第 39 卷 第 1 期 2015 年 1 月 10 日
DOI：10.7500/AEPS20141014013
电力系统自动化
Automation of Electric Power Systems
Vol.39 No.1 Jan.10，2015

智能电网调度控制系统安全防护技术及发展

高昆仑[1]，辛耀中[2]，李　钊[1]，孙　炜[2]，南贵林[2]，陶洪铸[2]，赵保华[1]
（1. 中国电力科学研究院，北京市 100192；2. 国家电网公司国家电力调度控制中心，北京市 100031）

摘要：对中国电网调度控制系统信息安全防护体系的发展历程进行梳理，总结为 3 个阶段，即基于边界安全的纵深防护体系阶段、基于等级保护的业务安全防护体系阶段以及基于可信计算的主动防御体系阶段。结合当前日新月异的新型威胁及国家级网络空间对抗新形势，提出基于可信计算技术，实现计算环境可信、应用行为可信、网络通信可信，构建以安全免疫为特征、以安全可控为目标的新一代智能电网调度控制系统安全主动防御体系，并介绍了其核心防御技术。

关键词：智能电网调度控制系统；网络安全；纵深防护；等级保护；可信计算；主动防御

0　引言

中国电网发展进入“电力流、信息流、业务流”高度融合的智能电网阶段，电网调度控制系统及通信网络是智能电网的“大脑”及“神经中枢”，管理控制电网的可靠运行。网络空间的信息安全风险可以通过对电网调度控制系统及通信网络的破坏，进而对智能电网实体形成致命威胁。

当前，网络安全已经成为国家安全的重要组成部分。中央成立了网络安全与信息化领导小组，提出“没有网络安全就没有国家安全”。网络安全概念从传统的信息系统安全防护发展到网络空间对抗。事实上，网络已成为陆地、海洋、天空和太空之后的第五作战空间。国际上已经围绕“制网权”展开了国家级别的博弈甚至局部网络战争。

1　中国电力监控系统安全防护体系发展历程

中国是世界上最早开始重视电力监控系统信息安全问题并建立防护体系的国家之一。其里程碑是 2000 年国家电力调度数据（骨干）网组网技术体制的确立。

1.1　电力调度数据专网专用的防护策略

调度数据网从基于 X.25 分组交换网向宽带 IP 数据网升级换代，有多个组网技术体制选择，主要包括基于异步传输模式（ATM）的 IP 专网、基于同步数字体系（SDH）物理电路的 IP 专网，以及 IP 虚拟专用网络（VPN）。综合考虑各路线的技术成熟性、先进性、经济性，重点比较了不同技术体制下调度数据网及其承载的调度控制业务的信息安全风险，确定了基于 SDH 物理电路构建电力调度数据 IP 专网的技术路线。在此基础上，进一步形成了中国电力系统第 1 个强制执行的信息安全法规，即中华人民共和国国家经济贸易委员会第 30 号令《电网和电厂计算机监控系统及调度数据网安全防护规定》（2002 年5 月 8 日发布）[1]。该法令以“防范对电网和电厂计算机监控系统及调度数据网络的攻击侵害及由此引起的电力系统事故，保障电力系统的安全稳定运行”为目标，规定了电力调度数据网络实现物理层面上与公用信息网络的安全隔离，并只允许传输与电力调度生产直接相关的数据业务，奠定了国内电力监控系统“结构性安全”的重要技术基础，成为中国电力监控系统信息安全防护体系建设启动的标志。

1.2　基于边界安全的纵深防护体系

随着电力监控系统自动化水平的提高、功能的丰富及调度数据网覆盖范围的延伸、用户的增加，电力监控系统信息安全威胁来源愈发多元化，不仅来自外部，也源于内部，不仅来自本地，也源于上下级调度单元；威胁形式多样化，既有恶意代码，也有人为操作；破坏效果多重化，包括通信中断、数据丢失、信号错误、系统瘫痪、功能失效、甚至恶意操控。

为了应对新的信息安全风险，2002 年国家科技部启动了国家高技术研究发展计划（863 计划）“国

收稿日期：2014-10-14；修回日期：2014-11-19。
国家高技术研究发展计划（863 计划）资助项目（2011AA05A118）；国家电网公司科技项目“基于可信计算的电力生产调度系统安全增强技术研究及应用”。

