

为机器人技术的未来发展筑牢安全防线：网络安全的作用

Manoj Rajashekaraiah, 首席工程师

摘要

本文探讨了机器人控制系统中的安全风险和有效安全措施。文中介绍了工业安全标准，并分析了满足工业安全标准所需达到的基本要求。

引言

工业4.0的核心是工厂自动化，工业机器人、自主移动机器人(AMR)和协作机器人对于实现现代工业4.0至关重要。机器人正日益智能化，协作能力不断增强，能够在有人或无人干预的情况下高效完成复杂任务。随着自动化程度和机器人使用率的提升，对机器人控制系统的安全和安防要求也不断提高。机器人最初主要用于工厂车间，但现在，机器人已应用于医疗、军事、物流、农业等众多领域。相较十年前，安全和安防的重要性显著提升。事故在所难免，但由恶意攻击引发的事故后果尤其严重。恶意劫持和控制机器人会造成严重的经济和财务损失。

机器人控制系统中的安全风险

图1展示了典型的安全风险，攻击者可以利用这些安全漏洞对机器人控制系统发起恶意攻击¹。

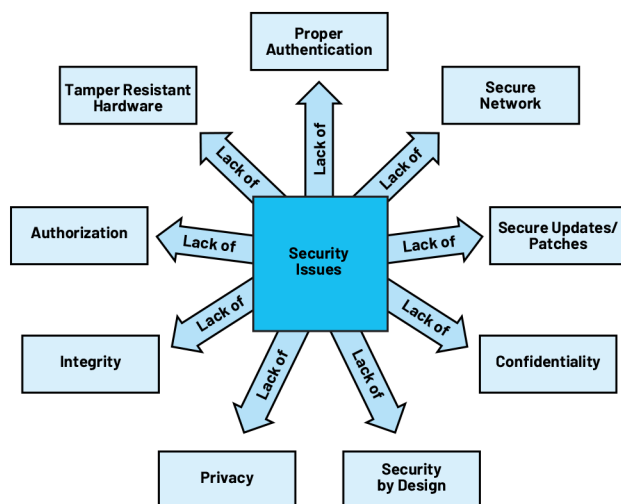


图1. 机器人控制系统中的安全风险

表1列举了一些需要关注的问题。

表1. 安全风险问题

缺乏	影响和说明
安全网络	机器人控制系统之间的通信变得不安全，容易被黑客伪造、篡改或窃听。还可能会影响系统的可用性。
适当的身份验证	- 这会导致攻击者利用默认用户名和密码进行未经授权的访问。 - 如果缺乏设备或外设身份验证机制，可能会导致机器人系统使用假冒外设/配件，从而带来安全或安防风险。 - 还会导致系统接受来自不受信任、身份不明来源的数据输入。
保密性	缺乏加密或加密算法薄弱，可能导致机器人敏感数据和设计方案被他人截获和泄露。
完整性	这可能导致存储或传输中的机器人敏感数据、配置和固件被更改。
安全引导和更新	- 若无安全引导，便无法确定机器人控制系统上运行的固件/软件是否为正版。 - 若缺乏安全更新，黑客就有可能通过回滚至存在安全漏洞的旧软件版本，或将非正版软件加载到机器人控制系统中，实现对系统的攻击。
防篡改硬件	有时机器人会存储极度敏感的信息（例如军用/国防用机器人）。保护这些信息不被未经授权方获取至关重要。如果没有防篡改硬件，就很难保护信息免受侵入性攻击。
安全设计	直到最近，大多数控制系统的开发都没有采用安全设计原则。这会使得攻击者能够侵入机器人系统的架构和设计，从而扫描并利用其中的安全漏洞来发动攻击。
更新	机器人操作系统、固件和软件若未及时更新，可能会成为网络物理攻击的目标。

注：相当一部分安全风险来源于软件漏洞。

工业和机器人领域的法律法规旨在增强网络韧性和保障安全运营

网络安全环境正快速演变，针对工业及机器人行业的法律法规日益增多。其中，针对网络安全的法规有《[欧盟网络安全法案](#)》、《[欧盟网络弹性法案](#)》和《[美国关键基础设施网络事件报告法案](#)》等。中国和印度的相关法律法规也在持续完善中。

