学校编码：10384　　分类号_____密级_____
学号：X2011230931　　UDC_____

厦门大学

工 程 硕 士 学 位 论 文

智能电网环境下信息主动安全监控系统的设计与实现

Design and Implementation of Active Safety Monitoring System in the Smart Grid

李 勇

指 导 教 师： 王 备 战 教 授
专 业 名 称： 软 件 工 程
论文提交日期： 2014 年 6 月
论文答辩日期： 2014 年 7 月
学位授予日期： 年 月

指 导 教 师：_____

答辩委员会主席：_____

2014 年 6 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（）课题（组）的研究成果，获得（）课题（组）经费或实验室的资助，在（）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于

年　月　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“ √ ”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘要

在智能电网环境下，维护信息系统的安全是一项重要功能。常见的安全监控目前主要从硬件和软件各自来进行，缺少集中管控。对于大规模的信息防护，依旧采取分散的管理方式，无法建立管控模型。各个级别的安全防护体系也独立运作配置，给审计和防控留下了较大的安全隐患。

基于此，提出《智能电网环境下信息系统主动安全监控系统的设计和实现》的思路和需求，力求达到既能实现对安全监控的实时监测，又能及时有效的对安全系统进行及时管理，实现对于信息系统的主动监控，动态实现对信息系统的安全监测及安全管理。

本系统以南方电网为研究对象，主要任务是设计了一套分布式的安全监控管理系统。主要工作包括三个方面：第一，分析了常见的攻击手段和防护方法；第二，设计了一套多级分布式安全管理系统。拥有多个安全管理功能，其中包括权限下发，规则下发等；第三，设计了一个基于 windows 的 IIS 和基于 Linux 的 Apache 的规则防护系统的模型。

论文首先从项目背景出发，介绍了系统开发的背景。然后分析了常见的攻击手段和防护策略，重点介绍了几种核心技术，最后给出了分布式框架和防护规则系统的设计与实现。

系统运行表明，系统在高负荷策略条件下可以很好地完成既定的分层管理任务。在实际的运行中分层分角色的安全监控很好地符合了企业的构架，为企业信息化过程中分布安全防护指明了道路，同时也带来了极大地便利。

关键词：分布式安全；模式识别；防护分析

Abstract

In the smart grid environment, maintaining the security of information systems is an important feature. Safety monitoring is currently mainly focusing on the hardware, lacking of centralized control.

Based on this proposed-i.e. " Design and Implementation of smart grid environment information system under active safety monitoring system ", the ideas and needs, we strive to construct not only security monitoring to achieve real-time monitoring , but also timely and effective security system management information systems .Such system should achieve the proactive monitoring , dynamic implementation of information systems security monitoring and security management.

The southern power grid system is studied for the main task is to design a distributed security monitoring and management system. The main work includes three aspects: first, the analysis of the common means of attack and protection methods; Second, the designing a multi-level distributed security management system, which has multiple security management features, including sending security under the authority, sending the rule under authority, etc.; Third, the designing of the model is a windows based (IIS) and Linux-based (Apache) rules of protection systems.

Dissertation starts from the project background and then describes the system development. It analyzes the common means of attack and defense strategy which is focusing on several core technologies. Finally, it gives the model design of distributed systems framework and protection rules.

Key words: Distributed Security； Protection Analysis； Firewall Pattern Recognition

