ICS 29.240.01
F 21

# 中华人民共和国国家标准

GB/T 38318—2019

# 电力监控系统网络安全评估指南

**Cyber security assessment guide for electric power system supervision and control**

2019-12-10 发布　　2020-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

# 目　　次

# 前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国电力企业联合会提出。

本标准由全国电力系统管理及其信息交换标准化技术委员会(SAC/TC 82)归口。

本标准起草单位:中国电力科学研究院有限公司、全球能源互联网研究院有限公司、国家能源局、国家电网有限公司、中国南方电网有限责任公司、国家电力投资集团公司、中国华电集团有限公司、中国华能集团公司、中国长江三峡集团公司、国家电网公司华东分部、国网宁夏电力公司、国网吉林省电力有限公司、国网山东省电力公司、国网重庆市电力公司、国网江苏省电力有限公司、南瑞集团信息通信技术分公司、北京科东电力控制系统有限责任公司、广东电网公司电力科学研究院。

本标准主要起草人:张涛、李凌、马媛媛、郑义、郭旭、费稼轩、黄秀丽、高可、陈雪鸿、王景欣、陶洪铸、朱朝阳、林为民、刘楠、单松玲、杨维永、张亮、张宏杰、胡可为、刘勇、欧睿、裴培、马骁、陶文伟、梁智强、余勇、詹雄、刘森、刘莹、郑晓崑、梁潇、王静、张珂、李旸照、陈刚、刘行、刘寅、张骞、石聪聪、张小建。

# 引　言

本标准与GB/T 36572—2018配套使用。

# 电力监控系统网络安全评估指南

## 1 范围

本标准规定了电力监控系统网络安全评估工作的评估内容、系统生命周期各阶段的安全评估、评估流程及方法、安全防护技术评估、应急备用措施评估、安全管理评估。

本标准适用于各电力企业电力监控系统规划阶段、设计阶段、实施阶段、运行维护阶段和废弃阶段的网络安全防护评估工作。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 9361 计算机场地安全要求

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336.2—2015 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能组件

GB/T 20272—2006 信息安全技术 操作系统安全技术要求

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

GB/T 21028—2007 信息安全技术 服务器安全技术要求

GB/T 21050—2007 信息安全技术 网络交换机安全技术要求(评估保证级3)

GB/T 22186—2016 信息安全技术 具有中央处理器的IC卡芯片安全技术要求

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 25058—2010 信息安全技术 信息系统安全等级保护实施指南

GB/T 25068.3—2010 信息技术 安全技术 IT网络安全 第3部分：使用安全网关的网间通信安全保护

GB/Z 25320(所有部分) 电力系统管理及其信息交换 数据和通信安全

GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南

GB/T 36572—2018 电力监控系统网络安全防护导则

## 3 术语和定义

GB/T 36572—2018和GB/T 20984—2007界定的以及下列术语和定义适用于本文件。

3.1

**自评估 self-assessment**

运行单位对本单位电力监控系统组织实施的安全评估，以及调度机构在调度管辖范围内(以下简称“调管范围内”)各运行单位自评估结果基础上，对调管范围内电力监控系统组织实施的安全评估。

3.2

**检查评估　inspection assessment**

由被评估单位的业务主管部门组织或委托安全评估机构，依据有关标准和管理规定，对电力监控系统进行的具有强制性的安全评估。

3.3

**上线安全评估　online implementation security assessment**

电力监控系统投运前及发生重大变更时，运行单位自行组织或委托评估机构对系统进行的安全评估。

注：重大变更包括，但不限于：

a) 增加新的应用或应用发生较大变更；

b) 网络结构和连接状况发生较大变更；

c) 技术平台大规模更新；

d) 系统扩容或改造；

e) 系统运行维护管理机构或人员发生较大规模调整。

3.4

**型式安全评估　type safety assessment**

电力监控系统设计、开发完成后，系统供应商自行组织或委托评估机构对系统进行的安全评估。

## 4 缩略语

下列缩略语适用于本文件。

FTP：文件传输协议(File Transfer Protocol)

HTTP：超文本传输协议(Hyper-Text Transfer Protocol)

IED：智能电子设备(Intelligent Electronic Device)

LAN：局域网络(Local Area Network)

OSPF：开放式最短路径优先(Open Shortest Path First)

SCADA：监视控制与数据采集系统(Supervisory Control And Data Acquisition)

SNMP：简单网络管理协议(Simple Network Management Protocol)

UPS：不间断电源(Uninterruptible Power System)

USB：通用串行总线(Universal Serial Bus)

VLAN：虚拟局域网(Virtual Local Area Network)

VPN：虚拟专用网(Virtual Private Networks)

## 5 评估内容

评估内容包括资产评估、威胁评估、脆弱性评估。

资产评估通过资产分类、资产调查、资产赋值等过程，最终形成资产列表和资产赋值报告。资产评估按照、国家等级保护相关标准及 GB/T 31509—2015 中 5.2.2 的规定执行。资产分类按照 GB/T 20984—2007 中 5.2.1 的规定执行。

威胁评估通过威胁分类、威胁调查、威胁分析和赋值等过程，最终形成威胁分析报告。威胁评估按照 GB/T 31509—2015 中 5.2.3 的规定执行。威胁分类按照 GB/T 20984—2007 中 5.3.1 和 GB/T 36572—2018 中 5.2 的规定执行。

