doi: 10.3969/j.issn.1672-6073.2023.01.024

地铁信号系统信息安全防御技术研究

张凤霞
（中铁上海设计院集团有限公司通号院，上海 200070）

摘 要： 随着无人驾驶技术、城轨云技术、互联互通等网络化新技术在城市轨道交通中的广泛应用，导致信号系统内外部接口大量增加，随之带来内部与外界对系统网络环境的恶意攻击。作为地铁的“大脑”，信号系统的信息安全尤为重要。通过分析信号系统的整体网络架构，针对信号系统信息网络的安全隐患及防护现状，提出了信号系统信息安全的主被动防御体系，将现有的主动防御和被动防御技术相结合，建立基于等级保护的被动防御模型，并从安全技术、安全策略、安全管理 3 个维度出发，提出主动防御模型，达到充分保障信号系统的信息网络安全的效果。

关键词： 地铁；信号系统；信息安全；被动防御模型；主动防御模型
中图分类号： U284 **文献标志码：** A **文章编号：** 1672-6073(2023)01-0168-06

Information Security Defense Technology of Subway Signal System

ZHANG Fengxia
(China Railway Shanghai Design Institute Group, Ltd., Shanghai 200070)

Abstract: With the extensive application of new networking technologies, such as self-driving technology, urban rail cloud technology, and interconnection in urban rail transit, the number of internal and external interfaces of the signal system has increased. This has resulted in malicious attacks on the system network environment from both the inside and outside. As the “brain” of the subway, the information security of the signal system is particularly important. By analyzing the overall network architecture of the signal system, the active and passive defense systems of the information network security of the signal system are proposed based on the hidden dangers and protection status. A passive defense model based on hierarchical protection was established by combining existing active and passive defense technologies. In addition, an active defense model was proposed from three dimensions: security technology, security policy, and security management, which can fully guarantee the information network security of the signal system.

Keywords: subway; signal system; information security; passive defense model; active defense model

1 研究背景

随着计算机、信息化技术与信号系统的深度融合，为了提高自动化水平，实现系统的互联互通，地铁信号系统产品越来越多地采用通用的协议、硬件和软件。在全自动驾驶技术与城轨云平台等高度市场化的环境下，信号系统与专用通信、综合监控、乘客信息、广播、时钟等多个外部系统互联互通，系统的网络环境也具有前所未有的开放性，新型病毒、木马和新的攻击手段等向信号系统扩散，使系统在面对网络威胁时

收稿日期：2022-11-03 修回日期：2022-03-18
作者简介：张凤霞，女，硕士，工程师，从事轨道交通设计工作，763670990@qq.com
引用格式：张凤霞. 地铁信号系统信息安全防御技术研究[J]. 都市快轨交通，2023，36(1)：168-173.
ZHANG Fengxia. Information security defense technology of subway signal system[J]. Urban rapid rail transit, 2023, 36(1): 168-173.

变得更加脆弱，信号系统的信息安全问题亟待解决。张峰[1]建立了基于策略树的主动防御模型，通过防护、检测、预警及响应，实现信息系统的动态互动，提出了入侵预警和抽样流量相结合的预测方法。林旺群等[2]针对静态博弈方法的不足，将动态博弈论和防御树相结合，建立了非合作动态博弈主动防御模型，以解决网络安全问题。陈安观[3]针对列车调度指挥系统的网络信息安全问题，提出“主动防御”体系的设计方案，通过统一封闭的远程管理系统，管理列车调度指挥系统设备，提高系统的整体可靠性和防御能力。倪国栋[4]通过比较分析主动防御技术和被动防御技术，将二者相结合，建立了基于可信计算技术的铁路综合视频监控系统的安全防御体系。陶伟[5]从信息安全标准等角度，分析了地铁信号系统的信息安全现状、可能存在的隐患，提出了信号系统的信息安全防护建议。包正堂[6]在列控系统信息安全防御中，引入攻防对策树的概念，结合信号系统故障导向安全的原则，对列控系统进行攻防建模，并给出选择方案。何坚安[7]构建了 3 种强大的蜜罐防御机制，以提高信息系统安全防御效果。李朝阳等[8]基于决策实验室分析法和攻击防御树模型，提出了一种综合能源系统信息安全的风险分析方法，计算攻防树模型中攻击序列风险程度与灵敏度指标。高锐等[9]从基于 IEEE 802.11 协议的 CBTC(列车自动控制系统)出发，探究了 CBTC 车地无线通信子系统面临的潜在信息安全风险，以及黑客可能采用的攻击形式．并分析了 CBTC 系统现有安全措施存在的问题。

