集成指南

# 安全设备集成指南

Anybus 嵌入式网络接口

# 第 1 部分： 工业自动化设备的网络安全法规与标准



# 第 2 部分： HMS Networks 的网络安全



# 第 3 部分： 最佳实践与安全集成

# 前言

### 背景

在工业数字化持续推进的背景下，工业网络早已突破工厂四壁的局限，实现了设备和机器的广泛互联，这既扩大了设备的可访问范围，也带来了更多潜在威胁。

《网络弹性法案》（CRA）等新法规的出台，进一步提升了业界对网络安全的认识和重视程度，凸显了其在保护本土产业方面的关键作用。

因此，在集成工业通信接口时，网络安全已成为必须考量的要素，既关乎通信的可靠性，也涉及对安全法规的合规性。

多年来，HMS Networks 始终紧跟市场对强化网络安全日益增长的需求，通过完善内部流程和提升产品稳健性积极做出响应。这一前瞻性举措使客户能够更轻松地实施安全通信接口。

### 文档目的

本文档旨在为计划将 Anybus 嵌入式网络接口集成至其工业产品的制造商提供操作指南。

本指南主题包含三个部分：

第 1 部分：现行网络安全法规与标准概述

第 2 部分：HMS Networks 的网络安全体系与相关流程介绍，并概述我们在解决方案中已实施的网络安全措施。

第 3 部分：针对设备制造商的指南，介绍满足当前安全要求的推荐实施方案。

# 第 1 部分：工业自动化设备的网络安全法规与标准

作为自动化设备制造商，推行网络安全举措是提高产品可靠性、最大限度减少潜在经济和声誉损失的有效做法。然而在当下，随着《网络弹性法案》（CRA）等对通信类产品产生影响的法规，以及 NIS2 等涉及生产和基础设施的法规相继出台，实施网络安全策略已从可选转变为强制要求。

目前，大多数法规仍有待进一步明确，协调性标准也尚未正式发布。这为设备制造商和机器制造商带来了不确定性，他们需要时间调整产品组合以确保持续合规。

- 本部分内容首先介绍直接影响通信接口类设备的法规，以及通过用户（采购要求）间接影响制造商的法规；
- 随后章节将阐述当前可供参考的网络安全标准，并为工业设备制造商提供初步的网络安全策略建议。

为帮助客户减轻合规负担，HMS Networks 持续关注相关法规动态，积极落实各项必要要求，并为工业设备提供即插即用、预认证的工业设备网络接口。采用我们的通信解决方案，可显著降低网络安全实施的工作量，同时减少对漏洞的持续监控与安全维护投入。

# 1. 法规与采购要求

对设备制造商而言，建立网络安全流程本身是一项良好实践，既能提升产品可靠性，也能减少潜在的经济与声誉损失。此前，网络安全防护等级可由各设备制造商自行决定；而随着 CRA、NIS2 等新法规的出台，网络安全已从可选项转变为强制性要求。

本章将介绍对设备制造商有直接或间接影响的主要网络安全法规；下一章将分析可用于证明法规合规性的技术标准。

## NIS2：网络与信息系统安全指令

欧盟指令 NIS2 已取代其前身 NIS1。NIS1 主要覆盖能源、交通、医疗、金融、水资源管理和数字基础设施等关键领域的网络安全要求。

NIS2 则进一步扩大了适用范围，新增公共电子通信服务提供商、数字服务企业、废弃物与污水处理机构、关键产品制造商、邮政与快递服务、中央及地区级公共行政部门，以及航天领域。

相关行业中的大中型组织必须采取适当的网络安全风险管理措施，并就重大安全事件向国家主管机构报告。

欧盟成员国原应在 2024 年 10 月 17 日前将 NIS2 转换为国内法。有 19 个成员国未能按时完成，欧盟委员会已对其启动了侵权程序。

尽管存在滞后，NIS2 仍对欧盟境内众多组织产生实质影响。与 CRA 和 RED 网络安全要求不同，NIS2 目前缺乏可用于推定符合性的协调标准，其具体实施要求由各成员国自行明确。

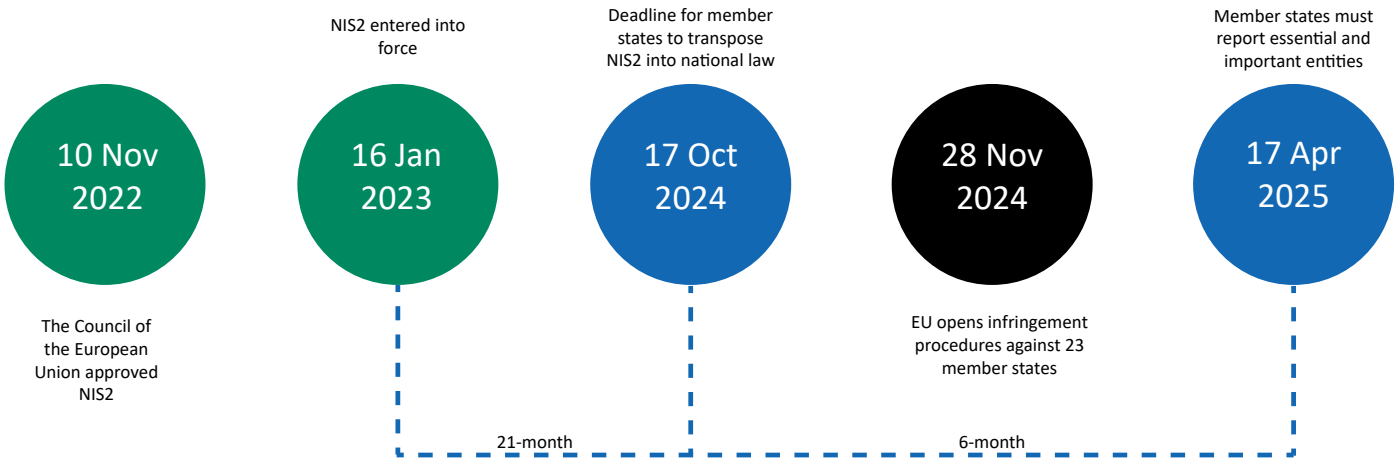


*图 1： 欧盟 NIS2 指令实施与执行的关键时间点*

在 IT 网络安全方面，常使用 ISO 27001 来证明符合 NIS2。该标准对 IT 系统、人员及物理安全覆盖全面，但对运营技术（OT）的适用性较弱。在 OT 领域，通常采用 IEC 62443 系列标准来证明合规。

设备制造商与机器制造商通常不直接受 NIS2 约束，但会间接受其范围内客户提出的采购要求影响。这些要求多基于 IEC 62443 系列标准。

**《网络弹性法案》：联网产品的更广泛网络安全框架**

欧盟《网络弹性法案》（CRA）为所有在欧洲销售的含数字元件的产品规定了强制性网络安全要求。

该法案对全球制造商均有约束力，要求其在产品整个生命周期内（至少 5 年）实施安全设计、漏洞管理并提供更新支持。

自 2026 年 9 月起，制造商必须主动报告已被利用的漏洞及严重安全事件；至 2027 年 12 月 11 日，需全面强制合规，包括准备技术文档、完成符合性评估以及提供软件物料清单（SBOM）。

