白皮书

# 内置网络安全：EtherCAT 提供经过验证的防护

**Guido Beckmann 博士** [1]，技术委员会主席，EtherCAT 技术协会（ETG）
**Florian Essler**[1], 一致性技术工作组主席，EtherCAT 技术协会（ETG）
**Torsten Förder**[1], 网络安全专家, Beckhoff Automation
**Alexander W. Koehler**[2], S&S 网络安全首席安全顾问， 德国 UL Solutions 公司
**Fatma Kotzaoglan**， 高级项目工程师 ， 英国 UL Solutions 公司
**Martin Rostan**, 执行董事 ， EtherCAT 技术协会（ETG）

1 欧洲电工标准化委员会 TC65X WG3 网络安全工作组 成员
2 德国电工委员会 TBKON 合格评定网络安全顾问委员会 主席

**EtherCAT 提供的网络安全功能和系统安全保障符合 IEC 62443 标准中安全等级 2 的网络安全要求。对于几乎所有常见应用场景，EtherCAT 协议无需任何修改或扩展即可满足《网络弹性法案》（CRA）的要求。对于最高安全等级 3 的攻击防护，向后兼容的软件扩展即可满足要求。UL Solutions 对此予以证实，该机构对基于 EtherCAT 现场总线的三种系统进行了评估，并根据 IEC 62443-3-3 标准完成了认证。**

欧盟《网络弹性法案》（CRA）也将网络安全提上了现场总线系统的议事日程。CRA 规定了在欧盟境内销售的含数字元件产品的网络安全要求；这不仅涵盖自动化组件，还包括搭载这些组件的机器和系统。亚洲和美国也在起草类似法规，使这一议题成为全球关注的共性问题。

因此，未来现场总线系统也必须符合 CRA 的要求。业界正以截然不同的方式应对这一挑战。

传统的现场总线系统以及某些工业以太网系统都采用了一种"单元保护"的理念--本质上是 OT 领域的 "IT 分区"：单元或区域与外部的通信通过防火墙、加密和访问控制等 IT 安全措施进行保护，因此单元内部的通信和组件无需额外的保护。然而，要实现有效的防护，必须确保单元内部不会发生任何因疏忽或蓄意导致的网络攻击：因此，必须有效防止操作员和其他人员直接访问现场总线。

如果现场总线系统被限制在一个上锁的控制柜内，这种方式或许奏效。但是，如果防护单元覆盖了整个机器或工厂，且现场总线电缆在物理上可以触及，情况就会变得棘手。分区防护理念也与"从传感器到云端"的一体化理念相悖——这曾是某些总线架构的核心卖点，如今却因安全合规的要求沦为过时设计。

其他方式则需要将 IT 安全集成到每一个现场设备中。由于认证加密技术已延伸至 I/O 模块，即便是操作人员可直接访问的工业以太网系统，也同样能满足 CRA 的要求。然而，这不仅会明显降低总线系统的性能，还会增加系统复杂性：管理必须定期更新的证书，不仅会使系统调试过程变得复杂，更重要的是，还会大大增加机器和系统的维护难度。

由于 EtherCAT 采用标准以太网帧（IEEE 802.3）和标准以太网物理层，人们有时会想

当然地认为：在网络安全层面，必须将其等同于普通以太网，并采用基于交换机的以太网网络所通用的 IT 安全措施进行防护。

然而，这种说法不完全正确。EtherCAT 独特技术特性使诸多在 IT 领域常见的攻击场景从一开始就不可能发生，因此无需采用常规的防护措施。倘若忽略这一点，IT 安全专家将检查标准的 IT 措施是否落实到位，而如果缺乏此类措施，通常会导致安全评级下调。但这种做法完全忽视了 EtherCAT 的独特特性，无异于要求电动汽车加装柴油颗粒过滤器，毫无意义。

EtherCAT 则另辟蹊径，基于工业自动化与控制系统网络安全国际标准 IEC 62443 进行设计。IEC 62443 被认为是这一领域的国际公认标准，目前欧洲业界正将其扩展为 CRA 评估系统和组件的基础。该标准同样高度适配 CRA 法案，因为二者都遵循基于风险的方法：仅采取必要的网络安全防护措施，而非一味堆砌防护手段。在开展风险评估时，必须结合具体应用场景与攻击潜在危害程度综合判断：一台工业洗衣机面临的安全风险，远远低于关键基础设施的配电系统。

