

信息安全技术丛书

空中交通管理信息安全评估

马 兰 吴志军 著



科学出版社

信息安全技术丛书

空中交通管理信息安全评估

马 兰 吴志军 著

科学出版社

北 京

内 容 简 介

空中交通管理(简称空管)系统采用航空通信与导航、卫星网络、数据链和计算机网络等技术,支持基于大数据的民航协同决策,保障航空运输的安全高效运行。

本书将安全系统工程理论应用到空管系统的信息安全管理中,结合动态系统控制思想,提出了空管系统信息安全评估方法。主要内容包括:①建立空管系统动态的信息安全评估模型,提出以静态、动态和状态评估为基础的评估理论,设计基于安全基线政策的评价指标体系;②研究基于灰色理论的空管系统综合多目标决策的信息安全评估方法,提出基于改进的后向传播和基于径向基神经网络的空管系统信息安全评估技术;③研究基于Diameter的空管系统的统一身份认证,提出基于安全访问路径的空管系统业务数据安全访问方法。

本书是一本针对空管系统信息安全评估的研究著作,可以作为民航网络安全研究领域科研人员和网络设计工程人员的参考书,对民航信息安全评估管理的技术人员有一定的参考价值。

图书在版编目(CIP)数据

空中交通管理信息安全评估/马兰,吴志军著. —北京:科学出版社,2015.6
(信息安全技术丛书)

ISBN 978-7-03-044773-9

I. ①空… II. ①马… ②吴… III. ①空中交通管制-信息安全-评估
IV. ①V355.1 ②G203

中国版本图书馆 CIP 数据核字(2015)第 123198 号

责任编辑:陈 静 纪四穗/责任校对:郭瑞芝

责任印制:张 倩/封面设计:迷底书装

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>

三河市骏立印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2015 年 6 月第 一 版 开本:720×1 000 1/16

2015 年 6 月第一次印刷 印张:14 1/4

字数:280 000

定价:72.00 元

(如有印装质量问题,我社负责调换)

前 言

空中交通管理(Air Traffic Management, ATM)(简称空管)是航空安全保障体系中保障民用航空交通运输安全运行的一个复杂的综合智能信息系统,是支持民航协同决策(Collaborative Decision Making, CDM)的重要基础设施。ATM 主要涉及空间(航空导航和通信卫星)、空中(航空飞行器)和地面(航空机场和公司)三个环境中的航空通信(communication)、导航(navigation)、监视(surveillance)和自动化系统(automatic system)设施,以及利用卫星系统、数据链、计算机网络和自动化技术提供航空通信、导航、监视、气象和航行情报、空中交通管制(Air Traffic Control, ATC)综合信息服务,实现安全、高效和环保的航空交通运输。

空中交通管理系统具有大型、复杂和开放的特点,面临严重的安全威胁,迫切需要建立和完善长效机制的空中交通管理信息安全保障和评估技术体系。

1. 背景和意义

信息化是建设强国战略的重要内容。金融、电信、证券、保险、电力、交通(民航、铁路和海运)、税收和海关 8 个系统,以及电信网络、广电网络和互联网络 3 个基础网络是我国信息安全网络的重中之重。

1) 背景

目前,空管系统进入一个崭新的发展阶段,以美国联邦航空管理局(Federal Aviation Administration, FAA)倡导的下一代航空交通运输系统(Next Generation Air Transportation System, NextGen)和欧洲航空安全组织(European Organization for the Safety of Air Navigation, EuroControl)提出的单一欧洲天空空中交通管理研究(Single European Sky ATM Research, SESAR)计划核心是以网络为使能(Network-enabled)的信息综合集成(Information-based ATM integration)的大规模网络系统。它采用空天地一体化网络、卫星通信链路和地空数据链实现全球航空交通运输信息的无缝链接,达到实现全球航班跟踪和监视的目的。

