电力系统信息安全等级保护研究

张文瀚（南方电网 电力调度通信中心，广东 广州 510623）

解决方案

摘　要：随着《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）和《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）的发布，明确了信息安全等级保护已作为国家信息安全保障的一项基本制度。《信息安全等级保护管理办法》（公通字[2007]43号）的出台标志着等级保护各项准备工作已经就绪，等级保护已进入实施阶段。探讨等级保护的基本原理以及如何在电力系统中构建等级化的安全体系。

关键词：信息安全；等级保护；安全域

1 基本原理

《信息安全等级保护管理办法》对信息安全等级保护做出了系统的描述——“信息化发展的不同阶段和不同的信息系统有着不同的安全需求，必须从实际出发，综合平衡安全成本和风险，优化信息安全资源的配置，确保重点。要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统。”

信息安全等级保护是根据信息系统在国家安全、经济安全、社会稳定和保护公共利益等方面的重要程度，将其划分成不同的安全保护等级，采取相应的安全保护措施，以保障信息和信息系统的安全。信息系统与安全保护措施级别划分关系如图1所示。

电力系统属于国家的关键基础设施，电力信息系统是涉及国家安全和社会稳定的重要信息系统，需要得到重点保护。

根据《关于信息安全等级保护工作的实施意见》对信息系统安全

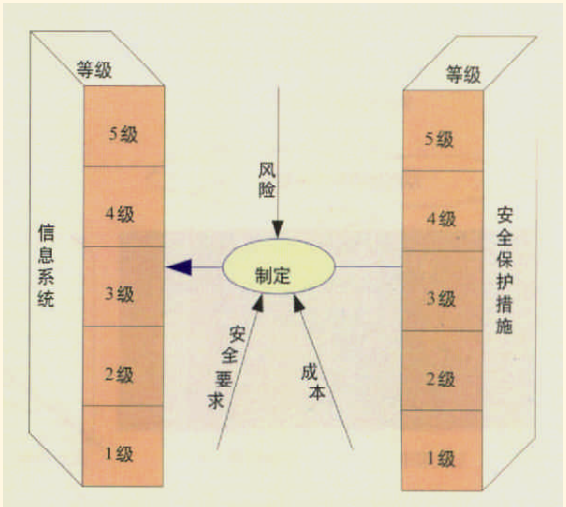

图1 信息安全等级保护级别的划分

等级的划分要求，系统安全等级共分为五级，从第一级到第五级，安全等级逐级升高，五级是系统的最高安全等级。五个等级的基本描述如下：

第一级为自主保护级，适用于一般的信息系统，其受到破坏后，会对公民、法人和其他组织的合法权益产生损害，但不损害国家安全、社会秩序和公共利益。

第二级为指导保护级，适用于一般的信息系统，其受到破坏后，会对社会秩序和公共利益造成轻微损害，但不损害国家安全。

第三级为监督保护级，适用于涉及国家安全、社会秩序和公共利益的重要信息系统，其受到破坏后，会对国家安全、社会秩序和公共利益造成损害。

第四级为强制保护级，适用于涉及国家安全、社会秩序和公共利益的重要信息系统，其受到破坏后，会对国家安全、社会秩序和公共利益造成严重损害。

第五级为专控保护级，适用于涉及国家安全、社会秩序和公共利益的重要信息系统的核心子系统，其受到破坏后，会对国家安全、社会秩序和公共利益造成特别严重损害。

2 设计方法

等级保护是国家信息安全的一项基本制度，但如何落实并在电力系统中实现呢？这里提出构建电力等级化安全体系的思路。

等级保护的核心是根据不同用户在不同阶段的需求、业务特性及应用重点，确定不同系统的重要程度，并给予重点保护。在电力安全等级保护体系设计中利用等级化与体系化相结合的安全体系设计方法，在遵循国家等级保护制度的同时，将安全等级保护思想融汇到产品、方案及应用中（见图2），建设一套覆盖全面、重点突出、节约成本、持续运行的安全保障体系。

