第41卷 第6A期
2014年6月

计 算 机 科 学
Computer Science

Vol. 41 No. 6A
June 2014

空管自动化系统信息安全评估研究

赖 欣 黄邦菊
(民航飞行学院空中交通管理学院 广汉 618307)

摘 要 根据国家相关信息安全保护与评估规范和基本要求,结合空管自动化系统特点,分析目前影响空管自动化系统信息安全的主要因素。在此基础上提出了信息安全评估体系。然后基于专家评价方法与证据融合理论提出了可量化评估方法,该方法既保持了专家评价方法的简洁可实施性,又采用证据融合算法消除了专家意见中存在的主观性。最后通过算例对该方法与模糊评估法进行了比较。

关键词 空管自动化系统,信息安全评估,D-S证据融合理论
中图法分类号 TP393 **文献标识码** A

Research of Information Security Assessment for ATC Automation Systems

LAI Xin HUANG Bang-ju
(Department of Air Traffic Control, Civil Aviation Flight University of China, Guanghan 618307, China)

Abstract According to relevant national information security standards and basic evaluation requirements, combined with the characteristics of ATC automation system, the main factors affecting the ATC automation system information security are analyzed and the information security evaluation system is proposed. Then based on expert evaluation methods and evidence fusion theory quantifiable assessment method is proposed which is easy to be implemented, and the subjectivity of expert opinions will be removed because of evidence fusion algorithm. Finally, according to an example the proposed evaluation method and fuzzy evaluation method were compared.

Keywords Air traffic control automation system, Information security evaluation, D-S evidence fusion theory

1 引言

空中交通管理系统是国家实施空域管制、保障飞行安全、实现航空高效运输的有序运行的综合系统。它涵盖了通信、导航、监视、管制等多个系统,其中空管自动化系统是空中交通管制员管理空中交通的主要手段之一,它通过对多雷达信号进行处理,将雷达信号与飞行计划动态相关联,使得管制人员面对雷达显示器就可以了解空中交通的实时动态。空管自动化系统由雷达信息处理、航班情报信息处理、飞行计划处理等子系统组成,其系统本质是由计算机网络结构与软件系统构成的信息管理系统[1]。如何保证空管自动化系统安全平稳运行是关系到飞行安全与空域使用效率的核心问题。目前我国空管系统正在大力开展SMS(Security Management System)建设,其中就着重提出了必须采取有效的方法对空管自动化系统的信息安全进行有效评估[2]。基于此,国内多位学者从业务信息流、安全评价指标等角度对空管自动化系统安全进行了研究[3,4]。本文首先着重对现行空管自动化系统结构进行了分析,根据《信息安全风险评估规范》(GB/T 20984-2007)以及《信息系统安全等级保护基本要求》(GB/T 22239-2008)等技术规范要求,总结目前影响空管自动化系统安全的风险因素。在此基础上构建空管自动化系统安全评价体系,并结合专家评价与证据融合理论提出了评估方法。

2 空管自动化系统结构及信息安全分析

2.1 系统结构

各国、各地区使用的空管自动化系统虽存在差异,但就其结构而言,空管自动化系统是一个复杂的分布式计算机网络系统。局域网将各设备与管制席位连接起来,系统基于对多雷达信号处理和融合,同时处理民航固定电信网电报和与多雷达信号进行自动相关。自动化系统主要包括了物理设备、网络拓扑、业务流、业务集成等多个模块。其中物理设备与网络拓扑为系统的硬件层面,具体包括了前端数据采集设备,如雷达、网络基础链路、交换路由设备、网络管理设备等;业务流管理与业务集成为系统的软件层面,及在硬件设备的基础上,按照业务流的来源与使用进行管理,具体包括了数据请求、数据采集、身份验证、事务处理、各个数据库调用等。硬件与软件之间还应包括中间件处理环节,主要负责数据格式转换、网络协议转换等。

2.2 信息安全分析

风险评估应贯穿于信息系统生命周期的各阶段中,本文侧重于对已建成且运行的空管自动化系统进行风险评估,该评估属于运行维护阶段风险评估。基于上述对自动化系统结

本文受空管信息系统信息安全保障研究(J2010-32),航空公司运行监察评估方法研究(Q2012-70)资助。
赖 欣(1977—),女,博士,副教授,主要研究方向为交通运输信息系统、信息安全,E-mail:lxrzg@163.com;黄邦菊(1966—),女,硕士,副教授,主要研究方向为交通运输、航空运行。