上述专业人员在各个领域的信息网络安全方面做了不同的探索，提出了相应的防御措施，取得了一定成果，但对于地铁信号系统信息安全防御的研究有限。文献[6]和文献[9]仅对信号个别子系统面临的网络安全风险和可能存在的问题进行了分析，缺乏系统性；文献[5]对地铁信号系统的信息安全现状及防护给出了建议，但缺乏具体实施细节。

2　地铁信号系统信息网络安全状况

2.1　信号系统网络架构

信号系统的各个子系统都是通过数据通信子系统(data communication system，DCS)网络相互连接，信号系统网络包括有线和无线两部分。有线网络为中心与车站、车站与车站，以及车站内部的信号骨干网、列车自动监控(automatic traffic supervision，ATS)网和维护支持系统(maintenance support system，MSS)网，一般通过光缆连接；DCS 骨干网通过有线方式，将控制中心设备、数据库、地面联锁设备、接入交换机等相互连接，实现地面与车载、地面与地面之间的数据通信。无线网络一般是通过长期演进(long term evolution，LTE)或者无线局域网(wireless local area networks，WLAN)实现车地通信的。地铁信号系统网络结构如图 1 所示，其中所有网络都是双网设计且互为冗余。

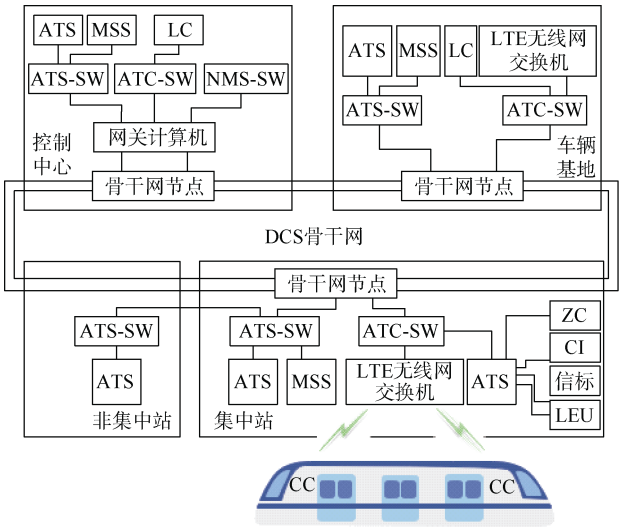

图 1　信号系统网络结构

Figure 1　Signal system network structure

2.2　信息安全隐患分析

目前轨道交通信号系统存在的信息安全隐患有两个方面。

2.2.1　网络安全

1) 信号系统与综合监控、站台门、通信系统等多个外部系统互联互通，且在该网络边界处缺乏访问控制功能，缺少为数据流提供明确的允许/拒绝访问的能力；

2) 不能对进出网络的信息内容进行过滤，不能实现对应用层协议命令级的控制；

3) 缺少防止地址欺骗的技术手段，容易遭受基本的网络攻击；

4) 缺乏对非授权设备私自连接到内部网络的行为进行检查、定位和阻断的能力，无法有效地检测到网络攻击行为，也无法对攻击源 IP、攻击类型等信息进行记录；

5) 无法在网络边界处对恶意代码进行检测。

2.2.2　主机安全

1) 缺乏有效的安全审计功能；

2) 采用传统网络防病毒软件，无法及时更新恶意代码库，无法识别新的恶意软件，起不到完整的主机防护作用；

3) 无法对重要程序的完整性进行检测，即使检测到完整性受到破坏，也不具有恢复能力；

4) 传统网络防病毒软件对业务应用的误杀现象突出，影响业务系统稳定运行等。

2.3 信息安全现状分析

根据《信息安全技术 信息系统安全等级保护基本要求》(GB/T 22239—2008)[10]、《信息系统安全保护等级保护实施指南》(GB/T 25058—2010)[11]、《中华人民共和国计算机信息系统安全保护条例》[12]等相关法规，地铁信号系统信息安全目前暂按三级标准执行，极大提高了信号系统信息安全的稳定性。但现有的等级保护系统设置多道屏障，采用层层保护的方法，缺乏完整性及主动性。

