国家电网公司部门文件

调网安〔2018〕10 号

国调中心关于印发《国家电网公司电力监控系统等级保护及安全评估工作规范（试行）》等 3 个文件的通知

各分部，各省（自治区、直辖市）电力公司，南瑞集团，国网新源公司，国网运行公司，国网直流公司，国网交流公司，国网信通公司，中国电科院，联研院：

为规范公司电力监控系统网络安全工作，国调中心组织编制了《国家电网公司电力监控系统等级保护及安全评估工作规范（试行）》、《国家电网公司电力监控系统网络安全事件应急工作规范（试行）》、《并网新能源场站电力监控系统涉网安全防护补充方案》等 3 个文件，现予印发，请各单位遵照执行。

执行中如有问题或建议，请及时反馈国调中心。

联系人： 刘　森 010-66597993

国调中心

2018 年 2 月 8 日

（此件发至收文单位本部及所属二级单位机关）

国家电网公司电力监控系统等级保护及安全评估工作规范（试行）

第一章 总则

第一条 为进一步落实国家和电力行业等级保护及安全评估要求，规范国家电网公司（以下简称公司）电力监控系统等级保护及安全评估工作，提高电力监控系统安全防护水平，依据《中华人民共和国网络安全法》、《信息安全等级保护管理办法》（公通字〔2007〕43号）、《电力监控系统安全防护规定》（国家发展改革委2014年第14号令）和《电力行业信息安全等级保护管理办法》（国能安全〔2014〕318号）等政令法规，制定本规范。

第二条 各单位要按照“谁主管谁负责，谁运营谁负责”的原则，将电力监控系统等级保护及安全评估纳入日常安全生产管理体系，确保等级保护及安全评估工作责任层层落实、具体到人。

第三条 本规范适用于公司所属各单位电力监控系统等级保护及安全评估，以及公司调控机构对并网电厂涉网部分的电力监控系统等级保护及安全评估的技术监督。

第二章 工作分工

第四条 公司各级调控机构负责管辖范围内电力监控系统等级保护及安全防护评估的归口管理，具体包括：

（一） 组织落实国家及行业有关电力监控系统等级保护和安全防护评估的政策法规和标准规范，制定电力监控系统等级保护及安全防护评估的管理制度。

（二） 组织开展公司电力监控系统等级保护、安全防护评估和整改治理等工作。

（三） 负责调管范围内电网调度控制系统、变电站监控系统等级保护及安全防护评估的安全管理。

（四） 负责配电自动化、负荷控制等其它电力监控系统等级保护及安全防护评估的技术管理以及建设实施方案的审查。

（五） 负责调管范围内并网发电厂涉网部分的电力监控系统等级保护及安全防护评估的技术监督管理。

（六） 负责组织公司电力监控系统等级保护和安全防护评估工作的监督检查、评价总结等工作。

第五条 运检、营销、信通等部门分别负责组织本专业管理范围内的配电自动化、负荷控制等系统的等级保护及安全防护评估工作，具体包括：

（一） 负责组织专业管理范围内电力监控系统等级保护及安全防护评估相关的建设管理，并落实国家、行业和公司相关要求。

（二） 负责专业管理范围内电力监控系统定级备案、等保测评、安全评估、整改治理的实施管理。

（三） 负责开展专业管理范围内电力监控系统等级保护和安全防护评估工作情况的统计、检查和评价。

（四） 配合等级保护归口管理部门组织开展专业管理范围内电力监控系统等级保护相关监督检查工作。

第六条 **国网运行公司、信通分公司，各省地检修机构、信通公司负责实施管辖范围内变电站监控系统的等级保护及安全防护评估工作，具体包括：**

（一） 负责落实运营范围内电力监控系统的等级保护和安全防护评估相关的网络安全责任。

（二） 负责开展运营范围内电力监控系统的等级保护和安全防护评估工作。

（三） 负责开展运营范围内电力监控系统等级保护和安全防护评估的问题整改治理工作。

第三章 定级备案

第七条 **根据《电力行业信息安全等级保护管理办法》的规定，电力监控系统的安全保护等级分为四级。**

（一）第一级，电力监控系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

（二）第二级，电力监控系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

（三）第三级，电力监控系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

（四）第四级，电力监控系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第八条公司电力监控系统运营、使用单位应依据《信息安全技术信息系统安全等级保护定级指南》（GB/T 22240-2008）和《电力行业信息系统安全等级保护定级工作指导意见》的要求，规范开展电力监控系统的定级备案工作。

（一）省级以上调控机构的电网调度控制系统的实时监控与预警功能模块的安全保护等级定为四级，调度计划与安全校核功能模块的安全保护等级定为三级，调度管理功能模块的安全保护等级定为二级。地级及以下调控中心的电网调度控制系统的实时监控与预警功能模块的安全保护等级定为三级。独立建设的备调系统可参照同级主调系统进行定级备案。

（二）配电自动化系统、负荷控制系统的安全保护等级定为三级。

（三）公司系统的变电站监控系统作为调度自动化系统子站部分，不作为独立系统定级备案。220 千伏及以上变电站监控系统（含开关站、换流站、集控站等）按等级保护三级进行保护，110 千伏及以下按等级保护二级进行保护。

（四）单机容量 300MW 及以上的火电厂监控系统 DCS（含辅机控制系统）的安全保护等级定为三级，以下定为二级；总装机 1000MW 及以上的水电厂监控系统的安全保护等级定为三级，以下定为二级；总装机容量 200MW 及以上的风电场、

光伏电站监控系统的安全保护等级定为三级，以下定为二级；核电站监控系统 DCS(含辅机控制系统)的安全保护等级定为三级。

第九条 公司系统的变电站监控系统原则上由直接调度管辖的调控机构负责将其纳入电网调度控制系统进行定级备案。多家调控机构共同调管的变电站，由最高一级调控机构或由其委托的调控机构负责。

第十条 公司系统外的其它产权的并网变电站监控系统的定级备案工作由产权方负责。

第十一条 并网发电厂电力监控系统的定级备案由相应发电厂组织开展。

第十二条 在电力监控系统建设或者改建过程中，应选择使用符合国家规定、满足等级保护要求的技术产品，同步建设符合规定等级要求的网络安全设施。

第十三条 新建或改建电力监控系统，应按照国家及行业相关要求及时到市级以上公安机关办理备案手续；系统退役后，应按照国家及行业相关要求及时办理备案撤销手续。

第四章 等保测评

第十四条 电力监控系统建设完成后，电力监控系统各运营单位应依据国家及行业相关标准规范要求，按照规定的周期委托有资质的测评机构开展电力监控系统等级保护测评工作。当系统发生重大升级、等级变化、系统变更或迁移