IEC 62443-3-3 描述了系统级（非单个组件）安全要求，因此是适用于 EtherCAT 这类总线系统的合适标准。

该标准将七项基本要求细分为 100 多项系统要求，并采用安全等级来划分相对应的攻击强度。

安全级别（SL）1 对应防范意外或非故意的中断，例如工厂网络中由恶意软件或勒索软件引发的中断。SL 2 涵盖了由无专业技能的攻击者发起的针对性攻击。SL 3 假定攻击者具备专业知识、相应的资源和攻击动机。SL 4 针对的是通常只有国家级主体才具备能力与资源的攻击者；针对此类攻击几乎无法实现有效防护，且在多数场景下缺乏经济性。

## EtherCAT 的工作原理

想要理解 EtherCAT 独特的技术特性，进而掌握其特定的网络安全机制，就必须先了解其工作基本原理。简要概述如下：

EtherCAT 是一种工业以太网技术，由主站设备（通常为自动化系统控制器）发送以太网数据帧，经由从站设备（即现场设备）进行实时处理。主站设备按照 IEEE 802.3 标准，通过带有介质访问控制器（MAC）的传统以太网接口发送数据帧。从站设备不使用 MAC，而是采用特殊的 EtherCAT 从站控制器（ESC）。ESC 本身不能发送数据帧。

EtherCAT 采用“on-the-fly”即时处理原理。与传统工业以太网网络不同，传统工业以太网中，MAC 先接收发往现场设备的以太网帧，再将其转发至主控制器的软件协议栈进行处理；而 EtherCAT 可在 ESC（从站控制器）中对数据帧进行持续处理。因此，EtherCAT 从站设备在接收数据帧的同时可转发该帧。在此过程中，数据帧仅经历极小的物理传输延时。“on-the-fly”即时处理原理要求 ESC 功能必须采用硬件实现：由于数据帧在任一给定时刻仅有少量 bit 可被访问，留给数据处理的时间仅有几纳秒。因此，ESC 功能无法通过软件实现。从网络安全角度来看，EtherCAT 从站控制器（ESC）采用硬件实现具备一大优势：想要对其进行篡改入侵需要付出高昂的代价。

此外，帧的处理始终具有固定的延迟。现场设备中的应用控制器无法访问芯片部分核心功能：例如，决定从经过的以太网帧中提取或向其中插入哪些数据的设置，只能通过 EtherCAT 总

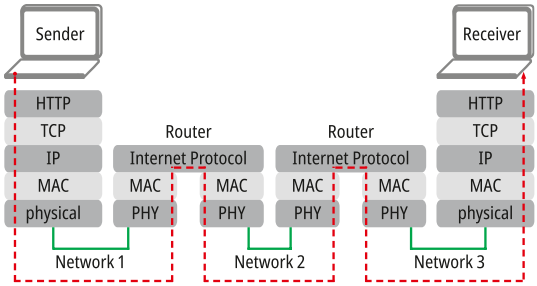
线系统（即由主站设备）从外部进行修改，而不能被现场设备中可能存在故障或已被篡改的固件私自更改。

## EtherCAT 系统特性

现在我们来探讨 EtherCAT 具体系统相关特性，以及这些特性对抵御潜在网络安全攻击的意义。

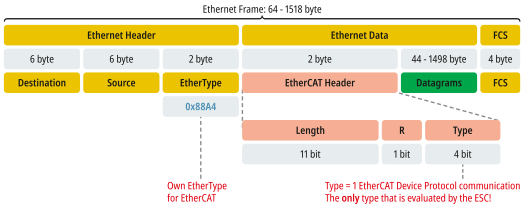
1. EtherCAT 系统架构最大限度缩小了攻击面。数据帧经过从站设备时，没有任何软件协议栈能够访问，仅由硬件逻辑完成处理。传输介质中仅存在 EtherCAT 帧。只有主站设备可以生成 EtherCAT 帧。