随着全球信息化的快速发展,网络与信息安全的问题日益突出。“棱镜门”事件将网络信息安全问题推到了一个全新的认识高度。2014 年 2 月 27 日,中央网络安全和信息化领导小组成立。该领导小组将着眼国家安全和长远发展,统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题,研究制定网络安全和信息化发展战略、宏观规划和重大政策,推动国家网络安全

和信息化法治建设,不断增强安全保障能力。中国共产党中央委员会总书记、中华人民共和国主席、中国共产党中央军事委员会主席、中央网络安全和信息化领导小组组长习近平在中央网络安全和信息化领导小组第一次会议提出的“没有网络安全就没有国家安全,没有信息化就没有现代化”、“建设网络强国的战略部署要与‘两个一百年’奋斗目标同步推进”等重要论断,深刻阐释了党中央关于加强网络安全和信息化工作的指导思想和方针路线。

目前,中国信息化水平与国际先进水平还有较大差距。尤其是民航的网络和信息安全形势不容乐观,全行业的网络和信息安全意识还比较淡薄,重要网络和信息系统还存在安全隐患,影响较大的网络与信息安全事故时有发生。因此,中国民用航空局(简称中国民航局)将2007年定为“民航信息安全工作推进年”。

鉴于上述背景情况,如何对民航航空信息系统安全保障体系建设成功与否进行衡量;如何确保航空信息系统的信息安全保障体系能够持续有效;如何针对航空信息系统的信息安全保障长效机制的有效性进行测算。这就迫切需要针对民航如此重要的行业和业务系统尽快研究建立科学的、可度量的和可操作的信息安全保障评价指标体系,对其信息安全保障的整体状态进行科学、客观的评价与描述,从而确定所建设的信息安全保障体系处于什么水平,是否达到了预期的目标,持续保障的时间等。

2) 意义

对空管系统的安全性进行评价是安全防御中的一项重要技术。目前,针对民航航空信息系统的安全威胁日趋严重,由航空信息系统存在的安全隐患造成的航空港关闭和机场大面积航班延误和取消的安全事件时有发生。因此,探寻科学、合理、实用的航空信息系统安全评价方法成为业界研究热点。

建立健全的空管信息系统的安全保障评价指标体系是实施民航信息安全战略的重要保证,借助信息安全保障评价指标体系对我国的航空信息系统和核心业务系统进行统一分析和综合比较,将有助于对我国航空信息安全防御态势做出量化的结论,为中国民航局提供决策支持,对我国航空信息安全建设的规划、信息安全建设的投入,乃至信息安全管理政策的制定、信息安全技术的研究与发展都具有重要意义。因此,建立健全空管信息安全保障评价指标体系是一项具有战略意义的研究。

2. 目标

中国民航总局在“十一五”科技计划中重点支持信息安全技术应用研发课题,建设民航信息技术科研基地,组织开发两个技术平台:

- (1) 民航网络与信息安全信息通报技术平台,用于信息通报和发布预警信息;
- (2) 民航网络与信息安全管理技术平台,用于分析、判断和应急协调。

空中交通管理信息化建设已进入全面推进和快速发展的重要时期。空中交通管理信息系统规模庞大、涉及应用多、用户广、业务依赖程度高,对信息安全保障体系提出了更高的要求。因此,建立空中交通管理信息安全保障体系,对空中交通管理信息系统实施有效的安全保障是下一步信息化建设的重点。

空中交通管理信息安全是一个系统性概念,它包括空中交通管理设备安全、自动化管理系统安全、各种航空数据安全、网络通信安全、人员管理安全、环境安全几个方面。安全策略、防护、检测和恢复响应组成了一个完整的动态的安全循环,在安全策略的指导下保证空中交通管理信息系统的安全。因此,本书的目标主要聚焦在以下几个方面。

(1)空中交通管理信息安全保障策略。安全保障策略是空中交通管理信息安全系统的核心。大规模信息系统的安全必须依赖统一的安全策略管理、动态的维护和管理各类安全服务。安全策略根据各类实体的安全需求,划分信任域,制定各类安全服务的策略。安全策略不仅制定了实体元素的安全等级,而且规定了各类安全服务互动的机制。每个信任域或实体元素根据安全策略分别实现身份验证、访问控制、安全通信、安全分析、安全恢复和响应的机制选择。

