附件 4：发电厂网络安全风险评估报告编制要求

电力监控系统安全防护评估报告

被评单位：_____

委托单位：_____

评估单位：_____

报告时间：_____

安全防护评估基本信息表

<table>
<tr><td>系统名称</td><td colspan="5"></td></tr>
<tr><td>评估结论</td><td colspan="5"></td></tr>
<tr><td colspan="6">委托单位信息</td></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="3"></td><td>邮编</td><td></td></tr>
<tr><td>评估对象</td><td colspan="5"></td></tr>
<tr><td rowspan="3">联
系
人</td><td>姓名</td><td></td><td>职务/职称</td><td colspan="2"></td></tr>
<tr><td>部门</td><td></td><td>办公电话</td><td colspan="2"></td></tr>
<tr><td>移动电话</td><td></td><td>电子邮箱</td><td colspan="2"></td></tr>
<tr><td colspan="6">评估单位信息</td></tr>
<tr><td>单位名称</td><td colspan="3"></td><td>评估日期</td><td></td></tr>
<tr><td>单位地址</td><td colspan="3"></td><td>邮编</td><td></td></tr>
<tr><td rowspan="3">联
系
人</td><td>姓名</td><td></td><td>职务/职称</td><td colspan="2"></td></tr>
<tr><td>部门</td><td></td><td>办公电话</td><td colspan="2"></td></tr>
<tr><td>移动电话</td><td></td><td>电子邮箱</td><td colspan="2"></td></tr>
<tr><td rowspan="3">审核批准</td><td>编制人</td><td></td><td>编制日期</td><td colspan="2"></td></tr>
<tr><td>审核人</td><td></td><td>审核日期</td><td colspan="2"></td></tr>
<tr><td>批准人</td><td></td><td>批准日期</td><td colspan="2"></td></tr>
</table>

目录

1. 概述

1.1 项目背景

（编写要求：介绍发电厂的地理位置、电力监控系统施工设计单位、业主单位、所属发电集团、装机规模等基本信息，以及对所评估系统的简要介绍）

1.2 项目目的

（编写要求：介绍电力监控系统安全防护评估项目目的）

1.3 项目依据

（编写要求：介绍本次评估参考的政策文件、标准规范）

1.4 评估范围

（编写要求：介绍本次评估范围）

1.5 工作方法

（编写要求：介绍本次评估工作方法）

1.6 评估过程

（编写要求：介绍本次评估过程）

1.7 报告分发范围

（编写要求：本报告的分发范围）

2. 评估对像描述

（编写要求：对评估对象涉网部分的电力监控系统进行描述）

3. 资产识别与赋值

3.1 资产类别

（编写要求：参照《电力监控系统安全防护评估规范》的定义对资产进行归并和分类）

3.2 资产识别

（编写要求：对评估范围内资产进行识别，按如下表所示进行记录）

3.2.1 物理资产

物理环境资产表

资产编号	资产名称	用途	位置	数量	重要程度
101					

3.2.2 网络设备资产

网络设备资产表

资产编号	设备名称	操作系统	品牌	型号	用途	IP	MAC	重要程度
201								

3.2.3 安全设备资产

安全设备资产表

资产编号	设备名称	操作系统	品牌	型号	用途	IP	MAC	重要程度
301								

3.2.4 服务器资产

服务器资产表

资产编号	设备名称	操作系统	版本	IP	MAC	业务应用	使用负责人	重要程度
401								

3.2.5 终端资产

终端资产表

资产编号	设备名称	操作系统	版本	IP	MAC	用途	使用负责人	重要程度
501								

3.2.6 业务系统资产

业务系统资产表

资产编号	软件名称	主要功能	版本	开发厂商	重要程度
601					

3.2.7 安全组织架构

安全组织架构

序号	姓名	岗位/角色	联系方式
1			

3.2.8 安全管理文档

安全管理文档资产表

序号	文档名称	主要内容	版本
1			

3.3.资产赋值

（编写要求：参照《电力监控系统安全防护评估规范》中关于资产机密性、完整性、可用性的赋值参考表 ,对每项资产都要从客户端、服务提供、业务处理、数据存储等方面进行机密性要求、完整性要求、可用性要求的赋值，并填写资产赋值表）

资产赋值表

业务系统	资产赋值	客户端						服务提供			业务处理			数据存储		
		管理员			普通用户											
		C	I	A	C	I	A	C	I	A	C	I	A	C	I	A
XX 电厂监控系统																