2. EtherCAT 协议直接封装在以太网帧中，因此位于 ISO-OSI 模型的第二层。第三层的互联网协议（IP）不用于传输 EtherCAT 有效载荷数据。由于 IP 的主要功能是跨子网路由数据，而恶意软件实际上几乎总是依赖 IP 层存在，因此直接封装在以太网帧内部的恶意载荷无法跨越子网边界。这意味着 EtherCAT 现场设备天生具备抵御常见恶意软件攻击的能力。



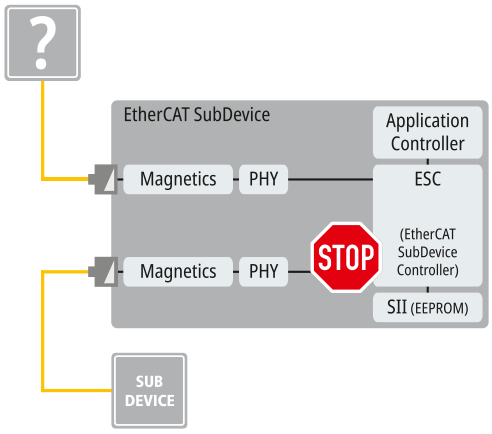

*IP 是恶意软件路由的先决条件*

EtherCAT 使用其专有的 EtherType（0x88A4），其后紧跟 EtherCAT 报文头。根据数据帧和 EtherCAT 报文头，EtherCAT 从站控制器可即时识别传入的数据帧是否为 EtherCAT 帧。




*EtherCAT：直接嵌入在以太网帧中*

所有其他类型的帧均由 EtherCAT 从站控制器硬件直接丢弃；因此，进入 EtherCAT 网段的非 EtherCAT 帧，会被下一个现场设备可靠地移除。这意味着从一开始，通过非 EtherCAT 帧发起的攻击就无从实施。



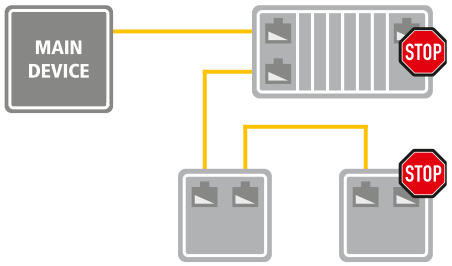

*ESC 销毁所有非 EtherCAT 帧*

3. EtherCAT 从站设备无法修改未寻址到它们的数据。这同样适用于过程数据和参数数据。由于 FMMU（ESC 中负责本地与全局内存间过程数据映射的硬件单元）无法通过从站设备的本地 ESC 接口进行配置，因此即使现场设备的固件遭到意外或恶意篡改，也无法在总线上激活 FMMU。即便有现场设备被

软件篡改并接入网络，也无法对其他设备造成任何影响。

4. 网络启动时，EtherCAT 主站可查询所有已接入从站的设备属性，并检测网络拓扑结构。查询的详细程度可根据应用程序的要求进行调整：例如，主站在启动时可仅查询设备类型及其通信属性，也可以同时比对固件版本和序列号，从而不仅能检测新增设备和拓扑结构的变更，还可以识别设备的更换。

5. EtherCAT 从站控制器最多可拥有 4 个端口，因此支持多种网络拓扑结构。主站可禁用未使用的端口，并从硬件层面进行封锁。




*禁用未使用的端口*

在这种情况下，通过未使用的端口接入设备无法建立逻辑连接：即便链路信号已连通，与 ESC 的通信仍会被阻断。因此，通过接入空闲端口实施的攻击完全无效，甚至可能通过额外的链路被检测到。

6. EtherCAT 网络中的数据流量可通过“网络监测仪”来进行监控与分析。监测仪属于硬件设备，必须安装在主站与现场设备之间，或是两台现场设备之间的网络中。但这些设备无法篡改数据，仅能接收数据。因此，监测仪可用来记录数据流量，但不能修改数据。仅凭记录的过程数据内容推断出机器或系统的功能极为复杂，若无法掌握那些未通过总线传输的机器机械结构和系统属性（如过程变量的命名），几乎无法实现。因此，如果攻击的目的是摸清机器或系统的工作原理，那么针对控制系统的攻击往往更具可行性、效果也更好。