“等级化”的特质在于符合国家等级保护制度，能够真正实现重点保护，节省投资。“体系化”的特质有3个方面：一是整体性，采用结构化的设计原理，系统地实现电力系统总体安全目标，确保内容全面；二是针对性，体系是根据电力系统业务发展战略目标确定安全目标，结合实际情况度身定做；三是可持续发展，体系中设计的框架是相对稳定，能够确保在一段时间内持续发展，逐步完善。

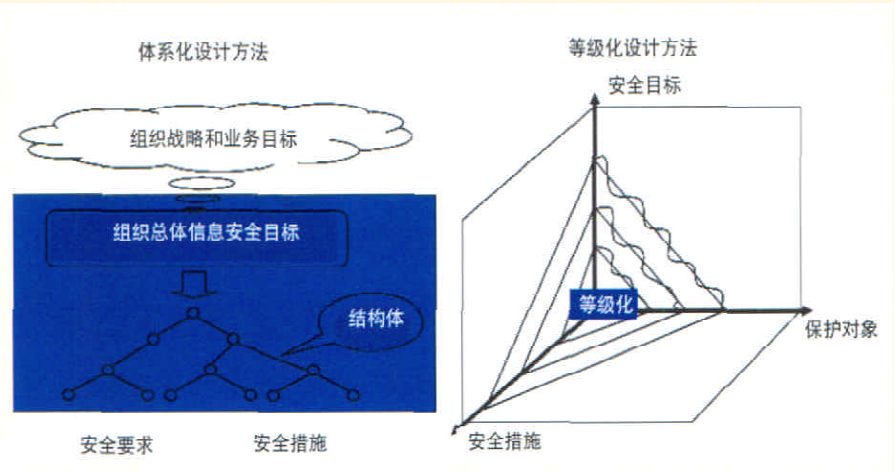

图2 体系化和等级化融合的设计方法

在建立和实施等级化安全体系后，电力系统会建立一套持续运行、涵盖所有安全内容的信息安全保障体系，这是安全工作追求的最终目标。

3 实施过程

电力行业涉及业务面广，企业、单位、人员众多，信息化建设和安全保护措施建设程度参差不齐。如何在行业发展中，谋求信息系统的安全生产、安全运营、安全管理、安全壮大，并把有限的资金、人员落实到关键保护对象，使电力企业能够以安全保发展，在发展中促安全，是摆在电力行业面前的一次技术与管理的挑战。

根据电力系统的安全实际情况，电力系统建立安全等级保护的主要过程包括（见图3）：

（1）系统识别与风险评估；

（2）系统定级；

（3）等级指标设计；

（4）安全解决方案域规划设计。

3.1 系统识别与风险评估

系统识别是对信息系统进行定级和安全保护措施的基础，正确识别系统、了解系统边界、区分系统信息和服务是系统识别过程的主要工作。

风险评估是等级保护的重要组成部分，等级的确定和安全措施的选择需要通过风险评估考核其必要性和重要性，在等级保护工作中风险评估可以采用简化或者齐备的方法，这根据系统复杂性和成本要求综合考虑。