CRA 还将产品按关键等级进行分类，不同类别对应不同的符合性评估方式。该法案不设“祖父条款”，即在截止日期后生产的产品，即使研发完成于期限之前，也必须符合新规。

欧盟委员会已要求制定协调标准，以明确法规具体释义，这也是证明 CRA 符合性的前提。更具要求，CRA 协调标准需以 RED 网络安全协调标准为基础。

然而截至 2025 年中，这些标准仍在制定中，给必须提前筹备的制造商带来了不确定性。

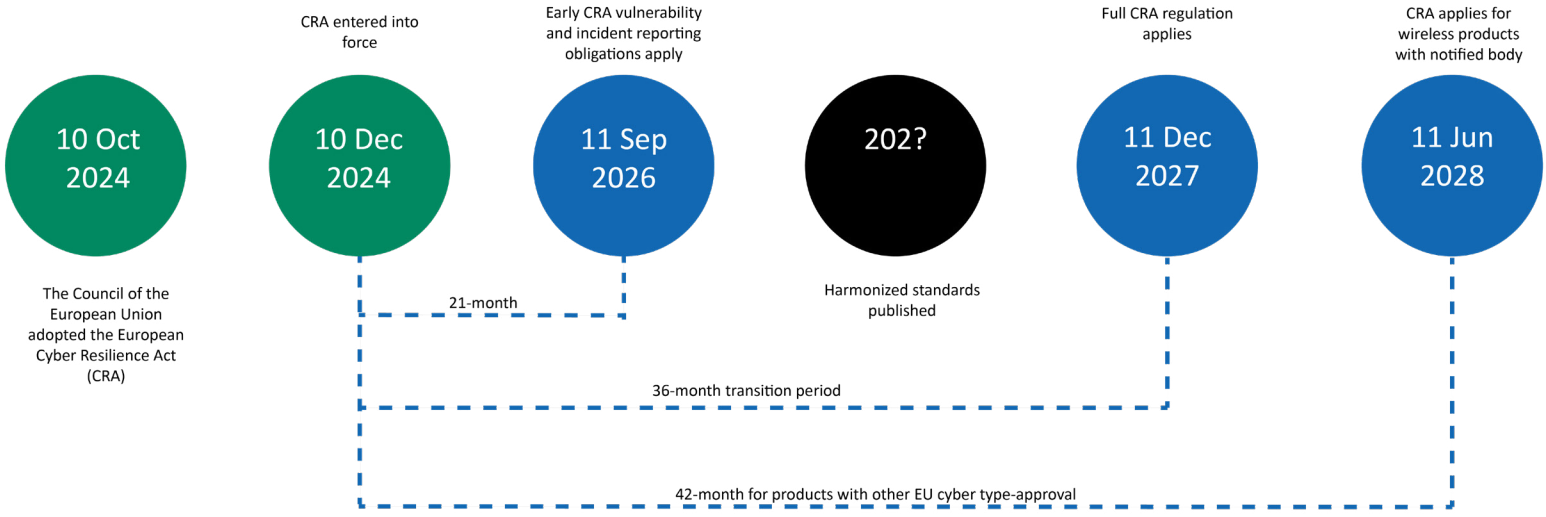


*图 2：网络弹性法案（CRA）关键时间点*

## RED 指令：加强无线产品的网络安全

无线电设备指令（RED）是欧盟的一项现行法规，旨在确保无线通信设备等无线电设备符合健康、安全及电磁兼容性要求。

2021 年，《授权法规（EU）2022/30》正式生效，激活了 RED 指令中的核心网络安全要求。

该要求适用于所有可接入互联网的无线产品，并自 2025 年 8 月 1 日起强制执行。工业有线设备本身虽不直接适用 RED 网络安全要求，但若集成了无线连接功能，则整机设备需纳入合规范围。例如，若某工业设备支持通过平板电脑或智能手机进行无线配置，则该设备可能整体适用于 RED 网络安全要求。

制造商必须确保支持无线功能的产品（包括具有 Wi-Fi、蓝牙或蜂窝网络连接的工业设备）具备必要的安全保障措施，以保护个人数据、防止未授权访问，并确保网络韧性。

对于工厂自动化而言，这意味着工业环境中使用的联网设备需内置网络安全功能以满足 RED 合规性。此要求影响广泛，从无线网关到边缘设备，尤其是那些与云系统或用户网络交互的设备均需符合。

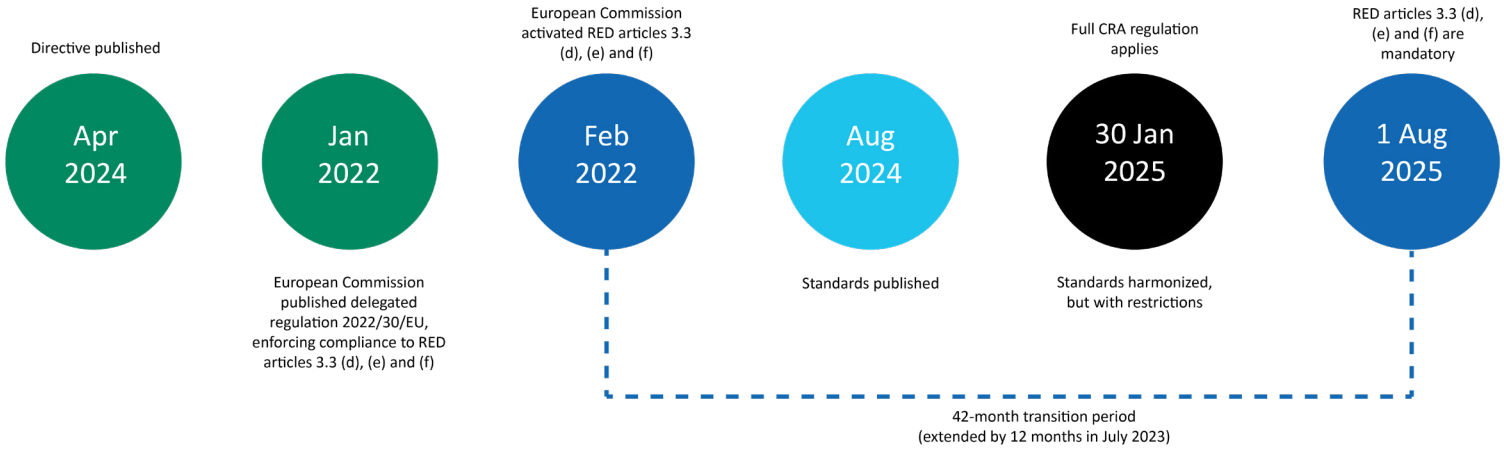


*图 3：无线电设备指令（RED）网络安全要求的关键时间点*

### 网络安全采购要求

大型企业及政府机构通常会在采购中提出网络安全要求。

尤其显著的是，向美国政府机构供货的订单通常需符合美国国家标准与技术研究院（NIST）制定的网络安全标准、指南与最佳实践。

尽管 NIST 合规并非法规强制要求，但由于美国政府的供应商和次级供应商数量庞大，其实际影响范围仍十分广泛。

### 网络安全保险要求

网络安全日益成为资产投保的先决条件。例如，在航运领域，新船舶需获得评级机构认证方可投保。

国际航运协会已制定《E27 船载系统与设备网络韧性标准》，该标准主要基于 IEC 62443，但剔除了与船舶无关的部分内容。

虽然船舶的网络安全要求直接适用于船东，但也间接影响到为海事领域提供设备与机器的制造商。

# 2. 标准

## IEC 62443 工业通信网络——网络与系统安全

IEC 62443 系列标准旨在解决自动化和控制系统中的运营技术（OT）安全问题，并对更侧重于信息安全管理体系（IT 基础设施）的 ISO 27001 标准形成补充。

