新能源电站二次系统安全防护

管理指导手册

2016 年 4 月

一、 编制目的

为指导青海新能源发电公司做好电力二次系统安全防护工作，保障青海电网二次系统网络安全，提高抵御黑客、病毒、恶意代码等各种形式的恶意破坏和攻击，特别是抵御集团式攻击的能力，防止电力二次系统崩溃和瘫痪及由此造成的电力系统事故，依据《电力监控系统安全防护规定》（发改委 14 号令）相关规定要求，特编制本指导手册。

二、 组织体系

新能源发电公司电力二次系统安全防护应按照“谁主管谁负责谁运营谁负责”的原则,建立电力二次系统安全防护组织体系，明确人员职责，将电力二次系统安全防护及其信息报送纳入日常安全生产管理体系。新能源发电公司组织体系设置如下图。

各岗位角色对应业务如下表。

序号	公司二次安防专（兼）责	电站二次安防专（兼）责	电站运行人员
1	负责执行和贯彻国家、电力行业和上级颁布的有关电力二次系统安全防护的标准。	负责执行和贯彻国家、电力行业和上级颁布的有关电力二次系统安全防护的标准。	负责执行和贯彻国家、电力行业和上级颁布的有关电力二次系统安全防护的标准。
2	制定发电公司调度数据网、安全防护设备运维管理有关标准和配套制度。	执行发电公司调度数据网、安全防护设备运维管理有关标准和配套制度。	执行发电公司调度数据网、安全防护设备运维管理有关标准和配套制度。
3	指导公司系统内二次系统升级改造工作。	组织开展站内二次系统升级及改造工作。	配合站内二次安防专责开展二次系统升级及改造工作。
4	审核公司系统内二次系统安全防护技术改造方案。	编制电站二次系统安全防护技术改造方案。	参与编制电站二次系统安全防护技术改造方案。
5	监督检查公司系统内二次系统安全防护工作，确保二次系统安全防护工作实施落实。	根据公司二次系统安全防护工作，落实实施电站二次系统安全防护工作。	根据公司二次系统安全防护工作,落实实施电站二次系统安全防护工作。
6	负责组织新能源发电公司二次安防培训工作。	参加新能源发电公司组织的二次安防培训，负责站内二次安防培训工作。	参加新能源发电公司及电站组织的二次安全防护培训工作。

7	参加调度机构组织的电力二次系统网络信息安全防护培训。	参加调度机构组织的电力二次系统网络信息安全防护培训。	参加调度机构组织的电力二次系统网络信息安全防护培训。
8	参加新改扩建电站二次系统工程自验收和电网公司组织的并网验收。	参加新改扩建电站二次系统工程自验收和电网公司组织的并网验收。	参加新改扩建电站二次系统工程自验收。
9	组织开展公司系统内二次系统安全防护检查工作	参加公司系统内二次系统安全防护检查工作。	配合开展电力二次系统安全防护各项检查工作。
10	建立公司系统内二次安防设备台帐。	准确掌握电站内二次系统安放设备的运行状态，建立电站设备台帐。	掌握电站内二次系统安放设备的运行状态,发现运行故障及时汇报站内二次安防专责。
11		加强电站二次系统实施厂商的管理，避免因厂商行为导致的安全防护事件发生。	加强电站二次系统实施厂商的管理，避免因厂商行为导致的安全防护事件发生。
12		开展电力二次系统运行设备日常巡视及维护，发现问题、缺陷及故障隐患及时处理。	开展电力二次系统运行设备日常巡视及维护，发现问题、缺陷及故障隐患及时向电站二次安防专责汇报。
13		向相应调度机构提报电站二次系统安全防护设备的图纸和技术资料。	
14		根据设备运行情况，负责电站安全防护装置的检修申请及实施工作。	
15		参与电站二次系统安全防护技术改造项目和验收。	
16		编制电站二次系统安全防护应急处置方案，及时上报电站二次系统安全防护事件，参与信息安全事件的调查，提出并落实整改、反措要求。	
17		按时统计上报电站安全防护设备的运行信息。	
备注：公司生产主管领导是公司安全生产第一责任人，通过组织开展公司系统内电力二次系统安全防护专业管理工作，实现公司系统内电力二次系统网络及信息安全。			

