工业控制系统保密管理模式探讨

●张子聪

[摘要]随着工业自动化水平的持续提升，工业控制系统在生产与管理领域的作用日益突显，在安全与保密方面的挑战也越来越严峻。本文分析了工业控制系统在保密管理中存在的问题，阐述了建立工业控制系统保密管理模式的措施，为工业控制系统的保密管理提供前瞻性建议。随着工业控制系统（ICS）在各个领域的广泛应用，ICS的数据安全和隐私保护问题也受到了越来越多的关注。工业控制系统是一个包括传感器、控制器、执行器等多种组件的复杂系统，它的运行涉及工业生产中的所有环节。因此，数据在工业控制系统中的安全性和隐私保护显得尤为重要。本文将讨论工业控制系统的数据安全和隐私保护技术的现状和未来发展方向。

[关键词]工业控制系统；保密管理；数据保护；访问控制

在当今数字化与网络化快速发展的背景下，工业控制系统已成为基础设施与关键生产部门的核心，这些系统的安全性直接影响着经济发展和大众生活的安全性。安全漏洞导致的数据泄漏和系统入侵等事件的发生，暴露了当前保密措施的不足。随着技术的不断进步，传统的保密管理方法已难以满足对工业控制系统安全性的高标准要求。探索和构建一个更加高效和全面的保密管理体系，对于确保工业控制系统的安全运行和信息安全，具有重要的理论和实践意义。

Q 工业控制系统保密面临的主要问题

（一）数据传输安全性不足

在工业控制系统中，数据传输的安全性常因为过时的加密措施和协议而受到威胁。一些系统依赖于传统的通信协议如 Modbus 和 DNP3，这些通信协议在设计时并没有考虑现代加密技术，导致数据在传输中容易遭到截取和修改。在无线通信环境中运行的工业控制系统如果仍采用弱加密技术如 WEP，极易被攻击者破解。即使是有线网络，如果网络设备如路由器和交换机的安全配置存在缺陷或陈旧，也可能存在安全漏洞。这些设备未经适当配置，可为攻击者提供可乘之机，进行中间人攻击，进而被窃听、记录或篡改传输中的敏感数据。

（二）系统访问控制漏洞

部分工业控制系统身份验证不够严格，缺少必要的身份验证和权限分配管理。还有系统仍然只利用简单的用户名和密码进行认证，这些信息容易被攻破或通过其他渠道获得。攻击者一旦获取操作人员的凭证，便可以轻松访问并获取系统内的关键信息。有些系统缺乏精细化的权限控制，权限较低的用户可能接触到不应该访问的敏感数据或操作。权限管理的不足不仅关系到操作人员，还涉及第三方服务和维护人员，缺少有效的审计和监控使得外部安全威胁有可能利用这些漏洞进入系统。

（三）内外部威胁的复杂性

工业控制系统内部威胁主要包括员工可能蓄意破坏或非故意的误操作，这可能源自不满的职场环境、被胁迫利用、操作失误或对系统功能的理解不足。一个操作员因为配置错误等原因可能会误操作，导致整条生产线的停工或设备损坏。

至于外部威胁，可能包括网络黑客、商业竞争对手、间谍活动及网络战争。黑客利用工业控制系统的网络接口入侵，利用钓鱼邮件或恶意软件侵入系统。系统一旦被控制，攻击者可随意获取系统内的数据，并能更改控制指令或数据，造成数据泄密或安全事故。

Q 构建工业控制系统保密管理模式

（一）数据保护技术的应用

1.数据加密技术

在工业控制系统中，应用数据加密技术可以有效防止在数据传递过程中信息被拦截或篡改，提高存储数据的保密性。数据加密的核心原理是利用特定算法将可读数据转换

为只有授权用户才能解读的密文，从而维护数据的保密性和完整性。 在数据传输方面，采用业界广泛认可的高级加密技术，例如高级加密标准(AES)和安全套接层(SSL)/传输层安全性(TLS)协议。 AES 支持多种密钥长度，常用的是256 位密钥，能有效抵御大多数密码攻击，确保数据在公网中传输的安全。 SSL/TLS 协议被广泛应用于互联网数据交换，能够保障 Web 数据传输的安全。 在工业控制系统中运用这些协议可以有效防止数据交换过程中的监听和数据篡改。 对于数据存储的加密，应运用磁盘加密和数据库加密技术。 磁盘加密可以对存储介质上的所有数据进行加密，全面保护硬盘上的数据安全。 数据库加密技术针对存储在数据库中的数据进行加密，可采用列加密或者整库加密等方式，保证在数据泄露事件中敏感信息无法被外部访问。

