

电子信息技术在安全保障管理中的应用

李晓虎

石家庄通合电子科技股份有限公司

摘要：在多种因素的共同作用下，电力工程因其工作点多、线长、面广的特征，其安全逐渐被人们重视，科学运用信息技术，强化电力工程建设安全管理有助于电力企业全面掌握安全生产动态，降低安全风险发生概率，增强事故应急救援和处置能力，切实提高企业管理水平。

关键词：电子信息技术；安全保障管理；实践应用

【DOI】10.12252/j.issn.2096-6261.2022.11.199

引言

当前，我国社会经济正处于稳步发展的关键时期，社会整体经济水平呈现出上升趋势，此时必然给电网建设布局、规划和设计提出更高要求，而提前谋划布局电网大规模建设需要引入大量外来作业人员以及其他专业人员参与，如何科学有效地对外包企业、其他专业人员进行安全管理成为当前电力企业面临的一大难题。根据过去电力工程建设工作中存在的问题分析，其中主要问题表现在信息化水平不高、人工统计和管理为主、工作效率低等，为了提升对外包企业、人员的安全管理水平，文章通过分析电力工程建设安全管理的重要性，总结了信息技术的运用技巧，旨在让电力工程建设安全管理更加科学，更加全面、精准地管控相关建设人员和工作。

一、电子信息技术在安全保障管理中的应用概述

（一）安全保障管理的概念和基本原则

（1）安全性原则：防止信息泄漏、篡改、破坏等安全事件的发生。（2）完整性原则：防止信息被篡改或损坏，确保信息的真实性和完整性。（3）可用性原则：确保信息系统能够正常运行，业务能够顺利开展。（4）保密性原则：防止信息被未经授权的人员获取，确保信息的机密性和私密性。（5）可追溯性原则：确保信息系统的操作记录和审计日志能够被有效地追溯和查找。

（二）电子信息技术的发展和应用现状

随着科技的不断进步，电子信息技术已经成为现代社会中不可或缺的一部分。它涵盖了电子、通信、计算机、网络、人工智能等多个领域，为人类的生产、生活、娱乐等方面提供了极大的便利。在电子领域，随着半导体技术的不断发展，电子器件的性能不断提高，尤其是微型化、高集成度、低功耗等方面的进步，使得电子产品的体积越来越小，功能越来越强大。例如，智能手机、平板电脑、智能手表等已经成为人们日常生活中必不可少的工具。在通信领域，随着移动通信技术的不断

断发展，人们可以通过手机、计算机等设备随时随地进行语音、视频通话，短信、邮件等方式通信，大大方便了人们的交流和沟通。在计算机领域，随着计算机硬件和软件技术的不断进步，计算机已经成为人们生产、生活中必不可少的工具。人工智能技术的发展，更是为计算机的应用带来了新的可能性。在网络领域，随着互联网技术的不断发展，人们可以通过网络获取各种信息，进行在线购物、在线教育、在线娱乐等活动，大大方便了人们的生活。总之，电子信息技术的发展和应用已经深入到人们的生产、生活、娱乐等各个方面，为人类的发展和进步做出了巨大的贡献。

（三）电子信息技术在安全保障管理中的应用现状

（1）视频监控系统：通过安装摄像头和监控设备，对公共场所、重要设施和关键部位进行实时监控，提高安全保障水平。据统计，全球视频监控市场规模已经达到了240亿美元。（2）生物识别技术：采用指纹识别、虹膜识别、人脸识别等技术，对人员身份进行验证，防止非法入侵和信息泄漏。据市场研究机构预测，全球生物识别市场规模将在2025年达到约400亿美元。（3）数据加密技术：通过对数据进行加密处理，保护数据的安全性和机密性，防止数据被非法获取和篡改。据统计，全球数据加密市场规模已经达到了150亿美元。（4）网络安全技术：采用防火墙、入侵检测、反病毒等技术，保护网络系统的安全性和稳定性，防止网络攻击和病毒侵袭。据市场研究机构预测，全球网络安全市场规模将在2025年达到约300亿美元。（5）无人机技术：通过无人机进行巡逻和监测，提高安全保障的效率和精度。据统计，全球无人机市场规模已经达到了120亿美元。

二、信息技术在电力工程建设安全管理中的重要性

在社会经济日新月异的新时期，电网规模、电网结构和电网组成都发生了巨大的变化，电力工程建设也呈现出大规模、多元化发展趋势，各类工程施工中出现了

作业人员多、施工范围广、施工量大、工程复杂程度高、危险性大等现象，同时随着大量外包团队的不断加入，电力安全危险系数正在不断地攀升，给工程施工建设和安全管理提出了新的挑战。面对这种情况，在电力工程建设安全管理工作中融入信息技术势在必行，其重要性不言而喻，具体表现在以下方面。

