IEC 62443系列标准：如何防御基础设施网络攻击

Christophe Tremlet，业务管理总监

摘要

本文探讨了IEC 62443系列标准的基本原理和优势。该标准包含了旨在确保网络安全韧性并保护关键基础设施和数字工厂的一系列协议。这一领先标准提供了一个全面的安全层；不过也为寻求认证的相关人员带来了一些挑战。本文将详细阐释安全IC如何为需达成工业自动化控制系统(IACS)组件认证目标的组织提供必要的帮助。

简介

尽管网络攻击的潜在威胁日益增加，但工业自动化控制系统(IACS)在采纳安全措施方面进展缓慢。部分原因在于此类系统的设计人员和运营人员缺乏共同的参照标准。IEC 62443系列标准为构建更安全的工业基础设施提供了一条途径，但企业必须学会如何应对其复杂性，并理解这些新挑战，以成功地加以应用。

工业系统面临风险

供水、污水处理和电网等关键基础设施进行了数字化转型，因此不间断访问这些关键基础设施对于日常生活至关重要。然而，网络攻击仍在给这些系统带来威胁，且其攻击能力预计还会提高[1]。

工业4.0需要高度互联的传感器、执行器、网关和聚合器。而这种更高程度的互联进一步增加了潜在网络攻击的风险，因此实施安全措施比以往任何时候都更加重要。美国网络安全和基础设施安全局(CISA)等组织的成立体现了保护关键基础设施、确保在防御网络攻击时具备强韧的恢复能力的重要性，同时也进一步表明了对此目标的决心[2]。

为什么需要IEC 62443？

2010年，Stuxnet的出现凸显了工业基础设施的脆弱性[3]。Stuxnet是首个全球范围内广为人知的网络攻击病毒，这次事件也表明从远处针对IACS发起攻击是可行的。随后的攻击再次强化了大众对于网络病毒的认识，人们由此确认针对特定类型设备的远程攻击也可能会对工业基础设施造成损害。

于是，政府机构、公用事业公司、IACS用户和设备制造商很快意识到：IACS需要得到保护。政府和用户理所当然地倾向于在组织层面采取安全相关措施并制定政策，而设备制造商则是针对硬件和软件研究了可能的反制措施。然而，由于以下原因，安全措施的采纳进展缓慢：

- 基础设施的复杂性
- 利益相关方的利益点和关注点不同
- 实施方案和选项过于多样
- 缺乏可衡量的目标

总的来说，利益相关方难以确定目标的安全级别，需要谨慎权衡防护强度与成本。

为围绕ISA99倡议建立共同参照标准，国际自动化协会(ISA)成立了相关工作组，最终共同发布了IEC 62443系列标准。该标准目前分为四个级别和类别，如图1所示。IEC 62443标准涉及面广，包含了组织政策、程序、风险评估以及硬件和软件组件的安全性。该标准涵盖安全防护的方方面面，切合当前实际需求，具有的超强适应性。此外，ISA采取综合方法来应对IACS涉及的所有利益相关方的各种利益问题。一般来说，不同利益相关方的