2.数据掩码和匿名化

数据掩码和匿名化是处理和使用敏感信息时的有效技术，使得数据在不暴露实际内容情况下仍然可用。 数据掩码是指改变敏感数据的表现形式避免原始数据的直接暴露，这种改变是不可逆的，保证了数据的安全性和使用的便捷性。 可将敏感信息替换为随机生成的数据，即使在进行系统测试、分析或外部实体合作时，也不会泄漏真实的数据信息。 掩码数据能在不危及数据安全的前提下，被广泛应用于系统开发和测试环节。 数据匿名化指从数据集中移除所有可识别个人身份的信息，进一步保护敏感人员的身份信息。 匿名化处理的数据，即便在被外泄的情况下，也无法追溯到任何具体个体。 在工业控制系统中，利用数据匿名化技术可以在进行大数据分析和机器学习训练时使用数据，而无需担心敏感人员信息泄漏的问题。

(二)系统访问控制策略

1.基于角色的访问控制

基于角色的访问控制(RBAC)是一种在企业和工业控制系统中普遍采用的权限管理策略，分配和管理不同的用户角色控制对系统资源的访问。 在 RBAC 模型中，权限不是直接授权予个别用户，而是赋予各个角色，用户被分配至一个或多个角色继承相应的权限。 这种方法不仅简化了权限的管理过程，也提升了系统的安全性，能够精确地控制不同角色的资源访问权限，减少权限过度扩展的风险。 在工业控制系统中部署基于角色的访问控制，需要明确定义系统中各个角色及其职责，例如操作员、设计员、工艺员、安全管理员和审计员等。 每个角色都有其特定的权限集，这些权限集详细规定了角色可以访问的数据类型、系统部分以及可执行的操作。 举例来说，操作员可能仅有权限访问操作控制界面和实时数据，而无权限更改系统设置或访问敏感的系统日志。 实行 RBAC 还需要建立角色管理和权限审计的制度。 角色管理涉及添加或移除角色成员以及修改角色权限，这些活动都需经过严格的审查流程和记录，以便跟踪权限的变更并确保系统的安全。 权限审计是一个定期进行的过程，保证角色的权限设置仍然符合组织的安全策略和业务需求，识别并纠正过高的权限或不符合安全策略的配置，从而降低安全保密风险。

2.双因素认证

双因素认证(2FA)提供了一种比传统单密码系统更高安全性的验证方式，要求用户为身份验证提供两种类型的认证因子。 在工业控制系统中，实施双因素认证能够增强系统的防护能力，特别是在抵御如恶意破解和钓鱼软件等类似攻击时。 双因素认证通常包括以下三种类型的认证因子：知识因素(如密码或 PIN 码，用户所知道的信息)、拥有因素(如智能卡、安全令牌或生成一次性密码的手机应用，用户所拥有的物理设备)以及生物识别因素(如指纹、虹膜或面部识别等，基于用户的生物特征)。 当下最常见的双因素认证方式是结合密码和基于时间的一次性密码(TOTP)，其中TOTP 可以利用安全令牌或手机生成。 部署双因素认证选择适当的第二认证因素时，需要考虑安全性的提升与用户操作便利性的平衡。 在对安全要求极高的环境中，可选择使用智能卡结合密码的方式，其中智能卡为物理安全提供保障，而密码是用户熟悉的认证方式。 系统还需要设立应急访问措施，应对双因素认证设备的丢失或损坏问题，提供系统的可用性和安全性，在意外情况下不受影响。

(三)网络与通信安全措施

1.隔离关键系统和网络分段

在工业控制系统的保密管理中，隔离关键系统与网络分段是保护系统安全的核心策略。 利用物理或逻辑手段将控制网络与企业其他网络环境分离，有效减少了可能的网络攻击路径。 应用隔离关键系统，促使重要操作和敏感数据不接受未授权访问，在一定程度上避免网络攻击的横向扩散。网络分段主要是指设置防火墙、虚拟局域网(VLAN)和子网，防火墙负责监控和控制网络流量，根据安全策略来组织或允许数据包的传输。 配置适当的防火墙规则，可以有效隔离网络，限制对关键系统的访问。 虚拟局域网在同一物理网络上创建分隔的逻辑网络，每个逻辑网络拥有独立的网络策略和安全控制，确保即便一个网络段遭到攻击，也不会影响到其他部分。 实施网络隔离和分段的重点是正确识别并确定哪些系统和数据属于关键信息，并优先获得保护。需要进行详细的风险评估，确定保护的优先级和相应的安全保密管理措施。