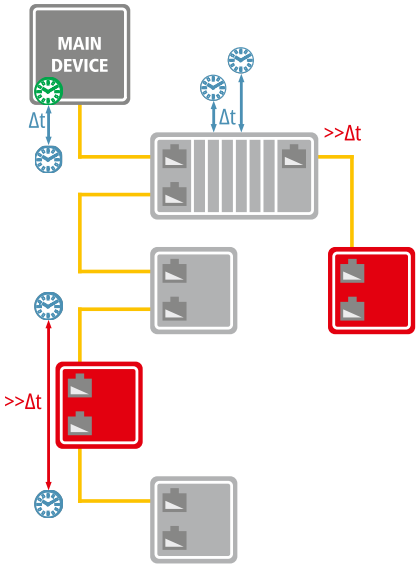
7. 尽管 EtherCAT 本身不采用互联网协议（IP），但该技术可通过“Ethernet over EtherCAT”扩展功能，对任意以太网流量进行隧道传输；例如从现场设备的网络服务器检索数据、传输 OPC UA 或其他协议，包括基于 IP 的流量。由于该数据流是通过隧道传输，因此其内容与 EtherCAT 本身的功能和所有参与传输的设备完全无关。但原则上，这可能会危及隧道末端防护不足的现场设备的安全--即隧道数据流的指定接收方设备。如果需要考虑防范此类攻击风险并采取措施缓解，可在主站中全局禁用或选择性禁用“Ethernet over EtherCAT”协议。

8. 得益于 EtherCAT 的高效率，主站设备可在每次上电启动时向从站设备写入配置数据。因此，所有离线写入设备的配置都会被覆盖，从而也让这种攻击途径失效。

9. 关于拒绝服务（DoS）攻击：由于入站数据帧由 ESC 硬件进行处理，突发流量不会造成影响，EtherCAT 帧可被即时处理。ESC 内部的三缓冲区机制可确保始终有内存可用于接收传入的过程数据，即便设备固件无法及时清空缓冲区也不受影响。参数等非周期性数据均采用应答确认，因此协议栈不会出现

过载。非 EtherCAT 数据帧会由 ESC 硬件直接丢弃。因此，DoS 攻击无效。

10. 如图所示，由于 EtherCAT 从站控制器的自身特性，从站设备既无法自行修改数据，也不能独立发送数据帧。因此，接入从站设备也无法构成有效的攻击场景；此外，在 EtherCAT 系统中，可通过信号传播时间的变化检测到新增设备。ESC 芯片测量帧传播延迟的精度远低于 50 纳秒。EtherCAT 主站读取这些值，以确保分布式时钟的高精度同步。如果这些值出现明显偏差（如重启后），则表明网络拓扑结构发生了变化，通常发生在接入设备时。




*通过 EtherCAT runtime 测量可检测出已接入的从站设备。*

11. 即便接入搭载专用“恶意” EtherCAT 从站控制器硬件的从站设备，也能通过该方式被检测出来。研发此类芯片需要深厚的专业技术知识和巨大的投入，因此这种攻击方式效率极低。只有在极少数系统中，才有可能实现这样的效果--在此情况下，大概是指对系统进行破坏--在经济层面值得投入这样的成本。或者说，通过其他非 EtherCAT 系统的攻击方案来实现这一目的不是更简单、更经济吗？

## 那么控制系统呢？

除 EtherCAT 之外，大多数 EtherCAT 控制系统还配备有其他接口，例如用于连接上层网络的以太网接口、存储卡插槽以及 USB 接口。EtherCAT 现场设备还可能具有其他类似的接口。当然，必须采取适当措施，严密保护这些接口以免受网络安全攻击！网络安全策略的这一核心部分不受 EtherCAT 网络影响，因此不纳入 EtherCAT 的安全考量范畴。

