C2om 40 产品中。它包括以下部分：

- HMS 工业网络：提供安全可靠的通信解决方案
- 文档
- 过程
- 设计中的安全性

第 2 部分描述了 Anybus CompactCom 40 内通信接口的安全相关信息，并为制造商提供了最佳实践，以确保 Anybus CompactCom 在其设备或机器内的安全运行。它包括以下部分：

- 连接概述
- Anybus CompactCom 通信接口的安全相关信息说明
- 制造商安全操作的最佳实践

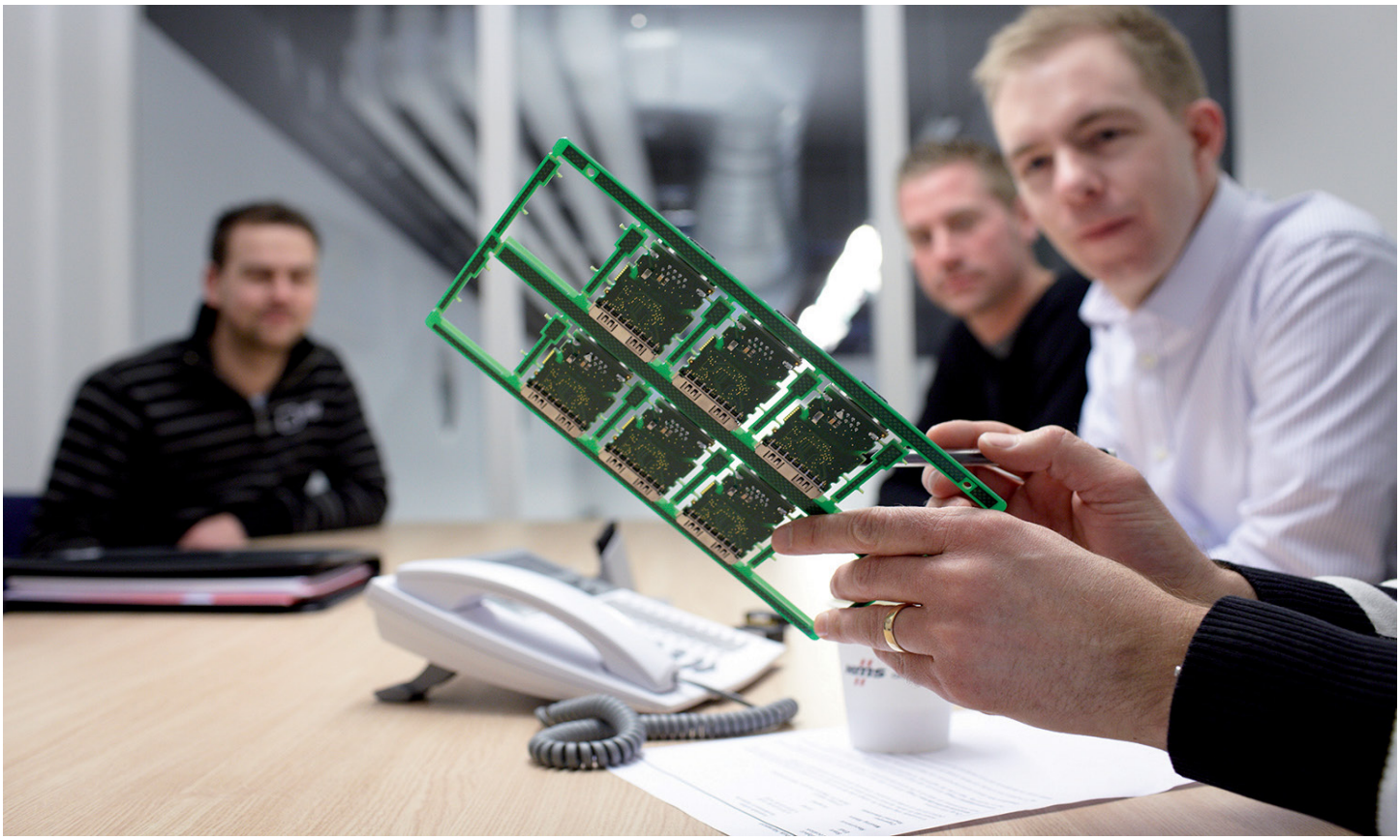
第 1 部分 : Anybus CompactCom 40 产品的安全保证

2. HMS: 提供安全可靠的通信

HMS 工业网络是工业信息和通信技术（ICT）领域的市场领导者，拥有超过 35 年的经验。在全球范围内，数千家公司已经集成了 1000 多万个 HMS 工业网络的产品，使他们的工业机器和设备能够有效地通信和共享信息。