构及业务流的分析，结合《信息安全风险评估规范》(GB/T 20984-2007)以及《信息系统安全等级保护基本要求》(GB/T 22239-2008)对信息系统风险评估的相关规定和建议流程，本文从网络安全、系统安全、管理安全3方面对空管自动化系统信息安全问题予以考察。

2.2.1 网络环境安全

自动化信息系统的物理布局、网络拓扑构成了信息系统的整体结构，网络结构中包括了多类外接网络数据信源，如外接雷达网络数据、外接报文网络数据、外接气象网络数据等。网络拓扑结构中主要包括了各类交换机、路由器、专用数据处理服务器等硬件设备。目前空管自动化系统的网络环境的安全主要体现在网络架构、边界防护、访问控制、网络病毒防护、入侵检测系统、审计系统等方面，具体表现如下[5,6]：

结构和规划不合理，具体表现为：

1)关键数据链路无备份或备份方式不合理，如存在原始数据引入网络采用直通网络方式的情况。

2)网络层次架构与区域划分不清晰，如大部分自动化系统都没有明显汇聚层，从而导致无法实现对流量的控制和对访问权限的约束。

网络访问控制存在缺陷，具体可表现为：

1)自动化系统网络区域边界控制粒度不足，如自动化系统中，过于信赖内部之间的访问将有可能导致越权访问，甚至会被恶意入侵者利用内部之间的信任关系。

2)对服务器访问控制力度不足，大多数自动化系统内部网络中仅在服务器区使用了防火墙保护，但多数服务器系统的安全访问控制策略都较松散或者缺乏。虽然自动化系统面临的访问都是来源于内部网络，但基于对内部用户的高信任将有可能导致被恶意利用。

3)关键设备没有做IP和MAC绑定。

网络设备防护不足，具体表现为：

1)网络设备维护权限管理不严，如没有对允许登录的域帐户进行限制，没有对各帐户分配不同权限。

2)对运维终端IP限制不严，如没有对管理员登录IP进行限制。

2.2.2 系统平台安全

空管自动化系统平台属于软件层面，其功能在于提供各项业务工作的人机界面和入口，主要包括的子系统有雷达数据处理子系统、报文处理子系统、飞行计划处理子系统、航迹融合子系统、显示子系统等，各类子系统涉及到大量不同数据格式的转换、快速计算(融合)、图形化显示以及辅助判决、空域使用规划等功能。此外系统中还包含管理体系规范与信息系统活动相关的各类活动，比如用户登录、权限管理等。目前我国一线管制单位所采用的自动化系统各有不同，但普遍存在的系统平台问题主要表现在以下几方面[5,7]。

软件及服务漏洞，具体可表现为：

1)第三方软件安全漏洞，系统平台主机可能安装的三方软件存在严重的远程缓冲区溢出漏洞，这将导致主机完全被控制，这类安全问题可通过部署漏洞扫描软件识别。

2)开放无用服务及端口过多，基于部分系统软件的设计原因，各类自动化系统中普遍开放了很多与业务无关的服务，比如WEB服务、SMTP服务、SNMP服务等。

不安全的共享与公用，具体可表现为：

1)多业务共用主机导致互相影响，多个子系统运行在同一个主机上，容易互相影响。其中某个系统的安全性或不稳定将直接影响到其他系统。

2)系统默认共享枚举，部分主机运行远程通过空连接等方式能获取目标主机的共享目录等信息。大多数机器均存在默认共享的目录。

不安全的系统密码，具体可表现为：

1)系统存在弱密码。部分主机及数据库存在弱密码，若其被利用将给系统带来严重影响。

2)未启用密码策略和账户锁定策略。考察的多数服务器由于默认配置存在隐患可能导致安全问题。

2.2.3 管理安全

空管自动化系统安全问题必须考虑到人为因素对它的影响。人为因素具有一定的随机性与突发性，对目前存在的信息系统不安全事件进行分析，80%的安全事故来源于人为的因素，但从管理角度可以规避或减少人为因素对自动化系统安全的破坏。管理安全应作为自动化系统安全体系中重要的组成部分予以考察。综合目前空管一线单位自动化系统的管理和使用流程，可发现管理中普遍存在的信息安全问题主要表现在以下几方面[5,8]。