三、 二次系统安全防护管理

（一）项目前期

1.设计阶段

在设计阶段，新能源发电公司应协调设计单位，按照《电力监控系统安全防护规定》相关要求同步开展二次安防实施方案（含网络拓扑图）设计工作。实施方案经本单位内部审查合格后，还应报送相应调度机构审查。

2．建设阶段

（1）在设备及系统采购阶段，新能源发电公司制定符合《电力监控系统安全防护规定》要求的设备采购技术规范书，要求投标厂商提供的设备必须具有国家指定机构安全检测证明、电力系统电磁兼容检测证明，同时提供设备在行业内的应用案例。

（2）在设备安装阶段，新能源发电公司严格按照调度机构批复的二次系统安全防护实施方案，组织施工单位开展二次系统的安装。严格按照机房及设备资源标准化规范要求，开展机房及设备资源标准化建设工作，根据二次系统业务分区，采用不同颜色的网络线缆对系统网络进行标识，同时做好线缆敷设工艺及标识标牌张贴悬挂。

（3）在系统调试阶段，按照“最小化”原则，设置安全防护设备安全策略，配置网络路由。生产控制大区的各业务系统禁止以各种方式与互联网连接；关闭或拆除主机的光盘驱动、USB 接口等；系统或设备调试，不得旁路纵向加密认证装置、防火墙、横向隔离装置。

（4）在自验收阶段，发电公司组织公司二次安防专责、电站二次安防专责按照调度机构批复的二次系统安全防护实施方案进行系统检查，确保满足以下条件。

1）二次安防结构和策略符合规程规定。

a.生产控制大区与管理信息大区之间应采用电力专用横向单向安全隔离装置，并正确配置安全策略；

b.电站向发电公司（集团）总部或其他第三方部门发送数据时，与运行在管理信息大区的数据接口机之间应部署电力专用横向单向安全隔离装置，并正确配置安全策略；

c.安全区 I 与安全区 II 之间应部署防火墙，并正确配置安全策略；

d.生产控制大区系统与调度端系统通过电力调度数据网进行远程通信时，应采用纵向加密认证装置，并正确配置安全策略，严禁明通方式与调度机构通信；

e.服务器、工作站、变电站自动化系统后台机等计算机设备 USB 接口应封锁，window 系统应安装杀毒软件；

f.自动化系统用户密码应杜绝账号借用、账号公用、随意使用管理员账号等情况，账户密码应由字母、数字等组合，区分大小写，并在 8 位以上。

2）二次安防各项资料完备，应包含但不限于以下内容：

a.上级部门规程规定：电力监控系统安全防护规定，电力二次系统安全防护总体方案，风电、光伏和燃气电厂二次系统安全防护技术规定；

b.二次安防技术资料：电站二次安防实施方案，电站二次安防网络拓扑图，站内二次安防设备说明书及检测合格证；

c.电站与相关二次厂商签订的合规性承诺书和保密协议。

3）已建立二次安防运维管理制度，明确了电站二次安防责任分工、运行维护规定、工作流程和管理要求。

4）配置 2 名及以上站内二次安防专（兼）职人员，组织完成站内二次安防专责和运行人员的二次安防知识培训及考试。

（二）验收阶段

新能源发电公司在完成电站二次安防自验收后，应出具自验收结论。在向电力交易部门上报并网验收申请时，同步向调度机构报送二次安防自验收资料，包括：二次安防自验收结论、二次安防网络拓扑图、二次安防运行管理规定、二次系统厂商管理规定、二次系统厂商合规性承诺书及保密协议。对未按规定报送或资料不符合要求的，电网企业不予安排并网验收。

发电公司相关人员配合电网公司组织的现场验收，对验收组提出的二次安防问题进行详细记录，并及时组织整改，在验收组复查合格后，方可认为验收通过。

（三）运行阶段

1.人员培训及管理

公司二次安防专责应每年组织电站二次安防专责及运行人员开展一次二次安防专项知识培训，内容须包括《电力监控系统安全防护规定》及调度机构相关要求、发电公司相关制度、电站二次系统安全防护方案等。