HMS 工业网络致力于提供和维护客户可以信赖的安全通信产品。作为一家经验丰富、稳定且财务健康的公司，HMS 工业网络可以实施和管理网络安全的长期挑战。行业领先地位、丰富经验、技术专长和有保证的产品维护相结合，使 HMS 工业网络的产品成为任何希望将 HMS 的产品与自己的设备或机器集成的制造商的安全投资。

有关 HMS 工业网络的更多信息，请访问：www.hms-networks.cn



3. 安全标准和流程

3.1 信息安全管理系统和安全相关认证

HMS 工业网络实施了信息安全管理系统(ISMS),以确保最高水平的质量和安全。作为 ISMS 流程的一部分,HMS 工业网络遵循以下认证:

- ISO 9001: 开发流程符合 ISO 9001 标准，确保最高的质量和可靠性。
- ISO27001: 管理风险并保护所处理数据和信息的机密性、完整性和可用性的系统。
- IEC62443-4-1 ML2: 实施的产品安全开发和管理流程涵盖了整个产品生命周期的安全方面。Anybus 目前也正在进行获得 IEC62443-4-1 ML3 的过程。

3.1.1 通用数据保护条例

HMS 工业网络遵守《通用数据保护条例》（GDPR）的规定。Anybus CompactCom 40 无需传输个人用户信息即可运行。

有关更多信息，请访问：HMS 客户隐私政策

3.2 ISMS 实施的安全措施

为了确保 Anybus CompactCom 40 产品生命周期的机密性和完整性，HMS 工业网络实施了表 1 中描述的安全措施：

要求	HMS 的实施措施
数据保密性	• 根据第 3.1 节中列出的与安全相关的证书，全面实施 ISMS 控制措施。
安全的开发与制造环境	• 仅授权人员可进行受限的物理和逻辑访问。 • 非工作时间内门禁上锁，警报系统启用。 • HMS Networks 维护完整的审计日志，详细记录所有访问和更改。 • 访客须由 HMS 员工陪同。 • 禁止摄影或类似录制行为。
对整个供应链完整性的保障	• 软件在固件和基于 PC 的配置软件及驱动程序中均使用证书。 • 硬件采用知名的工业 EMS 供应商，并由 HMS Networks 审核所有供应商。 • 内部会对产品进行完整性检查，以确保产品的完整性。

表 1：安全措施

4. 产品文档和信息

4.1 Anybus CompactCom 40 设计指南

Anybus CompactCom 40 设计指南全面描述了产品的功能、性能，并为在自动化设备中实施和配置产品提供了指导。

设计指南是产品信息的主要来源，可在 HMS 技术支持网页上找到。

4.2 固件更新

HMS 工业网络不断增强 Anybus CompactCom 40 固件，以改进功能、解决软件问题和减少安全漏洞。已安装的产品可以在现场更新到最新可用版本。

有关新固件版本的信息由 HMS 工业网络积极分发，遵守区域政策（GDPR 禁止在欧洲分发），或分发给 HMS 客户和分销商信息系统（CDIS）的注册用户。在此处查找有关 CDIS 的更多信息。

Anybus 固件管理器软件可确保现场安装的产品的更新，还可以支持基于以太网的模块的中央固件部署。更多固件更新选项也可用，请查看相关设计指南以获取更多信息。

为了防止下载未经授权的代码或恶意代码，Anybus CompactCom 40 只接受经过 HMS 工业网络数字签名的固件。

4.3 使用开源软件

HMS 工业网络可能会在 Anybus CompactCom 40 产品中集成开源软件。该软件已集成到产品固件中，HMS 工业网络负责软件的验证，并确保定期更新到最新版本。