后需重新进行测评。

第十五条 组织等保测评时，应选择国家信息安全等级保护工作协调小组办公室推荐的、安全可控的测评机构。对于第三级系统，应优先选择电力行业等级保护测评机构或具备 3 年以上电力监控系统安全服务经验的测评机构开展测评；对于第四级系统，应选择电力行业等级保护测评机构且具备 5 年以上电力监控系统安全服务经验的测评机构开展测评。

第十六条 电力监控系统运营单位应当定期对电力监控系统安全状况、安全保护制度及措施的落实情况进行自查。第二级电力监控系统应当每两年至少进行一次自查，第三级电力监控系统应当每年至少进行一次自查，第四级电力监控系统应当每半年至少进行一次自查。

第十七条 电力监控系统经测评或者自查确认未达到安全保护等级要求的，运营、使用单位应当制定方案进行整改。

第十八条 公司范围内的电力监控系统完成等级保护测评后，相关单位应将电力监控系统等级保护测评情况报送同级调控机构和上级专业主管部门。

第五章 安全防护评估

第十九条 各单位应按照《电力监控系统安全防护总体方案等安全防护方案和评估规范》（国能安全〔2015〕36 号）等文件要求，在电力监控系统的建设改造、运行维护和废弃

阶段开展安全防护评估工作。

第二十条 对于第三、第四级电力监控系统，应结合等级保护测评工作委托测评机构同步开展安全防护评估，评估周期最长不超过三年。单个评估周期内，电力监控系统运营单位应每年组织开展一次自评估工作。

第二十一条 对于第二级电力监控系统，应定期开展安全评估工作。评估方式一般采用自评估，评估周期最长不超过两年，也可根据需要委托专业机构进行评估。

第二十二条 电力监控系统在正式投运前，其运营单位应核查系统供应商提供的型式安全评估报告。

第二十三条 第三、第四级电力监控系统投运前或发生重大变更时，应由其建设或技改实施单位负责组织开展上线评估工作，具体实施可委托专业评估机构进行；第二级电力监控系统上线安全评估可按要求自行组织开展。

第二十四条 各单位在开展安全评估工作前，应根据确定的评估范围，对评估过程中可能引入的安全风险进行分析，编制应急预案并落实相关安全措施。

第二十五条 公司范围内的电力监控系统完成安全评估工作后，应将电力监控系统安全评估结论报同级调控机构和上级专业管理部门。

第六章 闭环管理

第二十六条 电力监控系统各运营单位应根据等级保护

测评及安全评估结果制定相应整改计划，明确整改的目标、项目、进度和责任人。

第二十七条 各单位应根据评估发现问题的严重程度，制定科学合理的整改方案。

（一）对于严重问题，应立即制定方案进行整改。

（二）对一般性问题（涉及配置策略调整、特征库更新、补丁安装、版本升级等问题），应限期进行整改。

（三）对于需涉及立项、采购设备、部署系统等的整改，应明确整改计划，并落实过渡期间的安全防护措施。

（四）对具有普遍性或关键性的重大问题，应组织开展技术攻关，研究制定整改方案。

第二十八条 各单位要强化评估发现问题整改的闭环管理，整改完成后应及时进行验收总结，确保整改彻底到位。

第二十九条 各单位要加强等保测评及安全评估工作的保密管理，实施前应签署保密协议，确保评估机构及其实施人员安全可靠，保证评估过程中产生或接触的所有信息得到有效保护。

第三十条 未经公司授权许可，禁止测评机构及其人员向任何第三方泄露等保测评及安全评估中知悉的公司商业秘密、系统信息、防护策略、风险隐患、个人隐私等敏感信息，不得利用测评过程中知悉的信息或漏洞对公司系统内任何单位进行探测和入侵。

第七章 保障监督

第三十一条 各单位应根据电力监控系统等级保护要求，统筹制定下一年度等级保护及安全评估工作计划，保障相关资金列入年度生产费用，确保电力监控系统等级保护测评及安全评估工作顺利开展。

第三十二条 各级调控机构要认真履行指导、检查和监督职责，督促管辖范围内相关单位做好电力监控系统等级保护及安全评估工作。

第三十三条 各级调控机构要加强并网电厂涉网安全防护的技术监督，督促等级保护及安全评估的有效实施。

第八章 附则

第三十四条 本规范由国调中心负责解释。

第三十五条 本规范自印发之日起执行。

国家电网公司电力监控系统网络安全事件应急工作规范（试行）

1 总则

1.1 编制目的

建立健全国家电网公司（以下简称“公司”）电力监控系统网络安全事件（以下简称“网络安全事件”）应急工作机制，最大限度减少网络安全事件的危害与影响，保障电网安全稳定运行和公司正常运营，有效维护社会秩序和国家安全。

1.2 编制依据

《中华人民共和国网络安全法》

《中华人民共和国突发事件应对法》

《国家电网公司安全事故调查规程》

《电力监控系统安全防护规定》

《电力监控系统安全防护总体方案》

《国家电网公司应急工作管理规定》

《国家电网公司应急预案管理办法》

《国家电网公司电力监控系统网络安全运行管理规定（试行）》

1.3 适用范围

本规范适用于公司总部、各分部，省（自治区、直辖市）公司和地（市）公司网络安全事件的应急处置和应急预案管理。

1.4 工作原则

1.4.1 归口管理，分级负责。按照“谁主管谁负责、谁运营谁负责”的原则，建立健全网络安全事件应急工作机制。各级调控机构是本单位网络安全事件应急的归口管理部门，负责调度控制系统和变电站监控系统网络安全事件的应急处置。各级运检、营销部门分别负责配电自动化系统、负荷控制系统网络安全事件的应急处置。

1.4.2 快速响应，处置优先。发生网络安全事件时，应快速发现并定位事件原因，立即隔离危险源，杜绝网络安全风险蔓延，最大限度减少网络安全事件的危害与影响，通过启用备调、备用设备等方式优先恢复系统和网络功能。

1.5 事件分级

根据《国家电网公司电力监控系统网络安全运行管理规定》，网络安全事件分为特别重大、重大、较大、一般四级。

2 应急组织机构

2.1 网络安全事件应急工作是公司专项应急事项，在公司各级应急领导小组和安全应急办公室领导下开展工作。

2.2 公司总部、各分部，省（自治区、直辖市）公司和地（市）公司成立网络安全事件应急处置工作小组（以下简称“应急工作小组”），组长由调控机构负责人担任，成员由运检部、营销部、检修单位、信通公司、电科院等部门（单位）负责人及相关人员担任，负责落实应急领导小组和安全应急办公室部署的网络安全事件应急处置任务，根据网络安

全事件专项应急预案组织跨专业应急处置工作。

2.3 各级调控、运检、营销等电力监控系统运行管理部门分别组织检修单位、信通公司等本专业电力监控系统运维单位成立专业应急处置小组（以下简称“专业处置小组”），负责落实应急工作小组部署的网络安全事件应急处置任务，根据现场处置方案开展本专业应急处置工作。

