华夏英才基金学术文库

吴克河 刘吉臻 张彤 李为 著

电力信息系统安全防御体系及关键技术

科学出版社

www.sciencep.com

ISBN 978-7-03-031724-7

9 787030 317247 >

工程技术分社
电　话：010-64033541
E-mail: zhangyanfen@mail.sciencep.com
销售分类建议：电力

定　价：88.00 元

華夏英才基金學術文庫

电力信息系统安全防御体系及关键技术

吴克河　刘吉臻　张　彤　李　为　著

科学出版社
北京

内 容 简 介

本书是以电力行业信息系统为研究对象，研究电力信息安全的理论、技术和应用，以电力信息系统现状及安全需求为全书的主要线索，将电力信息系统现状及安全需求分析作为以后各章研究的出发点。本书首先介绍了电力信息安全的理论研究，包括信息安全理论的概述、电力信息安全的概述、网络业务安全的理论研究、主动可控防御的理论研究和电力信息系统安全防御体系的理论研究；然后介绍了作者多年从事电力信息安全技术研究和开发所形成的技术成果，包括基于 MRC 的主机安全防御系统、网络二极管技术、移动终端安全接入平台、安全文件保护系统在内的多项适用于电力企业信息安全特殊要求的关键技术；最后介绍了作者的科研团队在电力信息安全领域的多个成功案例和典型应用实例。

本书可作为信息安全理论和技术研究人员、企事业单位信息专业人员从事信息安全工作的重要技术资料，也可作为高等学校信息安全专业、计算机科学与技术专业、自动化专业的本科学生和研究生的教材和教学参考书。

图书在版编目(CIP)数据

电力信息系统安全防御体系及关键技术/吴克河等著. —北京：科学出版社，2011

ISBN 978-7-03-031724-7

Ⅰ. 电… Ⅱ. 吴… Ⅲ. 电力系统：信息系统—安全技术 Ⅳ. TM7

中国版本图书馆 CIP 数据核字（2011）第 119701 号

责任编辑：张艳芬 / 责任校对：李 影

责任印制：赵 博 / 封面设计：陈 敬

科学出版社出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

新蕾印刷厂印刷

科学出版社发行 各地新华书店经销

*

2011 年 10 月第 一 版 开本：B5（720×1000）

2011 年 10 月第一次印刷 印张：25

字数：500 000

定价：88.00 元

（如有印装质量问题，我社负责调换）

关 于 本 书

随着电力信息化建设的快速推进，电力工业的生产和管理向着智能化和管控一体化的方向发展。电力工业的新应用和新发展，对电力信息安全提出了更高的要求。传统的信息安全以公共信息网络中数据的私密性保护为主要内容。在电力应用中，运行于网络之上的业务系统安全防护，包括控制网络中控制逻辑的完整性、实时性保护，业务逻辑的完整性和连续性保护，以及操作抗抵赖性等，是电力信息安全面临的新问题。在面向电力科研的实践中，面临许多信息安全的新问题。例如，2004 年，在“火电厂厂级运行性能在线诊断及优化控制系统”项目（获国家科学技术进步奖二等奖）的研发中，针对生产自动化系统网络与厂级监控实时系统网络的信息安全保护，以及厂级监控实时系统业务安全性问题，刘吉臻教授提出了“两级信息安全，三级业务安全”思想，解决了信息安全等级划分和业务安全等级划分问题。又如，2005 年，在“电网实时数据管理和综合数据挖掘应用系统”项目（获北京市科学技术进步奖二等奖）的研究中，涉及将电网调度自动化系统网络中的数据传送到生产管理系统网络中的问题，这是高等级业务安全网络向低等级业务安全等级的单向数据传输问题。针对电力信息安全的新问题，作者紧密结合电力行业的应用实际，进行理论研究和技术研究。