(2)空中交通管理系统动态安全模型。基于闭环控制的动态网络安全理论模型在 1995 年开始逐渐形成并得到了迅速发展,学术界先后提出了保护-检测-响应(Protection-Detection-Response, PDR)和安全策略-保护-检测-响应(Policy-Protection-Detection-Response, P2DR)。空中交通管理系统动态安全模型是在整体的安全策略的控制和指导下,在综合运用防护工具如防火墙、操作系统身份认证、加密等的同时,利用检测工具如漏洞评估、入侵检测等了解和评估系统的安全状态,通过适当的反应将系统调整到最安全、风险最低的状态。另外,空中交通管理系统的安全防护措施应能全方位地针对各种不同的威胁和系统脆弱性,这样才能确保网络信息的可靠性、可用性、保密性、完整性和不可抵赖性。

(3)空中交通管理信息安全评估。信息安全评估是空中交通管理信息安全保障体系建设和管理中的一个关键环节。通过开展信息安全评估工作,可以发现空中交通管理信息安全存在的主要问题和矛盾,找到解决诸多关键问题的办法。空中交通管理信息安全评估可以采用多种方法,例如,数学规划方法、软计算方法(如神经网络算法等)、静态的分析方法、动态的分析方法、基于模型的分析方法等。系统化的评估方法就是从战略、管理、工程和技术 4 个方面对空中交通管理系统的信息安全进行全面的评估。

(4)空中交通管理系统信息安全保障体系结构。空中交通管理系统信息安全保障的特点是系统的实时性、安全性和交互性非常强,并且系统必须具有很好的容差性。而采用公共密钥基础设施(Public Key Infrastructure, PKI)则可以解决大规模密钥分布的问题,适用于在地理和空间位置上分布广泛的空中交通管理系统的

信息安全支持。因此,本书提出一个基于 PKI 的可信任空中交通管理信息安全保障体系结构。

(5) 空中交通管理系统全网统一认证。为了保障空中交通管理系统重点数据库访问的安全性,必须能够有效地预先阻止分布式拒绝服务(Distributed Denial of Service, DDoS)攻击等多种恶意攻击,即使遭到攻击,也能够迅速进行自我修复,降低各种攻击导致的破坏和损失。同时空中交通管理信息网络是电报网、语音传送网、互联网和卫星通信网的综合应用,实现民航全网的统一认证具有非常重要的研究价值。

3. 内容安排

全书共 8 章,包括的内容如下。

第 1 章为绪论。该章主要介绍空中交通管理系统信息安全保障的背景和意义;分析国内外信息安全和空中交通管理系统信息安全保障方面的研究现状和发展动态;并描述信息安全标准和风险评估模型及方法等。

第 2 章为空中交通管理信息安全保障体系结构。该章主要研究空中交通管理系统的实际物理模型,其组成结构及各层的构成和功能;根据空中交通管理系统的组成结构研究基于 PKI 的可信任的空中交通管理系统信息安全保障体系结构。

第 3 章为空中交通管理信息安全保障综合评价模型。该章研究动态的基于状态观测的空中交通管理系统信息安全保障模型;并根据其面临的安全威胁进行仿真。

第 4 章为空中交通管理系统信息安全评价指标设计。该章主要介绍空中交通管理系统信息安全评价指标的设计原则、指标范畴、指标规范,并给出指标举例。

第 5 章为基于灰色系统理论的空中交通管理信息安全评估。该章主要介绍现有信息安全的评价方法,提出面向空中交通管理系统信息安全的多层次灰色综合评价算法,并给出计算举例。