公司二次安防专责应加强厂家技术人员管理，制定厂家技术人员管理办法，电站每年与厂商技术人员签订二次安全防护合规性承诺书及保密协议。

在厂商技术人员开展相关工作前，电站二次安防专责需对其进行二次安防培训及考试，明确交代二次安防注意事项，同时做好工作全过程监护，杜绝由于厂家技术人员工作随意及失误而导致的二次安防违规事件。

2.巡视管理

为规范电站二次安防设备巡视工作，电站二次安防专责和运行人员需将二次安防设备巡视纳入自动化系统日常巡视，同时结合省调下发的《新能源电站二次安防月度巡视作业指导书》（见附件 4），开展二次安防设备月度巡视工作，重点检查二次安防结构和策略是否合规、二次安防网络拓扑图是否与现场“图实”相符，对发现问题应及时组织整改。

3.检修管理

凡涉及电站二次安防结构变更、二次安防设备退运或对调度业务造成影响的二次系统运维检修工作，均应办理工作票，并履行签字许可手续。工作票上所填写的检修设备及工作内容应清晰明了，风险点、注意事项、安全措施等应考虑周全，重点做好二次系统安全防护风险分析，并采取有效的应对措施，避免因二次设备检修造成二次安防事件发生。现场检修安

全风险及管控措施参考新能源电站二次设备现场检修安全防护风险提示卡（见附件 2）。

对电站二次安防网络结构变更，应及时组织更新网络拓扑图，并于变更后 3 个工作日内上报相应调度机构。

4.应急管理

新能源发电公司应制定切实可行的二次安防应急预案，并定期组织开展应急演练，确保紧急情况下，及时隔离和处置安全事件，避免事件扩大，出现电网安全事故。

5.安全评估与持续改进

新能源发电公司应每年上半年、下半年各开展一次所辖电站二次安防专项检查即自评估工作，制定详细的检查工作方案和细则，对检查中发现存在问题，积极督促落实整改。

同时新能源发电公司应积极配合能源局、调控机构组织的二次安防专项检查，对检查中发现存在问题，积极督促落实整改，持续提升新能源发电公司二次系统安全防护能力。

新能源发电公司应根据所辖电站二次安防自评估情况，必要时候邀请第三方具备资质的检测机构对公司所辖电站二次系统的总体安全防护水平进行安全评估，及时发现和整治二次安防隐患，避免二次安防事件发生。

附录：

附录 1 新能源电站二次安全防护相关标准、制度清册

附录 2 新能源电站二次设备现场检修作业安全防护风险提示卡

附录 3 新能源电站新建二次系统或设备接入安全防护风险提示卡

附录 4 新能源电站二次设备日常使用安全防护风险提示卡

附录 5 新能源电站二次设备安全防护现场验收提示卡

附录 6 变电站（发电厂）第二种工作票（样票）

附录 7 新能源电站二次系统安全防护设备月度巡检作业指导书

附录 8 新能源电站（厂站）二次系统安全防护检查表

附录

附录 1 新能源发电公司及电站二次安防制度及记录清册

新能源发电公司及电站二次安防制度及记录清册

级别	类别	文件名称
公司	制度或规定	XX公司二次系统安全防护管理规定
		XX公司二次系统安全防护评估办法
		XX公司二次系统厂商现场工作管理规定
		XX公司所辖电站二次安防专项检查工作方案（含检查细则）
		……
	台账或记录	XX公司所辖电站二次系统设备清单
		XX公司所辖电站二次系统网络拓扑图
		XX 公司所辖电站二次安防专（兼）职人员安防知识培训及考试记录
		XX 公司所辖电站二次安防专项检查工作报告（含问题清单及整改计划）
		……
电站	制度或规定	XX电站二次系统系统安全防护实施方案
		XX电站二次系统接入调度数据网技术方案
		XX电站二次系统安全防护运行管理规定
		XX电站二次系统安全防护应急预案
		XX电站二次系统安全防护自评估方案
		XX电站二次系统厂商现场工作管理规定
		XX电站二次系统现场作业风险提示卡
		……
	台账或记录	XX电站二次系统设备清单
		XX电站二次系统网络拓扑图
		XX电站二次系统安全防护自评估报告
		XX电站二次系统厂商合规性承诺书