有关使用的开源软件和相应许可信息的详细信息，请参阅 HMS 技术支持网页上的相关网络指南。

4.4 漏洞管理和沟通

有关安全漏洞的信息发布在安全公告网页上，用户可以直接从网站订阅 RSS 提要，以接收有关更新内容的通知。

HMS 工业网络有一个 HMS 责任披露程序，使任何人都可以报告潜在的产品漏洞。在此处查看更多信息。

4.5 后门自由声明

Anybus CompactCom 40 不包含未记录的后门或隐藏账户。

Anybus CompactCom 40 不包括远程访问功能，也不与基于云的服务建立特定的外部通信。

5. 设计安全

安全性是 Anybus CompactCom 40 开发过程中每个步骤不可或缺的一部分，包括需求收集、设计、编码、测试、部署和归档。

经过安全培训的员工

所有员工都接受了网络安全意识培训。开发人员还接受安全编码培训，并进行源代码审查。

安全产品测试和验证

设计安全方法包括全面测试，重点是识别潜在漏洞。这涉及运行以安全为重点的测试用例，旨在发现任何可能被利用的意外产品功能或配置。

表 2 显示了 HMS 工业网络如何审查和测试 Anybus CompactCom 40 中使用的代码。HMS 选择符合产品要求的测试和审查。

审查或测试类型	合规情况
代码审查	所有代码在录入前都会经过审核
侵入测试	对产品的部分组件进行了入侵测试
静态代码分析	Synopsis Coverity 工具
模糊测试 / 健壮测试	针对PROFINET协议版本进行了网络负载测试
漏洞扫描器	Achilles

表 2: Anybus CompactCom 测试

产品发布后，HMS 工业网络对 Anybus CompactCom 40 进行定期测试，以确保其能够抵御新出现的威胁。

5.1 Anybus CompactCom 40 工业物联网安全

基于安全的产品

Anybus CompactCom 40 工业物联网安全产品的设计以安全性为设计重点，满足了对更高安全要求的需求。因此，它包括以下额外的安全措施：

- 符合 802.1AR 标准：安全设备标识

Anybus CompactCom 40 工业物联网安全产品符合 IEEE 802.1AR 标准，该标准侧重于安全设备标识（DevID），旨在增强网络环境中的设备身份验证和信任。

- 安全芯片

The Anybus CompactCom 40 工业物联网安全产品包括一个安全芯片，用于安全存储关键数据，如证书私钥。

- 安全启动机制

与 Anybus CompactCom 40 系列的所有产品一样，Anybus CompactCom IIoT 工业物联网安全产品只接受经过 HMS 工业网络数字签名的固件。为强化安全防护，该模块在每次启动时还会验证固件完整性。这种双重验证机制通过确认数字签名有效性和固件未篡改状态，显著提升设备安全性，有效防御未经授权的修改或恶意篡改。

- 信任根

Anybus CompactCom 40 工业物联网安全产品通过基于安全芯片的信任链延伸至证书验证机制，确保模块内所有组件的真实性与完整性，为整个系统的安全性奠定了坚实的可信基础。

- 加密

该模块采用安全通信协议对数据交互进行加密，有效防范第三方拦截或篡改。

第 2 部分 : 安全相关信息和最佳实践

6. Anybus CompactCom 40 连接概述

Anybus CompactCom 40 可以提供多种通信接口，以覆盖以下功能：

- 用于与自动化控制器交换过程数据的工业以太网
- 用于可选配置和诊断的基于 Web 的功能
- 用于与 IT 应用程序进行信息交换的 IIoT 协议
- 支持主机应用程序内集成的 API