第 6 章为基于神经网络的空中交通管理信息安全评估。该章主要针对空中交通管理系统中复杂的因素及其之间的关系,研究采用反向传播(Back Propagation, BP)和径向基函数(Radial Basis Function, RBF)模型神经网络进行空中交通管理系统的信息安全评估,解决空中交通管理系统中关系模糊的问题和指标量化问题。

第 7 章为基于安全访问路径(Secure Access Path, SAP)的空中交通管理业务数据安全访问。该章主要研究基于安全节点(Security Node, SN)的空中交通管理信息数据安全访问路径;研究基于 Diameter 的空中交通管理系统的统一认证方法;并针对分布式拒绝服务攻击进行仿真与结果分析。

第 8 章为空中交通管理系统信息安全在线评估系统。该章主要介绍评估系统的结构框架和功能组成,给出系统功能模块的设计与实现,进行空中交通管理系

统信息安全评估的仿真实验,并对实验结果进行分析。

4. 本书特色

国际上航空业发达的国家,将空中交通管理信息安全作为国家重点信息化行业信息安全的一部分进行整体考虑。这些国家从“信息战”的思考角度出发,将空中交通管理系统信息安全问题作为一个重要信息基础设施的安全来考虑。

在信息战中,敌对双方的攻击目标不仅包括对方的军、政信息基础设施,以破坏和控制其军事指挥和控制系统,而且还包括关系国家经济发展的基础设施,如公用通信网、电力、交通(水陆空)、供水、银行等民用设施,以破坏和控制敌国的经济命脉,扰乱其社会秩序,达到“不战而屈人之兵”的目的。尤为引人注意的是,信息战的攻击将不分是平时时期还是战争时期,无论出于经济目的还是军事目的,不分是战略的还是战术的。因此,空中交通管理系统的信息安全作为中国军用航空和民用航空的安全保障的关键问题,其重要性和地位可见一斑。

在世界多极化趋势下,通过科技革命来增强综合国力是“大势所趋”。继美国在世界上第一个推出了《信息系统保护国家计划》,其他发达国家纷纷效仿,紧锣密鼓地相继起草各自的21世纪信息安全保护计划。

目前信息安全的评估方法,多采用静态评估和单一算法的思路。有关网络信息系统的安全评价虽然存在着多种多样的具体实践方式,但在世界上还没有形成系统化和形式化的评价理论和方法。评价模型基本是基于灰色理论(Gray Theory)或者模糊(Fuzzy)数学,而评价方法基本上用层次分析(Alytic Hierarchy Process, AHP)法或模糊层次分析(Fuzzy-AHP)法,将定性因素与定量参数结合建立安全评价体系,并运用隶属函数和隶属度确定待评对象的安全状况。

上述各种安全评估思想都是从信息系统安全的某一个方面出发,如技术、管理、过程、人员等,着重于评估网络系统安全某一方面的实践规范。在操作上主观随意性较强,其评估过程主要依靠测试者的技术水平和对网络系统的了解程度,缺乏统一的、系统化的安全评估框架,很多评估准则和指标没有与被评价对象的实际运行情况和信息安全保障的效果结合起来。在目前的评估方法中,基础指标(技术、管理、工程和战略)是相互独立的;技术、管理、工程和战略措施是并行的;评价指标之间相互独立,导致评价精度下降,评价准确性偏差。

本书将系统安全工程(System Security Engineering, SSE)理论应用到空中交通管理系统的信息安全保障和评估中,结合动态系统控制(Dynamic System Control, DSC)的思想,从中国信息安全保障的国家战略、管理策略、工程规范和技术措施方面出发,提出以“安全基线政策”(Security Baseline Policy)为核心的信息安全评价指标体系和空中交通管理系统信息安全保障的方法。其主要的创新点如下。

(1) 提出了动态的空中交通管理系统信息安全评估模型。建立了以静态、动态和状态评估为基础的空中交通管理系统信息安全评估理论体系；提出了基于安全基线政策的信息安全保障评价指标体系；为空中交通管理系统信息安全等级评定奠定了理论基础。