安全关注点各不相同。以IP盗窃为例，IACS运营商会特别关注如何保护制造工艺，而设备制造商则可能更在意如何保护人工智能(AI)算法，使其免遭逆向工程。

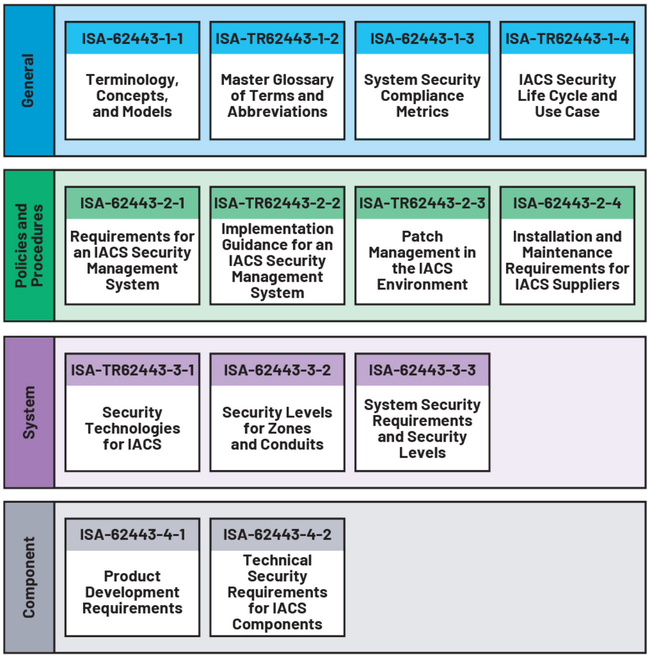

图1. IEC 62443是一项全面的安全标准

此外，由于IACS本质上很复杂，因此必须全盘考虑安全的各个方面。如果没有安全设备的支持，仅靠程序和政策是不够的。另一方面，如果程序没有正确规定如何安全使用组件，那么再坚固耐用的组件也将毫无用处。

图2中的图表显示了IEC 62443标准通过ISA认证的采用率情况。正如预期的那样，行业主要利益相关方定义的标准加速了安全措施的实施。

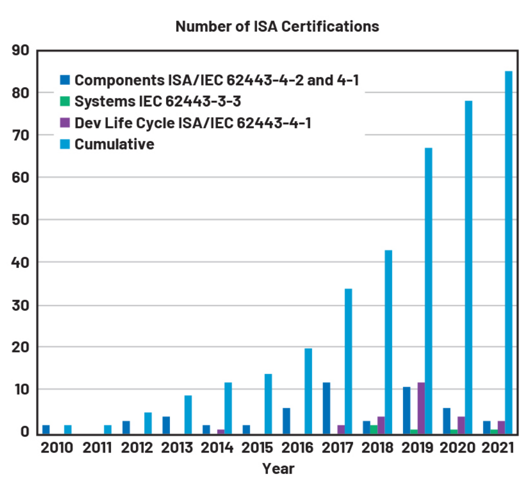

图2. ISA认证数量随着时间推移不断增加[4]

符合IEC 62443标准：复杂的挑战

IEC 62443是一个非常全面而有效的网络安全标准，但其复杂性可能超乎我们的想象。该文件本身长达近1000页。要清楚地了解该网络安全协议，就需要花时间学习。除了掌握技术语言之外，还必须注意将IEC 62443的每个小部分放在整体的上下文中进行考虑，因为各个概念都是相互依存的（如图3所示）。