家电网调度中心安全防护体系研究及示范”，提出了中国电力监控系统第一个全面的安全防护总体策略，即“安全分区、网络专用、横向隔离、纵向认证”。其中，“安全分区”将各项电力业务功能分别置于生产控制大区与管理信息大区中；“网络专用”利用网络产品组建电力调度数据网，为调度控制业务提供专用网络支持；“横向隔离”通过自主研发的电力专用单向隔离装置实现生产控制大区与管理信息大区的安全隔离；“纵向认证”通过自主研发的电力专用纵向加密认证装置为纵向传输的业务数据提供加密和认证保护，保证数据传输和远方控制的安全。形成了以边界防护为要点、多道防线构成的纵深防护体系，结构如图 1 所示。

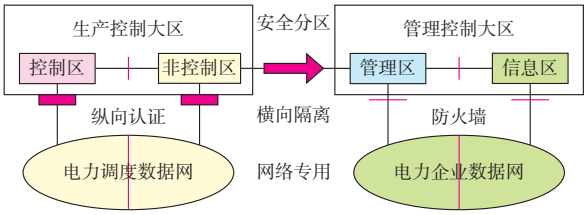

图 1　基于边界安全的纵深防护体系
Fig.1　Architecture of in-depth safeguard based on perimeter security

2004 年 12 月，该体系以国家电力监管委员会 5 号令《电力二次系统安全防护规定》[2] 等相关配套技术文件形式发布，成为中国电力监控系统第 1 阶段安全防护体系全面形成的标志。标志体系的具体实施内容包括安全区的划分、调度数据专网组网要求、横向边界隔离要求、纵向认证要求、调度数字证书系统、基础设施软硬件安全配置、通用安全防护产品部署、远程接入的防护，以及电力二次系统安全防护评估等。体系的实施范围为各级电力调度中心、各类变电站和发电厂、用电负荷管理等。

1.3　基于等级保护的业务安全防护体系

信息系统安全等级保护是中国信息安全领域中的一项基本制度，制度要求各信息系统依据系统业务使命的重要程度及系统遭到破坏后对国家安全、社会秩序、公共利益及公民、法人和其他组织合法权益的危害程度，从低到高依次划分为自主保护（1 级）、系统审计保护（2 级）、安全标记保护（3 级）、结构化保护（4 级）、访问验证保护（5 级）这 5 个安全保护等级。不同等级系统根据不同强度要求进行防护，对系统中使用的信息安全产品按等级进行管理，对系统中发生的信息安全事件分等级响应和处置。

2007 年国家电力监管委员会印发了《关于开展电力行业信息系统安全等级保护定级工作的通知》[3] 等系列文件，启动电力行业信息安全等级保护定级工作。2012 年印发了《电力行业信息系统安全等级保护基本要求》[4]，全面推进行业等级保护建设工作。

电力生产控制系统中，省级及以上调度中心的调度控制系统安全保护等级为 4 级，220 kV 及以上的变电站自动化系统、单机容量 300 MW 及以上的火电机组控制系统（DCS）、总装机 1 000 MW 及以上的水电厂监控系统、总装机 2 000 MW 及以上的梯级调度监控系统、电力负荷管理系统安全保护等级为 3 级，其余为 2 级。

在上一阶段纵深防护体系基础上，依据《电力行业信息系统安全等级保护基本要求》，构建形成电力监控系统层次化的等级保护体系，由物理安全、网络安全、主机安全、应用安全和数据安全防护这 5 个层面组成，每个层面包括若干安全控制点。结构如图 2 所示。