3 监测与预警

3.1 风险监测

3.1.1 监测信息

运行风险信息：电力监控系统主机、网络、安防设备运行日志、告警、审计等信息。

漏洞预警信息：国家信息安全漏洞共享平台、国家互联网应急中心、国家网络与信息安全信息通报中心等专业机构以及公司红队、重要厂商、网站发布的漏洞和预警。

公共风险信息：公安机关、能源监管机构等上级主管部门的网络安全通报，以及其他有关单位或部门的通知等信息。

3.1.2 监测机构

各级专业处置小组负责监测运行风险信息，联研院负责监测漏洞和预警信息。

3.1.3 风险报告

各级风险监测机构应将监测到的重要风险信息报应急工作小组和相关专业处置小组。

3.2 预警分级

网络安全预警分为四级，由高到低依次用红色、橙色、黄色和蓝色表示，分别对应可能发生特别重大、重大、较大和一般网络安全事件。

3.3 预警发布

蓝色预警由专业处置小组发布，同时报应急工作小组；黄色预警由应急工作小组发布；针对可能导致特别重大和重大网络安全事件的风险信息，应急工作小组应及时汇报应急领导小组，由应急领导小组发布红色及橙色预警（电力监控系统网络安全风险预警发布单模板见附录 1）。

3.4 预警响应

3.4.1 红色、橙色预警响应

（1）预警涉及单位的应急工作小组、相关专业处置小组开展应急值班，重要信息报应急领导小组；

（2）预警涉及单位的相关专业处置小组加强系统巡视、运行监测和安全加固工作，采取有效措施控制事态发展；

（3）预警涉及单位的有关人员进入待命状态，确保备调、备用设备和备用网络通道可用，设备备件充足。必要时可提请上级单位支援。

3.4.2 黄色、蓝色预警响应

预警涉及单位的相关专业处置小组做好巡视、监测、安全加固等工作，确保备用设备和备用网络通道可用。

3.5 预警调整及解除

按照“谁发布、谁调整，谁发布、谁解除”的原则，预警发布单位可根据预警阶段电力监控系统运行情况、预警行动效果，调整预警级别或解除预警，有关情况报应急工作小组。如进入应急响应状态，则预警自动解除。

电力监控系统网络安全预警发布和响应流程见附录 2。

4 应急响应

4.1 响应分级

网络安全事件应急响应分为Ⅰ、Ⅱ、Ⅲ级，分别对应发生重大及以上、较大和一般网络安全事件。

4.2 响应启动

（1）发生重大及以上网络安全事件，由事发单位应急领导小组启动Ⅰ级响应；

（2）发生较大网络安全事件，由事发单位应急工作小组启动Ⅱ级响应；

（3）发生一般网络安全事件，由事发单位相关专业处置小组启动Ⅲ级响应；

（4）因网络安全事件导致发生大面积停电事件时，应汇报至总部应急领导小组启动《国家电网公司大面积停电事件应急预案》进行处置。

4.3 响应行动

4.3.1 Ⅰ级响应行动

（1）事发单位召开应急领导小组会议，就有关重大应急问题做出决策和部署，应急工作小组和相关专业处置小组按照要求进入 24 小时应急值守状态；

（2）应急工作小组和相关专业处置小组根据专项应急预案和现场处置方案组织开展应急处置，按需及时启用备调、备用设备或备用网络通道；

（3）应急工作小组及时将应急处置情况报上级单位，上级单位视事态发展情况及影响范围确定是否需要启动更大范围的应急响应工作。

4.3.2 Ⅱ级响应行动

事发单位应急工作小组和相关专业处置小组根据专项应急预案和现场处置方案组织开展应急处置，有关专业处置小组开展应急值守。应急工作小组汇总分析事件信息，重要信息逐级上报。

4.3.3 Ⅲ级响应行动

事发单位有关专业处置小组根据现场处置方案开展应急处置工作，重要信息报应急工作小组。

4.4 响应调整和结束

响应行动启动后，事发单位应按照“谁启动、谁调整，谁启动、谁结束”的原则，及时根据事件危害程度的变化，调整事件响应级别。在事件及其衍生的其他风险得到有效解决的情况下，应及时结束应急响应。

电力监控系统网络安全事件应急响应及报告流程见附录 3。

5 信息报告

5.1 报告程序

5.1.1 预警阶段

（1）预警发布单位按预警级别逐级上报，红色、橙色预警报至总部，黄色预警报至分部，蓝色预警报至省公司。

（2）预警涉及单位向预警发布单位报告响应行动情况。

5.1.2 应急响应阶段

（1）发生一般网络安全事件，应在 1 小时内报告本级应急工作小组，并逐级上报至省级应急工作小组；

（2）发生较大网络安全事件，应在 30 分钟内报告本级应急工作小组，并逐级上报至分部应急工作小组；

（3）发生重大、特别重大网络安全事件，应在 15 分钟内报告本级应急工作小组，由应急工作小组报告应急领导小组，同时逐级上报至总部应急工作小组。特别重大网络安全事件由总部应急工作小组报告总部应急领导小组及总部网信领导小组。

应急响应结束后，事发单位 3 个工作日内报送《电力监控系统网络安全事件报告》，重大及以上网络安全事件报至总部应急工作小组，较大网络安全事件报至分部应急工作小组，一般网络安全事件报至省级应急工作小组（电力监控系统网络安全事件报告模板见附录 4）。

5.2 报告内容

5.2.1 预警阶段

（1）预警的发布、调整和结束情况。

（2）预警涉及单位的电力监控系统运行情况、风险发展趋势和已采取的措施等信息。

5.2.2 应急响应阶段

（1）网络安全事件发生的时间、地点和影响范围，事件描述及原因分析，对公司及社会的影响，已采取的措施等。

（2）系统受损情况，事件处置进展及发展趋势，应急技术力量、备品备件需求等情况。

6 后期处置

6.1 善后处置

6.1.1 事发单位整理受损系统、设备资料，及时更新网络拓扑结构和设备台账信息，做好系统数据备份。

6.1.2 事发单位尽快恢复系统正常运行方式，取代应急处置中采取的临时措施。

6.1.3 事发单位认真开展隐患排查和治理工作，避免再次发生同类事件。

6.2 事件调查

网络安全事件的调查依照公司安全事故调查相关规定执行。

6.3 应急处置评估

应急处置结束后，上级应急工作小组应对事发单位网络

安全事件应急处置情况进行评估，重点评估应急指挥、应急响应、系统恢复、信息报告等环节。重大及以上事件由总部组织评估，较大事件由分部组织评估，一般事件由省公司组织评估。