例如，根据IEC 62443-4-2，必须针对整个IACS开展风险评估，评估结果将决定设备的目标安全级别[5]。

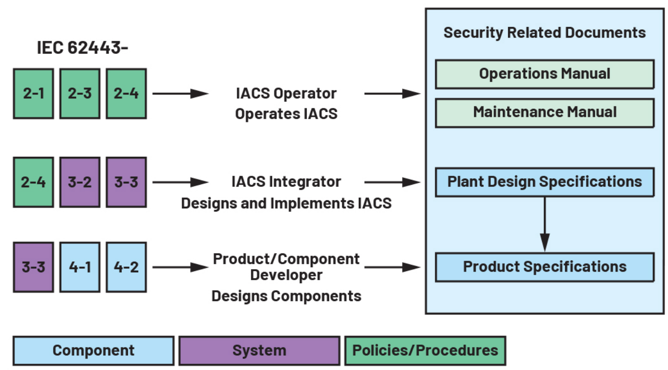

图3. 认证过程概要视图

设计符合IEC 62443标准的设备

硬件实现的最高安全级别要求

IEC 62443以直白的语言定义了安全级别，如图4所示。

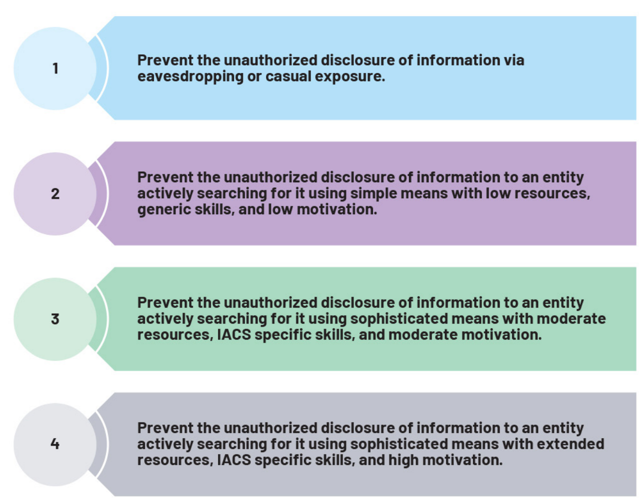

图4. IEC 62443安全级别

IEC 62443-2-1要求进行安全风险评估。在此过程的结果中，每个组件都将被分配一个目标安全级别(SL-T)。

根据图1和图3，标准的某些部分与流程和程序相关，而IEC 62443-4-1和IEC 62443-4-2则侧重于组件的安全性。根据IEC 62443-4-2，组件类型包括软件应用、主机设备、嵌入式设备和网络设备。对于各个组件类型，IEC 62443-4-2根据其满足的组件要求(CR)和增强要求(RE)定义了能力安全级别(SL-C)。表1总结了SL-A、SL-C、SL-T及三者之间的关系。

表1. 安全级别总结

	目标安全级别	能力安全级别	达到的安全级别
缩略语	(SL-T)	(SL-C)	(SL-A)
定义	根据系统级风险评估，设备应达到的安全级别	依照IEC 62443-4-2，根据设备支持的CR，设备能够实现的安全级别	设备达到的安全级别
目标	SL-T ≥ 风险评估定义的水平	SL-C ≥ SL-T	SL-A ≥ SL-T

以联网的可编程逻辑控制器(PLC)为例。网络安全要求对PLC进行身份验证，避免其成为攻击的入口。基于公钥的身份验证是一项广为人知的技术。根据IEC 62443-4-2标准：

- 1级不考虑公钥加密
- 2级要求使用普遍采用的流程，例如证书签名验证
- 3级和4级要求对身份验证过程中使用的私钥进行硬件保护

从2级安全开始，设备需要具备许多安全功能，包括基于秘钥或私钥的加密机制。对于3级和4级安全，设备在多数情况下需要具备基于硬件的安全保护或加密功能。在这方面，统包式安全IC将为工业组件设计人员带来许多优势，此类IC嵌入了基本安全机制，例如：

- 安全密钥存储
- 侧信道攻击防护
- 负责执行功能的命令，例如
  - 消息加密
  - 数字签名计算
  - 数字签名验证

有了这些统包式安全IC，IACS组件开发人员便无需将资源投入到复杂的安全原语设计中。安全IC的另一个好处是可以从本质上让通用功能与专用安全功能之间形成自然隔离。当安全功能集中在某个部分中而不是遍布整个系统时，将能更容易地评估安全功能的强度。这种隔离还可以带来的好处在于，无论如何修改组件的软件和/或硬件，都可以得到保留安全功能的验证。无需重新评估完整安全功能即可执行升级。

此外，安全IC供应商可以实施PCB级或系统级无法实现的超强保护技术。比如加固的EEPROM或闪存或物理不可克隆功能(PUF)，这些技术可以实现更高等级的防御能力，从而抵御更复杂的攻击。总体而言，安全IC是构建系统安全性的重要基础。