部分管理制度与规章缺失，具体可表现为：

1)部分管理制度内容的缺失，比如缺失针对外部人员安全管理、安全检查规范、安全事件报告等方面的制度。

2)部分管理规程没有具体内容，对实际工作的操作没有指导性。

3)缺乏完善的信息安全策略体系，目前大部分空管自动化系统信息安全管理制度体系不够完整，结构松散；针对非IT部门的信息安全责任不明确。

4)缺乏持续而完善的安全教育和培训计划，目前一线管制单位每年有组织信息安全培训，包括对管理层和对员工的信息安全意识和基础安全技术培训，但缺乏对信息技术和信息安全专业人员的再教育、新技术培训或认证培训。

3 DS理论基础

DS证据理论具有处理不确定性信息的能力，其在工程实践中表现出来的实用性能已得到了广泛的应用[9-11]。Shafer在其专著《证据的数学理论》中建立了证据理论[12]。Shafer定义了基本概率分配函数，即mass函数：设Θ是识别框，$\forall P \subseteq \Theta$，称函数$m(P):2^{\Theta}\to[0,1]$为$\Theta$上的mass函数，函数满足如下条件：$m(\Phi)=0$且$\sum_{P\subseteq\Theta} m(X)=1$。

mass函数可理解为对已有证据的主观表示，即$m(P)$表示该证据支持问题P，由于证据不足不支持P的任何真子集的程度，$m(P)$只能表示基本概率分配函数，不是P的总信任度，必须将支持问题P的所有子集的基本概率分配函数相加，才能得到总信任度。基于此可定义信度函数(Belief Function)：设Θ是一个识别框，m是Θ上的一个mass函数，$\forall P\subseteq\Theta$，则有函数$B_{el}(P)=\sum_{B\subseteq X} m(B)$，$B_{el}:2^{\Theta}\to[0,1]$为信度函数，即$B_{el}(P)$表示对问题$P$的信任程度。

DS理论的优势在于可进行可信函数的合成。合成过程使用到了Dempster规则，即假设在识别框Θ上有两个证据X与Y是对问题P的完全独立的基本可信函数，分别为m_1和m_2。进行证据合成的规则为：

$$m_{12}(P)=\frac{\sum_{X\cap Y=P} m_1(X)m_2(Y)}{1-K},P\neq\Phi$$

其中，$K=\sum_{X\cap Y=\emptyset} m_1(X)m_2(Y)$。

记 $m_{12}=m_1\oplus m_2$，m_{12} 反映了 m_1 和 m_2 对应的两个证据 X、Y 对命题 P 的联合支持程度。而 K 反映了在两个证据不完全一致时产生冲突的程度。K 值较小表明冲突较小，K 值较大表示冲突较大，$K=1$ 即表示两个证据源存在完全冲突。

4 安全评估模型建立

4.1 评价体系定义

根据上文对空管自动系统信息安全分析以及文献[13]中对信息安全评价体系设计的建议首先定义评价体系。因素集 $A=\{A_1,A_2,\cdots,A_m\}$ 是影响评价对象的各种因素组成的集合，其中 $A_i(i=1,2,\cdots,m)$ 分别代表各影响因素。以上述影响“网络环境安全”的风险概率为例，可定义 $A=$“网络环境安全”，其因素集为 $A=\{A_1=$结构和规划，$A_2=$网络访问控制，$A_3=$网络设备防护$\}$，其中各个因素又受到其它子因素的影响，如结构和规划与关键链路备份、关键设备单点备份、网络层次架构与区域划分等情况有关，由此可设为：

$A_1=\{$关键链路备份，关键设备单点备份，网络层次架构与区域划分$\}=\{A_{11},A_{12},A_{13}\}$；

同理有：

$A_2=\{$网络区域边界控制，服务器访问控制，IP 和 MAC 绑定$\}=\{A_{21},A_{22},A_{23}\}$；

$A_3=\{$网络设备维护权限，运维终端 IP 限制$\}=\{A_{31},A_{32}\}$

各个因素对评价对象的影响程度通常是不一样的，其重要性以各影响因素赋予相应的权数来表征，定义权重集为：$W=(\omega_1,\omega_2,\cdots,\omega_n)$，实际应用中要求满足非负性和归一性，即 $\sum_{i=1}^{r}\omega_i=1,\omega_1,\cdots,\omega_r\geqslant 0$。