目录

第一章绪论.....1

1.1. 项目研究背景及意义.....1

1.1.1. 项目研究背景.....1

1.1.1 项目开发意义.....1

1.2 国内外研究现状.....2

1.2.1 国内研究现状.....2

1.2.2 国外研究现状.....3

1.3 主要研究内容.....3

1.3.1 智能电网一般安全威胁形式.....4

1.3.2 可靠安全通信系统.....4

1.4 论文章节安排.....5

第二章关键技术介绍.....7

2.1 web 应用防火墙（WAF）.....7

2.2 安全动作响应系统.....7

2.3 本章小节.....8

第三章系统需求分析.....9

3.1 项目概述与项目规模.....9

3.2 功能概述.....9

3.2.1 功能性需求分析.....10

3.2.2 非功能性需求分析.....12

3.3 软硬件需求.....12

3.3.1 软件需求.....12

3.3.2 硬件需求.....12

3.4 性能要求.....13

3.5 其他要求.....13

3.5.1 安全性要求.....13

3.5.2 权限职责管理需求.....13
3.5.3 审计追踪需求.....14
3.5.4 界面需求.....14
3.6 本章小结.....14
第四章系统设计.....15
4.1 系统设计目标.....15
4.2 系统功能结构设计.....15
4.3 系统架构设计.....17
4.4 数据库设计.....20
4.4.1 概念结构设计.....20
4.4.2 逻辑结构设计.....21
4.5 主要功能模块设计.....28
4.5.1 系统登录鉴权.....28
4.5.2 安全规则管理.....29
4.5.3 安全规则下发.....30
4.5.4 安全事件查询分析.....31
4.5.5 信息系统接入.....32
4.5.6 信息系统安全规则个性化管理.....33
4.5.7 信息系统安全事件报告.....33
4.5.8 信息系统安全事件报警.....34
4.5.9 安全监控系统权限设定.....34
4.5.10 安全监控系统其他功能.....35
4.5.11 约束与假定.....35
4.6 系统配置方式设计.....35
4.7 本章小结.....37
第五章软件实现.....38
5.1 模块实现.....38
5.1.1 系统登录鉴权角色模块.....38
5.2 智能电网下的主动安全监控平台安全规则管理端.....41

5.2.1 登录注册功能.....41
5.2.2 帐号及权限分配管理功能.....42
5.2.3 安全子系统登记模块.....43
5.2.4 安全知识库规则库维护模块.....46
5.2.5 安全规则应用功能到信息子系统.....48
5.3 智能电网下安全监控及报警报告模块.....49
5.3.1 全局监控.....49
5.3.2 安全情况汇总分析.....49
5.3.3 安全子系统安全监控.....49
5.4 智能电网下的主动安全监控平台的其他模块.....49
5.4.1 系统安全代理定制模块.....49
5.4.2 安全代理前端的升级模块.....50
5.4.3 安全监控信息通告扩展模块.....50
5.5 智能电网下的主动安全监控平台安全前端代理.....51
5.5.1 驻留操作系统服务.....51
5.5.2 安全模块.....52
5.5.3 自动更新模块.....52
5.5.4 其他扩展模块.....52
5.6 本章小结.....53
第六章系统测试.....54
6.1 实验数据集.....54
6.2 测试方法及结果.....54
6.3 测试结果分析.....56
6.4 本章小结.....56
第七章总结与展望.....57
7.1 总结.....57
7.2 展望.....57
参考文献.....58