保护边缘安全

工业4.0意味着随时随地进行检测，因此需要部署更多边缘设备。IACS边缘设备包括传感器、执行器、机械臂、带有I/O模块的PLC等。每个边缘设备都连接到高度网络化的基础设施，也成为了黑客的潜在切入点。不仅攻击面随设备数量成比例地扩大，而且设备的多元化也不可避免地提高了攻击途径的多样性。应用安全和渗透测试供应商SEWORKS的首席技术官Yaniv Karta表示："现有平台存在许多可行的攻击途径，而且端点和边缘设备的风险敞口也都在增加。"例如，在复杂的IACS中，并非所有传感器都来自同一供应商，这些传感器的微控制器、操作系统或通信协议栈等也未共享相同的架构。每种架构本身都可能存在弱点。如此一来，所有这些漏洞不断积累在IACS之中，导致风险大大增加，如MITRE ATT&CK数据库[6]或ICS-CERT公告[7]所示。

此外，工业物联网IoT (IIoT)逐渐在边缘嵌入更多的智能功能[8]，业界正在开发可做出自主系统决策的设备。鉴于这些决策对于安全、系统运行等至关重要，确保设备硬件和软件可以被信任就显得更为关键。另外，常常还需要考虑如何保护设备开发人员的研发IP投资免遭盗窃（例如与AI算法相关的成果）。基于此，他们可能会决定采用受统包式安全IC支持的保护措施。

另外一个重要的观点是，网络安全防护不足可能会对功能安全产生负面影响。功能安全和网络安全之间的相互作用关系非常复杂，需要另写一篇文章才足以详细说明，但我们可以着重关注以下几点：

- IEC 61508："电气/电子/可编程电子安全相关系统的功能安全"要求根据IEC 62443开展网络安全风险分析。
- 虽然IEC 61508主要侧重于危害和风险分析，但也要求在每次发生严重网络安全事件后，进行后续的安全威胁分析和漏洞分析。

我们列出的IACS边缘设备是嵌入式系统。IEC 62443-4-2规定了对这些系统的具体要求，例如恶意代码保护机制、安全固件更新、物理防篡改和检测、信任根配置以及引导过程完整性。

使用ADI的安全认证器达成IEC 62443目标

ADI公司的安全认证器（也称为安全元件）专为满足上述要求而设计，同时还兼顾了易实施性和成本效益。这些固定功能IC带有用于主机处理器的完整软件协议栈，属于全包式解决方案。

采用ADI公司的安全实施方案后，组件设计人员将能更专注于其核心业务。安全认证器本质上是信任根，能够安全且不可变地存储根密钥/秘密和代表设备状态的敏感数据（如固件哈希值）。安全认证器包含一套全面的加密功能，包括身份验证、加密、安全数据存储、生命周期管理和安全引导/更新。

ChipDNA™物理不可克隆功能(PUF)技术利用晶圆制造过程中自然发生的随机变化来生成加密密钥，而不是将其存储在传统的闪存EEPROM中。该随机变化非常小，以至于即使是芯片逆向工程领域的高成本、超复杂、侵入性强的技术（扫描电子显微镜、聚焦离子束和微探测等）也无法有效地提取密钥。集成电路之外的任何技术都无法达到这样的防御水平。

安全认证器还支持证书和证书链管理[9]。

此外，ADI提供高度安全的密钥和证书预编程服务，以便可以为原始设备制造商(OEM)提供已配置完毕、能够无缝加入其公钥基础设施(PKI)或启用离线PKI的器件。该器件的稳健加密功能还为安全固件更新和安全引导提供支持。

安全认证器是为现有设计添加高级安全性的上佳之选。不仅有助于减少为安全性而重新设计设备架构的研发工作，而且BOM成本也较低。例如无需更改主微控制器即可使用该器件。举个例子，DS28S60和MAXQ1065安全认证器满足IEC 62443-4-2的所有级别要求，如图5所示。

DS28S60和MAXQ1065采用3 mm × 3 mm TDFN封装，适用于空间非常受限的设计，同时还具有低功耗特性，因此也十分适合于功耗较低的边缘设备。

表2. DS28S60和MAXQ1065关键参数汇总

器件特性	DS28S60/MAXQ1065
工作温度	–40°C至+105°C
主控接口	SPI (I^2C在开发中)
电源电压	1.62 V至3.63 V
最大工作电流	3 mA
典型空闲电流(25°C)	0.4 mA
关断电流(25°C)	100 nA