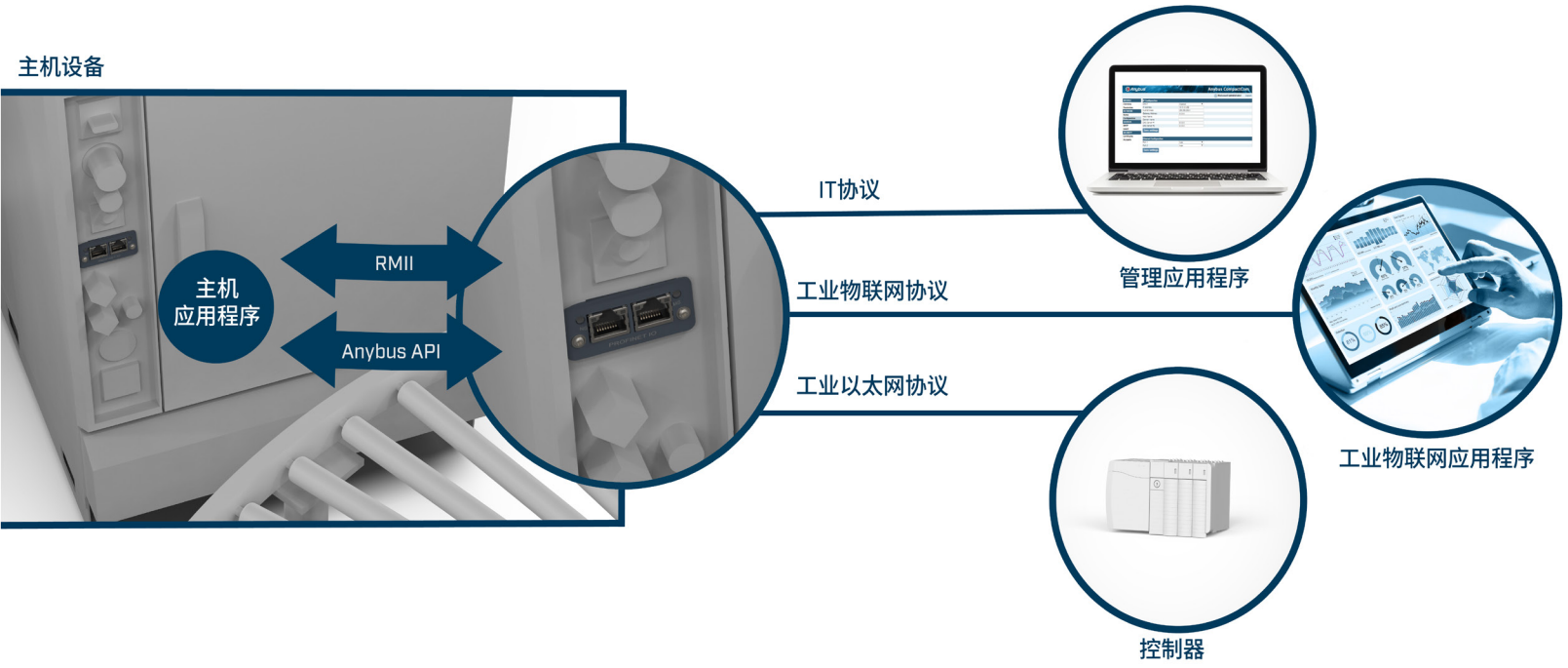


图 1: Anybus CompactCom 接口模块

基于串行的网络主要是逻辑上隔离的通信网络，这意味着实施网络攻击需要极高的定向性投入。因此，本文档所述安全规范不适用于采用串行工业通信协议的 Anybus CompactCom 系列产品。

本文档后续章节所述安全考量，主要针对 Anybus CompactCom 40 系列产品的网络连接及通信接口。对于提供扩展连接功能的产品版本（如 IIoT Secure 安全增强型），其内置的网络安全防护机制已进行专项强化。

表 3 概述了为 Anybus CompactCom 40 工业以太网和 Anybus CompactCom 40 工业物联网安全版本实现的通信接口和协议

	Anybus CompactCom 40 工业以太网	Anybus CompactCom 40 工业物联网安全
工业协议		
PROFINET	X	X
EtherNet/IP	X	X
Modbus	X	
EtherCAT	X	
POWERLINK	X	
CC-Link IE Field	X	
CC-Link IE TSN	X	
BACnet/IP	X	
工业物联网协议		
MQTT		X
OPC UA		X
IT 协议		
Web Server	X*	X
FTP Server	X*	
WebDAV		X
JSON	X*	X
E-mail Client	X*	X
Server side Include (SSI)	X*	
主机接口		
Anybus API	X	X
Transparent Ethernet (RMII)	X**	

