 DOI: https://doi.org/10.12349/iser.v5i6.2962

# Discussion on Information Security Management Measures in Electric Power Automation Communication Technology

**Yuna Li Baige Feng**

Zhengzhou Xianghe Group Co., Ltd. Dengfeng Branch, Dengfeng, Henan, 452470, China

**Abstract**

With the development of science and technology, automation technology has played an important role in the power communication system, but there are still some problems in the information security of power communication before the house, especially by the interference of external factors and internal factors, which seriously reduces the information security of power automation communication technology. Based on this, it is necessary to combine the actual situation, improve the information security management mechanism, optimize the equipment management and maintenance, and optimize the application of encryption technology, improve the personnel quality, improve the network management system, strengthen the security management of identity authentication, and further improve the information security management level of power automation communication technology. This paper mainly analyzes the influencing factors of information security of power automation communication technology, and puts forward targeted measures, so as to strengthen the information security of power automation communication technology and ensure the security of power communication.

**Keywords**

electric power automation; communication technology; information security; management measures

# 电力自动化通信技术中的信息安全管理措施探讨

李玉娜 冯白鸽

郑州祥和集团有限公司登封分公司，中国 · 河南 登封 452470

**摘 要**

随着科学技术的发展，自动化技术在电力通信系统中发挥了重要作用，但是当前电力通信信息安全方面还存在一定的问题，尤其是受到外部因素、内部因素的干扰，严重降低电力自动化通信技术的信息安全性。基于此，要结合实际情况，完善信息安全管理机制，优化设备管理和维护，并对加密技术进行优化应用，提高人员素养，完善网络管理系统，强化身份验证安全管理，进一步提高电力自动化通信技术的信息安全管理水平。论文主要对电力自动化通信技术的信息安全影响因素进行分析，并提出针对性的应对措施，从而强化电力自动化通信技术的信息安全，保障电力通信安全性。

**关键词**

电力自动化；通信技术；信息安全；管理措施

## 1 引言

电力自动化通信技术水平的提高，进一步保障电网系统安全性，为电力企业可持续发展奠定良好的基础。但是在自动化技术应用中，信息安全还存在一定的问题，容易发生信息泄露、丢失等现象，严重降低电力自动化通信服务质量。因此，要结合实际情况，采取科学合理的安全防护措施，尤其要对安全技术、加密技术进行优化应用，保障通信系统安全管理，减少用户信息泄露，为电力行业的长远发展奠定良好的基础。

【作者简介】李玉娜（1985–），女，中国河南登封人，本科，工程师，从事电气工程自动化研究。

## 2 电子系统通信自动化的重要性

电力自动化通信系统主要是在信息技术、计算机技术、网络技术、智能化技术、通信技术支持下，形成的电力系统，同时在数据传输协议、信号通信网络的支持下，提升电力系统通信能力，强化电网安全运行，进一步提高用户用电服务质量。同时还能够保障各类信息数据的快速传输[1]。在自动化技术支持下，还能够对相关数据进行全面收集，并对关键仪器设备的运行状态进行动态监测，为电力系统调试和维护提供数据依据，有效提升电力自动化通信系统应用效果。由此可见，自动化技术的应用，能够保障电力通信系统的安全可靠性运行，并精准控制电网运行中的不同环节，并减少系统运维成本，具有较好的经济性优势，具有良好的发展前景。

## 3 电力自动化通信技术的信息安全影响因素

### 3.1 外在因素

影响电力通信系统信息安全的外在因素主要包含人为因素、自然因素等。其中，自然因素具有不可抗力特点，如雨雪冰雹、雷击等现象，会加大火灾发生概率，对整体信息系统的安全性造成严重危害，不利于信息安全防护。此外，人为因素也是影响信息安全的重要因素，如人员操作失误等，会加大信息安全发生概率；人为蓄意、恶意行为也会引发网络安全问题，危害信息系统安全运行；电力企业缺乏完善的电力系统安全管理机制，对信息安全管理任务分配不合理，加大了信息安全问题发生概率，甚至容易引起信息泄露等现象，不利于整体电力通信系统的安全可靠性运行。