本书是在总结近年来信息安全理论研究和工程实践的基础上，以电力企业信息网络和电力信息安全的特殊要求为目标，研究“网络业务安全”的理论和电力信息安全的关键技术，最终设计建立了一个满足电力工业安全要求的电力信息系统安全防御体系。本书的主要内容有以下几点：

第一，信息网络可以简单地分为公共信息网和私有信息网。公共信息网，如 Internet、Chinanet、Cernet 等，功能是提供信息共享与信息交互服务。公共信息网的安全保护目标是网络信息内容安全和网络系统安全，即信息内容的私密性和完整性。私有信息网一般是指企业私有网，如电力调度数据网（SPDnet）、电力综合数据网（SPInet）等，除了实现信息共享与信息交互外，更重要的是支撑电力调度自动化系统和实现企业业务的网络化协同工作。私有信息网不仅是信息共享和信息交互的平台，更重要的是企业生产自动化系统和管理业务系统的协同工作平台。企业信息网的安全，不仅是网络系统安全和数据安全，更重要的是运行于网络系统之上企业业务的安全，即业务私密性、完整性、连续性和实时性，包括企业生产自动化系统控制逻辑的完整性和实时性，企业业务过程完整性和连续性等。本书针对电力企业私有网的安全保护实践，提出了“网络业务安全”的

概念，将企业私有网的安全保护的目标定义为内容安全、数据安全、网络安全和业务安全。

第二，传统的电力安全包含一次系统安全和二次系统安全。随着信息技术的快速发展，电力信息化程度的提高，尤其是智能电网的建设，使传统的相对孤立的电力控制系统网络、电力调度系统网络逐步与企业信息系统网络实现了互联互通，使得传统信息系统的安全威胁引申到电力二次系统，并且由此引发电力系统事故。更有甚者，有组织有目的地通过信息系统网络实施对电网的攻击破坏已成为未来网络战的首选手段。电力二次系统的安全保护与信息系统的安全保护，在目标、对象、措施，甚至理论与策略方面都有很大差别。电力二次系统的安全保护目标是控制逻辑的完整性和实时性，以及控制网络的可用性。传统的信息安全是以信息内容的安全性（私密性）保护为目标，并由此涉及数据安全和网络安全。由于电力工业的连续性特点，电力控制系统不能中断，这就要求电力二次系统的暴露攻击时间为零，传统的 PDR 理论不能适应电力信息安全保护的要求。本书针对电力二次系统网络特点（有限的网络边界、明确应用、确定的操作、固定的角色）及其安全保护要求，提出了一种“主动防御策略”，以保证电力二次系统的绝对安全。

第三，针对“电力信息安全主动防御策略”的应用和实现，研究相关的关键技术。主要有基于网络进程实时监控强制运行控制技术、对于特殊操作控制的基于主机硬件信号确认的强制硬件确认控制技术、基于单向物理链路和电信号接收应答的网络单向数据传输（网络二极管）技术，以及基于 **APN** 技术、应用虚拟化技术、智能体代理技术的安全接入平台等，为构建电力信息系统安全防御体系提供技术支撑。

本书是以电力信息系统安全保护应用需求为背景，在实践的基础上进行有针对性的理论研究和技术研究，以期解决实践中理论指导和技术支撑的问题。希望本书能为从事电力信息安全理论研究和从事电力信息安全实际工作的同志提供一些借鉴和引导，更希望广大读者针对本书的不足之处提出意见和建议，使本书起到抛砖引玉的作用。

作　者

2011 年 7 月

前　言

随着计算机网络技术的飞速发展，以及信息系统的应用和普及，网络信息系统的安全问题日益突出。网络信息安全已成为继海、陆、空和太空之后的第五大安全领域。信息安全作为非传统安全因素，已与各国的政治安全、国防安全、经济安全、文化安全共同成为国家安全的重要组成部分。由于电力工业在国民经济和社会生活中的支撑作用，电力信息安全已成为国家信息安全最重要的内容，具有特殊的经济和政治意义，也使得电力信息安全具有特殊的高要求。针对电力信息安全的特殊性和新特点，需要在信息的理论、技术和策略方面进行有针对性的研究，以满足电力信息安全的需要。