表 3: Anybus CompactCom 40 型号的通信接口和协议概述。 CC-Link IE 型号中未包含的功能。 ** 功能取决于订购的产品版本。*

7. Anybus CompactCom 通信接口

本节介绍 Anybus CompactCom 40 内通信接口的安全相关信息。设备制造商应充分理解本部分功能特性，以便在满足具体应用需求的同时，合理配置设备以提供安全接口。

请参阅第 6 节中的表 3，确认所述功能是否适用于您所采用的 Anybus CompactCom 产品型号。

有关本章所列功能的更多详细技术信息，请参阅相应的《网络设计指南》。

7.1 默认安全配置

所有 Anybus CompactCom 40 产品都符合各自网络协议的规范。相关网络组织负责定期更新协议标准，以持续提升抗网络攻击能力。

Anybus CompactCom 40 IIoT Secure（安全增强型） 专为安全接口管理设计，这意味着只能通过安全协议访问 Web 服务器和 WebDAV。

然而，值得注意的是，Anybus CompactCom 解决方案作为工业系统中的组件，其配置及运行由上位机应用程序控制。因此，在系统集成阶段需同步实施默认安全策略。

7.2 硬件

7.2.1 物理端口

Anybus CompactCom 40 有两个以太网端口。

除 CC-Link IE Field, CC-Link IE TSN, EtherCAT 和 POWERLINK 外，所有网络的端口都可以单独禁用。

7.2.2 管理接口

Anybus CompactCom 40 中集成的处理器有多个内部接口，这些接口都是安全的。串行接口作为服务接口，其只接受 HMS 签名的固件。Anybus CompactCom 40 还包括一个 JTAG 接口，用于印刷电路板（PCB）组件的连通性及功能测试。JTAG 接口在工业以太网型号上是可用的，但在 Anybus CompactCom 40 IIoT Secure（安全增强型）上是禁用的。

7.2.3 Anybus CompactCom 40 工业物联网安全

Anybus CompactCom 40 工业物联网安全中集成以下安全强化功能：

- 安全芯片：采用专用加密芯片安全存储证书私钥等关键数据，防止非授权访问。
- 硬件加密加速：通过专用硬件模块实现加密算法加速运算，显著提升处理效率

7.3. 安全和访问身份验证

7.3.1 Anybus CompactCom 40 - 用户和密码管理

设备制造商在集成 Anybus CompactCom 40 时，通过上位机应用程序接口（Host Application Interfaces）定义初始用户账户。支持基于用户权限级别，对 CompactCom 模块中的不同目录及功能模块进行访问限制。

Anybus CompactCom 40 对创建的密码没有任何具体要求。

Anybus CompactCom 40 中的密码存储是未加密的。

通信通道的用户管理

Anybus CompactCom 40 对每个通信通道使用单独的用户和密码管理。

- **FTP 服务器**

  对于此通信通道，对用户和密码有特定要求。有关更多信息，请参阅相应网络的《网络设计指南》。

- **WEB 服务器**

  对于此通信通道，对用户和密码有特定要求。对特定目录的访问也可以根据每个用户进行限制。有关更多信息，请参阅相应网络的《网络设计指南》。

7.3.2 Anybus CompactCom 工业物联网安全—用户和密码管理

Anybus CompactCom 40 工业物联网安全需要在设备的初始设置期间配置初始管理员帐户。有关如何配置第一个管理员帐户的更多信息，请参阅《网络设计指南》。Anybus CompactCom 40 工业物联网安全实现了中央用户和角色管理，这意味着只要用户有访问权限，一个帐户就可以用于所有通信通道。

Anybus CompactCom 40 工业物联网安全实现了密码创建的可配置要求，以确保密码的稳健性。有关更多信息，请参阅相应网络的《网络设计指南》。Anybus CompactCom 40 工业物联网安全中的密码存储是加密的。

Anybus CompactCom 40 工业物联网安全产品不与本地 LDAP/Active 目录连接。

角色

Anybus CompactCom 40 工业物联网安全使用角色来定义用户访问权限。所有用户都将拥有一个登录到其帐户的角色，有三个默认角色：管理员、操作员和用户。可以在主机应用程序中配置角色和每个角色的访问权限，也可以添加新角色。