		XX电站二次系统厂商保密协议
		XX电站二次系统检修记录及检修工作票
		XX电站二次系统月度安全防护巡视记录
		XX电站二次系统厂商安全防护考试记录
		XX电站运行人员安防知识培训及考试记录
		……

2 新能源电站二次设备现场检修作业安全防护风险提示卡

序号	工作类型/内容	典型风险	管控措施
一、计算机监控系统			
1	后台机调试及维护	1. 无线网卡插在后台机上。 2. 紧急情况厂家远程维护后台机。 3. 站内未安排专人对厂家行为进行监控。 4. 未经过杀毒的调试终端直接连接在后台机。 5. 现场接线与实施方案中网络拓扑图不一致。 6. 后台机非安全操作系统（国产且经权威安全部门检测），未安装杀毒软件，未定期杀毒。 7.ftp 、telnet 等通用服务未关闭。 8. 后台机空闲网络端口、USB接口、光驱等接口未关闭。 9. 用户密码分配及管理不符合规范要求。 10. 后台机配置存在多余 IP 地址及与业务无关的路由配置。 11. 与二区功率预测系统之间未配置防火墙或未按照“最小化”原则配置策略。 12. 随意使用未经杀毒的移动存储或笔记本电脑进行数据导出。	1. 与调试厂商签订二次安防合规性承诺书和保密协议。 2. 严禁无线网卡插在后台机。 3. 严禁厂商远程维护。 4. 调试前，调试终端应进行杀毒，确保设备中无病毒软件后再开展调试。 5. 现场工作，专人对厂商行为进行监控。 6. 严格按照现场网络拓扑图开展工作。 7. 后台机安装安装安全操作系统，杀毒软件，并定期升级杀毒软件。 8. 关闭 ftp 、telnet 等通用服务。 9. 关闭后台机空闲网络端口、USB接口、光驱等接口。 10. 严格执行用户账号及密码管理制度。按照实际情况设备用户名和密码，密码应满足不少于 8 位的字母、数字、字符的组合 11. 删除后台机多余 IP 地址及与业务无关的路由配置。 12. 与二区功率预测系统之间配置防火墙，按照“最小化”原则配置防火墙策略。 13. 数据导出前，须将所使用的移动存储或笔记本电脑

2	远动机调试及维护	1. 无线网卡插在远动机上。 2. 紧急情况厂家远程维护远动机。 3. 站内未安排专人对厂家行为进行监控。 4. 未经过杀毒的调试终端直接连接在远动机。 5. 现场接线与实施方案中网络拓扑图不一致。 6. 远动机非安全操作系统（国产且经权威安全部门检测），未安装杀毒软件，未定期杀毒。 7.ftp 、telnet 等通用服务未关闭。 8. 远动机空闲网络端口、USB接口、光驱等接口未关闭。 9. 用户密码分配及管理不符合规范要求。 10. 远动机配置存在多余 IP 地址及与业务无关的路由配置。 11. 与主站数据交互绕过纵向加密装置或纵向加密未明通模式。 12. 纵向加密装置策略未按照“最小化”原则配置。	1. 与调试厂商签订二次安防合规性承诺书和保密协议。 2. 严禁无线网卡插在远动机。 3. 严禁厂商远程维护。 4. 调试前，调试终端应进行杀毒，确保设备中无病毒软件后再开展调试。 5. 现场工作，专人对厂商行为进行监控。 6. 严格按照现场网络拓扑图开展工作。 7. 远动机安装安全操作系统，杀毒软件，并定期升级杀毒软件。 8. 关闭 ftp 、telnet 等通用服务。 9. 关闭远动机空闲网络端口、USB接口、光驱等接口。 10. 严格执行用户账号及密码管理制度。 11. 远动机配置存在多余 IP 地址及与业务无关的路由配置。 12. 与主站数据交互配置纵向加密装置，且纵向加密非明通模式。 13. 纵向加密装置策略按照“最小化”原则配置。