(2) 研究基于灰色理论的空管系统信息安全评估方法。采用灰色理论，通过系统分析，对空管系统在某一时间段所处的状态，针对预定的目标，提出一种半定性半定量的评价与描述方法，可以在更高的层次上，对空管系统的综合保障效果与整体安全水平形成客观的评价。

(3) 提出了基于神经网络模型的空中交通管理系统信息安全评估方法。采用综合多目标决策的灰色关联分析理论，提出了基于改进 BP 神经网络和基于 RBF 神经网络的空中交通管理系统信息安全评估方法，解决了空中交通管理系统中关系因素繁多且各种因素之间关系模糊的量化问题。

(4) 提出了基于 SAP 的空中交通管理系统业务数据安全访问方法。针对空中交通管理系统业务数据库的安全访问进行保护，防御和阻止各种恶意的入侵攻击。该方法在安全接入节点 (Security Access Node, SAN) 采用 Diameter 实现了空中交通管理安全系统的统一身份认证，为空中交通管理系统重点数据库的访问提供了信息安全保障。

5. 阅读建议

建议在阅读本书时先从信息安全评估和等级保护的概念和原理了解，逐步掌握安全评估的思路和流程；然后，熟悉空中交通管理系统的工作方式和系统组成，掌握空中交通管理系统信息安全评估的具体要素和指标体系，了解信息安全评估和等级保护的基本方法；最后，通过数据采集、指标定义、指标体系建立及评估算法和流程确定，进行空中交通管理系统的信息安全评估的实践。

本书是中国民航大学空中交通管理学院和电子信息工程学院航空电信网及信息安全研究实验室的老师与研究生多年研究开发的成果。本书内容是在师生的博士和硕士学位论文，以及共同发表的学术论文、撰写的技术报告和申请的发明专利的基础上整理而成的。全书约 30 万字。其中，马兰作为主编，负责全书的内容安排和结构设计，并编写了第 1~4 章和第 7 章的内容，约 20 万字；吴志军负责编写了第 5、6 和第 8 章的内容，约 10 万字。另外，参与本书研究工作的人员包括雷缙讲师、岳猛讲师，以及潘雯、彭越、刘颖、高伟、史荣、金宗辉、陶夏激、黄俊、张文涛、马俊杰、杨丽君、郎吉海和武肖峰等研究生；特别是 2013 级研究生王彩云及 2014 级研究生沈丹丹、沙永鹏、尹盼盼等在本书的整理、编辑和校正等方面做了大量艰苦的工作，在此对他们表示衷心的感谢！在本书的研究中，得到了中国民航局空中交通管理局技术中心教授级高级工程师齐鸣主任和国家信息

中心吕欣处长的指正，在此表示衷心的感谢！

本书的出版得到了国家自然科学基金面上项目(61170328 和 U1333116)、天津市应用基础与前沿技术研究计划(自然科学基金重点项目, 12JCZDJC20900)、2013 年民航科技引导资金项目(MHRD20130217)、中央高校基本科研业务费(3122013P007、3122013D007 和 3122013D003)和中国民航大学科研建设平台项目的资助，在此表示衷心的感谢！

本书是一本针对空中交通管理信息安全评估的研究著作，对研究信息系统和网络安全评估管理的技术人员具有一定的借鉴意义和参考价值。本书可作为网络安全研究领域科研人员和网络设计工程人员的参考书。全书内容由浅入深，涵盖了国家重要信息系统安全管理和设计人员需要掌握的知识，也为读者更深入地掌握信息安全评估技术，从事信息系统安全保护研究提供了参考。