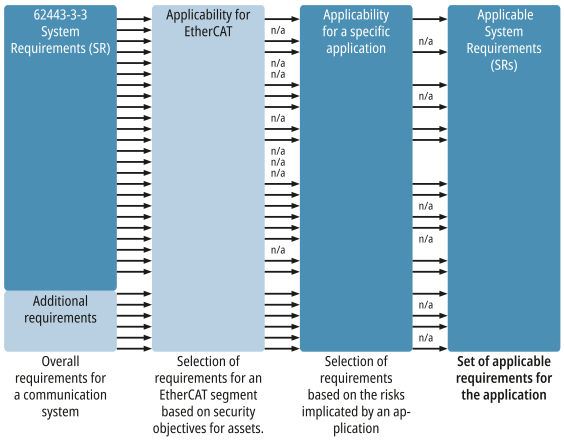
根据设计初衷，EtherCAT 主站实施广泛，从适用于低要求应用的简易设备，到支持更多 EtherCAT 功能的高性能控制器，不一而足。EtherCAT 的某些安全特性也取决于主站的实施。例如，并非所有控制器都会在启动过程中检测网络的变化，也并非所有控制器都会默认禁用从站设备上未使用的端口。因此，为了满足相关的网络安全要求，有必要选择合适的主站设备或控制器。

EtherCAT 技术协会（ETG）制定了行规规范，为终端用户、系统集成商、设备制造商及机械厂商提供指导，明确必须采用和实施哪些安全措施，以达到适当的安全等级。

## EtherCAT 无需更改即可达到安全等级 2

基于上述系统特性，即便不启用特定的安全扩展技术，EtherCAT 技术也已满足抵御安全等级 2 级别攻击的系统所要求的网络安全标准。这一点已通过综合分析得到验证：针对典型的 EtherCAT 工厂网络，对 IEC 62443-3-3 标准中 100 余项系统要求逐一进行了详细审查与评估。德国 UL Solutions 公司已在三种典型应用

场景下对运行中的 EtherCAT 协议的安全性进行了评估；并根据上述威胁场景筛选出的安全能力要求，颁发了三项 IEC 62443-3-3 证书。这三份证书由丹麦的 UL Solutions (Demko) 颁发，该公司是 IECEE 认可的国家认证机构，依托 IECEE 全球互认协议（MRA）网络，在欧盟及全球范围内均具备认证效力。




*系统要求：针对所考量场景下的 EtherCAT，开展适用性及合规程度评估。*

## 无需更改硬件，仅通过软件即可实现更高安全等级

对于需要防范攻击者安全等级 3 的系统，仅需在主站和配置工具中增加软件扩展功能即可满足防护要求。UL Solutions 也证实了这一点。因此，从站设备无需任何改动。除此之外，系统会启用 runtime 检测机制来抵御该等级的攻击强度，如前文所述，该功能可识别 EtherCAT 网段内新增的设备。

在 EtherCAT 中，设备描述文件被篡改带来的网络安全风险是可控的：毕竟这类文件仅由生成网络配置的工具读取一次。

修改后的文件可能会导致设备运行行为异常，而这类问题大概率会在系统调试和功能测试阶段被发现。如若没有：EtherCAT 技术协会（ETG）正在自建证书颁发机构（CA），以便 ETG 会员能够便捷、统一地对 EtherCAT 设备描述文件及软件进行签名和认证。

## EtherCAT 可选加密功能，无需证书管理

仅有极少数应用场景下，用户才需要对通过总线系统传输的过程数据和参数数据额外加密，以防止被窃听：尽管“加密”常出现在众多网络安全检查清单中，但在实际应用中，数据泄露可能造成的损失和风险通常微乎其微。针对网络安全要求极高的系统，EtherCAT 技术协会（ETG）正在扩展 EtherCAT 标准（并保持完全向后兼容）；引入一种量子安全的认证加密方法，可按需对全部数据或部分数据进行加密防护。密钥分发无需证书，省去了因证书到期而进行续期的工作，大大简化了管理。"完全向后兼容 "甚至意味着 ESC 芯片无需任何更改：该功能完全可以通过软件方式在主站和从站中进行增补实现。

参考文献：

**UL Solutions：3 项证书 IEC 62443-3-3 及技术报告 TRF**：EtherCAT 技术安全能力评估解决方案应用。由 IECEE 认证机构 UL Solutions (Demko) Denmark 颁发：DK-177530-UL/DK-178394-UL/DK-178399-UL. IECEE CBTL（测试实验室）：UL Solutions Northbrook, IL, USA.