致谢..... 60

Contents

Chapter 1 Preface.....1

1.1. Introduction.....1

1.1.1. Project's background.....1

1.1.1 Project's significance.....1

1.2 Research status of domestic and abroad.....2

1.2.1 Research status of domestic.....2

1.2.2 Research status of abroad.....3

1.3 Main study contents.....3

1.3.1 Threatens of Power Grid.....4

1.3.2 Safe and reliable communication system.....4

1.4 Dissertation structure.....5

Chapter 2 Introduction to system key technologies.....7

2.1 Web Application Firewall.....7

2.2 Security response system.....7

2.3 Summary.....8

Chapter3 System requirements analysis.....9

3.1 Overview of the project and the project scale.....9

3.2 Functional overview.....9

3.2.1 Analysis of functional requirements.....10

3.2.2 Analysis of non functional requirements.....12

3.3 The hardware and software requirements.....12

3.3.1 Software requirements.....12

3.3.2 Hardware requrements.....12

3.4 Performance requirements.....13

3.5 Other requirements.....13

3.5.1 Security requirements.....13

3.5.2 Responsibility management requirements 13
3.5.3 Audit trail requirements 14
3.5.4 UI requirements 14
3.6 Summary 14
Chapter4 System design 15
4.1 The purpose of system 15
4.2 The system function structure design 15
4.3 The structure of system 17
4.4 Database design 20
4.4.1 Conceptual Structure Design 20
4.4.2 logical organization design 21
4.5 Design of main function models 28
4.5.1 System login authentication 28
4.5.2 Rule management module 29
4.5.3 Safety rules module 30
4.5.4 Query and analysis module 31
4.5.5 Information system access module 32
4.5.6 Personalized management module 33
4.5.7 Information system security incident report module 33
4.5.8 Information system security event alarm module 34
4.5.9 Safety monitoring system permissions setting module 35
4.5.10 Safety monitoring system of other functional modules 35
4.5.11 Constraints and assumptions 35
4.6 The design of system configuration 35
4.7 Summary 37
Chapter5 System implementation 38
5.1 Modules Implementation 38
5.1.1 System login authentication and role model 38
5.2 Security rules management terminal 41

5.2.1 Login function module....41
5.2.2 Account assignment management module....42
5.2.3 Security subsystem registration module....43
5.2.4 Safety knowledge rule base maintenance module....46
5.2.5 Safety rules applied to information subsystem module....48
5.3 Alarm and report module safety monitoring in Smart Grid....49
5.3.1 Global monitoring....49
5.3.2 Safety analysis summary....49
5.3.3 Security subsystem safety monitoring....49
5.4 The other module active safety monitoring platform....49
5.4.1 System security agent customization module....49
5.4.2 The front end of the upgrade module security agent....50
5.4.3 Safety monitoring information notification extension module....50
5.5 Secure front proxy active safety monitoring platform....51
5.5.1 Resident operating system services....51
5.5.2 Security module....52
5.5.3 Automatic update module....52
5.5.4 Other extension modules....52
5.6 Summary....53
Chapter 6 System Testing....54
6.1 Experiment set....54
6.2 Measurement and results....54
6.3 Results analysis....56
6.4 Summary....56
Chapter7 Conclusions and Outlook....57
7.1 Conclusions....57
7.2 Outlook....57
References....58

Acknowledgements 60

第一章绪论

1.1. 项目研究背景及意义

1.1.1. 项目研究背景

在智能电网环境下，维护信息系统的安全是一项重要功能。安全监控目前主要从硬件和软件来进行，缺少集中管控。集中管控下的分布响应预防的需求不言而喻，如何集中管控监测信息系统，并主动进行信息系统的安全管控，这是当前安全管理的新课题。

基于此，提出《智能电网环境下信息系统主动安全监控系统的设计与实现》的思路和需求，力求达到既能实现对安全监控的实时监测，又能及时有效的对安全系统进行及时管理，实现对于信息系统的主动监控，动态实现对信息系统的安全监测及安全管理。

智能电网业务涉及电网调度自动化、继电保护和安全装置，发电厂控制自动化、变电站自动化、配网自动化，电力负荷控制、电力市场交易、电力用户信息采集、智能用电等多个领域。通过对广东电网进行深入分析，对不同的业务场景设计了三种业务模式：分散管理模式、集中管理模式和混合管理模式。在变电站的信息管理、工控系统等方面，分散管理模式充分适用；同时在电网营销业务、日常办公等业务场景下，集中管理模式可以充分发挥其集中管理、统一调度指挥等优势；而在电网实时数据管理安全方面，本文则采用混合管理模式，充分融合了集中管理和分散管理模式的优势，折中了各自的不足，保证了业务场景和模式的合理匹配。

1.1.1 项目开发意义

在智能电网环境下，建立一个能对信息系统进行监控的主动安全监测平台。实现对信息系统中的各安全设备的管理及安全保护，对智能电网环境下的信息的请求进行过滤，实现对各受控设备的主动安全监控管理。