7.4 网络功能

HMS 工业网络可确保 Anybus CompactCom 40 符合相关网络规范，并在网络组织发布新规范时更新 Anybus CompactCom40。

在 Anybus CompactCom 40 中，接口和服务旨在促进与定义对象的数据交换。这使用户能够高效地管理设备功能，或深入了解通信状态、质量和可靠性。有效实施和利用这些工业协议的所有计划功能对于高效和安全的接口实施至关重要。

Anybus CompactCom 40 IIoT: 为专用安全扩展做好准备—— CIP Security and PROFIsecurity

为了应对不断变化的网络安全要求，工业通信组织正在开发新的协议扩展，引入先进的安全机制来保护通信和应用程序。目前，这些扩展涉及 PROFINET, EtherNet/IP, 和 Modbus TCP 协议。它们的实施状态从早期阶段的适用性到正在进行的讨论不等。

Anybus CompactCom 40 工业物联网安全旨在满足现有的安全标准，但也将能够集成即将推出的工业协议安全扩展。

然而，值得注意的是，POWERLINK 和 EtherCAT 不需要特定的网络安全扩展。这是因为这些协议使用的是不基于 IP（互联网协议）的专有网络访问方法。此外，这些网络内的通信管理由专用设备控制。这种安排提供了高度的网络隔离和对常见网络攻击的保护。

专用设备可充当强大的守门员，确保网络安全，抵御外来威胁。

7.4.1 IIoT 协议

OPC UA

OPC UA 允许将状态和质量信息从车间设备传输到仪表板或更高层次的系统，而无需为每个第三方设备或应用程序开发定制软件。

激活和停用

默认情况下，OPC UA 处于禁用状态，可以由主机应用程序启用。

有关更多信息，请参阅在 Anybus CompactCom 40 工业物联网安全上启用和使用 OPC UA。

身份验证

本地用户管理 - 基于角色定义的授权。

OPC UA 可以用于不同级别的安全性和功能性，但是要建立安全的 OPC UA 连接，需要 CA 证书和设备证书。

有关如何生成和安装证书的更多信息，请参阅在 Anybus CompactCom 40 工业物联网安全上启用和使用 OPC UA。目前不支持 OPC UA 全局发现服务器（GDS）。

安全技术

基于 OPC UA 定义的技术构建

MQTT

MQTT 是用于物联网的 OASIS 标准消息传递协议，它是一种在 TCP/IP 之上运行的发布 - 订阅消息传递协议。

激活和停用

MQTT 默认情况下是禁用的，可以由主机应用程序启用。

有关更多信息，请参考在 Anybus CompactCom 40 工业物联网安全上启用和使用 MQTT。

身份验证

要设置安全的 MQTT 连接，需要 CA 证书和设备证书。

有关如何生成和安装证书的更多信息，请参阅在 Anybus CompactCom 40 工业物联网安全上启用和使用 MQTT。

安全技术

使用 TLS 1.2 版本来保护信息和维护隐私。

7.4.2 管理

Web 服务器功能

内置的 web 服务器为终端用户交互和配置提供了一个灵活的环境。JSON、SSI 和客户端脚本允许访问对象和文件系统数据，从而创建高级图形用户界面。

表 4 概述了与 Anybus CompactCom 40 工业以太网和工业物联网安全版本的 web 服务器相关的启用和停用、身份验证和安全技术。

	Anybus CompactCom 40 工业以太网	Anybus CompactCom 40 工业物联网安全
启用与停用	Web 服务器默认启用。可以在以太网主机对象（F9h）中完全禁用。	Web 服务器默认启用。可以在以太网主机对象（F9h）中完全禁用。
身份验证	由主机应用程序定义用户、密码和访问权限（参见第 8.4 节）。	基于角色定义的本地用户管理访问授权（参见第 8.4 节）。非活动的连接会在可配置时间后关闭。
安全技术	Web 服务器页面存储在 Anybus CompactCom 40 文件系统中，可通过 FTP 或主机应用程序访问。 服务器通信使用 HTTP 协议。	Web 服务器页面存储在 CompactCom 文件系统中，可通过安全的 WebDAV 连接或主机应用程序进行修改。服务器通信使用 HTTPS 协议。当 Anybus CompactCom 40 出厂时，初始设备身份证书已启用/激活用于 HTTPS 协议，以便在设备由终端用户配置前进行通信。使用 TLS 1.2 协议来保护信息并维护隐私。