脆弱性评估主要包括基础设施安全、体系结构安全、本体安全、可信安全免疫、应急备用措施、安全

管理等。

## 6 系统生命周期各阶段的安全评估

### 6.1 评估概述

电力监控系统生命周期包含5个基本阶段:规划阶段、设计阶段、实施阶段、运行维护阶段和废弃阶段。安全评估工作应贯穿于电力监控系统整个生命周期。各阶段中涉及的安全评估的原则和方法一致,但由于实施的内容、对象、信息安全需求不同,安全评估的对象、目的、要求等方面也不同。

### 6.2 规划阶段

规划阶段的安全评审是根据电力监控系统的业务使命和功能,确定系统建设应达到的安全目标。主要根据未来系统的应用对象、应用环境、业务状况、操作要求等方面进行威胁分析,重点分析系统应达到的安全目标。规划阶段的评审结果应包含在电力监控系统整体规划中。

### 6.3 设计阶段

设计阶段的安全评审需根据规划阶段明确的系统安全目标,对系统设计方案的安全功能设计进行判断,以确保设计方案满足系统安全目标,并作为采购过程风险控制的依据。设计阶段的评审结果最终应体现在系统设计方案中。

### 6.4 实施阶段

实施阶段安全评估是根据系统安全需求和运行环境对系统开发实施过程进行安全风险识别,并对系统建成后的安全功能进行验证。评估中需对规划阶段的安全威胁进行进一步细分,评估安全措施的实现程度,确定已建立的安全措施能否抵御现有威胁、脆弱性的影响,并对源代码进行安全测评。

### 6.5 运行维护阶段

运行维护阶段安全评估是掌握和控制电力监控系统运行过程中的安全风险,包括在线运行电力监控系统资产、威胁、脆弱性等各方面评估。运行维护阶段的安全评估应常态化开展。电力监控系统业务流程、系统状况发生重大变更(参见3.3的注)时,也需及时进行安全评估。

### 6.6 废弃阶段

电力监控系统的废弃阶段应重点分析废弃资产对组织的影响,对因系统废弃可能带来的新的威胁进行分析。安全评估可包括:

a) 系统软、硬件等资产及残留信息的废弃处置;
b) 废弃部分与其他系统或部分的物理或逻辑连接情况;
c) 在系统变更时发生废弃,对变更部分进行评估。

## 7 评估流程及方法

### 7.1 总体要求

#### 7.1.1 评估开展时间

电力监控系统网络安全评估工作应常态化、定期进行。电力监控系统的规划、设计阶段要进行安全

审查，实施、运行维护和废弃阶段均应进行安全评估，各阶段结合本阶段的实际情况开展安全评估工作。

#### 7.1.2 评估工作角色和职责

##### 7.1.2.1 运行单位

负责发起本单位的自评估工作，参加评估方案等文档的评审工作，配合检查评估实施工作，并根据安全评估结果落实整改方案。系统投运前及发生重大变更实施上线安全评估时，运行单位总体负责相关工作，可委托评估机构进行评估。

运行单位上级主管部门负责发起下属单位的自评估工作，监督下属单位安全评估实施过程，检查下属单位安全评估整改落实情况。

##### 7.1.2.2 调度机构

负责发起调管范围内的自评估工作，收集、汇总调管范围内各运行单位的自评估结果，参加评估方案等文档的评审工作，组织实施调管范围内电力监控系统的自评估，配合开展调管范围内的检查评估，根据安全评估结果督促、落实整改。

##### 7.1.2.3 系统供应商

负责系统设计、开发完成后实施型式安全评估，配合完成系统上线安全评估，在运行维护阶段支持、配合安全评估工作，配合执行安全评估整改工作。

##### 7.1.2.4 评估机构

负责编制安全评估实施方案，自行组织评审评估实施方案，实施安全评估，出具安全评估报告，提出整改建议，自行组织评审评估结果。

宜选择国家或行业有丰富经验的稳定、可靠、可控的评估机构。

#### 7.1.3 评估工作形式

电力监控系统网络安全评估包括4种工作形式：自评估、检查评估、上线安全评估和型式安全评估。具体要求包括：

a) 运行单位对本单位安全保护等级为第三级和第四级的电力监控系统定期组织开展自评估，评估周期原则上不超过一年；安全保护等级为第二级的电力监控系统定期开展自评估，评估周期原则上不超过一年。电力调度机构在定期收集、汇总调管范围内各运行单位自评估结果的基础上，自行组织或委托评估机构开展调管范围内电力监控系统的自评估工作，省级以上调度机构的自评估周期最长不超过三年，地级及以下调度机构自评估周期最长不超过两年。委托评估机构定期开展的安全评估工作可结合等级保护工作进行。

b) 业务主管部门根据实际情况对各运行单位的电力监控系统或调度机构调管范围内的电力监控系统组织开展检查评估。

c) 电力监控系统投运前或发生重大变更时，安全保护等级为第三级和第四级的电力监控系统，由运行单位委托评估机构进行上线安全评估；安全保护等级为第二级的电力监控系统可自行组织开展上线安全评估。

d) 电力监控系统供应商在安全保护等级为第三级和第四级的电力监控系统设计、开发完成后，委托评估机构进行型式安全评估；安全保护等级为第二级的电力监控系统可自行组织开展型式安全评估。