		1. 紧急情况厂家远程维护交换机。 2. 站内未安排专人对厂家行为进行监控。 4. 未经过杀毒的调试终端直接连接在交换机。 5. 现场接线与实施方案中网络拓扑图不一致。 6. 空闲网络端口、USB接口等接口未关闭。 10. 远动机配置存在多余 IP 地址及与业务无关的路由配置。 11. 与主站数据交互绕过纵向加密装置或纵向加密未明通模式。 12. 纵向加密装置策略未按照“最小化”原则配置。	1. 与调试厂商签订二次安防合规性承诺书和保密协议。 2. 严禁无线网卡插在远动机，严禁厂商远程维护。 3. 现场工作，专人对厂商行为进行监控，严格按照现场网络拓扑图开展工作。 4. 远动机安装安全操作系统，杀毒软件，并定期升级杀毒软件。 5. 关闭 ftp 、telnet 等通用服务。 6. 关闭远动机空闲网络端口、USB接口、光驱等接口。 7. 严格执行用户账号及密码管理制度。 8. 与主站数据交互配置纵向加密装置，且纵向加密非明通模式。 9. 纵向加密装置策略按照“最小化”原则配置。
4	AGC/AVC服务器维护	1. 无线网卡插在服务器上。 2. 紧急情况厂家远程维护服务器。 3. 站内未安排专人对厂家行为进行监控。 4. 未经过杀毒的调试终端直接连接在服务器。 5. 现场接线与实施方案中网络拓扑图不一致。 6. 服务器非安全操作系统（国产且经权威安全部门检测），未安装杀毒软件，未定期杀毒。 7.ftp 、telnet 等通用服务未关闭。	1. 与调试厂商签订二次安防合规性承诺书和保密协议。 2. 严禁无线网卡插在后台机。 3. 严禁厂商远程维护。 4. 现场工作，专人对厂商行为进行监控。 5. 严格按照现场网络拓扑图开展工作。 6. 后台机安装安装安全操作系统，杀毒软件，并定期升级杀毒软件。 7. 关闭 ftp 、telnet 等通用服务。 8. 关闭后台机空闲网络端口、USB接口、光驱等接口。 9. 严格执行用户账号及密码管理制度。按照实际情况设备用户名和密码，密码应满足不少于 8 位的字母、数字、字符的组合。 10. 删除服务器多余 IP 地址及与业务无关的路由配置。

		USB接口、光驱等接口未关闭。 9. 用户密码分配及管理不符合规范要求。 10. 服务器配置存在多余 IP 地址及与业务无关的路由配置。	
二、功率预测系统			
1	功率预测服务器、工作站调试及维护	1. 无线网卡插在服务器、工作站等计算机设备。 2. 紧急情况厂家远程维护服务器。 3. 站内未安排专人对厂家行为进行监控。 4. 未经过杀毒的调试终端直接连接在服务器和工作站。 5. 现场接线与实施方案中网络拓扑图不一致。 6. 服务器或工作站非安全操作系统（国产且经权威安全部门检测），未安装杀毒软件，未定期杀毒。 7.ftp 、telnet 等通用服务未关闭。	1. 与调试厂商签二次安防合规性承诺书和保密协议。 2. 严禁无线网卡插在服务器、工作站等计算机设备，严禁厂商远程维护。 3. 现场工作，专人对厂商行为进行监控，严格按照现场网络拓扑图开展工作。 4. 服务器或工作站安装安全操作系统，安装杀毒软件，并定期升级杀毒软件。 5. 关闭 ftp 、telnet 等通用服务。 6. 关闭服务器、工作站等计算机设备空闲网络端口、USB接口、光驱等接口。 7. 严格执行用户账号及密码管理制度。按照实际情况设备用户名和密码，密码应满足不少于 8 位的字母、数字、字符的组合。