7 预案管理

7.1 各级应急工作小组负责组织编制网络安全事件专项应急预案，各专业处置小组负责编制网络安全事件现场处置方案。

7.2 专项应急预案的评审和实施由本单位调控机构负责组织。现场处置方案的评审和实施，由本单位各专业运行管理部门负责组织。

7.3 各单位每年应至少组织一次应急演练，重点加强联合演习，验证预案的有效性和操作性。

7.4 应急预案每三年至少修订一次；当电力监控系统自身或运行环境发生变化时，应及时修订应急预案。

8 附则

8.1 本规范由国调中心负责解释并监督执行。

8.2 本规范自发布之日起执行。

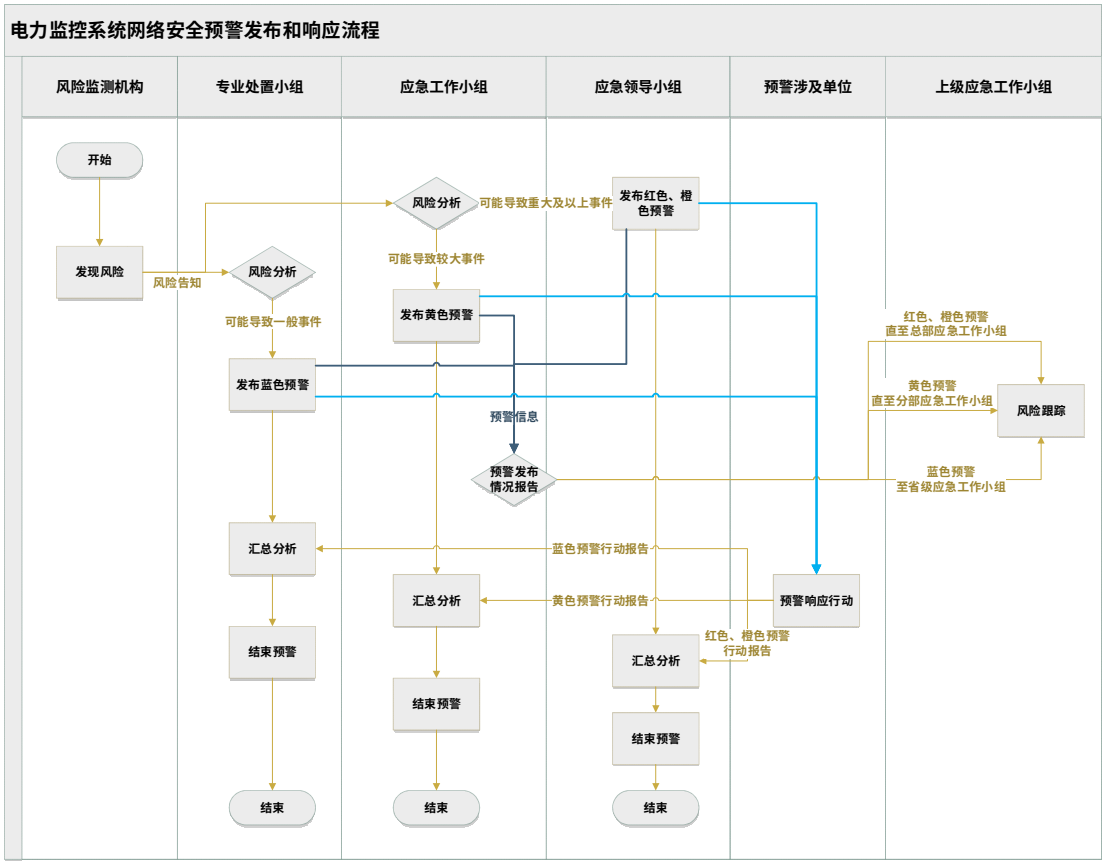
附录

附录 1 电力监控系统网络安全风险预警发布单

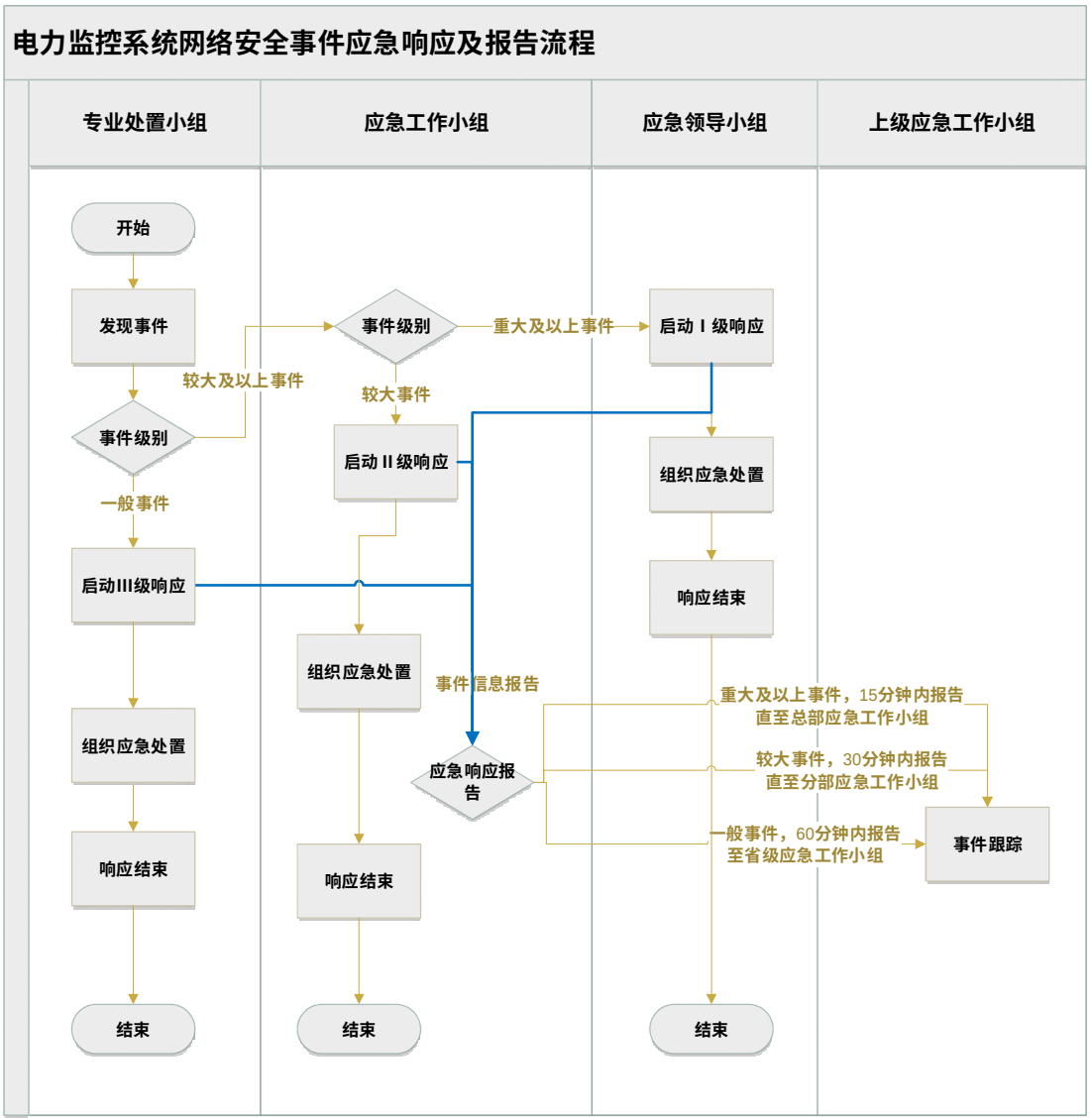
<table>
<tr><td colspan="4">电力监控系统网络安全风险预警发布单