## 7.2 评估流程

电力监控系统网络安全评估实施流程分为4个阶段:启动准备阶段、现场实施阶段、风险分析阶段和安全建议阶段。在安全评估实施完毕后,应根据评估结论进行安全整改。以上四种工作形式的安全评估宜根据图1所示的实施流程制定相应的评估方案。

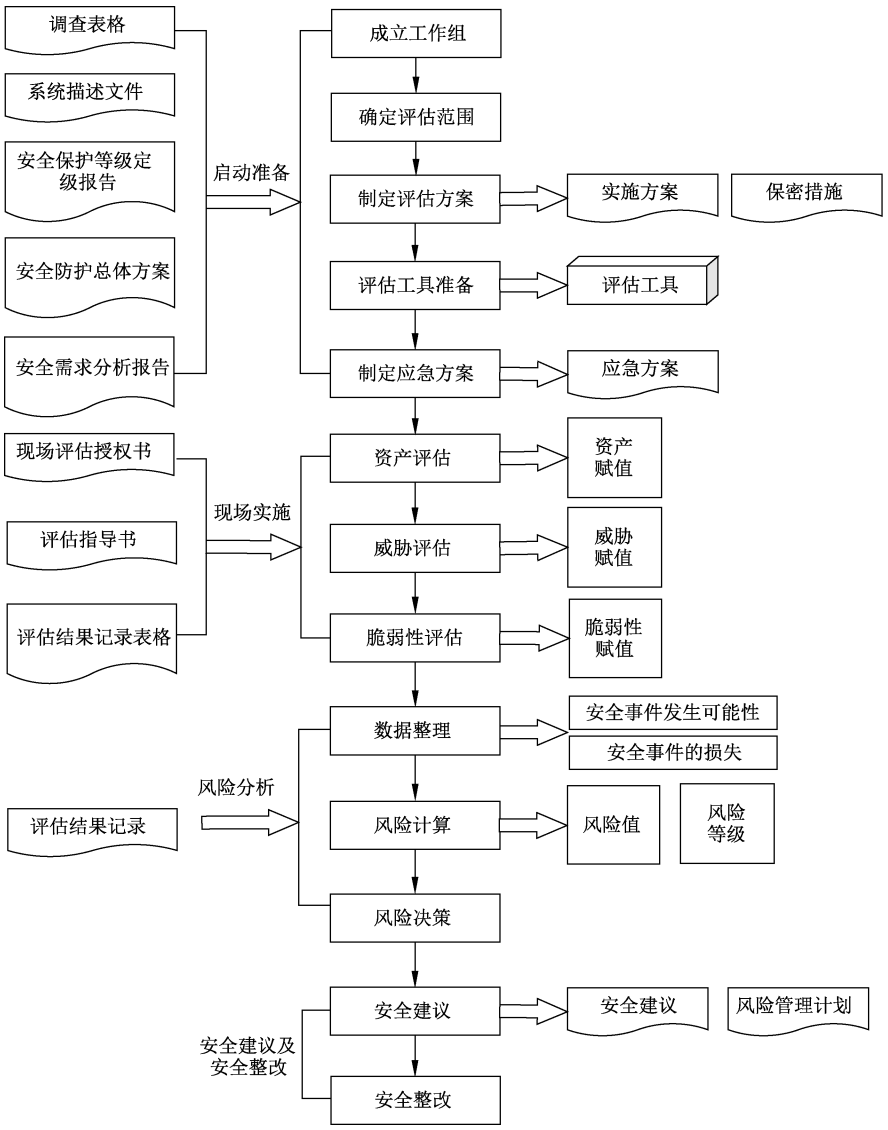


图1 电力监控系统网络安全评估实施流程

## 7.3 评估方法

电力监控系统网络安全评估涉及的评估方法主要包括:

a) 文档检查。检查被评估单位提交的有关文档(如系统配置文档、安全防护方案、自评估报告等)是否符合相关标准和要求。

b) 人工核查。根据评估方案和评估指导书,在合理的评估环境下,核查各项安全功能和防护能力是否与提交文档一致,是否符合相关标准和要求等。

c) 工具检查。根据评估方案,在被评估单位授权的前提下,选择适用的评估工具实施评估,工具

可包括网络评估工具、主机评估工具、资产识别工具等。

### 7.4 评估注意事项

#### 7.4.1 保密管理

应对评估资料和评估结果按照国家相关要求做好保密工作，可采取签订保密协议、最小接触原则、职业道德评估、人员保密管理、设备保密管理、文档保密管理等控制措施，明确问责和追责等处理办法，保证评估过程中产生、接触的所有记录、数据评估结果的安全、保密。

#### 7.4.2 风险控制

应对安全评估实施过程进行风险控制，可采取严格操作的申请和监护、操作时间控制、制定应急预案、搭建运行系统模拟环境、关键业务系统采用人工评估、评估人员选取、评估现场安全培训等风险控制手段，防止安全评估过程中引入的风险。