该标准涵盖从顶层策略、流程到底层组件的全方位安全要求，并特别强调工业控制系统的完整性和可用性。

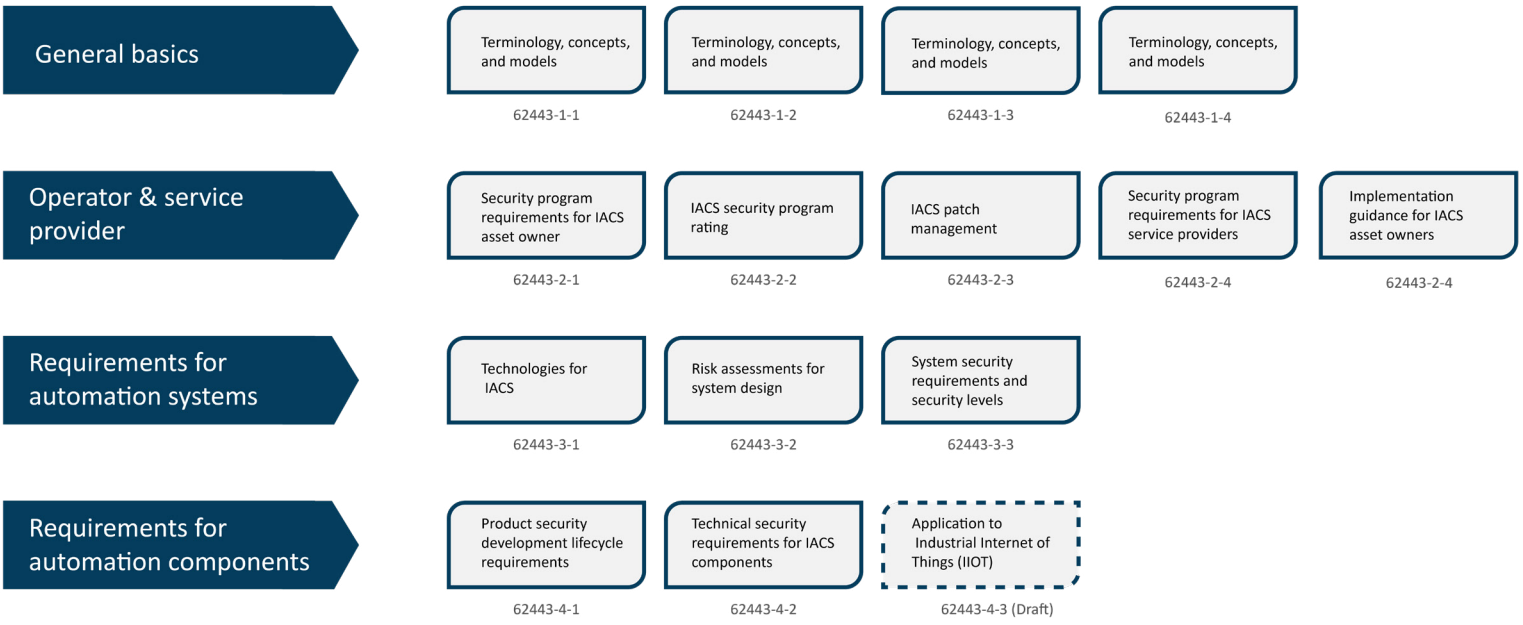


*图 4：工业网络安全领域 IEC 62443 系列标准的架构*

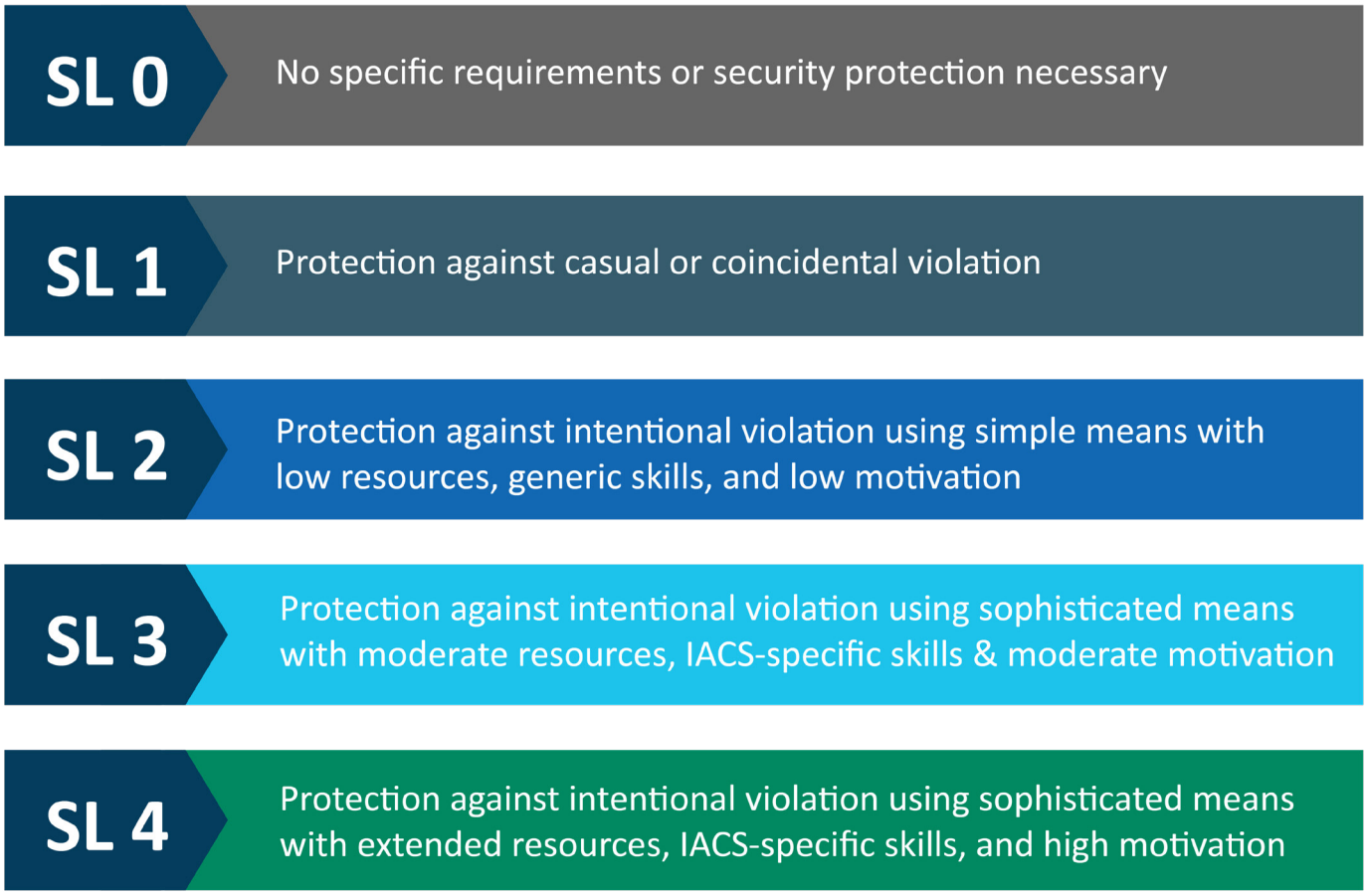


*图 5：IEC 62443 标准中 SL 0 至 SL 4 的安全等级*

标准定义了从 0 级到 4 级共五个安全等级，其中 0 级不做具体要求。

该标准既有助于设施所有者达成适当的网络安全水平，也可作为对外证明合规的依据：

- 证明符合 NIS2 等法规要求；
- 向保险公司展示已达到相应的安全等级；
- 向客户和股东证明已具备适当的网络安全能力。

设施安全的一项指导原则是对 OT 网络进行分段，并建立通信管道以监控和管理关键设备及生产线内部的工业通信，从而限制自动化设备的暴露面。

为实现设施所需的安全等级，其系统和组件也必须满足相应的网络安全要求。为满足这些期望，设备制造商可参考 IEC 62443-4-x 系列标准，获取有关自动化组件网络安全文档和实施要求方面的系统化、深入指导。

从 CRA 角度来看，IEC 62443 十分重要，因为目前正在开展相关工作，以扩展该标准系列，使其能成为 CRA 的协调标准。

这项工作包括为 IEC 62443-4-1 和 IEC 62443-4-2 制定欧洲扩展版本，并创建一系列新的 IEC 62443-5-x （称为“规范标准”）以及 IEC 62443-6-x（详细规定评估方法）标准。

### EN 18031 无线电设备的通用安全要求

EN 18031 系列标准是欧盟无线电设备指令（RED）的协调标准。无线电设备若依据这些标准通过测试，即可推定其符合该指令的网络安全要求。

从 CRA 角度来看，该标准同样重要，因为欧盟委员会已要求标准化组织基于 RED 网络安全标准来制定 CRA 的协调标准。因此，EN 18031 是准备满足 CRA 合规要求的一个良好起点。

EN 18031 也是首个实现协调化的网络安全标准。成为协调标准的要求之一，是依据该标准进行的测试应具备法律确定性。

换言之，通过标准测试的结果不应依赖于执行测试的人员。在这方面，EN 18031 与采用更具风险导向测试方法的 IEC 62443 有所不同。

### NIST FIPS 与特别出版物

美国商务部下属的国家标准与技术研究院（NIST）发布了一些列联邦信息处理标准（FIPS）以及众多关于网络安全的“特别出版物”。

FIPS 对网络安全的关键方面进行了标准化，例如：

- 高级加密标准（AES）：原名 Rijndael，现已被几乎所有网络服务器和大多数加密通信场景所采用；
- 安全哈希算法（SHA）：一系列加密哈希函数；
- 密码学安全的随机数生成器：大多数现代微控制器均配备经 FIPS 认证的基于硬件的随机数生成器。

特别出版物通常包含网络安全相关指南，例如 NIST 特别出版物 800-63B 就提供了关于密码的建议。

FIPS 和特别出版物是美国大多数联邦机构的强制性采购要求，同时也在联邦机构之外被广泛应用。IEC 62443 和 EN 18031 在涉及网络安全最佳实践时，均引用了 NIST 的出版物。

### UL 2900 网络连接产品软件网络安全标准

UL 2900 是一系列关于网络连接产品网络安全的标准，其中部分标准也已被美国国家标准学会（ANSI）采纳为国家标准。ANSI/UL 2900-1 涵盖通用产品要求，主要包括安全开发和测试方面的要求。

第 1 部分属于适用于所有产品的横向标准。

第 2 部分是一组针对特定产品类别的垂直标准:

- ANSI/UL 2900-2-1：针对网络连接医疗产品要求；
- UL 2900-2-2：针对工业控制系统（目前尚未被 ANSI 采纳）；
- UL 2900-2-3：针对安全与生命安全信号系统（目前尚未被 ANSI 采纳）。