预警通知〔****〕 第*号</td></tr>
<tr><td>发布部门</td><td colspan="3"></td></tr>
<tr><td>发布时间</td><td></td><td>签发人</td><td></td></tr>
<tr><td>预警级别</td><td colspan="3">□红色 □橙色 □黄色 □蓝色</td></tr>
<tr><td>主送单位</td><td colspan="3"></td></tr>
<tr><td>预警内容</td><td colspan="3"></td></tr>
<tr><td>预防措施</td><td colspan="3"></td></tr>
</table>

附录 2 电力监控系统网络安全预警发布和响应流程



附录 3 电力监控系统网络安全事件应急响应及报告流程



附录 4 电力监控系统网络安全事件报告

电力监控系统网络安全事件报告			
事件名称		事件等级	
发生时间		结束时间	
受影响范围			
事件描述			
原因分析			
处理情况			
后续防范措施			
单位（盖章）： 日期：			

并网新能源场站电力监控系统涉网安全防护补充方案

1．总则

1.1 为满足风电、光伏快速发展和大规模并网需要，有效治理并网新能源场站电力监控系统涉网安全防护问题，指导公司调控机构做好涉网安全防护技术监督，制定本方案。

1.2 本方案是在《电力监控系统安全防护总体方案》、《发电厂监控系统安全防护方案》（国能安全〔2015〕36 号）等行业文件的基础上，补充完善了新能源场站第三方边界、终端通信安全、安全接入区、监测应急等方面的要求，适用于并网风电场、光伏电站，以及通过数据网络与其生产控制大区相连接的汇集站及集控中心。

1.3 方案未及内容，应遵照《中华人民共和国网络安全法》、《电力监控系统安全防护规定》、《信息安全等级保护管理办法》、《电力监控系统安全防护总体方案》等国家法律法规和行业规范执行。

2．安全分区及边界防护

2.1 安全分区

2.1.1 新能源场站电力监控系统原则上划分为生产控制大区和管理信息大区。根据业务功能可能对一次设备造成的影响，生产控制大区可进一步划分为控制区（安全Ⅰ区）和非

控制区（安全II区），管理信息大区可进一步划分为安全III区和安全IV区。生产控制大区内业务系统使用公用通信网络、无线通信网络以及其它安全不可控网络与终端进行通信的，应设立安全接入区。

2.1.2 新能源场站电力监控系统原则上应严格遵循安全分区的部署要求。对于装机规模较小的场站，可在保持生产控制大区与管理信息大区之间物理隔离的前提下，简化两个大区内部的分区，但低安全区的系统和功能应按照高安全等级分区的要求进行管理。

2.13 不同安全分区的交换机或相当功能的网络设备，必须单独使用，严禁通过划分 VLAN 的方式将不同安全分区的设备接入同一交换机。

2.14 不同分区的设备必须连接到不同的网段，严禁主机设备通过双网卡等手段实现跨区联接。同一安全区内部不同业务系统进行数据交互时，应采取 VLAN 划分、访问控制等安全措施，控制交互的规模和频度，禁用 E-Mail、RLOGIN、FTP 等公共服务，控制区内禁止通用的 WEB 服务。

2.15 不同分区的设备不宜安装在同一屏柜内，确需组装在同一屏柜的，设备及网线必须要有明显规范的分区标识。

2.2 横向边界防护

2.2.1 生产控制大区与管理信息大区的边界防护

生产控制大区与管理信息大区之间必须采取物理隔离

措施，部署经国家指定部门检测认证的电力专用横向单向隔离装置。信息由生产控制大区传输到管理信息大区必须经过正向型隔离装置，信息由管理信息大区传输到生产控制大区必须经过反向型隔离装置。

2.2.2 安全Ⅰ区与安全Ⅱ区之间的边界防护

生产控制大区分设安全Ⅰ区与Ⅱ区的，Ⅰ区与Ⅱ区之间的数据通信应采取逻辑隔离措施，边界上应部署硬件防火墙或功能相当的设备。防火墙相关功能、性能必须经过国家指定机构的认证和检测。

2.2.3 安全III区与安全IV区之间的边界防护

安全III区与安全IV区之间的边界处必须部署硬件防火墙或功能相当的设备，防火墙的安全策略应采用白名单方式，禁止开启与业务无关的地址和服务端口。与生产管理无关的办公业务或生活网络应划分到安全IV区。

2.3 纵向边界防护

2.3.1 新能源场站生产控制大区在调度数据网入口的纵向边界，必须配备电力专用纵向加密认证装置，实现双向身份认证、访问控制和数据加密。纵向加密认证装置的隧道配置策略应细化至 IP 地址和服务端口，保证与主站的数据通信均为密通状态，并全面关闭不必要的服务和端口。场站侧纵向加密认证装置必须使用调控机构签发的调度数字证书，并接入调控机构网络安全管理平台。

2.3.2 新能源发电企业若采用汇聚站对区域内多个场站进行集中监视时，应通过专用网络组网并在场站纵向连接处部署电力专用纵向加密认证装置或加密认证网关。

2.3.3 新能源场站要制定运行管理制度，加强纵向加密认证装置的操作员卡（包括主卡及备卡）、Ukey 等身份认证工具的使用与管理，保证调试工作结束后及时收回并妥善保管相关卡证。

2.3.4 接入调度数据网的路由器、交换机必须采取有效的安全加固措施，关闭通用网络服务和网络边界的 OSPF 路由功能，避免使用默认路由，采用安全增强的 SNMP V2 及以上版本的网管协议，密码强度应满足国家规定要求，开启访问控制列表等安全措施。

2.4 其它网络边界的安全防护

2.4.1 新能源场站与远程集控中心、远程监视中心、设备制造厂商的纵向边界安全防护实施方案必须经调控机构审核，安全设备配置策略必须经过现场验证确认安全。

2.4.2 新能源发电企业远程集控中心与站端监控系统的数据传输通道，必须在物理层面实现与其它数据网络的安全隔离，应采用基于 SDH/PDH（推荐使用 SDH）不同通道、不同光波长、不同纤芯等方式的专用独立网络。当采用 EPON、GPON 或光以太网络等技术时应使用独立纤芯或波长。场站与集控中心纵向联接处应当设置经国家指定部门检测认证的电力