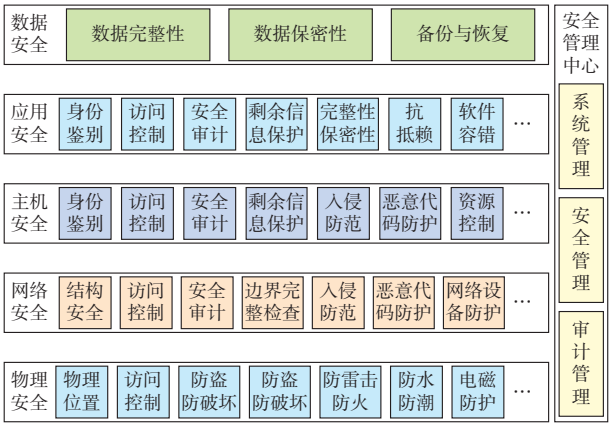

图 2　等级保护体系
Fig.2　Classified protection architecture

对于保护等级为 4 级的省级及以上调度中心的电网调度监控系统，需要实现结构化保护，即具有明确定义的形式化安全策略模型；将第 3 级系统中的自主和强制访问控制（MAC）扩展到所有主体与客体，加强鉴别机制；进行隐蔽通道分析。对于 4 级操作系统及数据库，需要对所有主体和客体实现安全标记，并基于安全标记进行 MAC。

为全面达到以上 4 级保护要求，自主开发了监控应用软件，并综合运用调度数字证书和安全标签技术实现了操作系统与业务应用的强制执行控制（MEC）、MAC 等安全防护策略，保障了主体与客体间的全过程安全保护，全面实现了等级保护 4 级的技术要求。

依托智能电网调度控制系统，建成了国家电网备用调度体系，实现了“国调网调异地互备、省级调度异地共备，地县调分布采集、上为下备”的分布式备用调度核心技术，建成了省级以上协调的分布式

备调系统，实现了实时数据采集、调度控制装备、实时调度业务 3 个层面的容灾备用，提高了电网调度抵御重大自然灾害、重大事故和外部攻击破坏的能力。

2　基于可信计算技术的新一代电网调度控制系统主动防御体系

经过以上 2 个阶段防护体系建设，形成了智能电网调度控制系统安全防护 3 道防线、层次化的保护体系，以及业务级的灾备体系，整体防护能力领先于国际电力行业。同时，国际信息安全形势的发展、网络战争形态及能力的演进，大量新型攻击方式快速涌现。“震网”病毒被认为是第 1 个对工业实体设施形成破坏能力的网络战武器，2010 年 9 月它突破了控制网络的物理隔离的“封堵”，成功攻击了伊朗核电站。安全威胁特征代码库规模的迅速增长，使得以“查杀”为核心的被动安全措施对于实时控制系统安全防护失去效率。为应对网络战环境下复杂的信息安全威胁，同时减小防护机制对电网调度控制系统实时性能的影响，亟需建立更为高效的主动防御体系。

2.1　基于可信计算技术的主动防御体系

可信计算改变了传统的“封堵查杀”等“被动应对”的防护模式。其核心思想是在计算的同时进行安全防护，使计算结果总是与预期一样，计算全程可测可控，不被干扰，是一种运算和防护并存、主动免疫的新型计算模式。

2014 年 8 月国家发改委印发了〔2014〕第 14 号令[5]《电力监控系统安全防护规定》及《电力监控系统安全防护总体方案》等配套技术文件。总体方案要求生产控制大区具备控制功能的系统，应用可信计算技术实现计算环境和网络环境安全可信，建立对恶意代码的免疫能力，应对高级别的复杂网络攻击。这标志着中国智能电网调度控制系统信息安全主动防御体系的正式确立。

综合上述分析，中国智能电网调度控制系统安全防护体系的整体发展历程可以划分为 3 个阶段，如图 3 所示。

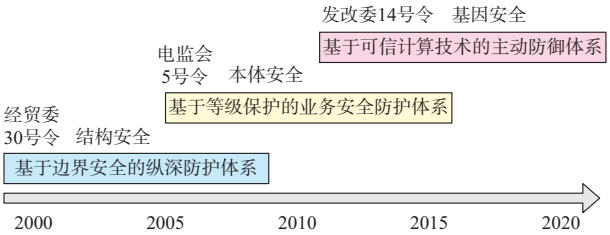

图 3　智能电网调度控制系统安全防护体系发展历程
Fig.3　Development process of cybersecurity protection architecture in smart grid dispatching and control system