		USB接口、光驱等接口未关闭。 9.用户密码分配及管理不符合规范要求。 10.安全防护设备安全策略和网络路由未按照“最小化”原则配置。 11.旁路纵向加密认证装置进行调试。 12.旁路反向隔离装置进行调试。 13.反向隔离装置未配置策略或明通模式。 14.随意使用未经杀毒的移动存储或笔记本电脑进行数据导出。	8.按照“最小化”原则,配置安全防护设备安全策略和网络路由。 9.严禁旁路纵向加密装置。 10.纵向加密装置及反向隔离装置策略正确配置，严禁明通模式运行。 11.严禁旁路反向隔离装置进行调试。 12.反向隔离装置配置策略,严禁明通模式 13.数据导出前,须将所使用的移动存储或笔记本电脑进行杀毒，确保设备中无病毒软件后再接入至设备。
三、向量测量系统（PMU			
1	向量测量装置设备调试及维护	1.紧急情况厂家远程维护服务器。 2.站内未安排专人对厂家行为进行监控。 3.设备空闲网络端口、USB接口未关闭。 4.配置存在多余 IP 地址及与业务无关的路由配置。 5.未关闭 FTP通用网络服务。 6.未设置用户名密码或设置的用户名与现场人员不符，密码强度不够。 7.调试用的笔记本电脑感染病毒，未经杀毒直接接入 PMU 设备。	1.与调试厂商签订二次安防合规性承诺书和保密协议。 2.严禁无线网卡插在远动机，严禁厂商远程维护。 3.从设备内部配置关闭空闲端口、接口. 4.规范设备中配置的静态路由，禁止配置超出业务使用范围外的目的网段。 5 关闭 FTP等通用网络服务。 6.严格按照实际情况设备用户名和密码，密码应满足不少于 8 位的字母、数字、字

			7.调试前，笔记本电脑应进行杀毒，确保设备中无病毒软件后再接入至PMU设备。
四、信息申报与发布工作站			
1	工作站安装调试	1.无线网卡插在工作站等计算机设备。 2.紧急情况厂家远程维护工作站。 3.站内未安排专人对厂家行为进行监控。 4.未经过杀毒的调试终端直接连接在工作站。 5.现场接线与实施方案中网络拓扑图不一致。 6.工作站非安全操作系统（国产且经权威安全部门检测），未安装杀毒软件，未定期杀毒。 7.ftp 、telnet 等通用服务未关闭。 8.工作站等计算机设备空闲网络端口、USB接口、光驱等接	1.与调试厂商签二次安防合规性承诺书和保密协议。 2.严禁无线网卡插在工作站等计算机设备，严禁厂商远程维护。 3.现场工作，专人对厂商行为进行监控，严格按照现场网络拓扑图开展工作。 4.工作站安装安全操作系统，安装杀毒软件，并定期升级杀毒软件。 5.关闭 ftp 、telnet 等通用服务。 6.关闭工作站等计算机设备空闲网络端口、USB接口、光驱等接口。 7.严格执行用户账号及密码管理制度。反向隔离装置策略正确配置。 8.按照“最小化”原则,配置网络路由。 9.数据导出前，须将所使用的移动存储或

		口未关闭。 9. 用户密码分配及管理不符合规范要求。 10. 安全防护设备安全策略和网络路由未按照“最小化”原则配置。 11. 随意使用未经杀毒的移动存储或笔记本电脑进行数据导出。	笔记本电脑进行杀毒，确保设备中无病毒软件后再接入至设备。
五、二次安防设备			
1	正向隔离装置调试及维护	1. 紧急情况厂家远程维护隔离装置。 2. 站内未安排专人对厂家行为进行监控。 3. 未经过杀毒的调试终端直接连接隔离装置上工作。 4. 现场接线与实施方案中网络拓扑图不一致。 5. 旁路正向隔离装置进行调试。	1. 与调试厂商签二次安防合规性承诺书和保密协议。 2. 严禁厂商远程维护。 3. 现场工作，专人对厂商行为进行监控。 4. 调试前，调试终端应进行杀毒，确保设备中无病毒软件后开展调试。 5. 严格按照现场网络拓扑图开展工作。 6. 严禁旁路正向隔离装置。 7. 正向隔离装置策略正确配置，严禁明通模式运行。 8. 按照“最小化”原则,配置隔离装置安全

		6. 正向隔离装置未配置策略或明通模式。 7. 隔离装置安全策略和网络路由未按照“最小化”原则配置。	策略和网络路由。
2	反向隔离装置调试及维护	1. 紧急情况厂家远程维护隔离装置。 2. 站内未安排专人对厂家行为进行监控。 3. 未经过杀毒的调试终端直接连接隔离装置上工作。 4. 现场接线与实施方案中网络拓扑图不一致。 5. 旁路反向隔离装置进行调试。 6. 反向隔离装置未配置策略或明通模式。 7. 隔离装置安全策略和网络路由未按照“最小化”原则配置。	1. 与调试厂商签二次安防合规性承诺书和保密协议。 2. 严禁厂商远程维护。 3. 现场工作，专人对厂商行为进行监控。 4. 调试前，调试终端应进行杀毒，确保设备中无病毒软件后开展调试。 5. 严格按照现场网络拓扑图开展工作。 6. 严禁旁路反向隔离装置。 7. 反向隔离装置策略正确配置，严禁明通模式运行。 8. 按照“最小化”原则,配置隔离装置安全策略和网络路由。