## 8 安全防护技术评估

### 8.1 基本要求

根据电力监控系统安全防护特点，如下要求中任何一项未满足即为不合格：

a) 分区分级(见 8.3.1)；

b) 网络专用(见 8.3.2)；

c) 横向隔离(见 8.3.3)；

d) 纵向认证(见 8.3.4)。

在上述基本要求都满足情况下，按照 GB/T 36572—2018 的安全防护要求开展其他内容评估。

### 8.2 基础设施安全

#### 8.2.1 评估要求

基础设施安全防护评估宜符合 GB/T 36572—2018 中 6.1 的要求。

#### 8.2.2 评估实施

评估实施主要包括以下内容：

a) 核查机房和设计方案、记录等文档，评估是否存在雨水渗透、因风导致的尘土严重、墙体或地面破裂的情况，所在建筑物防震、防风、防雨及机房位置选择是否符合 GB/T 9361 要求。如因客观因素不能避免机房选择在建筑物的高层、地下室或机房上层、包含用水设备的区域隔壁，是否采取有效补救措施(如对墙壁或楼板进行防渗透、防凝露、防裂加固，在水患区域部署水敏感检测设备等)。

b) 核查机房防护设施、设计方案等文档，评估机房防水、防潮、防火、防静电、防雷击、防盗窃、防破坏措施是否符合 GB/T 9361 要求。评估内容包括，但不限于：

   1) 是否采用密封或拆除窗户、墙壁粉刷防水涂层等方式防止漏水、渗水，是否部署精密空调或除湿装置调节空气湿度，是否在地板下、窗户附近等区域安装水敏感检测仪表或元件，与机房相关的给排水管道(用于机房空调、除湿机等)是否采用不易被水锈蚀和损坏的材质；

2） 是否将机房灭火设备放置在显眼位置并定期检查、维护，火灾自动消防系统是否能利用烟感、温感等装置检测火情、报警、灭火（场站可酌情考虑），机房、相关工作房间和辅助房（值班室、非在运行设备及物资存放室等）内外壁是否采用防火涂料、隔热板等阻燃或不燃材料建造或处理；

3） 对机房内的主要设备和机柜等是否设置接地措施，是否使用防静电地板；

4） 是否在机房所在建筑安装避雷装置，机房供电装置等位置是否安装防雷安保器（场站可酌情考虑），是否设置交流电源地线；

5） 是否将主要设备（服务器、通信设备、UPS、空调等）部署在机房内，并通过导轨、螺丝钉等方式固定在机柜上，是否设置不易除去标记，通信电缆是否铺设在地板管道或线槽中，备份存储介质、纸质档案等是否分类标识并存放在相应的区域，是否安装监控报警系统。

c） 核查稳压器、过电压防护设备部署和工作状态，评估机房供电线路电压保护情况。

d） 核查机房电力电缆线路，评估供电线路冗余或并行铺设情况。

e） 核查备用供电系统，评估备用供电系统容量是否能保证机房内设备在外部电力中断下仍能短期（一般情况下至少为两小时）正常运行。

f） 核查机房、在运设备，评估生产控制大区机房与管理信息大区机房独立设置情况，是否存在机房混用。

g） 核查机房电子门禁系统、视频和环境监控系统、人员出入登记表，评估物理访问控制情况。评估内容包括，但不限于：

1） 是否在机房各出入口配置电子门禁系统及具备存储功能的视频和环境监控系统（等级保护第四级安全区域配置第二道门禁）；

2） 人员出入登记表是否存在空缺，人员出入登记表宜包含进出人员身份、进入时间、离开时间等信息。

h） 核查机房关键设备或区域电磁屏蔽措施，评估电磁防护情况。评估内容包括，但不限于：

1） 是否将动力电缆和通信线缆隔离铺设；

2） 机柜等设施是否采用接地等防护措施防止外界电磁干扰和设备寄生耦合干扰；

3） 等级保护第四级系统的重要设备是否放置于电磁屏蔽机柜内。

i） 核查生产控制大区密码设施（对称密码、非对称密码、摘要算法、调度数字证书和安全标签等），评估当前使用的密码设施是否有厂商提供的国家有关机构的检测报告或认证证书。

## 8.3 体系结构安全

### 8.3.1 分区分级

#### 8.3.1.1 评估要求

分区分级宜符合 GB/T 36572—2018 中 6.2.2 的要求。

#### 8.3.1.2 评估实施

评估实施主要包括以下内容：

a） 核查电力监控系统网络拓扑图和网络设备，评估安全区划分情况。评估内容包括，但不限于：

1） 网络拓扑图中所示的网络结构是否符合安全区划分要求；

2） 生产控制大区是否有跨安全区纵向交叉连接等违规情况；

3） 各安全区网络设备部署情况与网络拓扑图是否一致；

4） 是否有不同安全区的设备混用、违规连接等违规情况。

b） 核查电力监控系统网络拓扑图，生产控制大区的网络中如存在业务系统在与其终端的纵向连接中使用无线通信网、电力企业其他数据网（非电力调度数据网）或者外部公用数据网的虚拟专用网络方式（VPN）等进行通信的情况，评估是否按要求设立安全接入区。

c） 核查边界安全防护设备、网络设备等可管控通用网络服务（FTP、HTTP、SNMP、远程登录、电子邮件等）的设备和系统，评估区域边界安全防护情况。评估内容包括，但不限于：