随着安全防护体系的演进，智能电网调度控制系统安全防护策略同步发展完善。在主动防御阶段，形成安全防护总体策略，如图 4 所示。

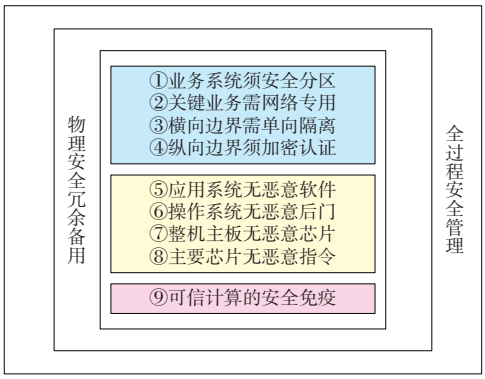

图 4　智能电网调度控制系统安全防护总体策略
Fig.4　Overall security protection strategy for smart grid dispatching and control system

2.2　可信计算技术原理

可信计算技术的基本原理是在硬件上建立计算资源节点和可信保护节点并行结构。首先，构建一个硬件信任根，在平台加电开始，从信任根到硬件平台、操作系统、应用程序，构建完整的信任链，一级认证一级，一级信任一级，把这种信任扩展到整个计算机系统，从而从源头上确保整个计算机系统可信，并且能够通过可信报告功能将这种信任关系通过网络连接延伸到整个信息系统。未获认证的程序不能执行，从而及时识别“自己”和“非己”成分，破坏与排斥进入机体的有害物质，实现系统自身免疫，构建高安全等级的防护系统。基本原理如图 5 所示。

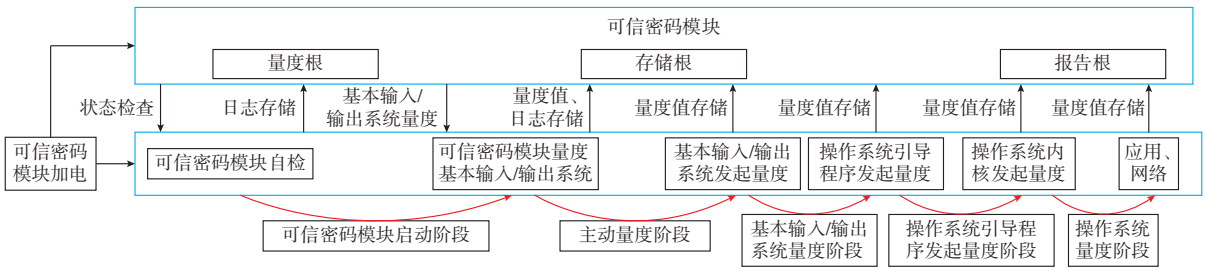

图 5　可信计算技术基本原理
Fig.5　Basic principles of trusted computing technology

2.3　电网调度控制系统可信计算平台

应用可信计算技术，建立调度控制系统主动免疫机制，提升对未知恶意代码攻击的免疫能力，实现计算机环境和网络环境的全程可测可控和安全可信。电力可信计算密码平台是实现智能电网调度控制系统安全免疫的核心，由可信密码硬件模块与可信软件基组成，其核心功能包括可信引导、完整性量度、MAC、MEC 和可信网络连接。平台体系结构如图 6 所示。

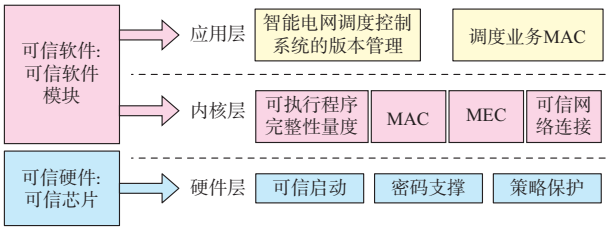

图 6　电力可信计算密码平台体系结构
Fig.6　Architecture of electric power trusted computing platform

1)可信引导。在智能电网调度控制系统中的核心服务器上，实现可信密码模块(可信根)对操作系统的可信引导，将信任链从可信密码模块传递到操作系统，保证系统的启动安全过渡到系统运行状态。通过对系统引导数据的验证，防止恶意程序对系统引导阶段的攻击及对系统引导行为的破坏。