2.持续的网络监控与异常检测

实时监控并检测网络活动中的异常行为，可以快速发现潜在的各类安全威胁和系统故障，并采取适当的应对措施。异常检测技术分为基于签名的检测和基于行为的检测。 基

于签名的检测是比对已知的攻击签名数据库识别恶意活动，这种方法在识别已知威胁方面效率很高。对抗新型或变异攻击时，这种方法可能无法提供准确的识别。基于行为的检测不依赖于已知签名，而是分析网络和系统行为中的异常模式识别潜在威胁。如果一个通常只处理少量数据的控制系统节点突然传输大量数据，这可能是系统受到攻击的迹象。为有效地实施这些监控和检测策略，需要部署先进的安全信息和事件管理(SIEM)系统，系统要与网络入侵检测系统(NIDS)和网络入侵防御系统(NIPS)结合起来。SIEM系统能够集中处理日志和事件数据，为安全分析人员提供一个全面的视角，帮助他们识别并响应安全事件。

工业控制系统保密管理的发展趋势

(一)应用人工智能与机器学习

在工业控制系统的保密管理领域，AI技术分析大量的网络流量和日志数据，能够识别正常与异常的行为模式。机器学习模型在大数据环境中进行持续的训练和优化，从而提升预测精确度。在工业控制系统中，从常规操作数据中提取学习，建立系统行为的基准模型。一旦检测到系统行为与这些基准模型出现偏差，机器学习算法就能迅速识别这些异常，并立即触发安全警报。AI和ML技术也被用来加强现有的安全措施，从而极大提高保密管理效果。

(二)引入量子通信技术

量子通信技术代表了通信安全技术的前沿发展，基于量子物理学原理，提供了理论上无法被破解的安全通信手段。量子密钥(QKD)作为量子通信的主要应用之一，能安全地分发密钥，任何试图侦听密钥的行动都将因量子态的扰动而被立即察觉。将量子通信技术应用于工业控制系统，主要是利用其出色的安全特性增强数据传输的安全。在控制系统中，保证控制命令和状态信息安全传输，未经授权的访问或数据篡改都可能引发严重后果。利用量子密钥分发，可以保证这些关键信息在传输过程中不受侵扰和窃听。尽管量子通信技术具有高度的安全优势，其实施仍面临技术和成本的双重挑战。当前量子通信设备通常较为庞大且造价昂贵，并对环境条件有较高要求，这些因素限制了其广泛应用。为了有效地集成量子通信技术，不仅需要解决物理设备的部署问题，还需要开发与之配套的网络协议和标准，促使该技术的顺利实施和运行。

结束语

本文对工业控制系统的保密管理模式进行了全面探讨，展示了结合数据保护技术、双因素认证等保密管理模式，分析引入人工智能、量子通信技术等未来发展方向。相关工作者应持续关注和研究最新的安全保密技术，不断完善和提升系统的安全保密防护措施。要定期组织安全保密培训和演练，加强员工的保密意识和操作技能，有效实施和持续优化所有的安全策略。要综合运用多种技术和策略，未来的工业控制系统将更加安全、智能，能够有效应对各种安全威胁。

参考文献

[1]薛金良,包贤晨,王鑫宇,等.核电工控系统信息安全管理体系建设研究[J].网络安全技术与应用,2023(09):99-100.

[2]韩永磊,李刚,邢卫强.面向离散制造的工控安全管理平台应用研究[J].科技与创新,2022(17):127-129,133.

[3]徐丽,许小林.大型炼化一体化项目控制系统网络安全设计[J].石油化工自动化,2022,58(02):41-44.

[4]陈翊璐,孙军,程晟滔,等.面向工控联网设备的安全管理技术[J].科学技术与工程,2021,21(33):14266-14272.

[5]李鸿培,忽朝俭,王晓鹏.2014工业控制系统的安全研究与实践[J].计算机安全,2014(05):36-59,62.

作者简介：

张子聪(1984—),男,汉族,湖南郴州人,本科,北京精密机电控制设备研究所,研究方向:航天企业保密技术应用。