1） 是否使用数据过滤、签名认证、访问控制策略、物理隔离等措施禁止通用网络服务穿越生产控制大区和管理信息大区之间边界；

2） 是否存在设备生产厂商或其他外部企业（单位）远程连接发电厂生产控制大区中的监控系统及设备的情况；

3） 发电厂生产控制大区因业务需求与地方行政部门进行数据传输时，其边界是否采用类似生产控制大区与管理信息大区间的安全防护措施。

d） 核查电力监控系统等级保护定级报告、专家论证和审定记录等相关文档，评估是否依照GB 17859—1999 中第 4 章、GB/T 22240—2008 中 5.5、GB/T 25058—2010 中 5.3 等国家标准及行业相关要求进行合理定级，系统定级结果是否经过定级系统相关部门和安全技术专家的论证和审定。

### 8.3.2 网络专用

#### 8.3.2.1 评估要求

网络专用宜符合 GB/T 36572—2018 中 6.2.3 的要求。

#### 8.3.2.2 评估实施

评估实施主要包括以下内容：

a） 核查网络拓扑图、组网设计方案等相关文档，评估网络安全隔离情况。评估内容包括，但不限于：

1） 网络拓扑图中生产控制大区专用通道上是否使用独立的网络设备组网；

2） 是否存在生产控制大区与其他网络直连、逻辑隔离或共用网络设备的情况；

3） 网络设备的配置信息是否包含与其他通信网络相关的配置内容；

4） 相关设计文档中生产控制大区组网方式和组网技术是否符合要求。

b） 核查生产控制大区网络拓扑图、组网设计方案等相关文档，评估子网划分情况。评估内容包括，但不限于：

1） 子网划分、构造技术、边界隔离措施是否符合要求；

2） 实时子网和非实时子网边界是否使用防火墙等逻辑隔离设备或措施进行隔离。

c） 核查各层协议对应的网络设备、加密认证相关措施，评估生产控制大区数据通信七层协议的安全措施是否符合 GB/Z 25320（所有部分）的要求。评估内容包括，但不限于：

1） 是否实现与其他网络的物理隔离；

2） 是否存在默认路由，是否按照业务需求划分 VLAN，是否关闭网络边界 OSPF 路由功能，是否采用符合要求的虚拟专网、加密隧道技术；

3） 是否使用符合国家要求的加密算法，是否使用调度数字证书实现安全认证。

#### 8.3.3 横向隔离

##### 8.3.3.1 评估要求

横向隔离宜符合 GB/T 36572—2018 中 6.2.4 的要求。

##### 8.3.3.2 评估实施

评估实施主要包括以下内容：

a) 核查电力专用横向单向安全隔离装置和厂商提供的检测报告或认证证书，评估装置的检测认证情况、部署位置及策略配置是否符合要求，反向安全隔离设施是否采取基于非对称密钥技术的签名验证、内容过滤、有效性检查等安全措施，限定传输协议、返回字节数和文件类型；

b) 核查生产控制大区内部的安全区之间具有访问控制功能的设备、防火墙或者相当功能的设施，评估访问控制设备或设施的部署位置及访问控制策略配置是否符合要求。

#### 8.3.4 纵向认证

##### 8.3.4.1 评估要求

纵向认证宜符合 GB/T 36572—2018 中 6.2.5 的要求。

##### 8.3.4.2 评估实施

核查生产控制大区与广域网的纵向连接处部署的电力专用纵向加密认证装置或者加密认证网关及相应设施、厂商提供的检测报告或认证证书，评估装置、网关及相应设施的检测认证情况、部署位置及策略配置是否符合要求。

#### 8.3.5 数字证书和安全标签

##### 8.3.5.1 评估要求

数字证书和安全标签宜符合 GB/T 36572—2018 中 6.2.6 的要求。

##### 8.3.5.2 评估实施

核查基于公钥技术的分布式电力调度数字证书及安全标签，评估是否按照电力调度管理体系要求进行配置，加密认证机制是否涵盖生产控制大区中的所有重要业务系统。

#### 8.3.6 防火墙和入侵检测

##### 8.3.6.1 评估要求

防火墙和入侵检测宜符合 GB/T 36572—2018 中 6.2.7 的要求。

##### 8.3.6.2 评估实施

评估实施主要包括以下内容：

a) 核查生产控制大区内不同系统间的防火墙等逻辑隔离措施，评估系统间逻辑隔离情况。评估内容包括，但不限于：

1) 逻辑隔离、访问控制、报文过滤等功能是否符合 GB/T 25068.3—2010 中第 6 章、第 7 章的要求；

2） 策略配置是否合理有效；

3） 是否存在未部署逻辑隔离措施的情况。

b） 核查生产控制大区已部署的入侵检测措施，评估检测规则是否配置合理有效，是否有特征码离线更新前的测试记录，是否存在直接连接因特网在线更新的情况。

#### 8.3.7 防恶意代码

##### 8.3.7.1 评估要求

防恶意代码宜符合 GB/T 36572—2018 中 6.2.8 的要求。

##### 8.3.7.2 评估实施

核查生产控制大区恶意代码防范措施，评估是否有特征码离线更新前的测试记录，是否存在直接连接因特网在线更新的情况，是否存在与管理信息大区共用一套恶意代码防护措施的情况。