由于作者水平有限，书中难免存在不足和纰漏之处，恳请广大读者批评指正。

作 者

2015 年 1 月

缩 略 词 表

缩略词	外文全称	中文全称
ABS	Abolish Message	取消重复与非重复性电报
ACARS	Aircraft Communication Addressing and Reporting System	飞机寻址和报告系统
ACP	Acceptance Message	管制协调接受报
ADDP	Air Data Distribution Processing	数据处理
ADS	Automatic Dependent Surveillance	自动相关监视
ADS-B	Automatic Dependent Surveillance Broadcast	广播式自动相关监视
AFTN	Aeronautical Fixed Telecommunication Network	航空固定通信网络
AGDP	Air-Ground Data Processing	空-地数据处理
AHP	Analytic Hierarchy Process	层次分析法
AIC	Aeronautical Information Circular	航行资料通报
AIP	Aeronautical Information Publish	航行资料汇编
AIRMET	Air Meteorological Information	低空气象情报
AIX	Advanced Interactive executive	高级交互执行程序
ALN	Alternate Message	备降报
ALR	Alerting Message	告警报
ANN	Artificial Neural Network	人工神经网络
AOC	Aeronautical Operational Control	航空运营管理
APC	Aeronautical Passenger Communications	航空旅客通信
API	Application Programming Interface	应用程序编程接口
APPDRR	Assessment-Policy-Protection-Detection-Reaction-Restoration	评估-策略-防护-检测-响应-恢复
ARR	Arrival Message	落地报
ART	Adaptive Resonance Theory	自适应谐振
ASPB	Airspace Strategic Planning Board	空域规划
ATC	Air Traffic Control	空中交通管制
ATCC	Air Traffic Control Centre	空中交通管制中心
ATM	Air Traffic Management	空中交通管理
ATN	Aeronautical Telecommunication Network	航空电信网
ATS	Air Traffic Service	空中交通服务

续表

缩略词	外文全称	中文全称
BGP	Border Gateway Protocol	边界网关协议
BP	Back Propagation	反向传播
BPA	Basic Probability Assignment	基本概率赋值
BPAF	Basic Probability Assignment Function	基本概率赋值函数
B/S	Browser/Server	浏览器/服务器
BSI	British Standard Institute	英国标准协会
CA	Certificate Authority	认证中心
CAAC	Civil Aviation Administration of China	中国民用航空局
CAN/ATM	Controller Area Network/Air Traffic Management	控制器局域网/空中交通管理
CC	Command Criteria For IT Security Evaluation	通用安全评估准则
CDP	Communication Data Processing	通信数据处理
CDM	Collaborative Decision Making	协同决策
CDN	Co-ordination Message	管制协调报
CDU	Control Display Unite	控制显示单元
CHG	Modification Message	修订领航计划报
CMC	Central Maintenance Computer	中央维护计算机
CMU	Communication Management Unit	通信管理单元
CNL	Flight Plan Cancellation Message	取消领航计划报
CNS/ATM	Communication Navigation Surveillance/Air Traffic Management	通信、导航、监视/空中交通管理
COR	Correction Message	修订飞行预报
COTS	Commercial-Off-The-Shelf	商用安全技术
CPDLC	Controller-Pilot Data Link Communication	管制员-飞行员数据链通信
CPL	Current Flight Plan Message	现行飞行变更报
CRL	Certificate Revocation List	证书撤销列表
C/S	Client/Server	客户机/服务器
CTCPEC	The Canadian Trusted Computer Product Evaluation Criteria	加拿大可信计算机产品评价准则
DBM	Data-Base Management	数据库管理
DDN	Digital Data Network	数字数据网
DDoS	Distributed Denial of Service	分布式拒绝服务
DEP	Departure Message	起飞报
DLA	Delay Message	延误报
DME	Distance Measuring Equipment	测距仪
DoS	Denial of Service	拒绝服务