电力信息安全主动可控防御体系及关键技术正是基于这一背景提出的。长期以来作者及其团队一直从事电力信息安全方面的科研和技术开发，取得了一些研究成果，积累了一些实践经验。作者想通过本书把自己的研究成果和实践经验与读者分享。

本书是以电力行业信息系统为对象，研究电力信息安全的理论、技术和工程应用的学术著作，以电力信息系统现状及安全需求为全书的主要线索，将电力信息系统现状及安全需求分析作为以后各章研究的出发点。本书分三篇，共 18 章。第一篇（第 1～6 章）为电力信息安全理论，主要介绍针对电力信息系统安全的特点，研究满足电力信息安全需求的新理论和新安全策略，包括“网络业务安全”安全模型“主动可控安全防御”策略，以及电力信息安全管控体系等。第二篇（第 7～12 章）为电力信息安全关键技术，主要介绍基于网络进程实时监控的强制运行控制技术，基于主机硬件信号实时监测的强制硬件确认控制技术，基于单向物理链路的网络单向数据传输（网络二极管）技术，以及移动安全接入技术，安全文件保护技术、安全自治愈技术和电力私有云安全技术等。第三篇（第 13～18 章）为电力信息安全工程应用，主要介绍电力信息安全保护对象及工程实践，以及电力信息安全的典型工程应用，智能电网环境下的电力信息安全等。

本书的特点是针对电力信息安全的特殊性，由实践出发研究理论问题，根据工程实践的难点研究技术问题。本书提出的网络业务模型，很好地解决了电力信息安全实践中根据业务进行安全等级划分的理论问题；根据电力二次系统的高安全需求，以及电力工业连续性生产过程的特点和管控一体化的要求，研究了网络二极管技术；根据智能电网信息交互的需要研究开发了移动安全接入技术等。

本书由吴克河教授、刘吉臻教授、张彤博士和李为副教授共同撰写。吴克河

教授和张彤博士对全书进行了审校。第 1～5 章由吴克河教授撰写，第 6～10 章由张彤博士撰写，第 11～13 章由刘吉臻教授撰写，第 14～18 章由李为副教授撰写。作者还要特别感谢关志涛、王竹晓、崔文超、陈飞、叶世超和陈龙等博士对本书的撰写所做出的贡献。

本书的撰写和出版得益于国家自然科学基金项目“广域防御体系下电力系统信息安全风险评估”(50877026)、国家 863 项目“基于 863 操作系统研究成果的全军装备信息保障一体化支撑平台及应用”(20004AA1Z2450)、北京市共建项目“北京电网信息安全防御体系及关键技术研究”、国家电网公司重点项目“移动终端安全接入系统”，以及华北电网有限公司重点项目“电网信息安全防御体系设计”等项目的研究成果。感谢有关专家对本书的推荐和鼓励，并向书中所有参考文献的作者表示感谢。