4. 威胁分析

4.1 威胁类别

（编写要求：参照《电力监控系统安全防护评估规范》的定义对威胁进行归并和分类）

4.2 威胁识别

（编写要求：对需要保护的每项关键资产进行威胁识别，编制威胁识别表）

威胁识别表

威胁分类	威胁名称	说明
非人为威胁	火山爆发	由火山爆发引起的故障

4.3 威胁赋值

（编写要求：参照《电力监控系统安全防护评估规范》中关于威胁对机密性、完整性、可用性的赋值参考表，对每项威胁进行机密性要求、完整性要求、可用性要求的赋值，并填写威胁赋值表）

威胁赋值表

威胁分类	威胁名称	说明	威胁可能性	威胁的严重程度				威胁赋值
				C	I	A	平均值	
非人为威胁	火山爆发	由火山爆发引起的故障	1	N/A	5	5	5	2

5. 脆弱性分析

5.1 脆弱性类别

（编写要求：参照《电力监控系统安全防护评估规范》的脆弱性识别分类表对脆弱性进行归并和分类）

5.2 脆弱性识别

（编写要求：本小节从技术脆弱性和管理脆弱性两大部分 10 个方面，参照《电力监控系统安全防护评估规范》规定的脆弱性评估要点进行脆弱性识别）

5.1.1 物理环境脆弱性分析

（编写要求:首先对物理环境进行整体介绍和分析,然后参照《电力监控系统安全防护评估规范》中的脆弱性评估表对物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等方面进行脆弱性识别，将评估结果填入物理环境脆弱性识别表）

物理环境脆弱性识别表

序号	脆弱性描述	严重程度
1	未设置光、电等技术的防盗报警系统。	中

5.1.2 基础网络脆弱性分析

（编写要求：首先对基础网络的拓扑架构进行整体介绍和分析，然后参照《电力监控系统安全防护评估规范》中的脆弱性评估表对网络结构安全、访问控制、安全审计、边界完整性检查、入侵防范、网络设备防护、安全加固等方面进行脆弱性识别，将评估结果填入网络

设备脆弱性识别表）

网络及安防设备脆弱性识别表

序号	设备编号	脆弱性描述	严重程度
1			

注：设备编号为其在 3.2 节中的资产编号。

5.1.3 主机系统脆弱性分析

（编写要求：首先对主机系统的防护现状进行整体介绍，然后参照《电力监控系统安全防护评估规范》中的脆弱性评估表对主机系统的身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范、资源控制安全免疫、安全加固等方面进行脆弱性识别，将评估结果填入主机系统脆弱性识别表）

主机系统脆弱性识别表

序号	设备编号	脆弱性描述	严重程度
1			

5.1.4 业务应用脆弱性分析

（编写要求：首先对业务应用的防护现状进行整体介绍，然后参照《电力监控系统安全防护评估规范》中的脆弱性评估表对业务应用的身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性、通

信保密性、抗抵赖、软件容错、资源控制等方面进行脆弱性识别，将评估结果填入业务应用脆弱性识别表）

业务应用脆弱性识别表

序号	应用名称	脆弱性描述	严重程度
1			

5.1.5 数据库系统脆弱性分析

（编写要求：首先对数据库系统的防护现状进行整体介绍，然后参照《电力监控系统安全防护评估规范》中的脆弱性评估表对数据完整性、数据保密性、备份和恢复等方面进行脆弱性识别，将评估结果填入数据库系统脆弱性识别表）

数据库系统脆弱性识别表

序号	资产名称	脆弱性描述	严重程度
1			

5.1.6 安全管理制度脆弱性分析

（编写要求：首先对安全管理制度进行整体介绍，然后参照《电力监控系统安全防护评估规范》中的脆弱性评估表对管理制度、制定和发布、评审和修订等方面进行脆弱性识别，将评估结果填入安全管

理制度脆弱性识别表）

安全管理制度脆弱性识别表

序号	脆弱性描述	严重程度
1		

5.1.7 安全管理机构脆弱性分析

（编写要求：首先对安全管理机构进行整体介绍，然后参照《电力监控系统安全防护评估规范》中的脆弱性评估表对岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等方面进行脆弱性识别，将评估结果填入安全管理机构脆弱性识别表）

安全管理机构脆弱性识别表

序号	脆弱性描述	严重程度
1		

5.1.8 人员安全管理脆弱性分析

（编写要求：首先对人员安全管理进行整体介绍，然后参照《电力监控系统安全防护评估规范》中的脆弱性评估表对人员录用、人员离岗、人员考核、意识教育和培训、外部人员访问管理等方面进行脆弱性识别，将评估结果填入人员安全管理脆弱性识别表）