2)完整性量度。包括静态完整性量度与动态完整性量度。静态完整性量度是指计算被测量对象(包括可执行程序、动态库、内核模块)的杂凑值，检查其完整性是否遭受破坏，保证系统运行对象初始状态可信。动态完整性量度是计算被测量对象(包括操作系统内核的代码段、只读数据段、关键跳转表和应用层的进程代码段)的杂凑值，检查其运行状况，确保系统运行状态的可信，为访问控制机制和可信证明机制提供支撑。

3)MAC 和 MEC。MAC 用于将系统中的信息分级和类进行管理，以保证每个用户只能访问到那些被标明可以由其他访问的信息的一种访问约束机制；MEC 的目标是对特定代码的执行进行限制，阻止其被恶意侵入的进程或误操作启动。要求指定程序/动态库不能在指定方式以外的情况下执行/加载。

4)可信网络连接。实现网络通信节点之间的可信认证及安全通信。

2.4　基于可信计算的主动防御体系效果验证

电网调度控制系统对实时性能要求很高。由于可信计算技术在操作系统、可执行程序的加载、启动执行环节引入了完整性量度等控制机制，不可避免地对系统的实时性及相关性能产生影响。为了定量评估这些影响以及主动防护效果，本文建立了电网调度控制系统主动防御仿真环境，仿真环境中部署了一个完整的智能电网调度控制系统，在系统的前置机、数据采集与监控(SCADA)服务器、数据库服务器、人机工作站上安装电力可信计算密码平台(包含可信密码模块和可信软件基)。测试环境采用当前主流的服务器，其上分别安装 XX，YY，ZZ 这 3 款安全操作系统。

依托仿真环境，对可信计算密码平台给控制系统引入的性能影响进行测试，包括：①可信计算密码平台占用资源测试；②进程加载时间影响测试；③访问响应时间影响测试。

可信计算密码平台对 CPU 及内存的影响如表 1 所示。可信计算密码平台对进程加载时间的影响如表 2 所示。可信计算密码平台对访问响应时间的影响如表 3 所示。

表 1　对 CPU 及内存的影响
Table 1　Impact on CPU and memory

测试环境	CPU 使用率/%			Memory 使用率/%		
	加载前	加载后	影响度	加载前	加载后	影响度
安全操作系统 1+服务器	0.01	0.02	0.01	1.02	1.03	0.01
安全操作系统 2+服务器	0.02	0.03	0.01	1.38	1.44	0.06
安全操作系统 3+服务器	0.03	0.04	0.01	0.85	0.91	0.06

表 2　对进程加载时间的影响
Table 2　Impact on process loading time

测试环境	启动进程次数	进程加载时间/s		影响度/%
		加载前	加载后	
安全操作系统 1+服务器	第 1 次	0.777	0.846	8.88
	第 2 次	0.071	0.088	23.94
	第 3 次	0.041	0.063	53.66
安全操作系统 2+服务器	第 1 次	2.358	2.371	0.55
	第 2 次	1.153	1.177	2.08
	第 3 次	0.589	0.631	7.13
安全操作系统 3+服务器	第 1 次	0.533	0.591	10.88
	第 2 次	0.182	0.231	26.92
	第 3 次	0.055	0.071	29.09

表 3　对访问响应时间的影响
Table 3　Impact on access response time

测试环境	访问响应时间/s		影响度/%
	加载前	加载后	
安全操作系统 1+服务器	0.851	0.871	2.35
安全操作系统 2+服务器	0.971	0.982	1.13
安全操作系统 3+服务器	0.535	0.563	5.23