感谢华夏英才基金对本书的出版提供的支持！

限于作者水平，书中欠妥和纰漏之处在所难免，恳请读者和同行不吝赐教，批评指正。

作　者

2011 年 7 月

目　　录

关于本书
前言

第一篇　电力信息安全理论

第 1 章　引论 …… 3
1.1　信息安全的内涵 …… 4
1.1.1　信息的概念 …… 4
1.1.2　信息安全的概念 …… 5
1.2　信息安全的发展历程 …… 8
1.2.1　信息安全发展的三个阶段 …… 8
1.2.2　信息安全相关概念的发展 …… 9
1.2.3　信息安全主流技术的发展 …… 12
1.3　信息安全面临的问题及发展趋势 …… 19
1.3.1　信息安全面临的威胁 …… 19
1.3.2　信息安全的发展趋势 …… 21
1.4　小结 …… 22
第 2 章　电力信息安全概述 …… 24
2.1　电网企业信息系统应用现状及安全保护需求 …… 24
2.1.1　电网企业信息系统应用现状 …… 24
2.1.2　电网企业信息系统安全保护需求 …… 27
2.2　发电企业信息系统应用现状及安全需求 …… 29
2.2.1　发电企业信息系统应用现状 …… 29
2.2.2　发电企业信息系统的安全需求 …… 32
2.3　电力信息化的发展和对信息安全的要求 …… 34
2.4　电力信息系统安全需求分析 …… 35
2.4.1　电力工业的特点及信息系统的特殊性 …… 35
2.4.2　电力信息安全的特性分析 …… 36
2.5　小结 …… 37
第 3 章　网络业务安全 …… 38
3.1　数据安全保护 …… 38
3.1.1　信息安全 …… 39

3.1.2 信息保障现状 …… 40
3.1.3 信息标准 …… 41
3.2 网络系统的安全保护 …… 43
3.2.1 网络体系结构 …… 44
3.2.2 网络安全体系结构 …… 44
3.3 网络业务安全理论概述 …… 51
3.4 网络业务安全的概念 …… 53
3.5 基于网络业务安全的理论研究 …… 54
3.5.1 强制运行控制模型 …… 54
3.5.2 强制访问控制模型 …… 56
3.5.3 基于网络业务安全的网间安全访问模型 …… 57
3.5.4 强制硬件确认控制模型 …… 59
3.5.5 角色访问控制模型 …… 61
3.5.6 通用访问控制模型 …… 63
3.6 小结 …… 64
第 4 章 主动可控防御理论 …… 65
4.1 防护与防御 …… 65
4.1.1 防护理论 …… 66
4.1.2 安全防御理论 …… 68
4.2 主动可控防御概述 …… 70
4.2.1 主动可控防御的概念 …… 70
4.2.2 主动可控防御系统的技术路线 …… 71
4.3 主动可控防御的理论模型 …… 71
4.3.1 模型的描述 …… 72
4.3.2 模型的约束 …… 74
4.3.3 主动可控防御状态的定义 …… 77
4.4 小结 …… 77
第 5 章 电力信息系统安全防御体系 …… 78
5.1 电力信息系统安全防御体系概述 …… 78
5.1.1 电力信息安全建设的总体目标 …… 78
5.1.2 电力信息安全防御体系设计的原则 …… 79
5.1.3 电力信息安全防御体系设计的内容 …… 80
5.1.4 电力信息安全防御体系的总体框架 …… 81
5.1.5 电力信息安全防御体系的技术路线 …… 83
5.2 电网企业信息系统安全防御体系 …… 84
5.2.1 电网企业业务安全等级的划分 …… 84
5.2.2 电网企业数据安全等级的划分 …… 86

5.2.3 电网企业信息系统安全防御体系设计 …… 87
5.3 发电企业信息系统安全防御体系 …… 89
5.3.1 发电企业网络业务等级划分 …… 89
5.3.2 发电企业信息系统安全防御体系设计 …… 89
5.4 小结 …… 91
第 6 章 电力信息安全管控体系 …… 92
6.1 电力信息安全管控体系架构 …… 92
6.2 分级分域防护 …… 94
6.3 分层防护 …… 95
6.4 安全管控体系 …… 95
6.5 小结 …… 96