续表

缩略词	外文全称	中文全称
DPR/DAF	Disaster Planning and Response/Data Audit Framework	灾难计划和响应/数据审计框架
DSP	Data Service Provider	数据供应商
DVOR	Doppler VHF Omni Range	多普勒甚高频全向信标
EST	Estimate Message	预计飞越报
FAA	Federal Aviation Administration	美国联邦航空管理局
FANS	Future Air Navigation System	新航行系统
F-AHP	Fuzzy Analytic Hierarchy Process	模糊层次分析
FDP	Flight Data Processing	飞行数据处理
FPCP	Flight Plan Conflict Probe	飞行计划冲突探测
FPL	Filed Flight Plan Message	领航计划报
FTN	Flight Telephone Automatic system	自动转报系统
GII	Global Information Infrastructure	全球信息基础设施
GM	Grey Model	灰色模型
GPS	Global Position System	全球定位系统
GRA	Grey Relation Analysis	多级关联度分析
GRIB	GRIdded Binary	气象处理
HF	High Frequency	高频
HMI	Human Machine Interface	人机界面
IATF	Information Assurance Technical Framework	《信息保障技术框架》
IBM	International Business Machines Corporation	国际商业机器公司
ICAO	International Civil Aviation Organization	国际民用航空组织
ICMM	Integrated Capability Maturity Model	综合能力成熟度模型
IDS	Intrusion Detection System	入侵检测系统
IETF	The Internet Engineering Task Force	国际互联工程任务组
ILS	Instrument Landing System	仪表着陆系统
ISMS	Information Security Management System	信息安全管理体系
ISO	International Organization for Standardization	国际标准化组织
ISS	Information System Security	信息系统安全
ISSE	Information Systems Security Engineering	信息系统安全工程
ITS	Information Technology Security	信息技术安全
ITSEC	Information Technology Security Evaluation Criteria	欧洲的安全评价标准
LAM	Logical Acknowledgement Message	逻辑确认报
LAN	Local Area Network	局域网

续表

缩略词	外文全称	中文全称
METAR	Meteorological Terminal Aviation Routine Weather Report	航空例行天气报告
MHS	Message Handling System	报文处理系统
MLS	Microwave Landing System	微波着陆系统
MMI	Man-Machine Interface	人机界面
MTP/SNMAP	Multi-radar Track Processing/Security Network Monitoring and Processing	多雷达航迹处理/安全网及监控处理
NAI	Network Access Identify	网络访问识别
NAS	National Airspace System	国家空域系统
NAV	Navigation	导航系统
NDB	Non-Directional Beacon	无方向性信标
NextGen	Next Generation Air Transportation System	下一代航空交通运输系统
NII	National Information Infrastructure	国家信息基础设施
NIST	National Institute of Standards and Technology	美国国家标准与技术研究院
NOC	Network Operations Center	网络运行中心
NOTAM	Notice To Airmen	航行通告
NSA	National Security Agency	美国国家安全局
OASYS	Open Architecture System	开放结构系统
OSI	Open System Interface	开放系统接口
PADIMEE	Policy-Assessment-Design-Implementation-Management-Emergency Response-Education	策略-评估-设计-执行-管理-应急响应-教育
PCIPB	President's Critical Infrastructure Protection Board	总统关键基础设施保护委员会
PDC	Pre-Departure Clearance	预起飞许可
PDCA	Plan-Do-Check-Action	策划-实施-检查-措施
PDR	Protection-Detection-Response	保护-检测-响应
P2DR	Policy-Protection-Detection-Response	安全策略-保护-检测-响应
PES	Personal Earth Station	个人地球站
PHP	Hypertext Preprocessor	超文本预处理器
PIB	Pre-flight Information Bulletins	飞行前公告
PKI	Public Key Infrastructure	公共密钥基础设施
PLN	Plan Message	飞行预报
PSR	Primary Surveillance Radar	一次监视雷达
QNH	Query Normal Height	修正海压
RA	Registration Authentication	注册中心
RBF	Radial Basis Function	径向基函数