4.2 基于 DS 理论的评价方法

完成的评价体系需建立合适的评语集，评语集的划分方式决定了度量结果的准确性，设定 $L_i=(L_1,L_2,\cdots,L_5)$ 为模型评语集，其中 $L_i=\{$高风险(L_1)，较高风险(L_2)，中等风险(L_3)，较低风险(L_4)，低风险$(L_5)\}$，若设定评估值为 $0\sim100$ 之间的自然数，以不同的取值区间代表不同的评语集因子。如设 $L(A)=(L(A_1),L(A_2),\cdots,L(A_i))$ 为模糊评语集给出的模糊评估值，$L(A_i)(i=1,2,\cdots,5)$ 为对应于评价因素 A_i 的评估值，那么取值范围在 $0\leqslant L(A_i)\leqslant100$，$L_5<60$ 表示低风险，$60\leqslant L_4<70$ 表示较低风险，$70\leqslant L_3<80$ 表示中等风险，$80\leqslant L_2<90$ 表示较高风险，$90\leqslant L_1<100$ 表示高风险。

以“网络环境安全”为例由 $A=\{A_{11},A_{12},A_{13},A_{21},A_{22},A_{23},A_{31},A_{32}\}$ 构成评价因素，请专家按评价规则进行评分，设定评分值为 $\{x_1,x_2,x_3,\cdots,x_8\}$，处于风险等级 L_i 的指标是 $\{x_{i1},x_{i2},\cdots,x_{in}\}$，那么风险评价基本概率分配函数在等级 L_i 的概率为：$p_i=\frac{x_{i1}+x_{i2}+\cdots+x_{in}}{x_1+x_2+\cdots+x_8}$，表示某一专家对于风险等级 L_i 的评价概率，由此可以获得该专家的识别框架基本概率分配函数即 mass 函数为 $m(A)=p_i$。若多位专家独立地对“网络环境安全”命题进行评价形成多个证据，可采用 DS 合成规则进行风险评价融合。

由于对命题的理解和各个专家的专业水平可能造成所得的证据具有冲突，如果冲突严重将导致对命题判断的结论与实际情况偏差过大，因此需要判断专家的证据冲突是否在可以容许的范围内，即需要计算证据冲突大小，并定义当冲突值超过某个设定阈值时，则评价无效。如 $A^{(1)}$ 和 $A^{(2)}$ 证据冲突为：

$$\begin{aligned}K&=\sum_{X\cap Y=\emptyset} m_1(X)m_2(Y)\\&=1-\sum_{A^{(1)}\cap A^{(2)}=\emptyset} m_1(A^{(1)})m_2(A^{(2)})\end{aligned}$$

同一命题不同专家的评价将产生不同的概率分配函数，利用合成公式进行合成，即按照指标 $(((1,2),3),\cdots,n)$ 次序进行合成计算，将得到多个专家的融合评价结果，形成对命题 A 的评价结果 $m(A)=m_{(((1,2),3),\cdots,n)}(A)$，取得评价等级的不同的等级信任函数，即 $Bel(L_i)=m(L_i)$ 取得的最大值即为本次融合得到的推荐评价结果

5 案例分析

本节通过对某一线管制单位空管自动化系统的“网络环境安全”命题进行分析，验证 DS 评价方法的有效性。设定请 5 位专家就评价命题网络环境安全的 8 项因素进行打分评价，并假设各因素对命题影响的权重一致。整理后得到的评价数据如表 1 所列。

表 1 专家评分

评价因素	专家 1	专家 2	专家 3	专家 4	专家 5
A_{11}（关键链路备份）	54	55	57	64	58
A_{12}（关键设备单点备份）	73	74	71	73	78
A_{13}（网络层次架构区域划分）	69	71	70	62	78
A_{21}（网络区域边界控制）	71	77	79	75	78
A_{22}（服务器访问控制）	76	67	78	75	74
A_{23}（IP 和 MAC 绑定）	74	62	73	71	70
A_{31}（网络设备维护权限）	67	71	64	75	69
A_{32}（运维终端 IP 限制）	78	81	77	83	75

