

# 新形势下电力监控系统网络安全的挑战与应对

王迟 左晨宇 王家慧

国网北京大兴供电公司 北京 102600

**摘要:** 随着云计算、大数据、物联网等新兴技术在电力监控系统中的广泛应用,电力监控系统的网络安全面临前所未有的挑战。本文首先分析了电力监控系统在新形势下所面临的网络安全风险,包括勒索病毒、蠕虫和木马等系统性风险,以及人员风险和安全威胁与建设实践的脱节风险。接着,本文探讨了这些风险对电力监控系统的影响,并提出了相应的应对策略,包括加强网络安全意识培训、完善安全制度、定期升级网络防火墙和入侵检测技术、建立数据全生命周期安全保障体系等。最后本文总结了电力监控系统网络安全的重要性,并强调了构建新型电力系统网络安全风险管控体系的必要性。

**关键词:** 电力监控系统; 网络安全; 勒索病毒; 数据全生命周期安全保障体系; 主动防御技术

## 引言:

电力监控系统作为电力系统的核心组成部分,其安全性和稳定性直接关系到电力系统的正常运行和供电质量。随着信息技术的飞速发展,云计算、大数据、物联网等新兴技术在电力监控系统中的应用日益广泛,极大地提高了电力系统的运行效率和智能化水平。然而,这些新兴技术的应用也带来了前所未有的网络安全挑战。本文旨在分析新形势下电力监控系统所面临的网络安全风险,并提出相应的应对策略,为电力监控系统的网络安全保障提供参考。

### 1. 电力监控系统在新形势下所面临的网络安全风险

电力监控系统作为现代电力系统的核心组成部分,承担着实时监控、控制和保护电力系统的重要任务。然而,在新形势下,电力监控系统面临着日益复杂的网络安全风险。这些风险不仅来源于外部恶意攻击,还涉及内部管理和技术应用等多个层面。以下将详细分析电力监控系统在新形势下所面临的三大网络安全风险。

#### 1.1 勒索病毒、蠕虫和木马等系统性风险

勒索病毒、蠕虫和木马等恶意软件是电力监控系统面临的主要系统性风险之一。这些恶意软件具有隐蔽性强、破坏性大、传染性高等特点,一旦成功侵入电力监控系统,将严重威胁系统的安全性和稳定性。

勒索病毒通常通过加密系统中的重要数据,迫使受害者支付赎金以获取解密密钥。在电力监控系统中,勒索病毒的攻击可能导致关键数据的丢失或无法访问,进而影响电力系统的正常运行。蠕虫病毒则能够在网络中自我复制和传播,

迅速感染整个生产网络,导致系统瘫痪或数据泄露。木马病毒则常常潜伏在系统中,窃取敏感信息或执行恶意操作,对电力系统的安全构成潜在威胁。

近年来,勒索病毒袭击国内外关键基础设施的事件频发,充分暴露了这种风险的严重性。电力监控系统作为关键基础设施的重要组成部分,必须高度重视勒索病毒等恶意软件的防范工作,加强系统的安全防护能力。

#### 1.2 人员风险

电力监控系统运维人员的网络安全意识不足也是导致网络安全风险的重要原因之一。目前,很多电力监控系统运维人员缺乏网络安全意识,对密码管理、权限控制等安全策略缺乏必要的认识和理解。

在实际操作中,一些运维人员可能采用默认密码、长期不修改密码等不安全行为,导致系统容易被恶意攻击者破解。此外将密码存放在互联网或云平台等公开环境中,也极易导致核心电力控制系统的用户名和密码泄露。一旦这些信息被恶意攻击者掌握,他们将能够轻松侵入系统,进行非法操作或窃取敏感信息。

同时部分员工对网络安全培训不重视,缺乏必要的安全知识和技能。在实际工作中,他们可能无法有效识别和应对网络安全威胁,导致系统安全防护措施形同虚设。因此加强电力监控系统运维人员的网络安全意识培训,提高他们的安全技能水平,是防范人员风险的重要措施。

#### 1.3 安全威胁与建设实践的脱节风险

电力监控系统的网络安全建设与实际应用存在脱节现

象,这也是导致网络安全风险的重要原因之一。一方面电力监控系统的网络安全管理很大程度上由合规性驱动。然而合规性防护策略只是安全防护的一个重要方面,它无法完全保证动态变化的电力监控系统是安全可靠的。

在实际操作中,一些电力企业可能过于注重合规性要求,而忽视了系统安全防护的实用性和有效性。他们可能简单地堆砌安全防护设备,而没有根据系统的实际需求和风险情况进行有针对性的安全防护。这种做法不仅浪费了资源,还可能导致系统安全防护能力下降。