#### 8.3.8 拨号认证

##### 8.3.8.1 评估要求

拨号认证设施安全防护宜符合 GB/T 36572—2018 中 6.2.9 的要求。

##### 8.3.8.2 评估实施

核查拨号认证设施，评估安全防护措施是否符合要求。评估内容包括，但不限于：

a） 在无连接需求时是否处于断电关机状态；

b） 是否存在直接连接核心交换机的情况；

c） 是否仅允许单用户登录，并采取严格监管审计措施；

d） 是否使用安全加固的操作系统，使用数字证书技术进行登录和访问认证；

e） 是否通过国家有关机构安全检测认证，有厂商提供的认证证书或测试报告。

### 8.4 本体安全

#### 8.4.1 基本要求

##### 8.4.1.1 评估要求

构成电力监控系统网络安全防护体系的各个模块的安全防护宜符合 GB/T 36572—2018 中 6.3.1 的要求。

##### 8.4.1.2 评估实施

核查新建或新开发的电力监控系统和不具备升级改造条件的在运系统，评估新建或新开发的电力监控系统是否符合 GB/T 36572—2018 中 6.3 的要求，不具备升级改造条件的在运系统是否已通过健全和落实安全管理制度和安全应急机制、加强安全管控、强化网络隔离等方式降低安全风险。

#### 8.4.2 电力监控系统软件安全

##### 8.4.2.1 评估要求

电力监控系统软件安全防护宜符合 GB/T 36572—2018 中 6.3.2 的要求。

#### 8.4.2.2 评估实施

评估实施主要包括以下内容：

a) 核查电力监控系统中的控制软件和厂商提供的检测报告或认证证书，评估是否通过了满足国家或行业要求的权威机构安全检测认证及代码安全审计。

b) 核查电力监控系统软件，评估软件设计安全情况。评估内容包括，但不限于：
   1) 软件设计方案中是否包含安全防护理念和防护措施；
   2) 通过软件设计方案和逻辑结构图进行分析、判断，确认业务系统软件的各业务模块是否合理部署在相应安全等级的安全区；
   3) 实时闭环控制核心模块是否得到有效防护。

c) 核查内部专用维护设施和维护记录，评估软件运维安全情况。评估内容包括，但不限于：
   1) 是否对登录账号进行身份认证，并使用安全审计措施对维护过程实施全程监控；
   2) 是否存在通过因特网进行生产控制大区远程维护的情况。

### 8.4.3 操作系统和基础软件安全

#### 8.4.3.1 评估要求

操作系统和基础软件安全防护宜符合 GB/T 36572—2018 中 6.3.3 的要求。

#### 8.4.3.2 评估实施

评估实施主要包括以下内容：

a) 核查重要电力监控系统中的操作系统、数据库、中间件等基础软件和厂商提供的检测报告或认证证书，评估是否通过了国家有关机构的安全检测认证。

b) 核查生产控制大区业务系统的操作系统、数据库、中间件等基础软件，评估其安全可靠性是否满足 GB/T 20272—2006 中 4.3 和 4.4 的要求，身份鉴别、访问控制、安全审计等安全功能和策略是否已启用并配置合理。

c) 核查生产控制大区业务系统的操作系统和基础软件，评估软件安装更新情况。评估内容包括，但不限于：
   1) 是否存在不必要的组件和应用程序；
   2) 是否在确保不影响业务运行前提下及时升级安装补丁；
   3) 漏洞补丁安装前是否进行安全性和兼容性测试；
   4) 是否存在直接连接因特网在线更新的情况。

### 8.4.4 计算机和网络及监控设备安全

#### 8.4.4.1 评估要求

计算机和网络及监控设备安全防护宜符合 GB/T 36572—2018 中 6.3.4 的要求。

#### 8.4.4.2 评估实施

评估实施主要包括以下内容：

a) 核查电力监控系统中的计算机和网络设备、电力自动化设备、继电保护设备、安全稳定控制设备、IED、测控设备等厂商提供的检测报告或认证证书，评估是否通过了满足国家或行业要求的权威机构安全检测认证；

b) 核查生产控制大区的计算机和网络设备，评估是否符合 GB/T 21028—2007 中第 4 章和第 5 章、GB/T 21050—2007 中 7.1 和 7.2、GB/T 18336.2—2015 中第 7 章要求，身份鉴别、访问控制、安全审计等安全功能和策略是否已启用并合理配置；

c) 核查生产控制大区的计算机和网络设备，评估是否使用防撕封条等工具封闭计算机和网络设备的空闲网络端口和其他无用端口，除调度数字证书所需的 USB 接口外的其他不必要的移动存储设备接口是否均拆除或封闭。

#### 8.4.5 核心处理器芯片安全

##### 8.4.5.1 评估要求

核心处理器芯片安全防护宜符合 GB/T 36572—2018 中 6.3.5 的要求。

##### 8.4.5.2 评估实施

核查重要电力监控系统中的处理器芯片和厂商提供的检测报告或认证证书，评估处理器芯片安全情况。评估内容包括，但不限于：

a) 核心处理器芯片是否通过了国家有关机构的安全检测认证；

b) 处理器芯片设计方案或安全测试报告等文档中是否包含安全可靠的密码算法、真随机数发生器、存储器加密、总线传输加密等安全防护措施的相关内容，是否符合 GB/T 22186—2016 中 7.1 要求。

