电气自动化系统中的数据安全与防护措施

李　杰
青龙管业集团股份有限公司　宁夏　银川　750000

摘　要：电气自动化系统中，数据采集与存取的安全至关重要。本文深入探讨了电气自动化数据采集与存取面临的安全风险，包括数据泄露、篡改、丢失以及系统入侵等。详细阐述了多种安全防护措施，如加密技术、访问控制、数据备份与恢复、安全审计等，并分析了不同采集存取方式（如本地采集存取、远程采集存取）的安全要点。同时结合实际案例，展示了安全防护措施的有效性和重要性，旨在为保障电气自动化数据采集存取安全提供全面的理论支持和实践指导。

关键词：电气自动化；数据采集；数据存取；安全防护

引言

电气自动化在现代工业中占据着核心地位，其数据采集与存取环节是系统正常运行和决策制定的基础。随着信息技术的飞速发展，电气自动化系统面临着日益复杂的安全威胁。数据作为电气自动化系统的核心资产，其安全性直接关系到企业的生产运营、经济效益乃至社会安全。因此，深入研究电气自动化数据采集存取方面的安全和防护措施具有重要的现实意义。

1 电气自动化数据采集存取面临的安全风险

1.1 数据泄露风险

在电气自动化系统中，大量的生产数据、设备参数、工艺配方等敏感信息在采集和存取过程中可能被非法获取。例如，在化工企业的电气自动化系统中，生产工艺参数、原材料配方等数据属于商业机密。黑客可能通过网络攻击入侵系统，利用系统漏洞或弱密码获取管理员权限，进而窃取这些敏感数据。内部人员也可能因疏忽或恶意行为导致数据泄露，如员工将存储敏感数据的移动设备丢失，或者违规将数据传输给外部人员。数据泄露不仅会给企业带来经济损失，还可能损害企业的声誉和竞争力，甚至影响企业的生存和发展。

1.2 数据篡改风险

数据在采集和存取过程中可能被恶意篡改，导致系统接收到错误的信息。这可能会使生产决策出现偏差，影响产品质量和生产效率。例如，在电力系统中，关键的运行数据如电压、电流、频率等如果被篡改，可能导致电网调度出现错误，引发大面积停电事故[1]。在制造业中，生产设备的运行参数被篡改，可能导致产品质量不合格，增加生产成本。

1.3 数据丢失风险

由于硬件故障、软件错误、人为操作失误等原因，电气自动化系统采集和存取的数据可能丢失。硬件故障如硬盘损坏、服务器崩溃等，软件错误如数据库系统漏洞、应用程序故障等，都可能导致数据丢失。人为操作失误如误删除数据、格式化存储设备等，也会造成数据不可恢复的损失。数据丢失会导致生产信息不完整，影响生产计划的制定和执行。例如，在自动化生产线上，如果生产数据丢失，可能导致生产流程中断，无法及时调整生产参数，影响生产进度和产品质量。

1.4 系统入侵风险

电气自动化系统通常与企业的其他信息系统相连，这使得其面临着来自外部网络的攻击风险。黑客可能利用系统漏洞入侵系统，获取管理员权限，进而控制整个系统。例如，黑客可以通过网络扫描发现系统存在的漏洞，如未打补丁的操作系统、弱密码的数据库等，然后利用这些漏洞进行攻击。系统入侵不仅会导致数据泄露和篡改，还可能破坏系统的正常运行，造成严重的经济损失。例如，黑客可能植入恶意软件，使系统瘫痪，导致生产停滞。

2 电气自动化数据采集存取的安全防护措施

2.1 加密技术

加密是保障数据安全的重要手段。在数据采集过程中，对采集到的数据进行加密处理，可以防止数据在传输过程中被窃取。例如，采用对称加密算法（如AES）或非对称加密算法（如RSA）对数据进行加密。对称加密算法使用相同的密钥进行加密和解密，加密和解密速度快，适合对大量数据进行加密；非对称加密算法使用一对密钥，即公钥和私钥，公钥用于加密，私钥用于解密，安全性更高，适合对少量敏感数据进行加密。在数据存取环节，对存储在数据库中的敏感数据进行加密存储。即使数据库被非法访问，攻击者也无法获取其中的

信息。例如，对用户的个人信息、企业的商业机密等数据进行加密存储。同时，在数据传输过程中，使用SSL/TLS等安全协议对数据进行加密传输，确保数据在网络传输过程中的安全性。