美国食品药品监督管理局（FDA）已认可使用 ANSI/UL 2900-1 和 ANSI/UL 2900-2-1 作为证明符合政府法规的一种途径。

### ISO/IEC 27000 信息安全管理体系（ISMS）

ISO/IEC 27000 系列标准规定了信息安全管理体系的要求。它涉及信息安全的相关方面，并提供了组织控制、人员控制、物理控制和技术控制措施。

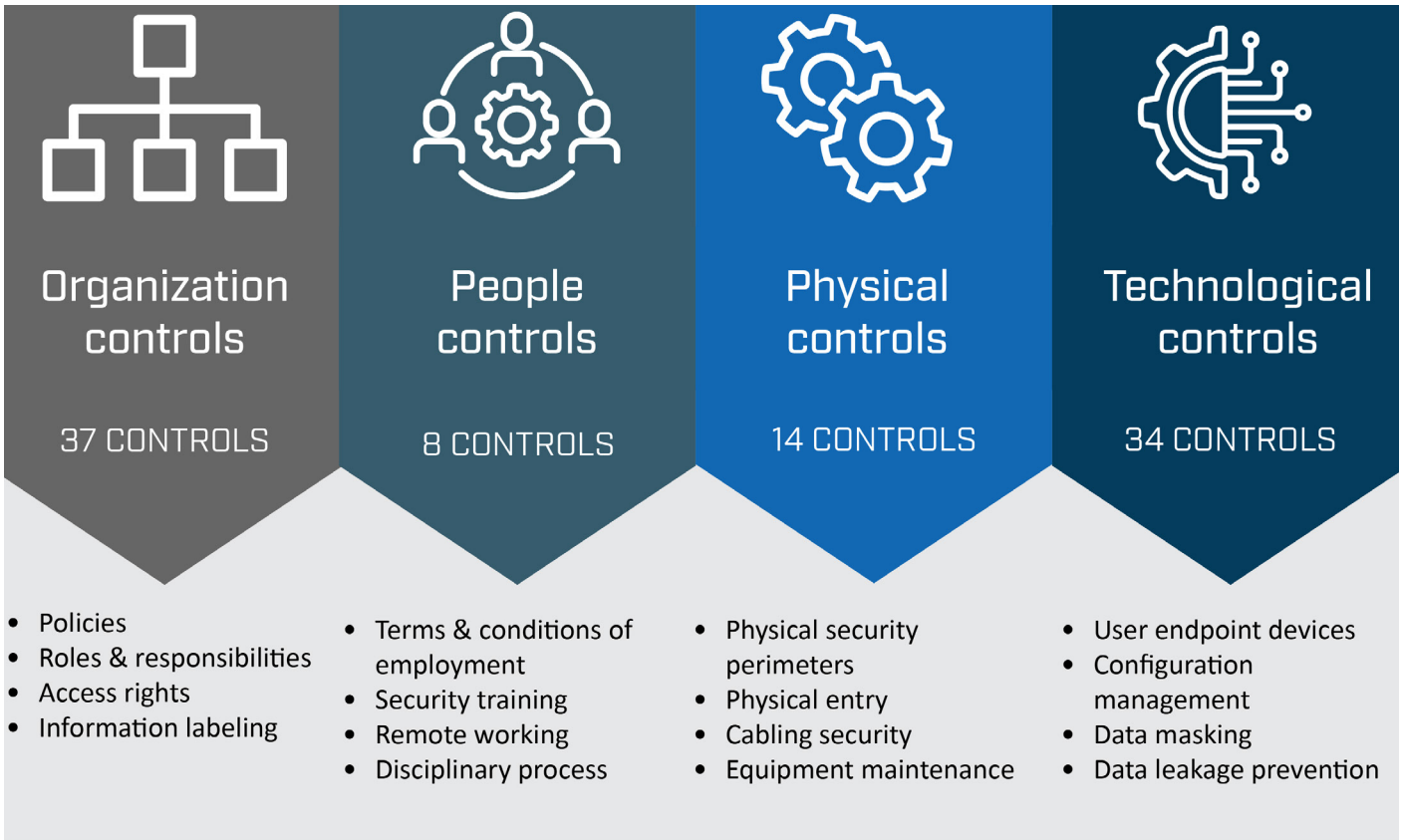


*图 6：ISO/IEC 27000 标准中信息安全管理体系的控制类别*

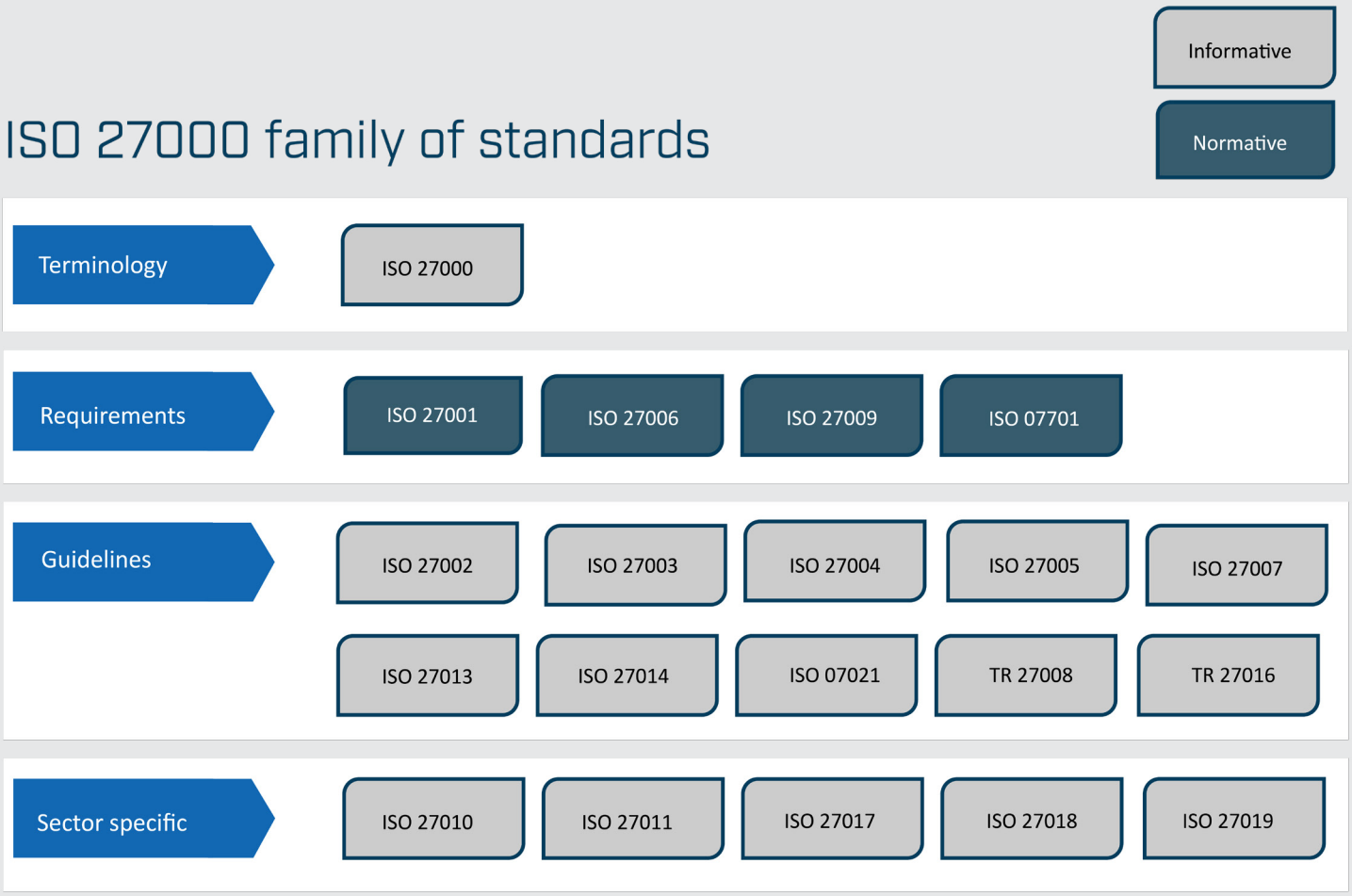


*图 7：ISO/IEC 27000 标准族包含 20 余项标准，这些标准既覆盖不同抽象层级的管控要求，也兼顾特定行业领域的专属需求。*

# 3. 设备制造商和机器制造商的网络安全要求

设备制造商和机器制造商的网络安全要求主要来自两个方面：

- 政府直接法规
- 客户的采购要求

此外，制造商自身也需具备良好的网络安全能力，以减少潜在经济损失并维护声誉。

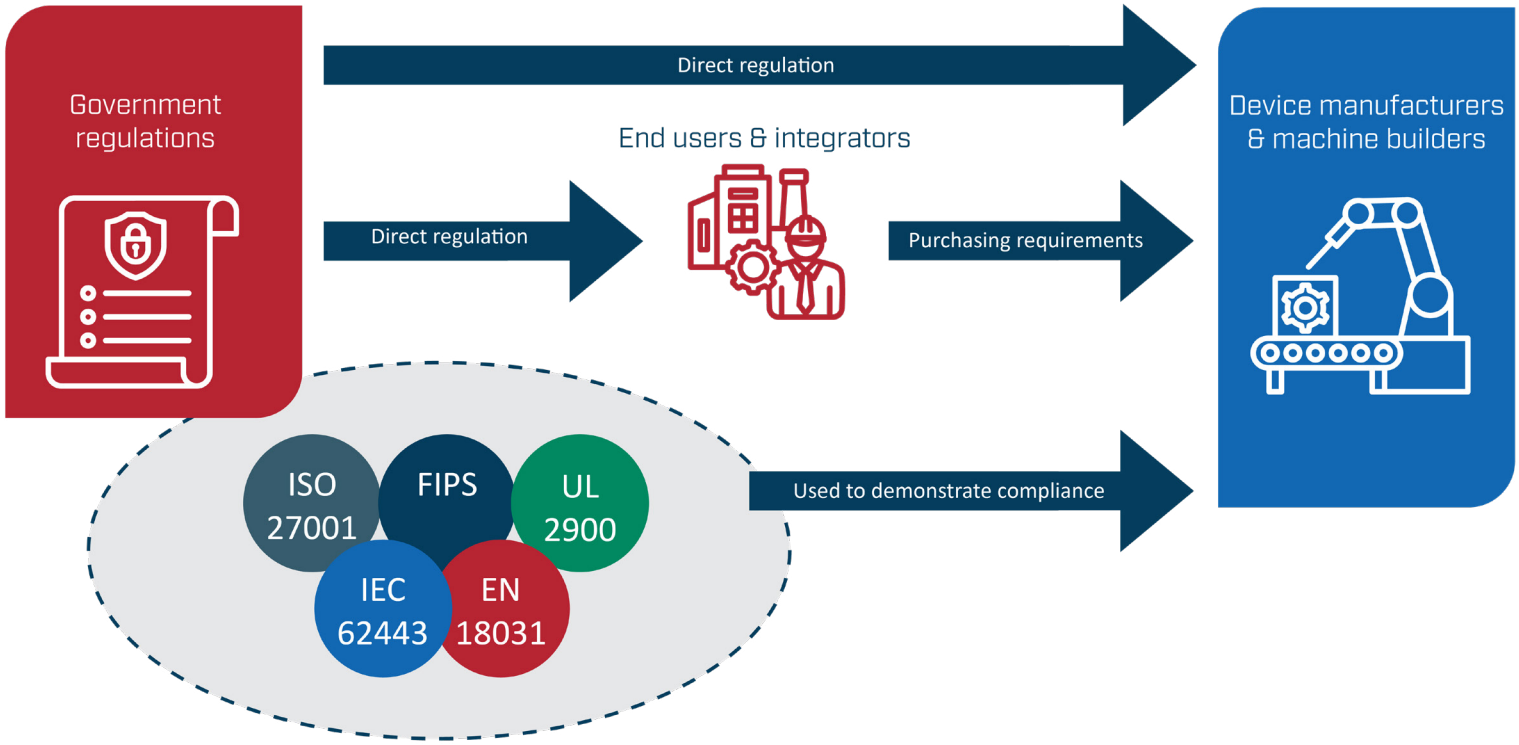


*图 8：面向设备制造商与机器制造商的网络安全要求来源*

为同时满足直接法规和采购要求，设备制造商和机器制造商需在产品中实现最低限度的网络安全功能，并对安全开发实践进行文件化记录。

为减轻合规负担，制造商可采用已通过预认证的网络接口。

这类接口已实现大部分必要的网络安全防护，并通过了相关网络安全标准的预认证。

欧盟《网络弹性法案》（CRA）已于 2024 年底获得批准，但目前必要的协调标准尚未完成制定。这给需要时间确保所有产品符合新法规的制造商带来了不确定性。

在采购要求方面，不确定性更大。因为终端用户和集成商目前对 NIS2 等法规的影响尚未完全明确，且需要将顶层要求转化为具体的采购条款。

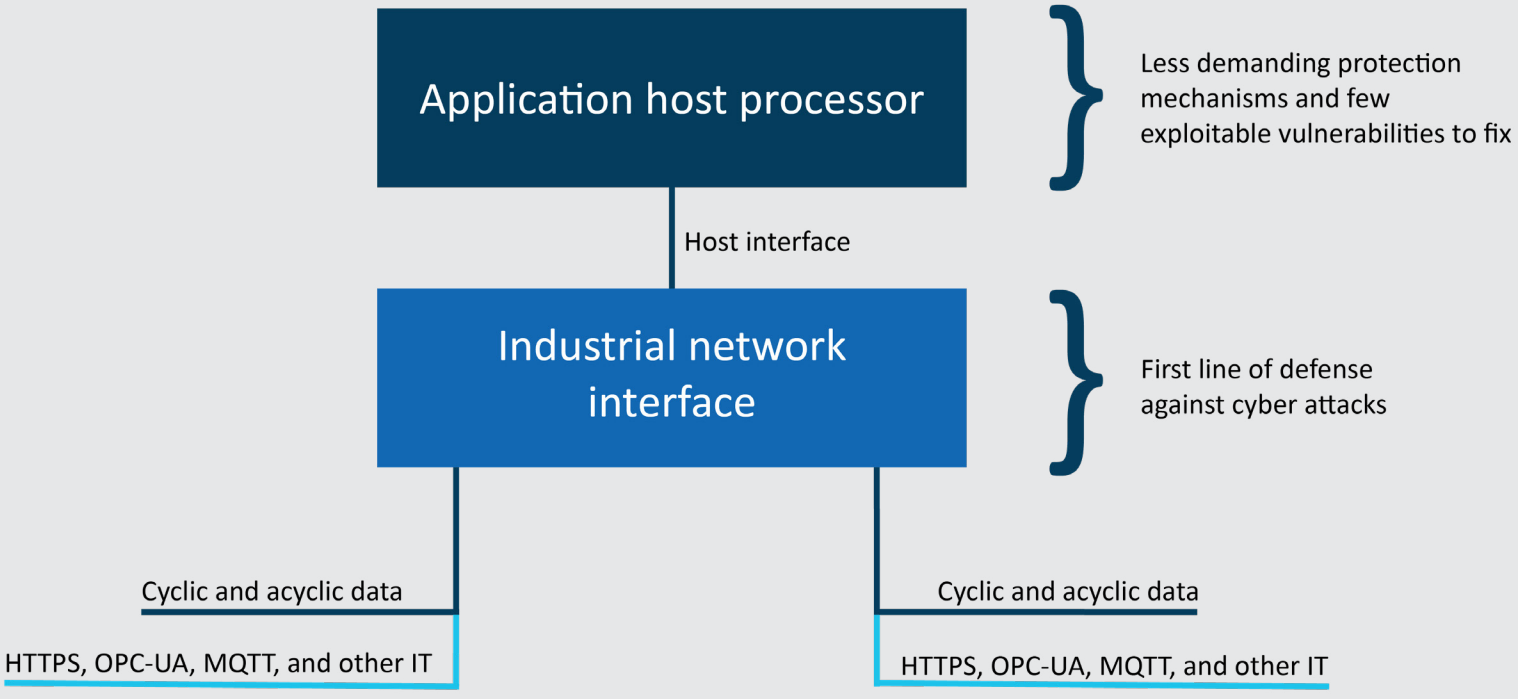


*图 9：预认证网络接口可作为抵御网络攻击的第一道防线*

以 CRA 为例，要在 2027 年 12 月后于欧洲市场合法销售产品，必须满足一长串的要求清单。

如下所示，采用预认证网络接口可以帮助制造商满足多项 CRA 所要求的任务：

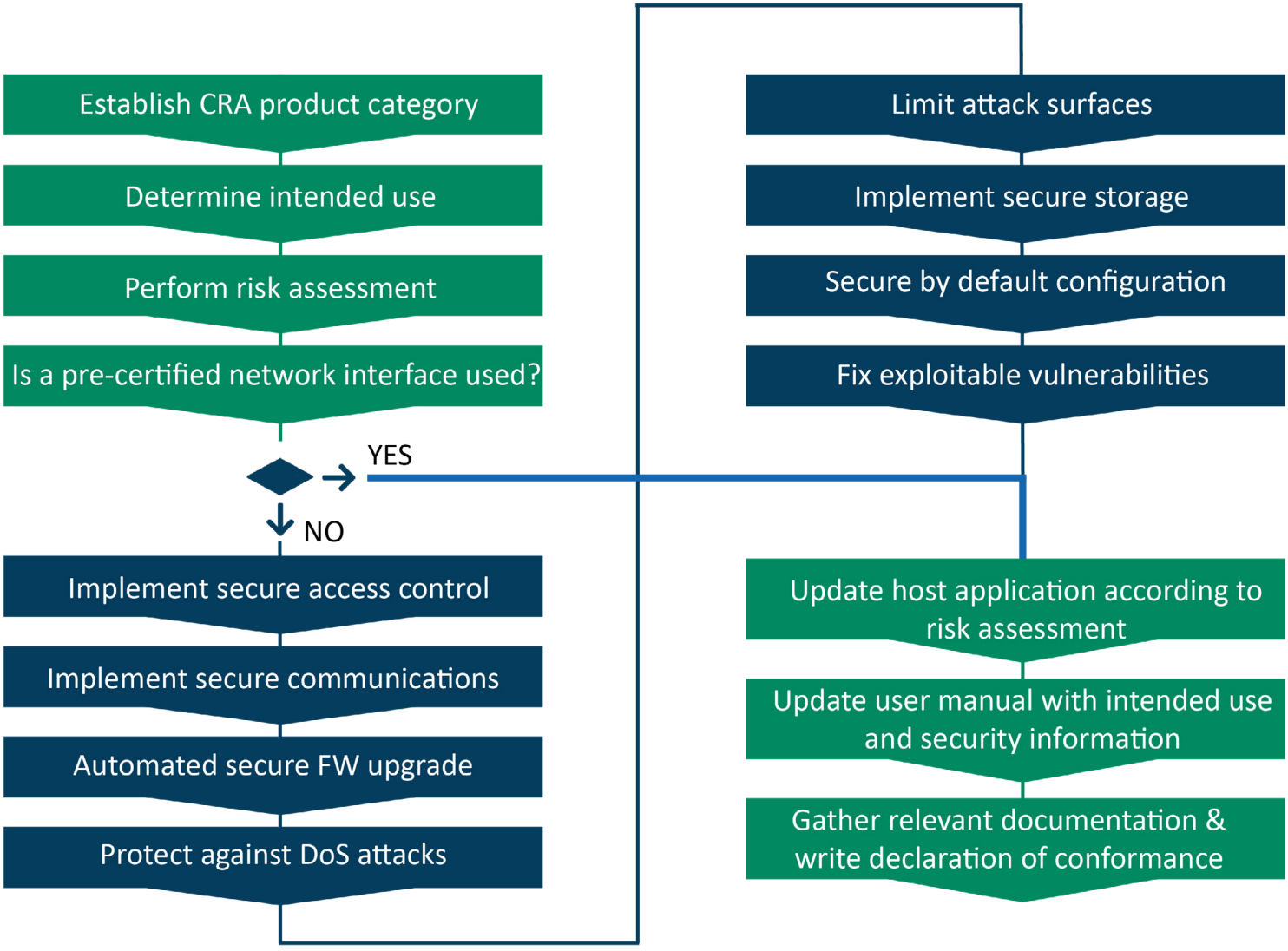


*图 10：网络弹性法案（CRA）合规工作流程及任务（突出预认证网络接口的应用优势）*

# 第 2 部分：HMS Networks 的网络安全

HMS Networks 是工业信息与通信技术（ICT）领域的市场领导者，拥有超过 35 年的行业经验。

全球已有数千家企业集成了超过 1000 万个 HMS Networks 产品，使其工业机器和设备能够高效通信并共享信息。

HMS Networks 致力于提供并维护客户可放心信赖的安全通信产品。作为一家经验丰富、运营稳定且财务稳健的公司，HMS Networks 有能力应对网络安全领域的长期挑战。