《[NIST操作技术\(OT\)安全指南](#)》和[IEC 62443](#)等标准为我们提供了系统指导，使我们能够采取“安全设计”的方法来设计和开发控制系统，从而提升系统抵御网络攻击的能力。

IEC 62443工业自动化和控制系统安全(IACS)要求

IEC 62443是针对IACS的安全标准。²它是工业自动化控制系统开发中广泛采用的标准，获得了大多数法规的推荐和认可，其重要性不言而喻。实施该标准有助于我们遵循相关法规，降低控制系统中潜在的网络安全风险，修复控制系统中的安全缺陷，保护关键资产，并实现其他诸多目标。

General	ISA-62443-1-1	ISA-TR62443-1-2	ISA-62443-1-3	ISA-TR62443-1-4
	Terminology, Concepts, and Models	Master Glossary of Terms and Abbreviations	System Security Compliance Metrics	IACS Security Life Cycle and Use Case
	ISA-62443-2-1	ISA-TR62443-2-2	ISA-TR62443-2-3	ISA-62443-2-4
	Requirements for an IACS Security Management System	Implementation Guidance for an IACS Security Management System	Patch Management in the IACS Environment	Installation and Maintenance Requirements for IACS Suppliers
Policies and Procedures	ISA-TR62443-3-1	ISA-62443-3-2	ISA-62443-3-3	
	Security Technologies for IACS	Security Levels for Zones and Conduits	System Security Requirements and Security Levels	
System	ISA-62443-4-1	ISA-62443-4-2		
	Product Development Requirements	Technical Security Requirements for IACS Components		
Component				

图2. IEC 62443是一项全面的安全标准

该标准的某些部分侧重于流程和程序，而IEC 62443-4-1和IEC 62443-4-2则专门解决组件安全性问题。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。该标准根据组件满足的组件要求(CR)和增强要求(RE)，定义了每种组件类型的能力安全级别(SL)。其中定义了四个安全级别(SL)：SL0至SL3。SL2和SL3级别明确要求采用基于硬件的安全机制。

开发机器人安全系统解决方案需要哪些能力和技术？

为了构建安全的机器人控制系统，需要解决“机器人控制系统中的安全风险”部分中重点指出的风险。所需的关键能力和技术包括：

- ▶ 安全认证：集成安全认证器来验证设备/组件身份。
- ▶ 安全协处理器：利用专用硬件实现安全存储和加密操作。
- ▶ 安全通信：实施加密协议以保护数据交换。
- ▶ 访问控制：实施细粒度权限管理机制，防止未经授权的系统访问。
- ▶ 物理安全措施：采取措施防止物理篡改。

交钥匙安全IC（例如安全认证器和协处理器）专为满足上述要求而设计，易于实施且具有成本效益。除了这些固定功能IC，还有专为主机处理器设计的全套软件协议栈。²

注：使用分立安全元件可防止被攻陷的应用处理器访问物理隔离的独立IC中存储的凭证，从而增强系统强韧性。

除了上述方面之外，系统开发人员还必须采用结构化的安全开发方法，涵盖需求收集、威胁建模、安全设计、实现、测试、认证和维护等环节。遵循安全开发生命周期(SDL)可确保从一开始就将安全性融入到开发过程中。

是什么让ADI公司成为打造机器人安全系统解决方案的理想合作伙伴？

ADI不仅仅是[MAXQ1065](#)和[DS28S60](#)等交钥匙安全IC的供应商，更是帮助机器人行业的客户满足多样化安全要求的合作伙伴。凭借在安全和机器人技术领域的深厚专业积累，ADI成为应对机器人系统安全方面独特挑战的理想解决方案提供商。我们深谙相关领域，能够帮助客户打造整合了硬件、软件和系统级考量的全面解决方案。