专用加密认证装置或者加密认证网关，实现双向身份认证、访问控制和数据加密。远程集控中心监控系统严格遵守《电力监控系统安全防护规定》及其配套文件的要求，并按照等保三级系统进行规划、建设、运维和管理。

2.4.3 新能源企业远程监视中心（具备场站数据的采集、监视和收集功能，但不具备控制功能），原则上应遵循与远程集控中心相同的网络和安全防护要求。如若通过运营商专用网络或 VPN 通道进行数据传输，必须在场站生产控制大区出口处部署电力专用横向单向隔离装置（正向型），实现数据从生产控制大区向外部的安全单向传输，禁止数据从外部向生产控制大区传输、开展远程控制和运维业务。

2.4.4 严格控制新能源场站生产控制大区与设备厂商之间的网络连接。确需将设备运行数据发送给设备厂商的，需在明确数据使用范围的前提下，设立专用服务器，并经过电力专用正向型隔离装置实现数据从生产控制大区向外部的安全单向传输。禁止数据从外部向生产控制大区传输、开展远程控制和运维业务。

2.4.5 网络边界部署的安防设备（防火墙、正向隔离装置、纵向加密认证装置等）应按照最小化原则配置安全策略。

2.4.6 严格保证与调控机构通信的采集服务器的独立性，严禁将其用于给非调控机构的其他单位转发数据。

2.5 就地终端接入防护

2.5.1 新能源场站须加强户外就地采集终端（如风机控制终端、光伏发电单元测控终端等）的物理防护，强化就地采集终端的通信安全。站控系统与终端之间网络通信应部署加密认证装置，实现身份认证、数据加密、访问控制等安全措施。终端连接的网络设备需采取 IP/MAC 地址绑定等措施，禁止外部设备的接入，防止单一风机或光伏发电单元的安全风险扩散到站控系统。

2.5.2 生产控制大区严禁任何具有无线通信功能设备的直接接入。站控系统与就地终端的连接使用无线通信网或者基于外部公用数据网的虚拟专用网路（VPN）等的，应当设立安全接入区。安全接入区与生产控制大区连接处应部署电力专用单向隔离装置，实现内外部的有效隔离。

3．综合安全防护管理

3.1 新能源场站应按照现场实际的网络拓扑和安全设备部署情况，编制新能源场站电力监控系统安全防护实施方案并提交审核，网络结构变更或业务系统增加时，应及时修订安全防护实施方案并重新提交审核。

3.2 新能源场站应严格落实用户身份认证、权限合理划分要求，实施用户的实名制和身份的安全认证。严禁网络设备、服务器、工作站、安全设备使用默认用户和口令。

3.3 新能源场站应建立电力监控系统安全防护日常巡视制度。现场运维工作需严格履行工作票制度，并做好安全措施，

严禁生产控制大区随意接入移动介质和便携式电脑。严禁运维过程中出现跨区直连、生产控制大区设备接入互联网、停运安防设备、开启空闲端口等行为。

3.4 新能源场站应按照《电力行业信息安全等级保护管理办法》要求，及时到公安机构开展电力监控系统定级备案；选择具有国家认可资质的测评机构，开展电力监控系统等级保护测评及安全防护评估，及时整改测评或评估发现的问题。

3.5 生产控制大区涉网部分的服务器、工作站、路由器等设备，应使用安全操作系统并加强安全配置管理。对于已经运行且使用非安全操作系统的设备，要采取防病毒、加强配置管理、强化访问控制等安全加固措施，并结合后续技术改造升级更换为安全操作系统。