性能测试结果表明可信计算密码平台对系统性能的影响较小，对进程加载时间和访问响应时间的

影响处于毫秒级别。

电网调度控制系统所面临的恶意程序主要包括恶意可执行程序、恶意脚本、恶意动态库以及恶意内核模块。为了验证基于可信计算的主动防御体系对电网调度控制系统的防护效果，本文在测试环境中模拟上述4类恶意程序，从恶意程序的传播、执行、感染和破坏4个阶段分别对系统进行100次攻击。测试结果表明，主动防御体系对于4类恶意程序在4个阶段的防御成功率均为100%。这说明可信计算密码平台可以防御恶意代码从各种途径入侵，防止恶意代码感染系统中的可执行程序，同时也可以防止恶意代码对系统实施破坏。可信计算密码平台从根本上解决了恶意代码问题，基于可信计算技术的主动防御体系可以为电网调度控制系统构建一个安全自主可控的执行环境。

2.5　工程实施和实现中需要解决的技术问题

基于可信计算的主动防御体系可以建立有效的恶意代码免疫能力，但在应用实现中尚需考虑可信计算技术与现有安全机制的有效结合，使各安全机制发挥最大效用。在工程实施中，应考虑如何区分业务应用的安全要求和软硬件条件，以分别采用不同形态的电力可信计算密码平台。

3　结语

中国电网调度控制系统安全防护体系发展经历了基于边界安全的纵深防护体系、基于等级保护的业务安全防护体系，以及基于可信计算的主动防御体系三大阶段。为应对日新月异的新型威胁及国家级网络空间对抗新形势，采用可信计算技术，实现计算环境可信、应用行为可信、网络通信可信，构建以安全免疫为特征、以安全可控为目标的新一代主动防御体系。根据应用场景，电力可信计算密码平台将以不同的形态，部署在调度中心、发电站、变电站的计算机系统中，或嵌入远程终端设备/馈线终端装置等各类智能测控单元中，在“十三五”期间推广应用，全面建成智能电网调度控制系统安全主动防御体系。

参 考 文 献

[1] 国家经济贸易委员会.经贸委30号令　电网和电厂计算机监控系统及调度数据网安全防护规定[S].2002.
[2] 国家电力监管委员会.电监会5号令　电力二次系统安全防护规定[S].2004.
[3] 国家电力监管委员会.电监信息44号　关于开展电力行业信息系统安全等级保护定级工作的通知[R].2007.
[4] 国家电力监管委员会.电监信息62号　电力行业信息系统安全等级保护基本要求[S].2012.
[5] 国家发展改革委员会.发改委14号令　电力监控系统安全防护规定[S].2014.

高昆仑(1972—)，男，通信作者，博士，教授级高级工程师，主要研究方向：电力系统及其自动化、网络与信息安全。E-mail：gkl@epri.sgcc.com.cn

辛耀中(1956—)，男，博士，教授级高级工程师，副主任，主要研究方向：电力系统自动化。E-mail：xin-yaozhong@sgcc.com.cn

李　钊(1986—)，男，博士，工程师，主要研究方向：电力系统及其自动化、复杂网络、网络与信息安全。E-mail：lizhao@epri.sgcc.com.cn

（编辑　王梦岩　章黎）

Development and Process of Cybersecurity Protection Architecture for Smart Grid Dispatching and Control Systems

GAO Kunlun[1], *XIN Yaozhong*[2], *LI Zhao*[1], *SUN Wei*[2], *NAN Guilin*[2], *TAO Hongzhu*[2], *ZHAO Baohua*[1]
(1. China Electric Power Research Institute, Beijing 100192, China;
2. National Electric Power Dispatching and Control Center, State Grid Corporation of China, Beijing 100031, China)

Abstract: The development process of cybersecurity protection architecture for the smart grid dispatching and control system in China is analyzed and summarized in three stages, namely, in-depth safeguard based on perimeter security, business security based on classified protection and active safeguard based on trusted computation. Then, with the current rapidly changing threats and the new situation of national cyberspace confrontation taken into account, a new generation of grid dispatching control system security active safeguarding architecture based on trusted computing technology is proposed. The purpose is to achieve a trusted computing environment, trusted application behavior and trusted network communication. The architecture proposed is characterized by security and immunity, and has security and controllability as its objective. The core safeguarding technologies are described.

This work is supported by National High Technology Research and Development Program of China (863 Program) (No. 2011AA05A118) and State Grid Corporation of China.

Key words: smart grid dispatching and control systems; cybersecurity; in-depth safeguard; classified protection; trusted computing; active defense