2.2 访问控制

建立严格的访问控制机制是防止未授权访问数据的关键。根据用户的角色和职责，为其分配不同的访问权限。例如，生产操作人员只能访问与其工作相关的设备运行数据，而管理人员则可以访问更广泛的数据以进行生产决策。采用多因素认证技术，如密码、指纹、令牌等，增强用户身份验证的安全性。密码是最常见的认证方式，但为了提高安全性，应设置复杂的密码，并定期更换。指纹识别技术具有唯一性和便捷性，可以有效防止密码被盗用。令牌是一种动态密码生成设备，每次登录时生成不同的密码，增加了安全性。同时，对系统的访问进行实时监控和审计，记录用户的访问行为和操作记录。如果发现异常访问行为，及时进行预警和处理。

2.3 数据备份与恢复

定期对重要数据进行备份是防止数据丢失的有效措施。备份数据应存储在安全的位置，如异地备份中心或云存储服务。异地备份可以防止因自然灾害、火灾等原因导致本地数据丢失。云存储服务具有高可用性、可扩展性和安全性，可以提供可靠的数据备份解决方案。建立数据恢复机制，以便在数据丢失或损坏时能够及时恢复。制定详细的备份策略，包括备份周期、备份方式等[2]。例如，每天进行全量备份，每小时进行增量备份。定期进行数据恢复演练，确保在紧急情况下能够快速恢复数据。同时，对备份数据进行加密存储，防止备份数据被窃取。

2.4 安全审计

建立安全审计机制，对数据采集和存取操作进行记录和监控。通过审计日志，可以及时发现异常操作行为，如非法访问、数据篡改等。安全审计还可以帮助企业满足合规性要求，为安全事件的调查和处理提供依据。设置审计规则，对敏感数据的访问和操作进行重点审计。例如，对用户的登录行为、数据查询和修改操作等进行审计。定期对审计日志进行分析和评估，发现潜在的安全隐患。同时，将审计日志存储在安全的位置，防止审计日志被篡改。

2.5 防火墙与入侵检测

在电气自动化系统的网络边界部署防火墙，可以阻止外部网络的非法访问。防火墙可以根据预设的规则，对进出网络的数据包进行过滤，只允许合法的流量通过。例如，设置规则只允许特定IP地址的设备访问系统，禁止外部网络的非法扫描和攻击。安装入侵检测系统（IDS）和入侵防御系统（IPS），实时监测网络中的异常行为，及时发现并阻止入侵攻击。IDS可以对网络流量进行分析，检测是否存在异常的网络行为，如端口扫描、暴力破解等。IPS不仅可以检测入侵行为，还可以自动采取措施阻止入侵，如阻断网络连接、发送警报等。

2.6 数据完整性校验

采用校验和、消息摘要等技术确保数据在存储和传输过程中的完整性。在数据采集时，对数据进行校验和计算，并将校验和与数据一起存储或传输。在数据存取时，重新计算校验和并与原始校验和进行比较，如果两者不一致，则说明数据可能被篡改。例如，使用MD5、SHA等哈希算法对数据进行完整性校验。哈希算法可以将任意长度的数据转换为固定长度的哈希值，如果数据发生变化，哈希值也会发生变化。通过比较哈希值，可以判断数据是否被篡改。

3 不同采集存取方式的安全要点

3.1 本地采集存取

本地采集存取是指数据在本地设备上进行采集和存储，如通过传感器采集设备的运行数据并存储在本地硬盘中。这种方式的安全要点包括：（1）物理安全：对本地设备进行物理保护，防止设备被盗取或损坏。例如，将设备放置在安全的机房内，安装防盗门窗和监控设备。对机房进行严格的门禁管理，只有授权人员才能进入。同时，定期对设备进行维护和检查，确保设备的正常运行。（2）访问控制：对本地设备的访问进行严格控制，只有授权人员才能操作设备。可以采用密码锁、指纹识别等方式进行身份验证[3]。设置不同级别的访问权限，如管理员可以进行设备的配置和维护，普通操作人员只能进行数据的采集和查看。（3）数据备份：定期对本地存储的数据进行备份，防止数据丢失。备份数据可以存储在外部硬盘或光盘中。将备份数据存放在不同的物理位置，以防止因火灾、洪水等自然灾害导致备份数据丢失。