3.6 生产控制大区中的业务系统应选用符合国家安全要求、无安全漏洞的产品，相关设备应通过相关部门指定的入网检测。

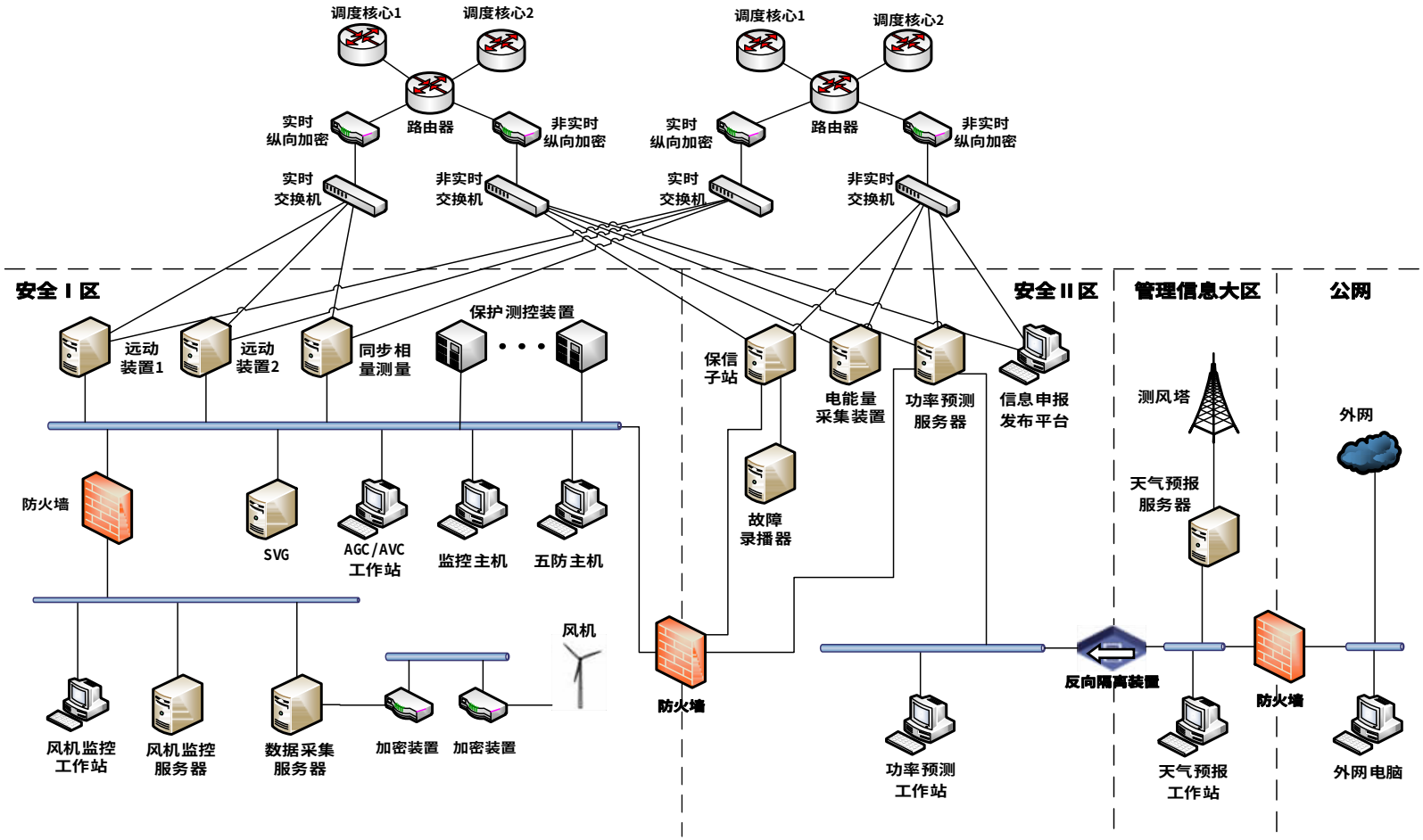
4．监测与应急

4.1 新能源场站应按照国家主管部门要求，在站内部署网络安全监视手段，实现涉网主机设备（包括服务器、工作站、网络设备、安全防护设施等）网络安全的实时监视、告警、分析和审计，并将重要告警信息接入相应的调控机构。

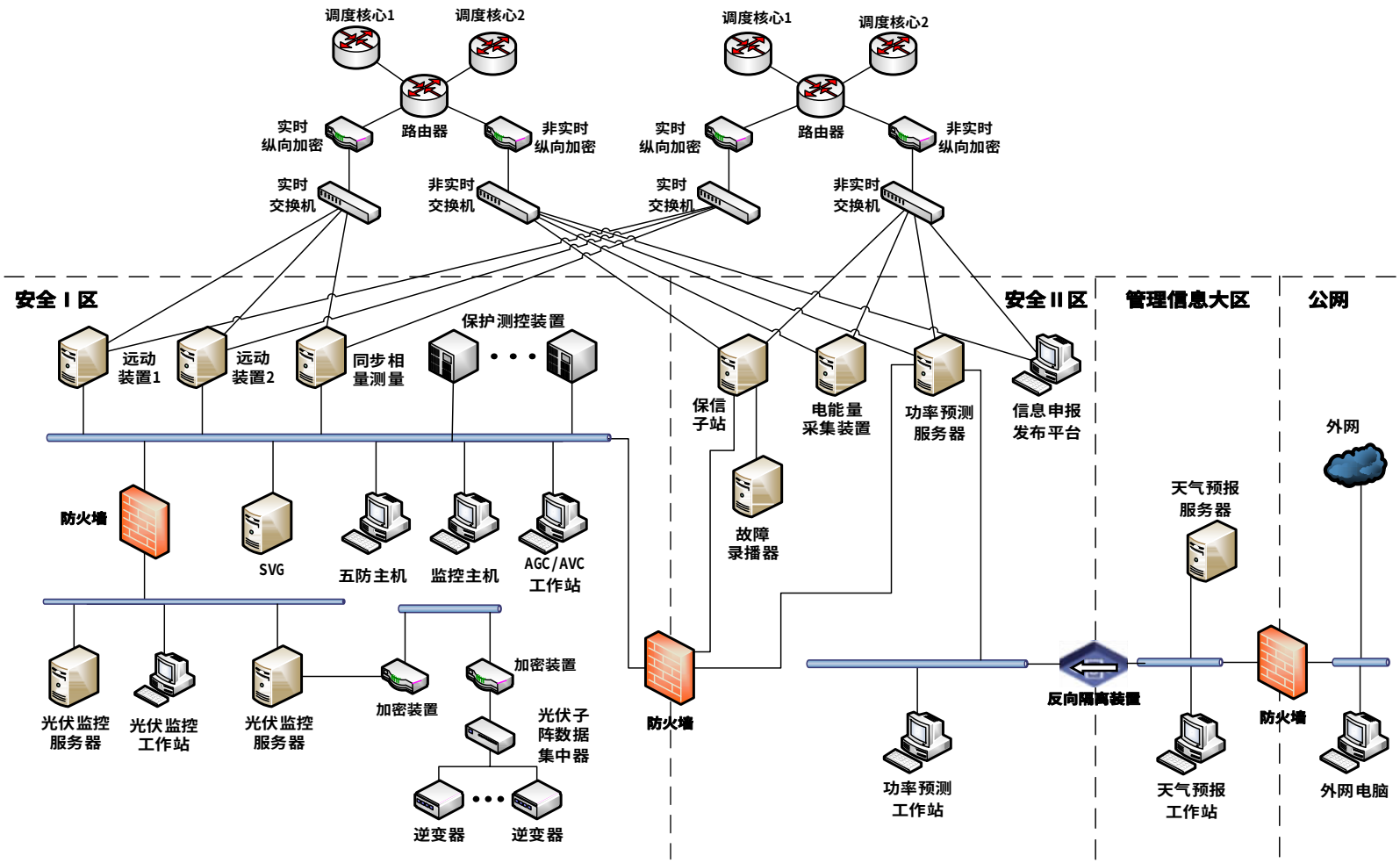
4.2 新能源场站要制定切实可行的安全防护应急预案，定期开展应急演练，提高网络安全应急事件的处置能力。