（一）有助于推动社会稳定发展

在如今人们日常生活、生产和工作中，电力已经成为不可或缺的组成，电力供应稳定与否直接关系到经济发展和社会稳定。目前，人们生活中各种电气设备的类型众多，如果电力企业供电不稳定，很容易影响到电能供应，最终影响到社会正常生产和人们日常生活。因此，在电力工程建设中落实安全管理十分必要，将信息技术融入其中可以确保电力供应稳定，进而保障人们生活、工作和生产的正常性，最终推动社会稳定发展。

（二）提高电力企业的竞争力

电力是当今社会发展中不可或缺的基础能源，电力企业的发展可以推动社会经济的稳定前行。如果电力企业工程建设环节出现安全事故，必然会给电力企业发展带来影响，甚至影响到区域电能供应。在目前不断增加的电能需求基础上，确保电力工程建设安全是保障电能供应稳定的关键，因此将信息技术融入其中十分必要，能有效提高电力企业的竞争力，实现企业可持续发展战略目标。

三、现阶段电力生产安全中存在的问题

（一）生产安全的管理没有从根本上落实

现在电力企业中会出现生产安全问题的根本原因还是因为关于电力生产的安全制度没有贯彻到位。安全制度的贯彻不应当仅存在于某个环节，或者某个环节的某个方面，电力生产是有着十分系统的操作，每一个操作环节都承担着一定的生产风险，如果单单将安全管理制度贯彻到某一个方面或者单一的某一个环节，那么根本就起不到保证生产安全的效果。而且，在颁布安全责任书的时候，很多部门没有重视生产安全问题，对员工进行安全指导的时候更是一切从简，指导的过程更是一笔带过，这也就直接导致了员工的生产安全意识迟迟无法树立，产业的生产安全规章制度的实施一直无法落地，最终导致了安全事故的出现。

（二）关于安全生产的相关制度执行困难

关于这个问题其实也是我国配电企业出现的老问题了，我国很多电力企业都制定了很多规章制度，其中包含了日常的管理制度，还有电力生产时的安全规章制度，若是这些制度能够被原原本本的贯彻落实，那么电

力企业的安全隐患问题将会大大减少。但是如今配电企业的安全问题依旧十分严重，这也就说明了这些有关安全生产的规章制度没有被严格的落实下去，企业里规定的制度和员工日常的行为存在着很大的差异，而安全隐患也正是由这些差异中慢慢滋生。而究其原因，其实还是因为配电企业所设定的规章制度篇幅过长，其中所包含的各项内容虽然全面，但大多都过于繁琐，员工在开始工作之前根本没有时间和精力逐一将这些规章制度一一阅读，而这样做也就导致了员工在开展日常工作时往往无法做到标准化作业，这也是导致生产安全问题最主要的原因之一。

（三）电力系统安全监测和预警的不足

电力系统安全监测和预警的不足主要表现在监测手段不完备、监测数据处理不及时、预警机制不完善、预警信息传递不及时等方面。为加强电力系统的安全监测和预警，可以采取一些措施，如加强监测手段的建设和更新、提高监测数据处理的速度和精度、完善预警机制、加强预警信息的传递和沟通等。

四、电子信息技术在安全保障管理中的具体应用

（一）加密认证技术

先进的加密技术采用如对称加密（例如AES-256，3DES等）、非对称加密（如ECC，RSA等）和混合加密（如SSL/TLS、SSH等）算法，可以确保数据在存储、传输和处理过程中的保密性、完整性和可用性。其中，AES-256提供高度安全的数据加密，而基于椭圆曲线密码学（ECC）的算法在计算负载和能耗方面具有优势，适用于资源受限的环境。在密码学衍生技术中，散列函数（如SHA-1、SHA-256等）广泛应用于生成消息摘要，而数字签名（如ECDSA、RSA签名等）使得数据来源和身份得到验证，保证数据传输的真实性和不可否认性。此外，数字证书（如X.509标准）通过可靠的认证机构颁发，用于建立身份信任链。对于电力信息系统中的鉴权部分，多因素认证技术在防止非法访问和恶意操作中发挥重要作用。这些技术整合了物理令牌（例如OTP密钥）、知识型证据（如密码和PIN码）以及生物特征识别（如指纹、虹膜和面部识别等）。这些认证方法常应用于关键设施，例如智能电表、远程管理系统和SCADA系统等。在特定应用场景中，加密与认证技术通过端到端加密实现了对智能电网、敏感数据和云计算资源等核心领域的安全防护。例如，IEC62351标准针对电力系统通信提供了一系列安全机制，包括报文完整性、报文加密和访问控制等。适应不同应用场景和环境的加密与认证技术为电力信息系统提供了关键的安全保障。