人员安全管理脆弱性识别表

序号	脆弱性描述	严重程度
1		

5.1.9 系统建设管理脆弱性分析

（编写要求：首先对系统建设管理进行整体介绍，然后参照《电力监控系统安全防护评估规范》中的脆弱性评估表对系统定级备案、安全方案设计、产品采购使用、软件开发、工程实施和安全服务商选择、测试验收、系统交付、等级评估等方面进行脆弱性识别，将评估结果填入系统建设管理脆弱性识别表）

系统建设管理脆弱性识别表

序号	脆弱性描述	严重程度
1		

5.1.10 系统运维管理脆弱性分析

（编写要求：首先对系统运维管理进行整体介绍，然后参照《电力监控系统安全防护评估规范》中的脆弱性评估表对资产管理、监控管理、网络和系统安全管理、密码管理、变更管理、备份与恢复管理、安全事件处置和应急预案管理等方面进行脆弱性识别，将评估结果填

入系统运维理脆弱性识别表）

系统运维管理脆弱性识别表

序号	脆弱性描述	严重程度
1		

5.3 脆弱性赋值

（编写要求：根据脆弱性对资产的暴露程度、技术实现的难易程度、流行程度等，采用等级方式对已识别的脆弱性的严重程度进行赋值，将赋值结果填入脆弱性赋值表）

脆弱性赋值表

业务系统	评估层面	脆弱性描述	脆弱性严重程度
XX	物理安全	未设置光、电等技术的防盗报警系统。	3

6. 安全措施有效性分析

6.1 技术类安全措施有效性分析

（编写要求：从物理安全、网络安全、主机安全、应用系统等方面，分析所采取安全措施的有效性）

6.2 管理类安全措施有效性分析

（编写要求：从人员管理、规章制度、系统建设、系统运维等方

面，分析所采取安全措施的有效性）

7. 风险计算和分析

7.1 风险分析模型概述

（编写要求：依据风险分析要素，进行风险分析模型介绍）

7.2 风险计算与分析

7.2.1 资产赋值

（编写要求：列出被评估对象的资产赋值表）

7.2.2 威胁赋值

（编写要求：列出被评估对象的威胁赋值表）

7.2.3 脆弱赋值

（编写要求：列出被评估对象的脆弱赋值表）

7.2.4 安全事件发生可能性

（编写要求：根据威胁赋值和脆弱性赋值计算安全事件发生的可能性，如采用矩阵方式进行计算，通过威胁出现的频率等级和脆弱性严重程度等级即可查找到相应的安全事件发生可能性值，并根据安全事件发生可能性值查找安全事件发生可能性等级）

安全事件发生可能性值矩阵表

安全事件发生可能性值		脆弱性严重程度				
		1	2	3	4	5
威胁赋值	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

安全事件发生可能等级表

安全事件发生可能性值	1-5	6-10	11-15	16-20	21-25
安全事件发生可能性等级	1	2	3	4	5

脆弱性安全事件发生可能性表

业务系统	评估层面	脆弱性描述	安全事件发生可能性值	发生可能性等级

7.2.5 安全事件损失计算

（编写要求：根据资产赋值和脆弱性赋值计算安全事件发生的可能性，如采用矩阵方式进行计算，通过资产值和脆弱性严重程度等级即可查找到相应的安全事件损失值，并根据安全事件损失值查找安全事件损失值等级）

安全事件损失值矩阵表

安全事件损失值	脆弱性严重程度				
	1	2	3	4	5

资产值	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

安全事件损失值及等级表

安全事件损失值	1-5	6-10	11-15	16-20	21-25
安全事件损失值等级	1	2	3	4	5

脆弱性安全事件损失值与损失等级表

业务系统	评估层面	脆弱性描述	安全事件损失值	发生事件损失等级

7.2.6 风险计算与分析

（编写要求：根据安全事件发生可能性等级和损失值等级计算风险值，如采用矩阵方式进行计算，通过安全事件损失值等级和安全事件发生可能性即可查找到相应的风险值，并根据风险值查找风险等级）

风险值矩阵表

风险值		安全事件损失值等级				
		1	2	3	4	5
安全事件发生可能性等级	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20