4.3 健全厂网联动的网络安全应急处置机制，当站内遭受网络攻击、发生网络安全事件时，应立即向相关调控机构报告，并按应急预案采取应急处置措施，防止事态扩大。

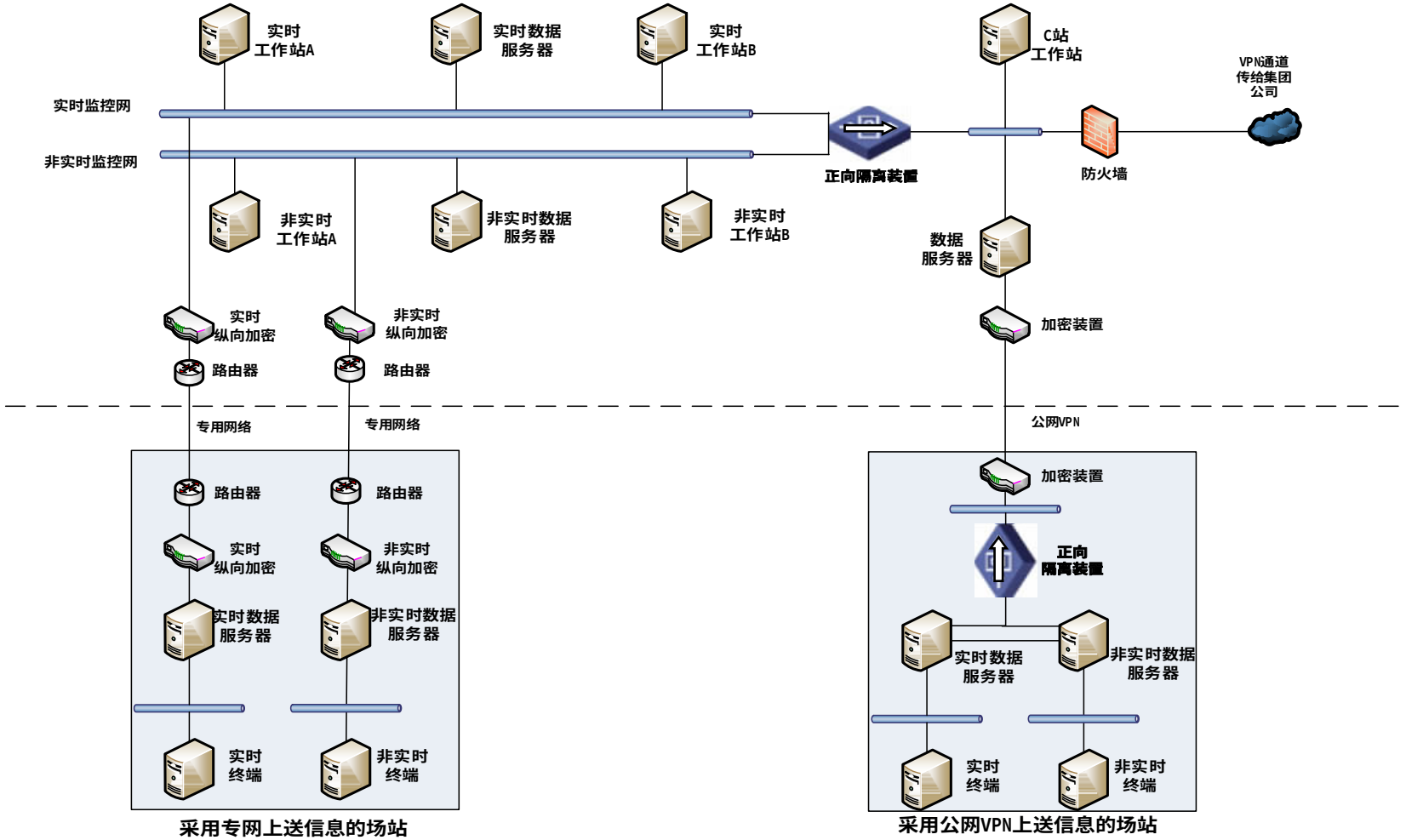
附录：1.风电场典型网络拓扑图



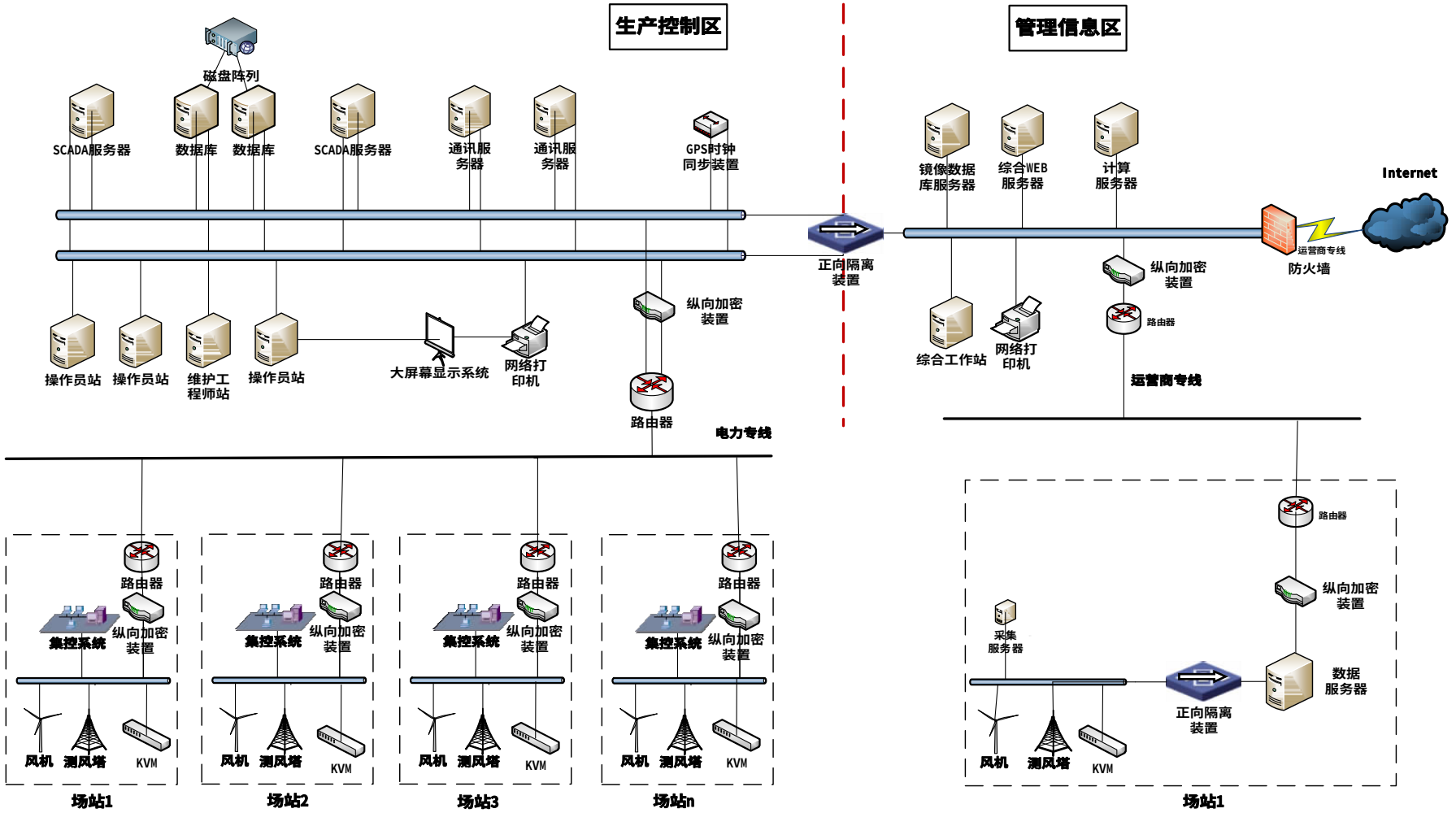
2.光伏电站典型网络拓扑图



3.新能源汇聚站典型网络拓扑图



4.新能源远程集控中心典型网络拓扑图



抄送：国家电网公司运维检修部，国家电网公司营销部（农电工作部），国家电网公司基建部，国家电网公司信息通信部。

国家电网公司办公厅　　2018 年 2 月 8 日印发