（二）硬件设备管理

在硬件设备的维护管理方面，需要加强对硬件设备的定期检修和维护工作，对于硬件设备的老化和损坏需要及时更换，避免因长期使用造成设备老化和损坏，同时还需要对硬件设备进行定期清洗和维护工作，在清洗维护过程中可以使用专业的清洗工具、专业的清洗剂 and 化学试剂。此外，在对硬件设备进行维护保养过程中可以选择一些保养周期较短、较为简单、方便快捷的清洁保养工具和化学试剂。在对电力系统自动化技术硬件设备进行检查和维护过程中，可以采用红外探测器、高频等方式对电力系统自动化技术硬件设备进行检查，同时还需要对电力系统自动化技术硬件设备的运行状态进行检测，如果发现存在异常情况需要及时进行处理。在电力系统自动化技术安全控制方面，需要加强对软件安全控制的管理和控制。

（三）人员管理

（1）制订完善的培训计划。电力系统自动化技术是一门专业性较强的技术，对于其运行人员也有着较高的要求，因此需要制订完善的培训计划。培训计划主要包括日常管理人员和技术人员两个方面的内容，日常管理人员主要是指能够对电力系统自动化技术进行简单操作以及维护工作的工作人员；技术人员需要掌握电力系统自动化技术，提高电力系统自动化技术应用水平。

（2）加强对员工的安全意识培训。在电力系统自动化技术的应用过程中，安全事故发生频率较高，因此需要加强对员工的安全意识培训，增强员工对安全事故的防范意识。加强员工的安全意识培训需要制定完善的安全管理制度，包括对员工进行安全培训以及监督工作等；需要制订完善的安全操作流程，对员工进行规范化操作培训；需要制订完善的培训计划，通过多种渠道和方式开展培训教育工作；需要定期组织培训活动，并制订详细计划，定期进行电力系统自动化技术相关知识和操作技能培训；需要对培训效果进行评价分析，根据实际情况制订培训评价指标体系。在电力系统自动化技术应用过程中，需要通过多种途径和方式加强对员工进行安全管理教育，以提高员工对电力系统自动化技术重要性和安全性的认识。

（四）负荷侧智能控制技术

（1）敏感负荷控制技术。敏感负荷控制技术专门针对电力系统中关键或易受干扰的负荷实施管理与控制，确保各种电网条件下都能得到稳定供电。现代电力系统内的多种负荷具备不同的电气特性与响应速度。对于被定义为“敏感”的负荷，如特定工业负荷或医疗设

备，选择恰当的控制策略具有至关重要的意义。敏感负荷对电压波动、频率变化或瞬时断电等电网问题显示出高度的敏感性。针对此类负荷的控制技术必须能够实时感知电网状态并作出适当调整，避免对负荷造成不良影响。（2）广域负荷控制技术。广域负荷控制技术致力于跨越广泛地域范围内的电力系统负荷管理与控制。其核心目标为确保各地负荷均衡，降低地域性电压和频率的波动，从而实现电力系统的稳定运行。考虑现代电力系统的复杂性和互联性，有效地管理广泛地域的负荷显得尤为重要。通过实时监测电网的运行状态，并根据各地的实际需求，实施负荷调度和控制，广域负荷控制技术能够实现负荷的优化分配。

（五）加强数据安全防护能力建设

制定新型电力系统企业级数据安全防护策略，加强源、网、荷、储等重要隐私、敏感数据保护，明确数据安全主体责任和防护要求。建立并优化跨网络分区的数据安全交换通道，完善数据交换策略，通过敏感数据保护、安全审计、数据安全治理等方式智能化保障电力数据在各能源链间的安全、合规流动；以中台数据为核心，加强对中台内数据使用和共享过程安全监测，及时分析处置安全风险，定期开展数据安全审计，防止中台数据泄露。强化动态脱敏、多方计算、联邦学习等数据安全关键技术攻关应用，构建完善的技术体系，全面防范化解各类数据安全合规风险隐患。强化数据安全风险评估，建立覆盖数据采集、传输、存储、应用等环节的安全风险评估机制，推动数据安全风险评估工作常态化、规范化、自动化。

结束语

综上所述，电子信息技术在安全保障管理中的应用已经成为不可或缺的重要手段。通过对各种安全威胁的预测、监测和应对，电子信息技术可以帮助企业和组织更好地保护自身的安全。然而，随着技术的不断发展，安全威胁也在不断变化，因此我们需要不断地更新和完善安全保障管理措施，以适应不断变化的安全环境。只有不断地学习和创新，才能更好地应对安全威胁，为发展赋能。

参考文献

- [1] 郭术明. 电力系统及其自动化技术的安全控制问题和对策[J]. 石河子科技, 2021(6): 12-13.
- [2] 陶彤. 信息化技术在电力安全管理中的应用研究[J]. 电气时代, 2020(3): 78-79.
- [3] 王蕾, 许德建, 朱明. 电子信息技术在企业安全管理中的应用研究[J]. 精品, 2020(4): 54.