另一方面由合规性驱动的电力监控系统建设容易出现资源浪费和防护能力不足的问题。面对跨网跨域的高级持续性攻击威胁,传统的安全防护设备和技术往往难以有效应对。因此,电力企业需要加强对新型网络安全威胁的研究和分析,采用更加先进和有效的安全防护技术和策略,提高系统的安全防护能力。

综上所述,电力监控系统在新形势下面临着勒索病毒、蠕虫和木马等系统性风险、人员风险以及安全威胁与建设实践的脱节风险等多重网络安全风险。为了保障电力系统的安全稳定运行,电力企业需要高度重视这些风险并采取有效的防范措施。通过加强系统安全防护能力、提高运维人员的网络安全意识以及采用更加先进和有效的安全防护技术和策略,我们可以共同应对这些挑战并保障电力监控系统的网络安全。

## 2. 电力监控系统网络安全风险的影响

电力监控系统作为现代电力系统的核心,其网络安全风险的影响不容忽视。这些风险不仅直接威胁到电力系统的安全稳定运行,还可能对电力企业的声誉和经济利益造成深远影响。以下将详细探讨电力监控系统网络安全风险的具体影响。

### 2.1 影响电力系统数据资料的安全性

勒索病毒、蠕虫和木马等恶意软件的入侵是电力监控系统面临的主要网络安全威胁之一。这些恶意软件具有强大的破坏性和隐蔽性,一旦成功侵入系统,将严重威胁电力系统数据资料的安全性。它们能够窃取、篡改或删除系统中的重要数据,如电网运行状态、设备参数、用户信息等,导致电力系统运行异常或瘫痪。这不仅会影响电力系统的正常供电,还可能引发一系列连锁反应,如设备损坏、电力负荷失衡等。

此外恶意软件还可能通过电力监控系统向其他系统或网络传播,进一步扩大安全威胁的范围。例如恶意软件可能利用电力监控系统的通信协议或漏洞,向相邻的电力系统或关键基础设施发起攻击,造成更广泛的安全风险。

### 2.2 破坏电力系统的稳定性

电力监控系统的网络安全风险还可能破坏电力系统的稳定性。一旦电力监控系统遭受网络攻击,如分布式拒绝服务攻击(DDoS)、SQL注入攻击等,可能导致系统瘫痪或运行异常。这将直接影响电力系统的正常供电,导致电力中断或电压波动等问题。

电力供应的不稳定会对用户造成极大的困扰,如家用电器损坏、工业生产停滞等。更为严重的是,电力供应中断还可能对交通运输、医疗卫生、公共安全等关键领域造成严重影响,甚至引发社会动荡。

### 2.3 损害电力企业的声誉和经济利益

电力监控系统的网络安全风险还可能损害电力企业的声誉和经济利益。一旦电力监控系统遭受网络攻击,导致电力供应中断或服务质量下降,将直接影响用户对电力企业的信任度和满意度。用户可能会因此对电力企业的服务能力和管理水平产生质疑,进而影响其品牌形象和市场竞争力。

此外网络攻击还可能导致电力企业面临法律风险和赔偿责任。如果电力监控系统遭受网络攻击导致用户遭受损失,电力企业可能需要承担相应的法律责任和赔偿责任。这将进一步增加电力企业的运营成本和经济负担。

综上所述,电力监控系统的网络安全风险对电力系统、电力企业和用户都构成了严重威胁。为了保障电力系统的安全稳定运行和电力企业的可持续发展,必须高度重视电力监控系统的网络安全问题,加强安全防护措施和技术研发,提高系统的安全性和可靠性。同时,还需要加强用户教育和安全意识培训,提高用户的安全防范意识和能力。只有这样,才能有效应对电力监控系统网络安全风险带来的挑战和威胁。

## 3. 电力监控系统网络安全的应对策略

电力监控系统作为电力系统的神经中枢,其网络安全问题直接关系到电力系统的稳定运行和能源安全。为了有效应对电力监控系统面临的网络安全风险,电力企业需要从多个方面入手,加强网络安全防护。以下将详细探讨电力监控系统网络安全的应对策略。

### 3.1 加强网络安全意识培训

提高电力监控系统运维人员的网络安全意识是构建稳固网络安全防线的基石。电力企业必须将网络安全培训置于战略高度，确保运维团队具备应对复杂网络安全挑战的能力。

培训内容的设计需全面且深入，既要包含网络安全的基础知识，如网络架构、协议原理、数据加密等，也要涉及密码管理的重要性，教育员工如何设置强密码并定期更换，以及如何识别并防范钓鱼邮件、恶意软件等常见网络威胁。此外，针对电力监控系统的特殊性，培训还应详细介绍网络攻击的常见手段，如DDoS攻击、SQL注入、跨站脚本攻击等，并教授相应的防范措施和应对策略。