为满足IEC 62443-4-2要求，有些IACS组件架构已经配备带安全功能的微控制器，安全认证器的密钥和证书分发功能也将让这些架构大受裨益。OEM或其合同制造商无需再为处理秘密IC凭证购买所需的昂贵制造设施。这种方法还会保护微控制器中存储的可通过JTAG等调试工具提取的密钥。

如需完整的产品系列和产品详情，请访问：analog.com/cn/product-category/secure-authenticators.html。

Secure Authenticator Features	IEC 62443 High Level Requirements	SL1	SL2	SL3	SL4
ECDSA/HMAC/AES MAC	Communication Integrity	X	X	X	X
Secure Boot	System Integrity: Boot Firmware, Configuration Data Integrity	X	X	X	X
AES Encryption	Data Confidentiality (at Rest, in Transit)	X	X	X	X
ECDSA Verification	User Authentication	X	X	X	X
ECDSA Signature/Verification	Device Authentication		X	X	X
Dedicated ECDSA/SHA/AES Engines	Hardware Security for Authentication			X	X
x.509 Certificate Verification	Certificate-Based Authentication, Standard PKI		X	X	X
ECDSA Signature	Protection of Audit Information		X	X	X
ECDSA Signature	Multifactor User Authentication			X	X
External Tamper Input	Tamper Resistance and Detection, Notification of Attempts			X	X
Security IC Firmware Update + System	Secure Updates (Security Module and System)		X	X	X
ChipDNA-Based Secure Storage	Hardware Secure Storage for Private Keys			X	X

图5. 安全认证器具有符合IEC 62443要求的功能

结论

通过整合并采用IEC 62443标准，IACS利益相关方为构建可信赖且安全性强的基础设施铺平了道路。安全认证器为未来打造符合IEC 62443标准的组件打下了坚实基础，也为这些组件提供了更为稳健的基于硬件的安全性。安全认证器将帮助OEM获得所需的认证，让其更有信心地进行设计。

参考资料

1 Lorenzo Franceschi-Bicchierai。“Ransomware Gang Accessed Water Supplier's Control System（勒索软件团伙侵入供水公司控制系统）”。Vice，2022年8月。

2 “Protecting Critical Infrastructure（保护关键基础设施）”。美国网络安全和基础设施安全局。

3 Bruce Schneier。“The Story Behind The Stuxnet Virus（Stuxnet病毒背后的故事）”。Forbes，2010年10月。

4 “ISASecure CSA Certified Components（ISASecure CSA认证组件）”。ISASecure。

5 Patrick O'Brien。“Cybersecurity Risk Assessment According to ISA/IEC 62443-3-2（根据ISA/IEC 62443-3-2开展网络安全风险评估）”。全球网络安全联盟。

6 “ATT&CK Matrix for Enterprise（企业ATT&CK矩阵）”。MITRE ATT&CK®。

7 “Cybersecurity Alerts & Advisories（网络安全警报和公告）”。美国网络安全和基础设施安全局。

8 Ian Beavers。“边缘智能第1部分：边缘节点”。ADI公司，2017年8月。

9 “Trust Your Digital Certificates—Even When Offline（相信您的数字证书 — 哪怕处于离线状态）”。Design Solutions，第56期，2017年5月。

作者简介

Christophe Tremlet是EMEA安全认证器产品线的业务管理总监。他在安全IC方面拥有超过25年的经验，曾管理过多个产品工程和应用。Christophe曾在专注于安全微控制器的初创公司Innova Card中担任首席技术官。此外还曾在Maxim Integrated担任过工程和业务相关职位。在Thales担任营销和销售总监三年后，Christophe加入了ADI公司。

TA24493sc-4/23