### 8.5 可信安全免疫

#### 8.5.1 评估要求

可信安全免疫宜符合 GB/T 36572—2018 中 6.4 的要求。

#### 8.5.2 评估实施

评估实施主要包括以下内容：

a) 核查电力监控系统安全防护措施，评估不具备升级改造条件的在运系统是否通过健全和落实安全管理制度和安全应急机制、加强安全管控、强化网络隔离等方式降低安全风险。

b) 核查重要电力监控系统关键控制软件和厂商提供的检测报告，评估强制版本管理情况。评估内容包括，但不限于：

1) 操作系统和监控软件的全部可执行代码在开发或升级后是否通过了指定的具有安全检测资质的检测机构的检测；

2) 可执行代码在启动运行前是否通过了对其生产厂商和检测机构签名的审查。

c) 核查重要电力监控系统基于可信计算的静态安全启动机制，评估静态安全免疫情况。评估内容包括，但不限于：

1) 设计方案、部署方案等相关文档中是否包含有效的静态度量技术；

2) 是否符合 GB/T 36572—2018 中 6.4.3 的要求。

d) 核查重要电力监控系统基于可信计算的动态安全防护机制，评估动态安全免疫情况。评估内容包括，但不限于：

1) 设计方案、部署方案等相关文档中是否包含有效的动态度量技术；

2) 动态度量对象是否包括系统进程、数据、代码段及业务网络，各项度量内容是否符合 GB/T 36572—2018 中 6.4.4 要求。

# 9 应急备用措施评估

## 9.1 冗余备用

### 9.1.1 评估要求

冗余备用措施宜符合 GB/T 36572—2018 中 7.1 的要求。

### 9.1.2 评估实施

评估实施主要包括以下内容：

a) 核查地市及以上电网调度控制中心硬件设施、包含调控人员组织结构和人员职责等内容的文档、发电厂和变电站的关键设备和备份数据等，评估是否在实时数据采集、自动化系统、调度场所、调度控制职能、调控人员等层面存在单系统、单场地、单人单岗的无备用情况。

b) 核查发电厂和变电站关键设备（控制器、可编程逻辑控制单元、工业以太网交换机、工控主机等）、特别重要设备（如现场运行系统及设备关键部位）数据备份设施、备份介质，评估内容包括，但不限于：

   1) 是否定期对数据进行备份，备份方式、备份频度等策略设置是否合理，是否按照策略执行备份操作；

   2) 关键设备是否以双机或双工的方式实现冗余备用；

   3) 特别重要设备是否配备自动化控制机制和手动操作设施两种控制方式，并对手动操作相关设备设施有计划进行检修。

c) 核查各级电网调度控制中心、发电厂和变电站电力监控系统的监控措施、预警措施、人员巡视要求和记录、故障处理流程等，评估内容包括，但不限于：

   1) 是否部署了运行状态监控和故障预警措施；

   2) 是否制定了人员巡视要求、故障处理流程等故障发现、处理、恢复相关的处理流程和管理办法，人员巡视记录是否完整。

## 9.2 应急响应

### 9.2.1 评估要求

应急响应措施宜符合 GB/T 36572—2018 中 7.2 的要求。

### 9.2.2 评估实施

评估实施主要包括以下内容：

a) 核查各电力企业应急相关制度、应急处理预案、应急演练方案、应急演练记录等应急响应相关文档，评估内容包括，但不限于：

   1) 应急相关制度是否合理、完整；

   2) 是否制定了整体应急预案和针对各系统可行的应急预案；

   3) 是否定期修订应急制度和应急预案；

   4) 是否定期开展应急演练，演练记录是否详细完整。

b) 核查生产控制大区安全事件应急预案或包含相关内容的应急预案、应急操作手册、事件处理过程记录，评估内容包括，但不限于：

1） 安全事件应急预案中是否包含上报上级主管部门、断开网络连接等应急技术措施、开展调查取证等相关内容，且符合相关要求；
2） 应急操作手册中操作流程和操作方法等内容是否描述详细，且具有可操作性；
3） 事件处理过程记录是否详细完整。

### 9.3 多道防线

#### 9.3.1 评估要求

多道防线措施宜符合 GB/T 36572—2018 中 7.3 的要求。

#### 9.3.2 评估实施

评估实施主要包括以下内容：

a） 核查电力监控系统的横向单向安全隔离设施、内外网隔离设施、防火墙等，评估是否在外部公共因特网、管理信息大区、生产控制大区的控制区及非控制区等横向边界部署相应安全措施，是否在国调、网调、省调、地调、县调间，以及各级调度机构与其直调的发电厂、变电站之间的纵向边界部署相应安全措施；
b） 核查网络安全监视措施，评估是否能根据部署要求实现主机设备、网络设备、安全设备等的信息采集、安全审计、实时监视告警等功能。

## 10 安全管理评估

### 10.1 安全管理体系

#### 10.1.1 评估要求

安全管理体系宜符合 GB/T 36572—2018 中 8.1 的要求。

#### 10.1.2 评估实施

评估实施主要包括以下内容：

a） 核查各电力企业安全工作总体方针等包含安全管理工作的职能部门、主要责任人等相关内容的管理制度，评估内容包括，但不限于：
1） 相关制度中是否明确了安全管理工作职能部门，负责安全防护工作的具体落实；
2） 是否确认了电力企业主要责任人是本单位信息安全第一责任人，对本单位的网络与信息安全负全面责任。
b） 核查各电力企业电力监控系统安全管理制度，评估内容包括，但不限于：
1） 安全管理制度体系是否符合运营单位自身需求；
2） 是否制定了安全工作的总体方针和安全策略，落实了安全管理责任；
3） 日常安全生产管理制度中是否包含电力监控系统安全防护、向上级单位信息报送、所辖范围内计算机和数据网络管理的相关内容。