凭借行业领导地位、丰富的实践经验、深厚的技术专长以及对产品维护的坚定承诺，HMS Networks 的产品是各类制造商的安全选择，可将其设备或机器与 HMS 产品安全集成。

在 HMS Networks 内部，工业嵌入式通信接口的相关业务由工业网络技术（INT）事业部负责，并以 Anybus 品牌推向市场。

**“在 INT，我们专注于实时通信、工业控制和网络安全。我们视其为工业自动化的三大支柱。”**

*——HMS Networks 工业网络技术事业部高级副总裁 Bartek S. Candell*

如需了解更多关于 HMS Networks 的信息，请访问：
www.hms-networks.cn/about-us

# 4. HMS 安全标准与流程

### 信息安全管理体系与安全相关认证

HMS Networks 建立了信息安全管理体系(ISMS)，以确保最高水平的质量和安全。作为该体系的一部分，HMS Networks 严格遵循以下认证要求：

- ISO 9001: 产品开发流程符合 ISO 9001 标准，确保高质量与高可靠性；
- ISO 27001：建立了管理风险管并保障所处理数据和信息的保密性、完整性和可用性的体系；
- IEC 62443-4-1 ML3：Anybus 产品开发流程可满足成熟度等级 3 的要求，在整个开发过程及产品全生命周期内提供增强的安全管理。查看认证。

HMS Networks 严格遵守《通用数据保护条例》（GDPR）的相关规定。Anybus 嵌入式网络接口在运行时无需收集或传输任何用户个人信息。

如需了解更多信息，请访问：HMS 客户隐私政策 www.hms-networks.com/privacy-policy

### ISMS 实施的安全措施

为确保 Anybus 嵌入式网络接口在整个生命周期中的保密性和完整性，HMS Networks 实施了表 1 所述的安全措施：

| 要求 | HMS 实施方式 |
|---|---|
| 数据保密性 | 完全按照第 5.1 节所列安全相关认证的要求，实施 ISMS 控制措施。 |
| 安全的开发与生产环境 | • 仅向授权人员提供有限的物理和逻辑访问权限；<br>• 非工作时间锁闭大门并启动警报；<br>• 完整记录所有访问和变更操作，形成审计跟踪；<br>• 访客需由 HMS 员工全程陪同；<br>• 禁止拍照或类似记录行为。 |
| 全供应链完整性保障 | 软件对固件及基于 PC 的配置软件和驱动程序采用证书验证；硬件采用知名工业电子制造服务（EMS）供应商的产品，并对所有供应商进行审计；开展内部产品完整性检测，确保产品质量。 |

*表 1：安全措施*

### 设计即安全

安全已深度融入 Anybus 开发流程的各个环节，包括需求收集、设计、编码、测试、部署和文档编制。

### 安全培训员工

所有员工均须接受网络安全意识培训；开发人员还需额外接受安全编码培训，并参与源代码审查。

### 安全产品测试与验证

“设计即安全” 理念包括全面的测试环节，重点在于识别潜在漏洞。

我们执行以安全为导向的测试用例，旨在发现产品中可能被利用的非预期功能或配置问题。