表 4：关于 Anybus CompactCom 40 各型号 Web 服务器的启用与停用、身份验证及安全技术的摘要

固件更新协议

Anybus CompactCom 40 工业以太网型号使用内置 FTP 服务器，允许使用标准 FTP 客户端进行固件更新和系统文件访问。Anybus CompactCom 40 IIoT Secure 使用 WebDAV 进行固件更新和访问 CompactCom 的文件系统。

表 5 概述了与 Anybus CompactCom 40 工业以太网和工业物联网及安全版本的固件更新相关的启用和停用、身份验证和安全技术。

	Anybus CompactCom 40 工业以太网	Anybus CompactCom 40 工业物联网安全
启用和停用	默认情况下启用 FTP 服务器，可以在以太网主机对象 (F9h) 中禁用它。	默认情况下启动 WebDAV。可以在以太网主机对象（F9h）中禁用它。
身份验证	web 服务器需要特定于此通信通道的用户管理。为每个用户分配一个主目录；用户将无法访问分配目录之外的任何目录。	本地用户管理 - 基于角色定义的授权。Anybus CompactCom 40 工业物联网安全将在设定时间后关闭非活动连接，此时间可在WebDAV配置中配置。
安全技术		WebDAV 是 HTTPS 协议的扩展，为 WebDAV 使用单独的端口号可以阻止路由器和防火墙中的 WebDAV 操作，但仍然允许 web 流量通过。

表 5: Anybus CompactCom 40 型号固件更新相关的启用和停用、身份验证和安全技术摘要。

7.5 主机应用程序接口

7.5.1 Anybus API

Anybus API 是针对设备主机应用程序的 HMS 专用中性协议 API。该 API 使用消息传递接口进行配置和诊断，并有一个专用接口用于过程数据交换。

Anybus API 是一个内部接口，因此不存在直接访问的风险。然而，主机应用程序确实需要保护，以防攻击。

7.5.2 RMII [透明以太网]

Anybus CompactCom 40 的透明以太网版本可用于特定的网络协议。默认情况下禁用透明以太网。它可以在 Anybus 对象（01h）中启用。精简媒体独立接口（RMII）在网络和主机应用控制器之间提供透明连接。这意味着 CompactCom 无法确保该接口的安全。应在设备的主机应用程序中采取所有适当的安全措施。

7.6 信息和活动记录

Anybus CompactCom 40 无需传输个人用户信息即可运行。

Anybus CompactCom 40 不进行任何事件或活动记录。

7.7 停用

当停用 Anybus CompactCom 40 时，执行出厂重置将删除存储在 Anybus CompactCom 40 上的用户帐户和特定模块配置信息。

8. 安全操作的最佳实践

本节概述了制造商确保 Anybus CompactCom 在其设备或机器内安全运行的最佳实践。强烈建议制造商使用这些指导原则，以保持较高的安全级别并防止潜在漏洞。

此列表并不详尽，应根据您的应用程序和所需的安全级别进行考虑。

8.1 使用适合的 Anybus CompactCom

Anybus CompactCom 40 工业以太网型号（见第 6 节表 3）适用于只需要工业以太网通信的应用。这些型号实现了相关协议规定的所有通信标准。

对于同时需要工业以太网通信和 IIoT 或 web 服务器连接的应用，Anybus CompactCom 40 IIoT Secure 型号是最佳选择。此选项提供了额外的安全功能。

Anybus CompactCom 40 IIoT Secure 也是一个面向未来的解决方案，能够主要通过固件更新来满足长期的安全要求。

使用标准 Anybus CompactCom 40 的现有应用程序可以通过通用 Anybus Host API 以最小的工作量更新到 IIoT Secure 型号。