3.2 远程采集存取

远程采集存取是指通过网络将远程设备的数据采集到本地系统，并进行存储和处理。这种方式的安全要点包括：（1）网络安全：确保网络通信的安全性，采用加密协议（如VPN）进行数据传输，防止数据在传输过程中被窃取或篡改。VPN可以在公共网络上建立一个安全的隧道，对数据进行加密传输。同时，对网络进行分段管理，设置防火墙和访问控制列表，限制不同网络区域之间的访问。（2）身份认证：对远程设备的身份进行

认证，确保只有合法的设备才能接入系统。可以采用数字证书、MAC地址绑定等方式进行身份认证。数字证书是一种电子身份凭证，可以验证设备的身份和合法性。MAC地址绑定可以将设备的MAC地址与系统的访问权限进行绑定，防止非法设备接入[4]。（3）访问权限管理：根据远程设备的角色和职责，为其分配不同的访问权限，防止未授权访问。例如，远程监控设备只能进行数据的采集和传输，不能进行数据的修改和删除操作。

4 实际应用案例分析

4.1 案例背景

某大型制造企业采用电气自动化系统进行生产管理，系统涉及大量的生产数据采集和存取操作。该系统包括生产设备监控系统、生产计划管理系统、质量管理系统等多个子系统，各个子系统之间通过网络进行数据交互。为了确保数据的安全，该企业采取了一系列安全防护措施。

4.2 安全措施实施

加密技术应用：对采集到的生产数据进行加密处理，采用AES加密算法对数据进行加密传输和存储。在数据传输过程中，使用SSL/TLS协议对数据进行加密，确保数据在网络传输过程中的安全性。只有经过授权的用户才能使用正确的密钥解密数据。

访问控制策略：建立了严格的访问控制机制，根据用户的角色和职责分配不同的访问权限。例如，生产一线员工只能访问与其工作相关的设备运行数据，而生产管理人员则可以访问生产报表和统计分析数据。采用多因素认证技术，用户登录系统时需要输入密码，并进行指纹识别验证。

数据备份与恢复方案：制定了详细的数据备份策略，每天对重要数据进行全量备份，每小时进行增量备份，并将备份数据存储在异地备份中心。同时，定期进行数据恢复演练，确保在数据丢失时能够快速恢复。备份数据采用加密存储，防止备份数据被窃取。

安全审计与监控：建立了安全审计系统，对数据采集和存取操作进行实时记录和监控。通过审计日志，及时发现并处理异常操作行为。设置审计规则，对敏感数据的访问和操作进行重点审计，如用户的登录行为、数据查询和修改操作等。

防火墙与入侵检测部署：在电气自动化系统的网络边界部署防火墙，设置规则只允许特定IP地址的设备访问系统。安装入侵检测系统（IDS）和入侵防御系统（IPS），实时监测网络中的异常行为，及时发现并阻止入侵攻击。

4.3 实施效果

通过实施上述安全防护措施，该企业的电气自动化数据采集存取安全得到了有效保障。在一段时间内，未发生数据泄露、篡改和丢失等安全事件，生产运营稳定有序。同时，安全审计系统帮助企业及时发现并处理了一些潜在的安全隐患，提高了系统的安全性。例如，通过审计日志发现有个别员工尝试非法访问敏感数据，企业及时对该员工进行了调查和处理，避免了安全事故的发生。

结语

电气自动化数据采集存取的安全与防护是一个系统工程，需要从多个方面采取措施。加密技术、访问控制、数据备份与恢复、安全审计等手段可以有效降低数据安全风险。同时，针对不同的采集存取方式，应采取相应的安全要点。通过实际应用案例可以看出，合理的安全防护措施能够保障电气自动化系统的稳定运行，为企业的生产和发展提供有力支持。未来，随着技术的不断发展，电气自动化数据采集存取的安全防护也需要不断更新和完善，以应对日益复杂的安全威胁。企业应加强对安全防护技术的研究和应用，提高员工的安全意识，共同营造一个安全可靠的电气自动化数据采集存取环境。

参考文献

[1]高小芊.调度自动化系统及数据网络的安全防护技术研究[J].通讯世界,2024,31(11):25-27.

[2]乌兰.电网系统调度自动化数据网络的安全防护措施探究[J].电子世界,2020,(10):179-180.

[3]杨天丽.调度自动化系统及数据网络安全防护技术[J].通讯世界,2019,26(12):266-267.

[4]王宇鹏.调度自动化系统及数据网络安全防护[C]//中国电力技术市场协会.2021年电力行业技术监督优秀论文集.新疆华电高昌热电有限公司;,2021:1462-1465.