智能电网的兴起所形成的多网融合将使得广东电网公司信息网络的边界延伸至用电用户侧，这一变化意味着信息安全的“广域时代”来临。同时，智能电网要求必须明确各利益主体的保密程度和权限，并保护其资料和经济利益。因此，

必须研究复杂智能电网系统下的防御手段、措施。建立一套覆盖物理层到应用层的纵深信息安全防御体系作为对智能电网的基础支撑。我们对常用防护体系进行了分析如表 1-1 所示。

表 1-1 防护体系分析

	服务	服务	服务	服务	服务	服务
安全技术维	鉴别服务	访问控制	数据完整	数据保密	抗抵赖性	
	√	√		√		
安全保障维	制度保障	人事保障	培训保障	审计保障	管理平台保障	
	√	√				
安全策略维	预警	保护	检测	响应	恢复	反击
	√	√	√	√		√

1.2 国内外研究现状

1.2.1 国内研究现状

在我国，电力监管委员会颁布了“电力二次系统安全防护规定”、信息系统安全等级保护基本要求等重要文件，将电力企业内部业务系统，原则上划分为生产控制大区和管理信息大区。在生产控制大区与管理信息大区之间必须设置专用横向单向安全隔离装置，在生产控制大区与广域网的纵向交接处，应当设置专用纵向加密认证装置或者加密认证网关[1]。在不同级别的网络中同样应遵循相关规定，并且结合智能电网下的新特点，设计更严格的安全防护措施，保证电力安全。

信息系统及其运行环境的复杂，对现有信息安全防护体系提出了严峻挑战[2]：

1、 更多类型的不同利益主体。

2、 更大规模、更复杂的信息系统。

3、 更加开放的系统环境。

4、 更加复杂多样的系统接口、业务流及信息流。

5、 复杂多样的通信网络，GPRS/CDMA、3G/4G、WIFI、传感网络。

现有信息安全防御策略需要进一步优化以适应智能电网应用效能。

智能电网将引入海量的数据，对数据的安全管理带来新挑战。包括数据的识别、验证、准确性、数据更新、时间标记和数据库一致性等问题。保密性问题等成为必需考虑的问题。随着大量智能表计、智能家电的接入，网络边界进一步向用户侧延伸，用户侧的安全风险将越来越突出。智能电网带来新的挑战大量智能终端的广泛应用，成为新的攻击目标众多新的信息技术的应用，伴随的是更加多样化和智能化的攻击手段。

1.2.2 国外研究现状

近年来，黑客攻击工厂企业网络的事件逐年增加。2009 年，美国联邦能源管理局(FERC)正式批准了 CIP-002 至 CIP-009 关键基础设施保护 8 个强制性标准[3][4]CIP 标准由北美电力保障组织(NERC)负责制定。

美国国家标准技术研究院(NIST)于 2010 年 2 月颁布了“NISTIR7628 院智能电网网络安全策略和要求”标准[5]。该标准已提交美国联邦能源管理局审核，经过一段时间实践后，将会成为美国国家强制标准。

1.3 主要研究内容

在定义网络攻击前，我们梳理了常见的对于电网信息管理网络的攻击。并从物联网、应用层、无线网络三个方面详细分析了其可能出现的攻击手段。定义了攻击手段后，方便制定多层次策略和安全知识库的内容。

本文还负责设计了通信层的安全协议。原有的单机引擎为自主设计得安全协议，随着发展，出现了计算能力不够、扩展性差、无法证明安全或证明计算安全等特点，于是提出迁移到 OpenSSL 的 SSL 协议上，并对 SSL 的加密和摘要算法选择给出了详细的选择理由。

在本文需求分析和设计中，我们提出了分层分角色管理安全的理念。即我们将管理员的角色转变为安全规则库的管理者，操作员负责分发不同的管理规则到不同的设备上。安全规则库是各个包拦截或特征拦截的规则主要仓储，这作为资源分配给管理员配置。在各级的操作中，通过良好的通信架构，降低了每一级产生的计算负荷和分发负荷。这部分内容将在下一章进行阐述。