3	防火墙调试及维护	1.紧急情况厂家远程维护防火墙。 2.站内未安排专人对厂家行为进行监控。 3.未经过杀毒的调试终端直接连接防火墙调试。 4.现场接线与实施方案中网络拓扑图不一致。 5.旁路防火墙进行调试。 6.防火墙未配置策略或明通模式。 7.防火墙安全策略和网络路由未按照“最小化”原则配置。	1.与调试厂商签二次安防合规性承诺书和保密协议。 2.严禁厂商远程维护。 3.现场工作，专人对厂商行为进行监控。 4.调试前，调试终端应进行杀毒，确保设备中无病毒软件后开展调试。 5.严格按照现场网络拓扑图开展工作。 6.严禁旁路防火墙进行调试。 7.防火墙策略正确配置，严禁明通模式运行。 8.按照“最小化”原则,配置防火墙安全策略和网络路由。
4	纵向加密装置调试及维护	1.紧急情况厂家远程维护纵向加密装置。 2.站内未安排专人对厂家行为进行监控。 3.未经过杀毒的调试终端直接连接纵向加密装置调试。 4.现场接线与实施方案中网络拓扑图不一致。 5.旁路纵向加密装置进行调试。 6.纵向加密装置未配置策略或明通模式。	1.与调试厂商签二次安防合规性承诺书和保密协议。 2.严禁厂商远程维护。 3.现场工作，专人对厂商行为进行监控。 4.调试前，调试终端应进行杀毒，确保设备中无病毒软件后开展调试。 5.严格按照现场网络拓扑图开展工作。 6.严禁旁路纵向加密装置进行调试。 7.纵向加密装置策略正确配置，严禁明通模式运行。 8.按照“最小化”原则,配置纵向加密装置安全策略和网络路由。

		7.纵向加密装置安全策略和网络路由未按照“最小化”原则配置。	
六、调度数据网			
1	安装调试	1.空闲端口未封锁。 2.未设置登录用户名和密码，或设置的登录密码为弱口令或通用密码。 3.未设置 super 或 enable 密码，用户权限过大。 4.路由策略不符合“最小化”原则。 5.未开启日志功能。 6.未关闭 telnet 、ftp 、http 等通用网络服务。 7.调试用的笔记本电脑感染病毒，未经杀毒直接接入路由器。 8.接线方式与二次系统安全防护实施方案不一致。 9.调度数据网交换机接入至非调度数据网络。 10.交换机中未设置 acl 控制策略。 11.纵向加密装置未调试或未接入调度端内网安全监视平台。 12.纵向加密装置策略不满足“最小化”原则。	1.严格按照省调下发的调度数据网设备参数配置规范进行设备配置。 2.网络设备须配置设备登录用户名和密码，密码应满足不少于 8 位的字母、数字、字符的组合。 3.网络设备中须配置登录和 super（enable ）两级密码，且密码不得相同，密码应满足不少于 8 位的字母、数字、字符的组合。 4.路由策略中仅允许通过业务和网络管理所必须的源端和目的端，其他地址应全部禁止。开启日志记录功能。 5.关闭 telnet 、ftp 、http 等通用网络服务。 6.调试前，笔记本电脑应进行杀毒，确保设备中无病毒软件后再接入至调度数据网设备。