8.2 默认安全 - 通信接口

制造商必须关闭或禁用 Anybus CompactCom 上设备应用程序不需要的所有逻辑或物理接口。

- 停用任何未使用的物理通信端口，如第二个以太网端口。或者，为最终用户提供激活或停用未使用的以太网端口的能力。
- 禁用设备预期操作不需要的任何通信功能，如 web 服务器。
- （尽可能）激活 MQTT 的加密功能，并确保 OPC UA 保持安全。

8.3 配置，备份和恢复

使用安全接口，并根据角色和职责定义访问权限。使用单个或有限数量的接口来定义行为和配置。在固件更新期间计划备份、恢复和维护。

8.3.1 指定主机应用程序中的固定功能和行为

在处理设备的固定行为和功能时，特别是在通信特性和功能方面，必须在主机应用程序的实现中优先考虑这些行为的明确定义。通过这样做，这些行为在固件中根深蒂固，可以通过设备的固件本身进行更新，而无需备份或恢复程序。这种方法可确保指定的行为保持一致和可升级，从而保护设备的预期操作。

8.3.2 利用网络描述文件进行用户设备配置

使用工业协议方法，如专用网络描述文件（GSD、EDS）来获取用户定义的配置参数。这些专用配置参数在每次通信初始化期间由 PLC 传输到设备，随后存储在控制器项目文件中。

8.3.3 通过专有软件工具进行设备配置

如果使用专用或专有软件工具进行设备配置，请通过主机应用程序传输信息。主机应用程序然后可以存储特定配置参数，并通过主机 API 设置 Anybus CompactCom 40 through the host API。

此外，制造商的工具或应用程序可以实现配置备份和恢复功能，以及对配置参数的身份验证和访问控制。

8.3.4 使用Anybus web 服务器进行配置

制造商可以使用 Anybus web 服务器来配置网络参数。他们还可以创建自己的网页，提供专用的设备配置参数。注意以下事项：

- Anybus 网页不提供配置参数的备份和恢复功能。
- 制造商必须确保配置网页有必要的保护和访问控制。

8.4 访问保护和用户管理

设备制造商应建立适合特定应用要求的用户结构。这种结构应该明确定义各种用户角色，每个角色都有不同的访问权限级别。

尽可能激活接口的用户和密码标识，以防止未经授权访问接口。

8.5 遵守网络协议

使用各自协议特定的专用标识元素或机制，提供有关其设备版本、状态和诊断信息的清晰信息。Anybus CompactCom 网络指南中列出了相关的专用信息元素或机制。

确保设备通过相关工业网络的性能和一致性测试，以获得网络证书。

8.6 提供设备文档

提供全面的设备文档，概述全局设备接口并详细说明 Anybus CompactCom 40 功能的实现。

为了保持整个系统的有效版本管理，集成与 Anybus CompactCom 40 相关的版本管理。这应该包括主机应用程序和固件的特定组件，这些组件可以反映在 Anybus CompactCom 40 接口中。

制造商可将 Anybus CompactCom 40 中使用的开源软件或硬件的 HMS 声明纳入自己的文档中，并根据实施情况对其进行补充。HMS 开源声明可在相关网络指南中找到。

8.7 让您的设备保持最新状态

保持 Anybus CompactCom 模块的最新状态，以保持一贯的高安全级别。

随时了解 Anybus CompactCom 的更新：

- 向 HMS 的 CDIS 申请接收产品变更通知，在此处查找 CDIS 的更多信息。
- 直接从 HMS 网站订阅 RSS 提要，以接收有关更新内容的通知。安全建议可在此处获取。

制造商负责评估 HMS 发布的与设备应用相关的产品变更通知和安全建议的相关性和影响。

不要忘记更新版本信息，以便准确跟踪现场安装的设备。

9. 附录

9.1 相关文件

文件	作者	文件 ID
Anybus CompactCom 40 软件设计指南	HMS	HMSI-216–125
Anybus CompactCom M40 硬件设计指南	HMS	HMSI-216-126
Anybus CompactCom B40 硬件设计指南	HMS	HMSI-27-230
Anybus CompactCom 主机应用程序实施指南	HMS	HMSI-27-334
Anybus CompactCom 40 网络指南（每个支持的现场总线或网络系统的单独文档）	HMS	-