利用评价数据，按照风险评价基本概率分配函数计算得到专家的基本概率分配函数，如表 2 所列。利用证据冲突计算公式可得证据冲突值：

$$\begin{aligned}K&=1-(0.084\times0.089+0.227\times0.241+0.531\times0.217\\&\quad+0.151\times0.421)\\&=1-0.241=0.759\end{aligned}$$

表 2 基本概率分配函数

评价等级	$m(A^{(1)})$	$m(A^{(2)})$	$m(A^{(3)})$	$m(A^{(4)})$
L_1	0.084	0.089	0.090	0.000
L_2	0.227	0.241	0.236	0.223
L_3	0.531	0.217	0.386	0.638
L_4	0.151	0.421	0.288	0.139
L_5	0.000	0.000	0.000	0.000

若取冲突控制阈值为 0.8，那么第一次融合评判是有效的。利用合成法则，进一步计算各风险等级的信任程度，例如评级 $A^{(1)}$ 和评价 $A^{(2)}$ 融合时，对风险等级 L_1 有

$$m(L_1)=\frac{0.084\times0.089}{1-0.759}=0.031$$

依次按照 $(A^{(1)},A^{(2)}),((A^{(1)},A^{(2)}),A^{(3)}),((A^{(1)},A^{(2)}),A^{(3)}\cdots A^{(6)})$ 进行合成运算，得到如表 3 所列的各个风险等级的信任度。表 3 最后一行表示 5 位专家就影响“网络环境安全”的因素进行评价后合成的不同风险等级的信任数，其中风险等级 L_3 的信任度数值最大，表明专家评价结果最终为该空

（下转第 493 页）

码和加删应用等操作的安全性。

综上所述，通过分析现有各种多应用智能卡的架构，结合具体的应用要求，开发适合各行业发展要求的多应用智能卡产品，将成为今后智能卡技术研究和开发的重点方向。

参 考 文 献

[1] ISO/IEC 7816-4:2005(E). Identification cards--integrated circuit cards--Part 4:organization, security and commands for interchange [S]. Switzerland: ISO/IEC, 2005

[2] Chen Zhi-qun. Java card technology for smart cards: architecture and programmer's guide[M]. Boston: Addison-Wesley Longman Publishing Co., Inc., 2000

[3] Oracle and/or its affiliates. Java card 3 platform runtime environment specification, classic edition version 3.0.4[EB/OL]. http://www.oracle.com/technetwork/Java/Javacard/specs-jsp-1364 30.html, 2013-09

[4] Oracle and/or its affiliates. Java card 3 platform virtual machine specification, classic edition version 3.0.4[EB/OL]. http://www.oracle.com/technetwork/Java/Javacard/specs-jsp-136430.html, 2013-09

[5] GlobalPlatform Inc. GlobalPlatform card specification version 2.2[EB/OL]. http://www.win.tue.nl/pinpasjc/docs/GPCardSpec-v2.2.pdf, 2013-09

[6] MULTOS. An introduction to MULTOS [EB/OL]. http://www.multos.com/uploads/MULTOS-8-page-brochure.pdf, 2013-09

[7] Mayes K, Markantonakis K. Smart cards, tokens, security and applications[M]. New York: Springer-Verlag, 2008

[8] ZeitControl cardsystems GmbH. The compact, enhanced, and professional BasicCards version 4.50[EB/OL]. https://dspace.ist.utl.pt/bitstream/2295/49097/1/BasicCrd.pdf, 2013-09

[9] ZeitControl cardsystems GmbH. Overview[EB/OL]. http://www.basiccard.com/index.html?overview.htm, 2013-09

(上接第 476 页)

管自动化系统"网络环境安全"为"中等风险"程度。

表 3 融合结论

融合次数	m(L_1)	m(L_2)	m(L_3)	m(L_4)	m(L_5)
1	0.031	0.220	0.508	0.241	0
2	0.017	0.142	0.561	0.280	0
3	0	0.086	0.780	0.069	0
4	0	0.074	0.913	0.013	0