	5	5	10	15	20	25

风险等级表

风险值	1-5	6-10	11-15	16-20	21-25
风险等级	1	2	3	4	5

风险值与风险等级表

业务系统	评估层面	脆弱性描述	单项风险值	风险等级	风险值总和
信息网络	物理安全	未设置光、电等技术的防盗报警系统。	6	2	25

风险总值排序与最高风险等级

资产名称	最高风险等级	风险总值
网络	4	25

7.3 综合分析与评价

（编写要求：对风险评估综合分析与安全评价）

8. 安全风险整改建议

8.1 安全风险整改原则

（编写要求：介绍安全风险整改的原则）

8.2 安全风险整改目标及方式

（编写要求：介绍安全风险整改的目标及方式）

8.3 安全风险整改建议

（编写要求： 给出各项安全风险的整改建议）

序号	脆弱性描述	单项风险值	整改建议
1			
2			

附件 1：网络拓扑结构

（编写要求：给出被测评对象整体网络拓扑图，以及全部网络设备和安防设备正反面照片，照片要能够清晰反应网络接线情况并且与整体网络拓扑图的接线情况一致）

附件 2：电力监控系统漏洞扫描摘要

（编写要求：采用主流绿盟、网御星云主流漏扫产品对所有设备进行漏扫，并确保特征库为当前最新版。将漏扫工具信息、漏扫结果基本信息、漏洞风险分析和整改建议进行具体说明）

附件 3：安防设备配置信息

（编写要求：列出被测评对象的横向隔离、防火墙、纵向加密、网络安全监测装置、入侵检测等安防设备的配置文件或配置截图）

附件 4：安全加固检查记录

（编写要求：列出被测评对象的主机设备、网络设备和安防设备逐一核查加固项，将加固结果记录到加固核查表中，并将每项核查截图作为佐证材料）

加固核查表

序号	加固项	已加固资产编号	未加固资产编号
Linux 操作系统			
01	用户账户配置		
02	密码复杂度策略配置		
03	账户登录失败锁定策略配置		
04	口令有效期配置		
05	桌面配置		
06	消除无关软件、程序		
07	禁用默认路由配置		
08	umask 权限		
09	安全内核（模块）配置		
10	操作系统防火墙配置		
11	禁用 bluetooth		
12	禁用无用服务		
13	禁用无用端口		
14	禁用大容量存储介质（USB 存储设备）		
15	消除多余网络接口		
16	禁用 cdrom		

17	限制远程管理地址配置		
18	SSH 远程管理超时自动退出配置		
19	禁止 root 用户远程登录		
20	远程用户资源限制配置		
21	消除无用日志		
windows 操作系统			
01	用户权限策略配置		
02	用户口令周期策略		
03	用户口令过期提醒		
04	用户口令复杂度策略		
05	禁止用户修改 IP		
06	禁止用户更改计算机名		
07	开启屏幕保护程序		
08	用户登录失败锁定		
09	系统不显示上次登录名		
10	关闭默认共享		
11	用户账户控制设置（UAC）		
12	禁止未登录关机		
13	关机时清除虚拟内存页面文件		
14	禁止非管理员关机		
15	启用 SYN 保护		
16	设置最小挂起时间		
17	敏感信息标记		
18	删除或禁用系统无关用户		
19	系统重要数据访问控制		
20	数据执行保护（DEP）		
21	禁止普通用户修改审计策略		

22	删除默认路由配置		
23	卸载无关软件		
24	补丁管理		
25	高危漏洞补丁加固		
26	安装防病毒软件		
27	安装防病毒统一管理服务器		
28	关闭不必要服务		
29	关闭不必要的系统端口		
30	开启防火墙功能		
31	配置访问控制规则		
32	关闭远程主机 RDP 服务		
33	限制远程登录 IP		
34	限制匿名用户远程连接		
35	限制远程登录协议		
36	限制远程登录时间		
37	修改远程桌面默认服务端口		
38	主机间登录禁止使用公钥验证		
39	禁用大容量存储介质（USB 存储设备）		
40	关闭自动播放功能		
41	禁止使用无线网卡		
42	配置日志策略		
网络设备			
01	空闲端口管理		
02	console 密码		
03	远程管理使用 ssh 代替 telnet		
04	远程登录源限制		

05	设置非法登录次数		
06	设置超时策略		
07	默认路由		
08	口令密文存储		
09	密码认证登陆		
10	关闭未用服务		
11	BANNER 信息		
12	进行静态 MAC 绑定		
13	ntp 设置		
14	设备版本管理		
15	ACL 访问控制		
16	OSPF 认证		
17	日志审计		
18	使用不安全的 snmp		
19	snmp 团体名		
安全防护设备			
01	运行可靠性		
02	系统时间		
03	集中管理		
04	用户管理		
05	口令管理		
06	登录管理		
07	本地登录管理		
08	远程登录管理		
09	安全策略配置		
10	白名单管理		
11	日志管理		

12	安全审计		

文档审核

技术审核：　　（签字）

年　月　日

质量审核：　　（签字）

年　月　日