第二篇 电力信息安全关键技术

第 7 章 基于 MRC 的主机安全防御系统 …… 99
7.1 主机防御系统研究背景 …… 99
7.2 国内外主机防御系统研究现状 …… 100
7.2.1 国外主机防御系统研究现状 …… 100
7.2.2 国内主机防御系统研究现状 …… 101
7.3 电力主机安全防御系统 …… 101
7.4 电力主机安全防御系统的关键技术 …… 102
7.4.1 MRC 技术 …… 103
7.4.2 MHCC 技术 …… 107
7.5 电力主机安全防御的系统设计 …… 114
7.5.1 系统功能简介 …… 114
7.5.2 系统技术架构 …… 115
7.5.3 系统模块组成 …… 117
7.5.4 系统功能特性 …… 118
7.6 应用实例 …… 122
7.6.1 网络部署 …… 122
7.6.2 单机部署 …… 123
7.7 小结 …… 123
第 8 章 网络二极管技术 …… 124
8.1 产生背景 …… 124
8.2 发展历程 …… 125
8.3 设计思想 …… 126
8.4 具体实现 …… 127
8.5 实际应用 …… 134

8.6 小结 …… 135
第 9 章 移动终端安全接入平台 …… 136
9.1 移动终端的接入 …… 136
9.2 国内外研究现状 …… 138
9.2.1 安全接入技术研究现状 …… 138
9.2.2 安全接入应用情况 …… 140
9.3 电力企业安全接入的需求分析 …… 141
9.4 安全接入技术方案 …… 143
9.4.1 安全接入必须解决的问题 …… 143
9.4.2 安全接入的总体架构 …… 144
9.4.3 接入终端安全 …… 148
9.4.4 传输通道安全 …… 150
9.4.5 应用系统安全 …… 151
9.5 安全接入平台的特色 …… 153
9.5.1 技术特色 …… 153
9.5.2 专业特点 …… 157
9.5.3 应用特点 …… 160
9.6 部署模式 …… 161
9.6.1 内平台两级部署 …… 161
9.6.2 外平台一级部署 …… 162
9.7 典型应用 …… 163
9.8 小结 …… 166
第 10 章 安全文件保护系统 …… 167
10.1 电力企业数据安全需求分析 …… 167
10.2 安全文件保护系统介绍 …… 169
10.2.1 系统特性 …… 171
10.2.2 系统优势 …… 171
10.3 安全文件夹技术 …… 172
10.4 小结 …… 173
第 11 章 电力私有云及其安全 …… 174
11.1 云模型与云安全 …… 174
11.2 私有云的安全 …… 176
11.3 云计算在电力企业中的应用 …… 178
11.3.1 电力私有云 …… 178
11.3.2 在电力系统中的应用展望 …… 179
11.3.3 电力私有云的安全 …… 180
11.4 小结 …… 182

第 12 章　安全自治愈技术 …… 183
12.1　概述 …… 183
12.2　自治计算 …… 184
12.3　自适应、认知型防御关键技术 …… 187
12.3.1　可防御化 …… 187
12.3.2　自治动态响应 …… 188
12.3.3　不可预测性的使用 …… 190
12.3.4　高容错性 …… 191
12.3.5　生存性体系结构 …… 192
12.3.6　基于认知方法的可生存系统 …… 193
12.4　自治愈的电力安全接入平台 …… 193
12.5　小结 …… 195

第三篇　电力信息安全工程应用

第 13 章　电力信息系统安全保护实例 …… 199
13.1　电力信息系统安全整体设计 …… 200
13.2　电力二次系统安全防护方案 …… 202
13.2.1　电力二次系统的安全防护需求 …… 203
13.2.2　电力二次系统的安全风险分析 …… 204
13.2.3　电力二次系统的安全防护措施 …… 206
13.3　电力营销系统安全接入解决方案 …… 221
13.3.1　设计目标及原则 …… 222
13.3.2　营销系统现状分析 …… 223
13.3.3　安全风险分析 …… 224
13.3.4　营销系统安全接入总体架构 …… 225
13.3.5　营销系统安全接入应用 …… 228
13.3.6　安全接入对营销系统的益处 …… 234
13.4　电力企业数据中心的建设及安全保护 …… 235
13.4.1　电力企业信息系统的结构进化 …… 235
13.4.2　电力企业数据中心建设的新思路 …… 237
13.4.3　电力企业数据中心的安全防护 …… 238
13.5　小结 …… 240
第 14 章　电力信息内网搜索系统 …… 241
14.1　概述 …… 241
14.1.1　内网搜索的概念 …… 241
14.1.2　国内外内网搜索系统研究发展现状 …… 242
14.2　电力企业内网搜索现状及需求分析 …… 243