基于同样的专家评分结果，采用模糊评价算法得到 5 个评价等级 $L_i=(L_1, L_2, \cdots, L_5)$ 的概率分别为(0, 0.142, 0.731, 0.065, 0.062)。建立折线图比较两种评价结论，由图 1 可得如下结论：两种评价方法评估值变化趋势具有一致性，但 DS 证据理论评价值在等级 L_3 即中等风险处取得较大概率，可信度更高，说明 DS 证据方法更能确定风险发生可能等级。对等级 L_1、等级 L_5，DS 证据理论评估值均为 0，表明在定义的低风险和高风险两个等级处 DS 证据理论均排除了其存在的可能性，而模糊评估方法在 L_5 处仍存在评估取值，且 L_4 等级的评估值与 L_5 等级评估值趋于一致，无法对两者进行有效区分。可见 DS 证据理论结论具有更准确、更有效地取得有效评估等级的能力。

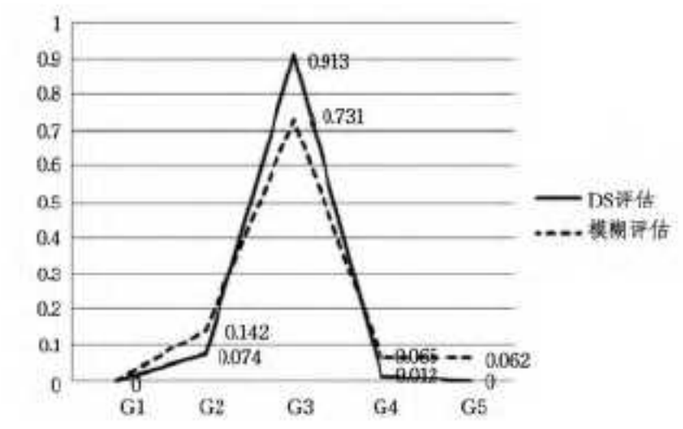

图 1 两种评价方法的风险等级比较

依此方法可以对空管自动化系统的"系统平台安全"、"人员管理安全"设计合理的评价因素。采用多位专家评价结果进行有效融合得到各方面的评价结果，为管制单位空管自动化系统信息安全程度评估提供客观的评判结论。

结束语 本文分析了影响空管自动化系统信息安全的各项因素，为实施客观准确的信息安全评估提出了评价体系。考虑切实的可实施性，评价过程仍采用了传统的专家评分方法，但结合 DS 证据融合理论，可使得该方法的评价结论更准确有效。本方法评价过程直观简易，在实际信息安全评估过程中具有可操作性。

参 考 文 献

[1] 中国民用航空局. 民用航空空中交通管理管理系统技术规范 MH/T 4018.1[S]. 2004

[2] 中国民用航空总局. 中国民航空管系统安全管理体系建设与实施指南[S]. IB-TM-2010-003, 2013

[3] 张文涛. 一种基于业务信息流的空管信息系统安全评价指标体系[J]. 计算机安全, 2009(4): 15-20

[4] 马兰, 吴志军, 潘雯. 民航 ATM 信息系统安全性评价指标体系的研究[J]. 微计算机信, 2010, 26(3): 39-43

[5] 中华人民共和国国家质量监督检验检疫总局. 信息安全风险评估规范 GB/T 20984-2007[S]. 2007

[6] 李大海. 民航空管网络与信息安全管理体系的构建研究[D]. 天津: 天津大学, 2009

[7] 潘雯. 民航 ATM 系统安全性评价指标体系的研究[D]. 天津: 中国民航大学电子信息工程学院, 2008

[8] 田春岐, 邹仕洪, 王文东, 等. 一种新的基于改进型 D-S 证据理论的 P2P 信任模型[J]. 电子与信息学报, 2008, 30(6): 1480-1484

[9] 韦勇, 连一峰, 冯登国. 基于信息融合的网络安全态势评估模型[J]. 计算机研究与发展, 2009, 46(3): 353-362

[10] 石波, 谢小权. 基于 D-S 证据理论的网络安全态势预测方法研究[J]. 计算机工程与设计, 2013, 34(3): 821-825

[11] Shafer G. A Mathematical Theory of Evidence [M]. Princeton: Princet on University Press, 1976

[12] 中华人民全国信息安全标准化技术委员. 信息系统安全等级保护定级指南 GB/T 22240-2008[S]. 2008