（1）系统识别。实施等级保护工作首先要求政务机构对其拥有的或拟建的电子政务系统进行深入的识别和描述，识别和描述的内容至少包括如下信息：

1）系统基本信息：系统名称、系

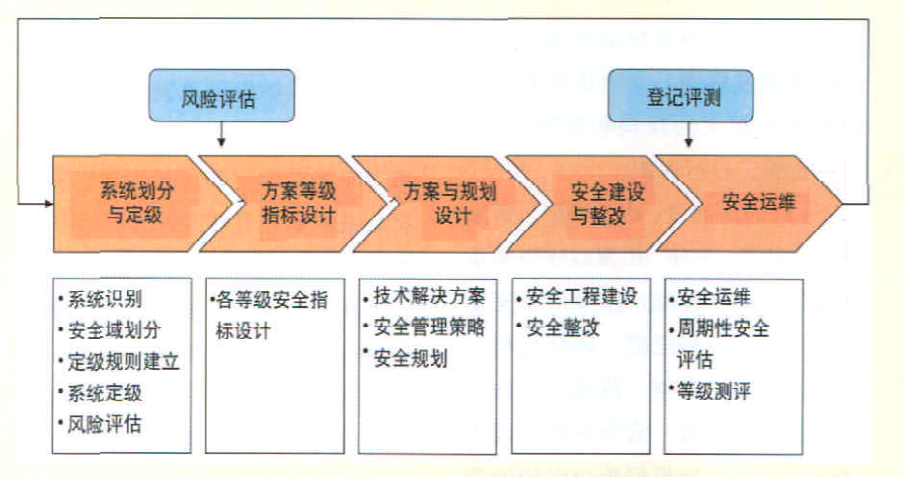

图3 电力系统信息安全等级保护过程

统的简要描述、所在地点等。

2）系统相关单位：负责定级的责任单位、系统所属单位、系统运营单位、主管部门、安全运营单位、安全主管部门等。

3）系统范围和边界：描述系统所涵盖的信息资产范围、使用者和管理者范围、行政区域范围和网络区域范围等，并清晰描述出其边界。

4）系统提供的主要功能或服务：从整体层面描述系统所提供的主要功能或服务，即对公众、企业、相关政府机关、内部用户等提供的主要服务。

5）系统所包含的主要信息：描述系统所输入、处理、存储、输出的主要信息和数据。

(2)风险评估。在等级保护实施工作中风险评估工作的处理方式比较灵活，风险评估的目的在于识别风险进而管理风险，风险评估主要包括资产评估、弱点评估、威胁评估等。

3.2 系统定级

信息系统的安全等级主要由4个要素决定：

(1)信息系统所属类型，即信息系统资产的安全利益主体；

(2) 信息系统主要处理的业务信息类别；

(3)信息系统服务范围，包括服务对象和服务网络覆盖范围；

(4)业务对信息系统的依赖程度。

其中第1、2个要素决定信息系统内信息资产的重要性，第3、4个要素决定信息系统所提供服务的重要性，而信息资产及信息系统服务的重要性决定了信息系统的安全等级。

上述定级要素是适用于各行业的通用定级要素，对不同行业信息系统定级的主观性较大，不同人员对定级要素的理解不一致，定级结果容易出现分歧。因此，针对电力行业信息系统应对定级要素进行细化，每个定级要素在电力行业中细化为多个类别的具体情形。

对于电力信息系统，可以在遵循国家定级指南的基础上，经过业务分析和风险评估，细化信息系统的定级规则，确定符合电力业务特点的定级要素和赋值标准，简化定级过程，提高定级精度和科学性，精细化掌控信息系统的安全要求和保障措施。

3.3 等级指标设计

不同级别的信息系统都对应安全目标和安全措施，也就是等级化的安全指标体系，安全指标体系从国家层面有一套推荐指标系统，由于国家级别的指标体系面向所有信息系统，不能充分考虑行业特性和业务特点，电力系统应在充分了解业务应用的基础上，结合风险评估制定符合电力系统特点和要求的指标体系，提高系统的可操行性。

电力行业等级安全指标体系是各等级系统要达到的安全要求。安全指标体系主要依据以下方面进行设计：

（1）依据信息系统安全等级保护基本要求，提供电力信息安全应达到的基本要求；

（2）通过电力行业信息系统风险评估，识别电力信息系统的主要安全风险，进行根据行业特性补充各等级安全要求

通过上述2部分工作，设计电力行业的安全指标体系，作为安全建设的基础依据。

3.4 安全解决方案域规划设计

安全解决方案设计的主要依据所建立的安全指标体系，评估现有安全措施与相应等级安全指标之间的差距，设计相应的技术解决方案和安全管理策略并实施，使系统安全水平达到相应等级的安全要求。