实践是检验真理的唯一标准。因此，培训不应仅限于理论讲解，而应结合模拟攻击和防御演练，让运维人员在真实或接近真实的场景中锻炼技能，提升应急响应速度和处置能力。通过角色扮演、情景模拟等方式，让学员亲身体验从发现威胁到分析、响应、恢复的全过程，从而加深理解和记忆。

为了激发运维人员的学习热情，电力企业应建立科学的网络安全考核机制，将培训成绩与员工的个人发展紧密挂钩。通过设立奖励机制，如表彰优秀学员、提供晋升机会等，鼓励员工积极参与网络安全学习和实践，形成人人重视网络安全、人人参与网络安全建设的良好氛围。这样的激励机制不仅能提升员工的技能水平，更能从根本上增强整个团队的网络安全意识，为电力监控系统的安全稳定运行提供坚实保障。

### 3.2 完善安全制度

完善电力监控系统的安全制度是确保网络安全稳固的基石。电力企业需全方位构建一套详尽的网络安全管理体系，以制度为纲，规范为绳，明确各级人员的职责与权限，为网络安全保驾护航。

1. 电力企业应制定一套全面的网络安全管理制度，涵盖从网络安全策略、安全操作规程到安全审计制度等多个维度。这些制度需贯穿电力监控系统的全生命周期，从设计、建设、运维直至退役，确保每一环节都严格遵循网络安全标准。

2. 建立高效的网络安全事件应急响应机制至关重要。电力企业应精心制定应急预案和处置流程，涵盖事件的识别、

快速报告、有效处置及后期恢复等关键环节。一旦遭遇网络安全事件，能够迅速启动预案，有效控制事态，最大限度降低损失和影响。

3. 在与第三方合作伙伴的合作中，电力企业的网络安全管理同样不容忽视。在与第三方系统或设备接入电力监控系统时，务必签订详尽的网络安全协议，明确双方的安全责任与义务。同时，对第三方系统或设备进行严格的安全审查和测试，确保其符合既定的网络安全标准，从源头上防范潜在的安全风险。通过这些措施，电力企业能够构建起一道坚不可摧的网络安全防线，为电力监控系统的稳定运行提供有力保障。

### 3.3 定期升级网络防火墙和入侵检测技术

网络防火墙和入侵检测系统是防范网络攻击的重要防线。电力企业应定期对电力监控系统的网络防火墙和入侵检测系统进行升级和更新，确保其能够识别和防御最新的网络攻击手段。

1. 电力企业应关注网络防火墙的升级和更新。随着网络攻击手段的不断演变，网络防火墙的防护能力也需要不断提升。电力企业应定期更新防火墙的规则库和算法，提高其对恶意流量的识别和过滤能力。

2. 电力企业应加强对入侵检测系统的配置和优化。入侵检测系统能够实时监测网络流量，发现异常行为并发出警报。电力企业应根据电力监控系统的特点和需求，合理配置入侵检测系统的参数和规则，提高其检测精度和效率。

3. 电力企业还应建立网络安全漏洞管理机制。定期对电力监控系统进行漏洞扫描和修复，确保系统不存在已知的安全漏洞。同时，电力企业还应加强对漏洞信息的收集和整理，及时了解和掌握最新的漏洞信息，为漏洞修复提供有力支持。

综上所述，电力监控系统网络安全的应对策略需要从多个方面入手，包括加强网络安全意识培训、完善安全制度、定期升级网络防火墙和入侵检测技术等方面。只有全面加强网络安全防护，才能确保电力监控系统的安全稳定运行，为电力系统的安全发展提供有力保障。

### 结论

电力监控系统的网络安全是保障电力系统正常运行和供电质量的关键。随着云计算、大数据、物联网等新兴技术在电力监控系统中的广泛应用，电力监控系统面临的网络安

全风险日益复杂和严峻。因此电力企业应加强对电力监控系统网络安全的管理和防范工作,提高员工的网络安全意识,完善安全制度和技术措施,建立数据全生命周期安全保障体系,加强新型电力系统公共管控平台网络安全防护,构建“零信任”架构的接入安全防护体系等。通过这些措施的实施,可以有效降低电力监控系统面临的网络安全风险,保障电力系统的正常运行和供电质量。

**参考文献:**

- [1] 罗骏. 电力监控系统中的网络安全策略分析 [J]. 集成电路应用, 2023, 40(4):184-185.
- [2] 王辉煌. 浅谈电力监控系统网络安全防护问题 [J]. 电子世界, 2020(4):1.DOI:CNKI:SUN:ELEW.0.2020-04-118.
- [3] 黄丹娟. 电力监控系统网络安全防护与关键技术分析 [J]. 华东科技: 综合, 2018(6):1.
- [4] 李凤霞. 电力监控系统网络安全的现状与改进研究 [J]. 数码设计, 2023(12):66-68.
- [5] 黄华伟. 新形势下电力监控系统网络安全风险分析与防护对策 [J]. 大众文摘, 2022(19):0174-0176.