续表

缩略词	外文全称	中文全称
RBP	Radar Bypass Processing	雷达旁路处理
RCF	Radio Communication Message	无线电通信失效报
RDP	Radar Data Processing	雷达数据处理
RECP	Record Processing	记录备份处理
RF	Radio Frequency	射频
RFP	Radar Data Front Processing	雷达数据前处理
ROFOR	Route Forecast	航路预报
RQP	Request Flight Plan Message	请求飞行计划报
RQS	Request Supplementary Flight Plan Message	请求领航计划补充信息报
RTN	Return Message	返航报
SAN	Security Access Node	安全接入节点
SAP	Security Access Path	安全访问路径
SARPs	International Standards and Recommended Practices	国际标准和推荐措施
SAT	Satellite communication	卫星通信
SCPC/DAMA	Single Channel Per Carrier/ Demand Assigned Multiple Access	单路单载波/按需分配
SCTP	Stream Control Transmission Protocol	流控制传输协议
SEIPT	Security Equipment Integrated Product Team	安全设备综合产品小组
SESAR	Single Europe Sky Air Traffic Management Research	单一欧洲天空空中交通管理研究
SIGMET	significant meteorological information	重要气象情报
SN	Security Node	安全节点
SOC	Security Operations Center	安全运行中心
SOM	Self-Organization Map	自组织映射
SoN	Source Node	源节点
SOS	Security Overlay Service	安全覆盖服务
SPECI	Special Weather Report	特殊天气报告
SPL	Supplementary Flight Plan Message	领航计划补充报
SPN	Security Passing Node	安全通过节点
SQL	Structured Query Language	结构化查询语言
SRN	Security Routing Node	安全路由节点
SSE	System Security Engineering	系统安全工程
SSE-CMM	Systems Security Engineering Capability Maturity Model	系统安全工程能力成熟度模型
SSR	Secondary Surveillance Radar	二次监视雷达
ST	Security Target	安全目标

续表

缩略词	外文全称	中文全称
TAF	Terminal Aerodrome Forecasts	终端机场天气预报
TCP/IP	Transmission Control Protocol/Internet Protocol	传输控制协议/因特网互联协议
TCSEC	Trusted Computer System Evaluation Criteria	可信计算机系统评价标准
TDB	Target Data-Base	目标数据库
TDI	Trusted Database Interpretation	可信数据库解释
TDM/TDMA	Time Division Multiplexing/Time Division Multiple Access	时分复用/时分多址
TES	Telephone Earth Station	电话地球站
TN	Target Node	目标节点
TND	Trusted Network Description	可信网络解释
TOE	Target of Evaluation	评价目标
URL	Uniform Resource Locator	统一资源定位符
VCCS	Voice Communication Control Systems	语音通信控制系统
VHF	Very High Frequency	甚高频
VOR	Very High Frequency Omnidirectional Radio Range	甚高频全向信标
VPN	Virtual Private Network	虚拟专用网
VSAT	Very Small Aperture Terminal	甚小口径终端
WAN	Wide Area Network	广域网络
WPDRRC	Warning-Protection-Detection-Response-Recovery-Counterattack	预警-保护-检测-响应-恢复-反击
XSS	Cross Site Scripting	跨站点脚本

目 录

前言

缩略词表

第 1 章 绪论	1
1.1 背景和意义	1
1.2 研究现状	3
1.2.1 空管信息安全国际研究现状	4
1.2.2 空管信息安全国内研究现状	11
1.2.3 空管信息安全保障策略	14
1.3 信息安全与风险评价	16
1.3.1 信息安全概述	16
1.3.2 风险评价概述	17
1.3.3 信息安全与安全风险评价的关系	17
1.4 安全管理模型介绍	17
1.4.1 P2DR 模型	18
1.4.2 PADIMEE™ 模型	18
1.5 国内外安全标准介绍	20
1.5.1 可信计算机系统评价标准	20
1.5.2 信息技术安全评价准则	20
1.5.3 加拿大可信计算机产品评价准则	21
1.5.4 信息技术安全性评价通用准则	21
1.5.5 信息安全管理体系标准	21
1.5.6 系统安全工程能力成熟度模型	23
1.6 风险评价方法	25
1.6.1 定量评价方法	26
1.6.2 定性评价方法	26
1.6.3 定性与定量相结合的综合评价方法	26
1.7 本章小结	27
第 2 章 空中交通管理信息安全保障体系结构	28
2.1 空中交通管理系统三层模型	29