### 10.2 全体人员安全管理

#### 10.2.1 评估要求

人员安全管理宜符合 GB/T 36572—2018 中 8.2 的要求。

#### 10.2.2 评估实施

评估实施主要包括以下内容：

a) 核查各电力企业安全管理职能部门组织结构、岗位职责等相关文档，评估内容包括，但不限于：
   1) 安全管理职能部门组织结构及相关文档中是否明确设立安全主管、安全管理等岗位，是否配备一定数量的安全管理员、系统管理员和安全审计员，数字证书系统等关键系统及设备配备了专门管理员，是否明确岗位职责、分工和技能要求；
   2) 是否存在安全管理员由其他岗位人员兼任的情况。
b) 核查电力监控系统安全防护的管理、运行、维护、使用等人员录用时的审查记录、保密协议、人员离岗管理制度、人员离岗后取消访问权限和回收软硬件设备的记录、各岗位人员安全技能及安全认知考核记录、安全培训教育记录、厂家维护及评估检测等第三方人员访问管理制度和访问受控区域记录等，评估是否符合 GB/T 22239—2019 中有关安全管理人员的要求，评估内容包括，但不限于：
   1) 在人员录用时是否进行身份、背景、专业资格等方面的审查；
   2) 是否与安全管理员、系统管理员、网络管理员等关键岗位的人员签署保密协议；
   3) 是否取消离岗人员访问权限和回收软硬件设备，关键岗位人员离岗前是否签订了保密协议；
   4) 是否对各岗位人员定期开展安全意识教育和安全技术培训；
   5) 是否制定了厂家维护、评估检测等第三方人员访问管理制度或相关规范。

### 10.3 全部设备及系统安全管理

#### 10.3.1 评估要求

设备及系统安全管理宜符合 GB/T 36572—2018 中 8.3 的要求。

#### 10.3.2 评估实施

评估实施主要包括以下内容：

a) 核查电力监控系统中全部业务系统软件模块和硬件设备(特别是安全防护设备)台账或资产清单，评估中可考虑以下内容，但不限于：
   1) 设备台账或资产清单是否包括全部业务系统的软件模块和硬件设备，其中记录的软件模块和硬件设备信息是否详细准确；
   2) 采购的安全防护设备和重要电力监控系统及设备中是否包含被国家相关部门检测通报存在漏洞和风险的系统及设备(包括控制器、可编程逻辑控制单元、工业以太网交换机、工控主机等)。
b) 核查电力监控系统的相关系统、设备接入技术方案、接入申请单，评估已接入电力监控系统网络的相关系统、设备是否制定接入技术方案，安全防护措施是否合理有效，是否经过安全管理部门审核、批准。
c) 核查安全风险评估报告、整改记录或报告，评估内容包括，但不限于：
   1) 是否以风险评估相关标准要求为依据，结合实际情况对本单位和下属单位已投运的电力监控系统定期开展安全风险评估；
   2) 是否对评估中发现的问题及时进行整改。

### 10.4 全生命周期安全管理

#### 10.4.1 评估要求

全生命周期安全管理宜符合 GB/T 36572—2018 中 8.4 的要求。

#### 10.4.2 评估实施

评估实施主要包括以下内容：

a) 核查电力监控系统及设备的规划设计、研究开发、施工建设、安装调试、系统改造、运行管理、退役报废等全生命周期各阶段的安全管理制度、操作流程图等安全管理措施相关文档，评估是否制定了有针对性的详细可行的管理制度及相关文档，且定期修订。

b) 核查软硬件产品采购合同、技术服务合同及相关文件，评估内容包括，但不限于：

1) 供应商是否在软硬件产品采购合同或其他文件中明确保证所提供的设备及系统符合 GB/T 36572—2018 及国家和行业信息系统安全等级保护的相关规定，并在设备及系统生命期内对此负责的相关承诺，是否包含开发制造单位承诺其产品无恶意安全隐患并终身负责的内容；

2) 检测评估单位、规划设计单位是否在技术服务合同或其他文件中承诺对其工作终身负责。

c) 核查保密协议、安全协议等相关文件，评估是否与重要电力监控系统及专用安全防护产品的开发、使用人员签订保密协议，是否与产品的开发、使用及供应商签订保密协议或安全协议，明确安全责任。

d) 核查电力监控系统及设备运维单位的验收记录、验收意见等相关文档，评估安全防护专项验收的验收记录、验收意见等相关文档是否齐全，是否存在未验收或验收未通过即已上线运行的情况。

e) 核查电力监控系统及设备运维单位的安全防护管理制度、运维操作流程、设备操作规程、运维人员岗位职责、自评估报告、整改方案等文档，评估日常运维和安全防护管理情况，评估内容包括，但不限于：

1) 是否制定了日常运维和安全防护的相关管理制度、操作规程等管理措施，并依照执行，定期修订；

2) 是否定期开展运行分析和自评估工作，实现隐患排查整改闭环。

f) 核查系统和设备退役报废时含敏感信息的介质和重要安全设备的销毁记录等相关文档，评估是否按照相关要求进行销毁。