鉴于机器人系统的安全性需要全盘考虑，因此ADI不仅提供元器件，更着眼于系统整体层面。我们综合考虑硬件、软件、通信和集成等因素，确保所有关键组件无缝集成。

ADI的无线电池管理系统(wBMS)是与汽车行业成功合作的典范，充分展现了ADI在实施强大安全措施方面的出色能力。通过与客户密切合作，ADI开发出了高度安全可靠且通过ISO 21434认证的wBMS系统，彰显了ADI致力于提供全面解决方案的承诺。在机器人行业推动类似协作，将能充分发挥ADI在安全实施方面的专业能力。通过与利益相关方密切合作，ADI可以利用自身在汽车领域的经验和成功实践，为开发安全可靠的机器人系统做出贡献。

ADI凭借全面的技术能力和对安全的高度关注，成为系统设计领域的理想合作伙伴，在所有与网络安全相关的工作中提供可靠的专业知识和支持。

如需了解更多信息：

- ▶ 加入[EngineerZone™](#)上安全主题博客的讨论，与嵌入式安全社区互动。搜索“安全”，查找有关安全主题的价值文章和资源。分享见解、提出问题并积极参与，为正在进行的对话做出贡献。
- ▶ 探索我们丰富的安全产品，并访问[嵌入式安全](#)和[I-Wire®](#)以获得有价值的见解。浏览最新的技术文章、应用笔记和视频，增强您对安全主题的理解。及时掌握安全领域的最新进展，发现有关我们安全产品的更多信息。
- ▶ 阅读《模拟对话》文章“[在无线电池管理系统\(wBMS\)的新时代，安全成为焦点](#)”，了解安全如何成为ADI wBMS系统的焦点。

机器人关节控制器中的用例

图3展示了机器人关节内一种可能的机器人关节控制系统设计。

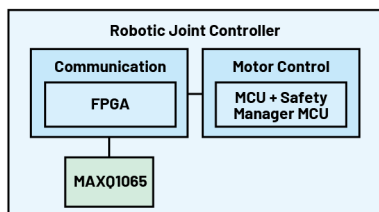


图3. MAXQ1065在机器人关节控制系统中的可能用途

在这项设计中，MAXQ1065的潜在价值得到了明确体现，它能够实现安全引导功能，进而提升整个系统的安全性。MAXQ1065还具备多种附加特性，例如安全密钥存储、安全通信协议和加密操作。后续文章将深入探讨这些用例，并探索实际应用。

结论

机器人技术的未来发展，离不开网络安全的保驾护航。安全认证、加密通信和供应链安全等强有力的措施，对于防范威胁至关重要。通过把网络安全置于优先位置，并充分发挥ADI的专业优势，我们不仅能够全面释放机器人技术的潜力，还能有效应对互联世界中的新兴风险。

在下一篇文章“[机器人安全用例与实施：护航未来安全](#)”中，我们将更深入地探讨网络安全与机器人技术的交叉领域，并展示ADI安全产品在现实场景中的实际应用。

参考文献

- ¹ Jean-Paul A. Yaacoub、Hassan N. Noura、Ola Salman、Ali Chehab，“[Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations](#)”，*International Journal of Information Security*，2021年3月。
- ² Christophe Tremlet，“[IEC 62443系列标准：如何防御基础设施网络攻击](#)”，ADI公司，2023年4月。

作者简介

Manoj Rajashekaraiah是ADI公司安全事业部的首席工程师，主要负责软件系统设计工作。他专注于嵌入式设备安全，尤其擅长为汽车和物联网应用开发安全、安保和传感器软件。Manoj是一位经验丰富的演讲者和博主，热衷于分享知识，曾在IEEE INIS和VDA Automotive SYS等会议上分享个人见解。他在[embedded.com](#)上发表过文章，并定期在卡纳塔克邦的研究所发表演讲。Manoj拥有印度彼拉尼BITS的嵌入式系统硕士学位。

在线支持社区



访问ADI在线支持社区，中文技术论坛
与ADI技术专家互动。提出您的棘手设计问题、浏览常见问题解答，或参与讨论。

请访问[ez.analog.com/cn](#)