表 2 展示了 HMS Networks 对 Anybus CompactCom 40 所采用代码的审查与测试方式。HMS 会根据产品具体要求选择相应的测试与审查项目。

产品发布后，HMS Networks 会定期进行产品接口测试，以确保产品具备抵御新兴威胁的抗风险能力。

| 审查或测试类型 | 合规要求 |
|---|---|
| 代码审查 | 所有代码在提交前均需经过审查 |
| 渗透测试 | 根据产品要求执行，测试产品相关部分 |
| 静态代码分析 | 使用 Synopsis Coverity 工具 |
| 模糊测试 / 稳健性测试 | PROFINET 版本使用 Netload；<br>其他版本使用 Achilles |
| 漏洞扫描 | 使用 Achilles 工具 |

*表 2：Anybus CompactCom 测试*

# 5. 产品文档和信息

### 产品文档、设计指南与符合性声明

专用的产品手册和网络用户手册全面描述了产品的功能和特性，并提供了在自动化设备中实施与配置产品的指导。

本安全设计指南是对现有产品用户手册的补充，重点提供与 Anybus 嵌入式网络接口设计和生命周期管理相关的安全内容与指导。

此外，产品安全数据表提供了详细且针对具体产品的安全信息与操作说明。

HMS Networks 会发布符合性声明文件，证明产品符合相关网络技术或地区标准（如欧盟和英国标准）。

上述文档可通过以下途径获取：

- HMS Networks 技术支持网页 —— 选择产品型号 / 支持与下载栏目： www.hms-networks.cn/technical-support
- Anybus CompactCom 开发者门户：：www.hms-networks.com/embedded-network-interfaces/developer-portal/overview

### 生命周期管理

HMS Networks 已建立完善的产品生命周期管理流程，可根据产品所处的成熟度阶段提供相应的功能与安全维护。如需了解产品特定详情，可参考相关产品的安全数据表。

更多信息请访问： www.hms-networks.cn/support/tech-support/product-life-cycle

### 新固件更新

如需获取产品的最新固件，请联系我们的技术支持团队。

若希望接收新固件发布的通知，请注册 HMS 客户与分销商信息系统（CDIS），并在我们支持页面的 “产品和安全警报” 栏目点击 “订阅警报”。
www.hms-networks.cn/technical-support

HMS 提供多种 用于更新 Anybus 嵌入式网络接口的解决方案，并在更新过程中通过专用机制验证固件的有效性。具体信息请参阅本手册的“最佳实践”部分及产品安全数据表。

### 开源软件的使用

HMS Networks 可能会在 Anybus 嵌入式网络接口中集成开源软件。这些软件被整合到产品固件中，HMS Networks 负责对其进行验证，并确保妥善处理相关的安全漏洞。