### 3.2 内在因素

在电力自动化通信技术应用中，加密技术、硬件安全管理不到位，这是引起通信信息安全问题的关键因素之一[2]。其中，加密技术是保障电力系统通信安全的重要基础，但是在实际系统运行中，信息加密、秘钥管理等工作还存在一定的不足之处，严重降低加密技术的应用效果，容易加大信息泄露概率。一旦出现这种情况会严重降低电力企业运行水平，且容易兴起用户信用危机，破坏电力企业的市场形象。如果电力企业使用的加密技术与自身实际情况不相符，往往会受到非法攻击等形象，降低通信信息安全。在硬件安全管理方面，企业硬件陈旧老化，没有及时更新，严重降低硬件安全管理。部分企业硬件设备准备不齐全，不能保障信息安全。一旦硬件设备管理不到位，会降低电力系统的安全防护能力，加大被攻击的概率，甚至容易被非法分子窃取信息。由此可见，加密技术、硬件安全等问题，都有可能降低电力系统信息安全管理效果。

## 4 电力自动化通信技术的信息安全防护措施

### 4.1 完善安全防范机制

为了保障电力自动化通信系统安全运行，需要结合实际情况，完善安全防范机制，保障自动化电信系统的高效运行，减少信息安全问题的出现几率。在构建安全防范机制过程中，要严格按照逻辑性原则要求，并根据电力企业的具体状态，精细划分重点防范区域，且对不同分区设置差异化的访问权限，保障重要安全数据、资料信息的针对性防护。在构建安全防范机制过程中，要对不同主体的管理范围、责任进行明确划分和落实[3]。

### 4.2 完善设备安全机制

网络设备是电力自动化通信系统的重要硬件设备，是进行信息安全防范的关键保障。因此，为了实现电力通信系统的信息安全，要结合实际情况，建立完善的设备管理机制，提高设备管理水平，减少信息安全发生概率。同时，还要优化信息网络规划设计，实现设备采购、安装调试、运行维护、技术更新等工作的优化管理，并引进激励奖罚体制，强化工作人员的责任意识，激发主观能动性，保障安全防范效果的提升。

### 4.3 强化防火墙安全

在网络安全防护工作中，防护墙发挥重要的屏障作用，能够对内部可信网络和外部不可信网络之间搭建单点安全链接，从而提升通信信息安全管理水平。基于此，要结合网络安全防范体系的实际要求，强化防火墙建设力度，进一步提升整体通信系统的安全防御能力，减少信息安全事故的出现几率。当前，常用的防火墙技术包含过滤防火墙、基于代理的防火墙、基于状态分析的防火墙。其中，最后一种防护墙具有较好的伸展性和扩展性，且在使用过程中的安全性较好，具有较高的安全防范效果。所以，在电力自动化通信系统设计中，要对安全防范技术进行优化选择，一般要利用基于状态分析的防火墙技术进行安全防范。随着科学技术的发展，电力企业面临的网络恶意攻击类型、方式越来越多样化，需要电力企业对防火墙技术进行定期升级，强化防火墙技术性能，减少网络恶意攻击，保障整体系统信息的安全性。

### 4.4 强化身份验证安全管理

影响电力自动化通信网络管理系统运行效果的因素有通信系统规模、通信网络结构、技术经济指标等。在具体操作中，要根据实际情况，优化应对措施，实现管理系统的可靠性运行。为了保障整体系统安全，要完善网络管理系统，实现通信系统的实时监控，并优化应用密码技术，对信息安全管理状态进行动态监控。要对信息安全管理工作进行优化，做好安全认证管理，减少非法获取信息问题的发生概率[4]。其中，要对身份验证安全管理技术进行优化应用，对用户身份进行严格验证，减少非法访问网络的现象，避免重要资料被窃取。在具体操作中，要先对用户身份进行识别，然后进行身份认证。前者需要用户向系统提供证明身份的信息，并要对用户 ID 进行识别；后者需要系统对用户提供方身份信息进行验证，确保用户拥有访问权限，保障信息安全。此外，还需要做好系统安全登录、身份认证、访问控制、访问统计、审计等工作的协同性开展。

### 4.5 完善网络管理系统

完善的网络管理系统是提升信息安全的重要保障。其中系统包含网元数据采集层、业务管理层、网元管理层等。且该系统的功能较为多样化，如全自动拓扑发现技术、多维度监控、故障智能预测与分析、支持多操作平台、支持分布式管理等。通过网络管理系统的建设，可以实现各类数据的动态化采集，并对其实时传输，并能够对系统故障进行在线预测和分析，促进网络安全的全面覆盖管理，促进系统管理工作的自动化与智能化，减少成本投入，保障经济效益的增加。通过全面管理系统的构建和应用，能够实现信息安全管理，避免出现安全事故，实现整体电力系统的可靠性运行。