			7.调试完毕后，调度数据网设备和线缆应按实际情况设置标识标牌，并做好核对。 8.调度数据网接线，应严格按照二次系统安全防护实施方案进行。 9.禁止将调度数据网设备接入至其他非调度数据网网络。 10.严格按照省调下发的调度数据网设备参数配置规范进行设备配置。 11.须与调度机构完成纵向加密装置接入内网安全监视平台的相关调试。 12.纵向加密装置策略中仅允许业务所使用的IP 地址、端口通过，且纵向隧道和策略设置为密通。
3	设备故障处理	1.调试用的笔记本电脑感染病毒，未经杀毒直接接入路由器。 2.随意更改接线。 3.业务调试过程中，随意退出纵向加密装置。 4.随意删除网络设备中配置的安全策略。 5.随意更改纵向加密装置中配置的安全策略。	1.调试前，笔记本电脑应进行杀毒，确保设备中无病毒软件后再接入至调度数据网设备。 2.调度数据网接线，应严格按照二次系统安全防护实施方案进行。 3.未经省调许可，禁止退出纵向加密装置。 4.未经省调许可，禁止删除网络设备中配置的安全策略。 5.未经省调许可，禁止随意更改纵向加密装置中配置的安全策略。

附录3 新能源电站新建二次系统或设备接入安全防护风险提示卡

新能源电站新建系统或设备接入安全防护风险提示卡

典型风险	管控措施
1.无线网卡插在服务器、工作站等计算机设备。 2.紧急情况厂家远程维护服务器。 3.厂家调试，站内未安排专人对厂家行为进行监控。 4.未经过杀毒的调试终端直接连接在服务器和工作站。 5.现场接线与实施方案中网络拓扑图不一致。 6.服务器或工作站非安全操作系统（国产且经权威安全部门检测），未安装杀毒软件，未定期杀毒。 7.ftp 、telnet 等通用服务未关闭。 8.服务器、工作站等计算机设备空闲网络端口、USB接口、光驱等接口未关闭。 9.用户密码分配及管理不符合规范要求。 10.安全防护设备安全策略和网络路由未按照“最小化”原则配置。 11.旁路纵向加密认证装置进行调试。 12.外网气象服务器与二区功率预测服务器调试，旁路反向隔离装	1.与调试厂商签订二次安防合规性承诺书和保密协议。 2.严禁无线网卡插在服务器、工作站等计算机设备。 3.严禁厂商远程维护。 4.调试前，调试终端应进行杀毒，确保设备中无病毒软件后再开展调试。 5.现场工作，专人对厂商行为进行监控。 6.严格按照现场网络拓扑图开展工作。 7.服务器或工作站安装安全操作系统，并安装杀毒软件，并定期升级杀毒软件。 8.关闭 ftp 、telnet 等通用服务。 9.关闭服务器、工作站等计算机设备空闲网络端口、USB接口、光驱等接口。 10.严格执行用户账号及密码管理制度。按照实际情况设备用户名和密码，密码应满足不少于 8 位的字母、数字、字符的组合。 11.按照“最小化”原则,配置安全防护设备安全策略和网络路由。 12.与电站集控中心通信配置正向隔离，同时严禁旁路纵向加密装置。 13.纵向加密装置及正向、反向隔离装置策略正确配置。 14.严禁旁路纵向加密装置及正向、反向隔离装置。 15.纵向加密装置及反向隔离装置策略正确配置，严禁明通模式运行。 16.非调度相关业务接入调度数据网，必须报备省调，且经许可才可

置进行调试。 13. 与电站集控中心通信未配置正向隔离或旁路正向隔离装置进行调试。 14. 正向隔离装置未配置策略或明通模式。 15. 反向隔离装置未配置策略或明通模式。 16. 未经省调许可，接入非调度相关业务。 17. 未按调度结构分配的业务 IP 地址，各业务混用业务网段 IP 地址。 18. 接入调度数据网的业务线缆未设置标识，线缆混乱未整理。 19. 业务调试过程中，随意退出纵向加密等安全防护设备。 20. 随意使用未经杀毒的移动存储或笔记本电脑进行数据导出。	接入。 17. 严格按照调度分配的业务地址，禁止混用和乱用。 18. 业务接入时，做好接入线缆的整理绑扎和标识标牌。 19. 未经省调许可，禁止退出纵向加密装置。 20. 数据导出前，须将所使用的移动存储或笔记本电脑进行杀毒，确保设备中无病毒软件后再接入至设备。

附录 4 新能源电站二次系统日常使用安全防护风险提示卡

新能源电站二次系统日常使用安全防护风险提示卡

典型风险	管控措施