所使用的开源软件详细信息及相应许可信息可在相关网络指南中查找，这些指南可在 HMS Networks 技术支持网页获取：www.hms-networks.cn/technical-support

### SBOM 软件物料清单（SBOM）

根据客户要求，HMS 可提供相关固件的软件物料清单（SBOM）。

### 漏洞管理与沟通

安全漏洞相关信息会发布在以下网站，用户可直接通过网站订阅 RSS 提要，获取内容更新通知： www.hms-networks.cn/cyber-security

HMS Networks 设有“责任披露计划”，使任何人都可以通过该计划报告潜在的产品漏洞。更多信息，请访问 www.hms-networks.com/cyber-security/responsible-disclosure-program

### 无后门声明

Anybus 嵌入式网络接口不包含任何未公开的后门或针对外部接口的隐藏账户。

Anybus 嵌入式网络接口不具备远程访问功能，也不会与基于云的服务建立特定的外部通信连接。

# 6. Anybus 嵌入式网络接口连接概述

Anybus 嵌入式网络接口专为设备制造商集成设计，使其产品能够通过工业网络共享数据。

它们提供多种通信接口，涵盖以下功能：

- 工业以太网网络：用于与自动化控制器进行过程数据交换；
- 基于 Web 的功能：用于可选的配置与诊断；
- 工业物联网（IIoT）协议：用于与 IT 应用程序进行信息交换；
- 应用程序编程接口（API）：用于支持在主机应用程序内部集成。

关于这些通信端口、接口和协议的详细产品特定说明，请参阅相应的产品安全数据表。

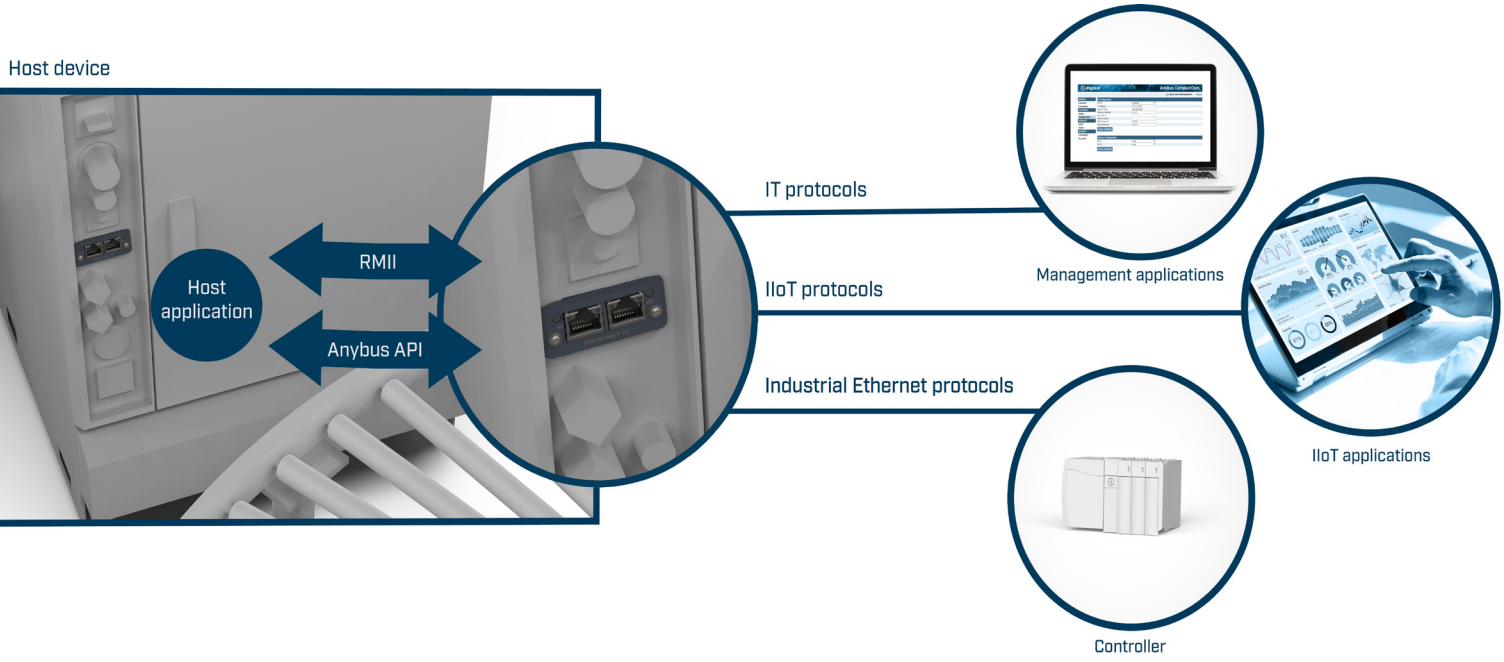


*图 11：Anybus CompactCom 40*

### Anybus CompactCom 40: 标准型与 IIoT 安全型

Anybus CompactCom 40 嵌入式网络接口提供标准型和 IIoT 安全型两种版本。

Anybus CompactCom 40 标准型侧重于基于串行或基于以太网的工业通信协议，仅包含少量面向 IT 的管理协议。

Anybus CompactCom 40 IIoT 安全型则结合了基于以太网协议（PROFINET 或 EtherNet/IP）、额外的 IIoT 协议（OPC UA、MQTT）以及 IT 管理通信功能，并提供了增强的安全特性。

有关各版本的详细信息，请参阅相关产品安全数据表。

### 工业以太网协议及其安全扩展的安全考量

为应对不断发展的网络安全要求，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以保护通信和应用程序。

目前，这些扩展涉及 PROFINET、EtherNet/IP、Modbus TCP 和 BACnet 协议，其实施状态从早期适用到持续讨论不等。而 POWERLINK 和 EtherCAT 协议目前尚无支持安全扩展的相关标准。

Anybus CompactCom 40 IIoT 安全型的设计符合网络安全最佳实践。

目前，安全工业以太网的市场接受度仍然较低，但从硬件角度看，该产品已具备支持加密型 OT 协议的能力。此外，我们已与其他厂商进行了相关测试：

- 在 modbus.org 框架下完成了 Modbus 安全协议的互操作性测试；
- 与 ODVA 内的其他厂商合作集成了 CIP 安全协议，并在全球行业展上进行了演示。

### 串行工业网络的安全考量

基于串行的网络主要事逻辑隔离的通信网络，这意味着发起网络攻击需要高度针对性的投入，因此这类网络的漏洞暴露风险较低。

因此，本文档不涉及支持基于串行工业通信协议的 Anybus CompactCom 产品。

# 第 3 部分：最佳实践与安全集成

本部分概述了设备制造商在集成 Anybus 嵌入式网络接口时应遵循的最佳实践，旨在帮助制造商增强其设备或机器的安全性，并为即将到来的安全法规做好准备。

本部分重点介绍我们最新的 Anybus CompactCom 40 产品系列 —— 这是目前处于活跃产品阶段的最新接口系列，HMS Networks 承诺该系列将满足未来的 CRA 要求。