在解决方案设计主要描述每项技术控制方案的技术选型、产品选择原则、产品选型建议、部署方案、配置方案和相关的管理策略。

安全策略设计主要包括安全方针和系列安全制度和规范。安全方针的目标是为信息安全管理提供清晰的策略方向，阐明信息安全建设和管理的重要原则，阐明信息安全的所需支持和承诺。各类管理规定、管理办法和暂行规定主要规定的安

全各个方面所应遵守的原则方法、具体管理规定、管理办法和实施办法，

根据安全指标体系的要求，以风险评估为基础，在安全等级保护体系基础上，结合信息化规划、预算等实际情况，对用户信息安全等级保护体系的建设和管理提出规划方案，实现信息安全总体规划、分步实施、重点落实的建设方法。

4 电力行业实施信息安全等级保护制度的原则

电力行业实施信息安全等级保护制度应该遵循以下基本原则：

(1)明确责任，共同保护。通过等级保护，组织和动员电力行业各企业和单位共同参与信息安全保护工作；各方主体按照等级保护的规范和标准分别承担相应的、明确具体的信息安全保护责任。

(2)依照标准，自行保护。电力行业和企业和单位应运用国家强制性的规范及标准，要求信息和信息系统按照相应的建设和管理要求，自行定级、自行保护。

(3)同步建设，动态调整。信息系统在新建、改建、扩建时应当同步建设信息安全设施，保障信息安全与信息化建设相适应。因信息和信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级。等级保护的管理规范和技术标准应按照等级保护工作开展的实际情况适时修订。

(4)指导监督，重点保护。电力行业和企业和单位应通过国家指定信息安全监管职能部门通过备案、指导、检查、督促整改等方式，对重要信息和信息系统的信息安全保护工作进行指导监督。

5 结语

等级保护是信息安全领域一项基本国策，我国等级保护的相关技术标准还在制定和完善中，这就要求组织的管理者在实施等级保护要求中，不断探索和实践，把等级保护工作真正落实到实处。电力行业正在实施的二次防护工作，就是一种用等级保护的思想，保证发电系统、调度系统等重要电力信息系统的安全保障工作，它对全面推进等级保护在电力行业中的推广有着积极的作用。

责任编辑 王思宁
收稿日期：2007-12-24

作者简介：

张文瀚(1970-)，男，江苏连云港人，高级工程师，从事电力通信方面的工作和研究。

解决方案

新品集锦

2GHz功耗仅1W 英特尔新一代MID处理器

英特尔在最近的国际固态电子电路大会(International Solid State Circuits Conference，ISSCC)上，透露了更多下一代移动联网装置(Mobile Internet Device)所采用的Silverthorne处理器数据。据悉，新一代Silverthorne处理器将采用全新45nm High-K金属闸极CMOS制程，最低可以把耗电量控制到1～2 W。

具体参数方面，Intel Silverthorne处理器采用全新低耗电IA微架构，此微架构以双码(dual-code)、双指令执行(dual-issue)、循序执行(in-order execution)为基础，采用16阶处理器管线(16-stage processor pipeline)，与x86指令集完全兼容。此微架构采用突破性的电源管理技术，如Deep Power Down (C6)状态、非格状频率分送(non-grid clock distribution)、电源最佳化缓存器档案(power-optimized register-file)、频率闸控(clock gating)、CMOS总线模式，并采用Split I/O电源供应方式以大幅降低动态变化(dynamic)与漏电(leakage power)。

由于采用了这些创新的电源管理技术，45nm high-k金属闸极材质的Silverthorne处理器可望将产生的热量功耗(thermal power)相较2006年推出的超低电压(Ultra Low Voltage)单核心英特尔处理器降低达10倍，并可提供执行完整因特网与各种应用软件的高效能。

Intel表示，Silverthorne将提供低功耗运算效能(sub-watt performance)，未来则可能在1W功耗下以2GHz的速度运行。