14.2.1 内网搜索现状 …… 243
14.2.2 需求分析 …… 244
14.3 电力内网搜索系统 …… 245
14.3.1 总体架构 …… 246
14.3.2 技术要点分析 …… 247
14.4 小结 …… 253
第 15 章 信息系统安全漏洞扫描 …… 254
15.1 概述 …… 254
15.1.1 常用的漏洞扫描工具 …… 254
15.1.2 国内外研究现状及发展趋势 …… 255
15.2 风险分析 …… 257
15.3 需求分析 …… 258
15.4 企业信息系统安全漏洞扫描解决方案 …… 259
15.5 小结 …… 261
第 16 章 电力应用安全建设方案 …… 262
16.1 安全开发 …… 262
16.1.1 安全开发标准 …… 262
16.1.2 电力系统安全开发现状 …… 266
16.1.3 电力系统安全开发建设方案 …… 267
16.1.4 电力系统安全开发实施阶段 …… 268
16.2 代码安全检测 …… 273
16.2.1 电力系统代码安全检测现状 …… 273
16.2.2 代码安全检测的必要性 …… 273
16.2.3 代码安全检测关键技术 …… 274
16.2.4 代码安全检测建设方案 …… 275
16.2.5 部署实施措施 …… 276
16.3 小结 …… 278
第 17 章 智能电网安全防护典型应用 …… 280
17.1 输变电线路状态在线监测系统 …… 280
17.1.1 系统概述 …… 280
17.1.2 风险分析 …… 282
17.1.3 防护目标 …… 283
17.1.4 防护方案 …… 283
17.2 用电信息采集系统 …… 291
17.2.1 系统概述 …… 291
17.2.2 风险分析 …… 293
17.2.3 防护目标 …… 293

17.2.4 防护方案 …… 297
17.3 电力光纤到户 …… 310
17.3.1 系统概述 …… 310
17.3.2 风险分析 …… 314
17.3.3 防护目标 …… 315
17.3.4 防护方案 …… 315
17.4 电动汽车充电管理系统 …… 321
17.4.1 系统概述 …… 321
17.4.2 风险分析 …… 324
17.4.3 防护目标 …… 325
17.4.4 防护方案 …… 326
17.5 95598客户服务网站 …… 332
17.5.1 系统概述 …… 332
17.5.2 风险分析 …… 335
17.5.3 防护目标 …… 336
17.5.4 防护方案 …… 336
17.6 小结 …… 345
第18章 电力信息安全等级保护建设方案与应用 …… 346
18.1 电力信息安全等级保护及其发展状况 …… 346
18.1.1 国外信息安全等级保护基本状况 …… 347
18.1.2 国内信息安全等级保护基本状况 …… 351
18.1.3 电网信息安全等级保护基本状况 …… 353
18.2 电力企业二级信息系统等级保护设计方案 …… 356
18.2.1 基本要求 …… 356
18.2.2 关键技术 …… 358
18.2.3 方案示例 …… 364
18.3 电力企业三级信息系统等级保护设计方案 …… 366
18.3.1 基本要求 …… 366
18.3.2 关键技术 …… 368
18.3.3 方案示例 …… 371
18.4 电力企业系统等级检测方案 …… 373
18.4.1 检测手段及工具 …… 373
18.4.2 检测流程 …… 374
18.4.3 方案示例（测试所需表格） …… 374
18.5 小结 …… 380
参考文献 …… 381

第一篇　电力信息安全理论