注：本最佳实践列表并非详尽无遗，也不能单独保证符合任何法规要求。每个项目和应用都应单独进行风险评估，并根据所需安全等级确定相应措施。

下文所述功能的详细信息及集成方法，请参阅相应的产品用户手册。

# 7. 预期用途 —— 选择合适的 Anybus CompactCom

### 安全集成

Anybus CompactCom 应集成到最终产品中。最终产品应确保未经授权的人员无法访问其主机接口或任何内部部件。

若未授权人员获得主机接口的访问权限，则可能会窃听通信内容并修改配置。

Anybus CompactCom IIoT 安全型支持安全通信，其机密加密密钥存储在安全芯片中，即使能够物理接触硬件，也无法读取这些密钥。

### 安全网络

由于工业以太网协议本身不具备安全特性，因此 Anybus CompactCom 应仅连接到可信网络。

Anybus CompactCom IIoT 安全型支持除工业以太网之外的其他协议的安全通信。

这些协议可在不可信网络中使用，但仍必须确保不可信网络无法访问工业以太网通信，这可通过防火墙或数据二极管即可实现。

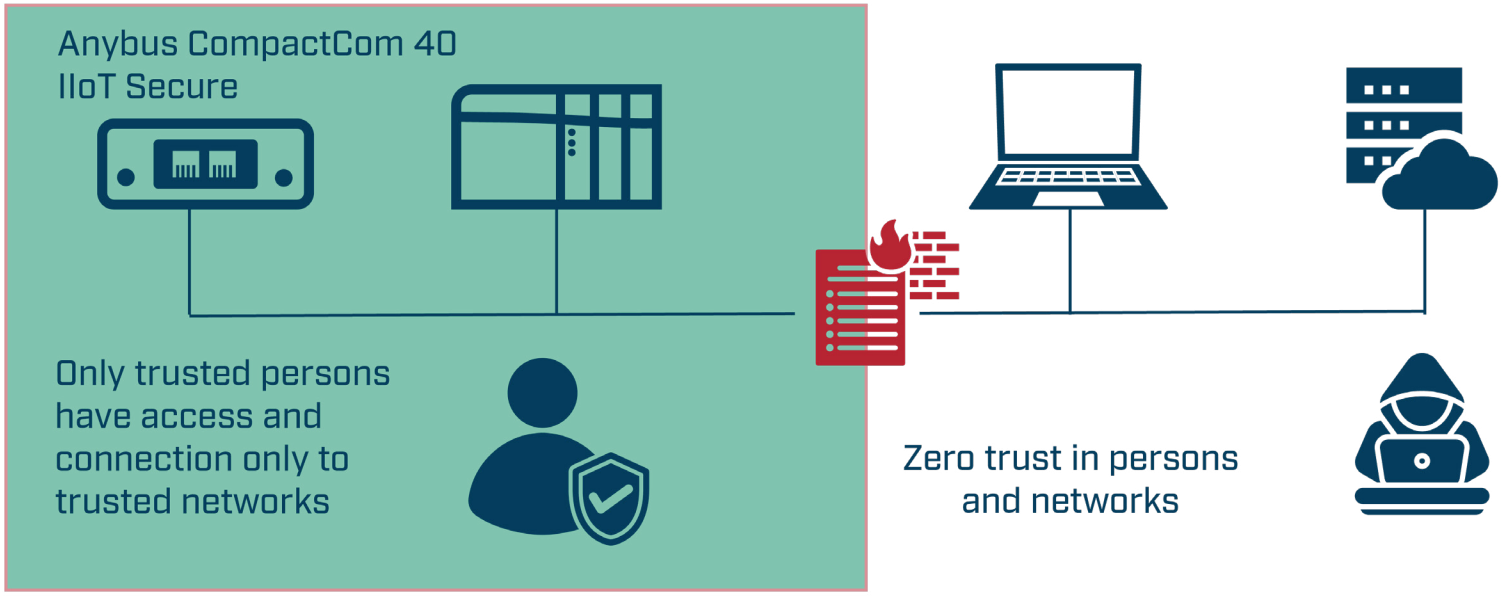


*图 12：Anybus CompactCom 40 IIoT 安全型的预期用途示意图*

### 选择合适的 Anybus CompactCom

Anybus CompactCom 40 工业以太网标准型适用于可信环境和可信网络内的工业应用（见 CRA 部分）。

该标准型适用于所有工业协议（基于串行或以太网）。

对于既需工业以太网通信，又需 IIoT 或 Web 服务器连接的应用场景，Anybus CompactCom 40 IIoT 安全型是最佳选择。该版本提供额外的安全功能，可减少客户对额外外部安全措施的需求，并支持在可信网络之外进行安全通信。

Anybus CompactCom 40 IIoT 安全型也是一个面向未来的解决方案，能够满足长期的安全要求和加密型 OT 通信扩展需求。这种演进主要通过固件更新来实现。

由于采用了通用的 Anybus 主机 API，使用标准型 Anybus CompactCom 40 的现有应用可以轻松升级到 IIoT 安全型，所需工作量极小。

### 默认安全 - 通信接口

制造商必须关闭或禁用 Anybus CompactCom 上所有与设备应用无关的逻辑或物理接口。

- 停用任何未使用的物理通信端口（如第二个以太网端口）；或为终端用户提供启用 / 禁用未使用以太网端口的功能；
- 禁用任何设备预期运行不需要的通信功能（如 Web 服务器、FTP、SNMP 等）；
- （尽可能）激活协议（如 MQTT 或 OPC UA）的加密功能。

### 配置、备份与恢复

本章概述了 Anybus CompactCom 40 接口以及确保设备设置可靠备份和恢复的推荐方法，旨在简化设备配置、提升安全性，并在整个设备生命周期内保持可预测的行为。

### 一般建议

在配置 Anybus CompactCom 40 接口时：

- 限制配置点：使用单一接口或尽可能少的接口来定义设备的行为和配置；
- 安全配置通道：优先选择安全通信接口。如果可用，应定义访问权限并为用户分配具备配置权限的角色（例如，通过 IIoT 安全型的集成 Web 服务器）；
- 规划备份与恢复：尽可能采用支持设置备份和恢复的配置方法；若该功能并非固有的，应在设备应用程序中实现。

### 在主机应用程序中指定固定功能和行为

对于具有静态行为或固定通信功能的设备应用，应优先直接在主机应用程序固件中实现这些功能。

- 这确保了设备行为的一致性和可预测性，无需单独的备份或恢复步骤。
- 固件定义的行为可以作为标准固件更新的一部分进行更新，从而在不同设备版本中保持预期的操作。

**核心优势：**简化维护，并消除了对固定功能进行外部配置管理的需要。

### 利用网络描述文件进行用户设备配置

如果您的设备支持用户定义的选项，例如可变数据映射或可选行为，请利用 GSD、EDS 或类似的网络描述文件等工业协议初始化机制。这些文件：

- 允许用户在 PLC 环境中定义配置参数。

- 在每次初始化过程中自动将参数传输至设备；
- 将配置信息存储在控制器项目文件中，确保持久性和一致性。

**核心优势：**支持灵活的、用户特定的配置，无需在设备上进行手动干预。

### 通过专有软件工具进行设备配置

若设备需要通过专用软件工具进行配置：

- 主机应用程序应从工具接收配置数据或文件。
- 并通过 Anybus CompactCom 40 主机 API 存储和应用配置。

在此配置中，必须在专有工具和主机应用程序中解决以下问题：

- 配置数据的备份和恢复能力；
- 对敏感配置参数进行身份验证和访问控制。

**核心优势：**集中管理配置数据（主机应用程序和通信接口），同时确保安全性和可恢复性。

### 通过 Anybus Web 服务器进行配置

Anybus CompactCom 40 中 的集成 Web 服务器可用于配置网络设置，并托管用于设备特定配置的自定义网页。需注意以下要点：

- 内置 Web 服务器不支持配置参数的备份或恢复；
- 制造商必须实施访问保护和用户身份验证以保护配置接口的安全；
- 对于 IIoT 安全型，web 服务器支持：
  - 加密通信
  - 基于用户和角色的访问控制。

但即使在这些版本中，备份和恢复功能仍不可用。

**核心优势：**提供了便捷的配置接口，特别适合需要远程设置的设备，但用户需自行负责备份策略。

### 访问保护与用户管理

当使用文件传输协议（FTP）或 Web 服务器等 IT 管理功能时，应建立适合特定应用需求的用户结构。

该结构应定义不同的用户角色，每个角色分配不同级别的访问权限。激活接口的用户名和密码身份验证功能，并使用复杂密码防止未经授权的访问。

### 标识与版本控制

利用 API 中的 Anybus 标识对象来获取设备的版本、状态和诊断信息。Anybus CompactCom 40 使用各自协议规范中专用标识元素或机制，以标准化方式与应用控制器或网络管理工具共享此资产管理信息。

相关信息元素或机制可在 Anybus CompactCom 网络指南中查询。

### 提供文档

应提供全面的设备文档和安全说明，概述基于 Anybus CompactCom 40 功能实现的全局设备接口能力。请使用提供的 Anybus CompactCom 40 安全数据表来创建设备安全说明。

为保持整个系统的有效版本管理，应集成与 Anybus CompactCom 40 相关的版本控制，这包括主机应用程序和固件的特定组件，这些信息可以体现在 Anybus CompactCom 接口中。

制造商可（或应）在其自身文档中包含 Anybus CompactCom 40 所使用的开源软件或硬件相关的 HMS 声明，并根据其实现情况进行补充。HMS 开源声明可在相关网络指南中找到。

### 确保网络通信合规

确保整个设备实现通过相关工业网络的性能和一致性测试，以获得网络认证。HMS 确保每个新的硬件或固件版本都符合相应协议技术并进行预认证，从而简化集成该接口的设备的合规流程。

根据不同的网络组织政策，在整个设备生命周期内保持网络合规性为最新状态。

### 保持设备更新

保持 Anybus CompactCom 模块为最新状态，以维持高水平的安全性。

请随时了解 Anybus CompactCom 产品动态、固件更新和安全公告，并注册我们的主动通信渠道（参见相应章节）。

制造商有责任评估 HMS 发布的产品变更通知和安全公告对其设备应用的相关性和影响。

更新时请不要忘记更新版本信息，以确保现场安装设备的准确可追溯性。

### 停用

停用 Anybus CompactCom 时，执行恢复出厂设置将清除存储在 Anybus CompactCom 上的用户账户和特定模块配置信息。

# 与 HMS 合作
# 是实现工业通讯和
# 工业物联网的最佳选择！



www.hms-networks.cn