### 4.6 做好日常维护工作

在电力自动化通信信息日常维护管理工作中，为了保

障信息安全，要安全专业人员定期查看软件、硬件的运行状态，并及时查看交换器、路由器的运行情况，一旦发现异常情况，需要及时维修、更换，保障维持良好的运行状态，有效控制系统故障的出现几率。还需要定期更新升级软件系统，引进最新版补丁，保障用户软件安全。要对各类模式的自动化通信系统进行有效性维护，其中包含不定期检查、定期检查等方式，强化系统信息安全性 [5]。

### 4.7 完善加密技术

为了保障电力通信系统信息安全，需要保障设备终端设备，对其严格认证，确保用户信息安全。此外，传输过程安全是实现电力通信系统信息安全的重要保障，防止非法人员随意访问。所以，要对加密技术进行合理应用，强化电力自动化通信技术信息安全，保障用户信息安全，并优化加密方法，对其定期升级。例如，需要利用现标准化的数据加密标准算法（如图 1 所示），强化信息安全有效性维护，加大密码破解难度，有效提升电力自动化通信技术的信息安全。此外还包括公开密钥算法等方式进行信息安全防护，如图 2 所示。

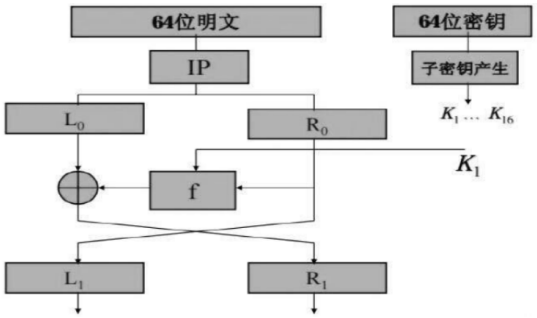


图 1 数据加密标准算法实现流程

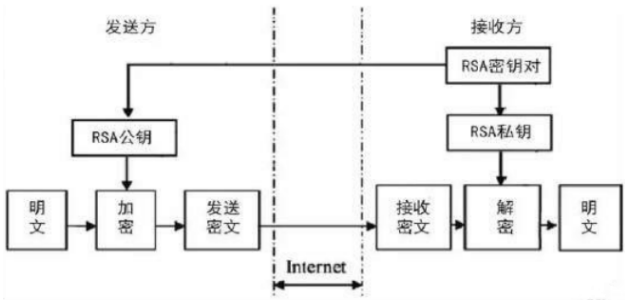


图 2 公开密钥算法实现流程

### 4.8 无线终端防护

无线传输是实现自动化中心与各个通信子站点间进行信息通信的重要基础。因此要做好无线终端防护工作，尤其要完善认证系统，对用户身份进行严格认证。只有拥有访问权限的用户才能通过认证，并能够对电力通信信息进行正常访问，且禁止非法用户访问，同时构建黑名单，防止出现电力信息数据泄露、丢失等问题的出现。此外，在信息传输过程中，还需要做好信息加密处理，保障电力信息通信安全，减少信息安全问题的出现。

### 4.9 优化安全管理机制

完善的安全管理机制是保障电力自动化通信系统信息安全的重要保障。因此，要结合电力企业发展需求，优化安全管理机制，并完善相关法律法规，为安全信息问题的解决提供法律依据。电力企业还需要结合相关法律要求，实现通信技术信息安全等级升级。要优化网络安全体系，实现系统信息安全。加大该方面的资金投入，定期组织开展安全培训工作，邀请相关方面的专家传授安全知识，强化工作人员的综合素养，保障电力通信自动化系统的安全运行。

## 5 结语

综上所述，随着科学技术的发展，自动化技术在电力通信系统中发挥了重要作用，进一步提高通信系统运行效率。为了解决信息安全问题，要采取科学合理的防护措施，尤其要引进信息加密技术，优化安全防护措施，做好日常维护工作，减少信息泄露、丢失等问题，保障整体电力自动化通信系统的安全可靠性运行。

### 参考文献

[1] 李永华.关于电力自动化通信技术与信息安全问题的分析[J].信息记录材料,2020,21(7):94-95.

[2] 崔秀敏,丁禾羽.电力自动化通信技术中存在的信息安全问题及对策分析[J].江西电力职业技术学院学报,2020,33(6):5-6.

[3] 何艾玲,刘畅.电力自动化通信技术中信息安全问题剖析及预防[J].技术与市场,2019,26(12):157+159.

[4] 胡俊,胡振保.电力自动化通信技术中信息安全问题剖析及预防[J].科技风,2018(35):62.

[5] 税明星.浅析电力自动化通信技术中的信息安全问题[J].通讯世界,2018(6):202-203.