3 信息安全主被动防御体系建模

3.1 主被动防御体系的提出

现有的信息安全防御措施包含主动防御和被动防御。被动防御通过设置规则库、内容过滤、分析提取攻击特征集等来对已知的攻击进行防御，比较常用的有增加防火墙、关键数据加密、操作人员身份认证和入侵检测技术等。主动防御技术是指能够在网络攻击未发生或者还未造成巨大损失之前，积极主动地采取防御措施，提前部署，转移攻击或欺骗攻击，从而保护系统的安全。常用的主动防御技术有：静态和动态取证技术、蜜罐及蜜网技术、拟态理论与拟态防御技术、安全模型分析技术、漏洞扫描技术。

通过分析地铁信号系统信息安全防护的现状，结合国家对地铁信号系统信息安全等级保护的要求，建立地铁信号系统信息安全的主被动防御体系，如图 2 所示。

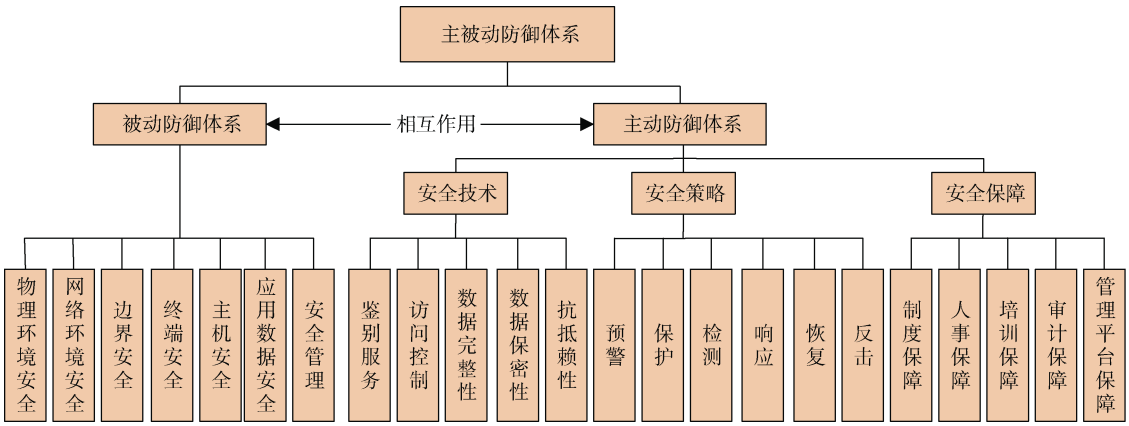

图 2 信号系统信息安全主被动防御体系

Figure 2 Signal system information security active and passive defense system

3.2 信息安全被动防御模型

被动防御基于等级保护，从物理、网络、主机、应用和数据等几个层次出发，建立信号系统信息安全被动防御模型。

1) 物理环境安全主要是指采取一些物理措施，从设备机房的选址、物理访问、防火、防盗、防潮等方面，以及设置信号系统集中监测系统、预警装置等，增强系统的安全性。

2) 网络环境安全主要包括设备、结构、信息流、数据流等的安全。信号系统网络环境安全防护主要包括网络协议、设备、无线网 3 个方面。设备安全防护主要从加强安全审计和身份认证入手，防止内、外人员进行违规操作和攻击破坏，加强对管理员操作的审计；网络协议的安全是信号系统信息安全的关键，可通过添加消息验证码和安全认证码进行保护。

3) 为保证信号系统边界网络安全，可以通过安装工业防火墙来达到隔离的目标，工业防火墙可通过数据包的源地址、目的地地址、传输层协议、应用层协议、通信协议、接口协议、端口信息等，制定访问规则，仅允许有用的业务数据通过，禁止其他非正常的业务请求，从而保障系统网络的安全性。同时，充分利用安全审计、入侵检测技术，对各个网络间的通信进行实时监测。一方面，在信号主干网、深灰网、浅灰网、交换机等处部署监测审计设备；另一方面，采取基于特征和行为的方法，对访问数据包的行为特征进行论证分析，及时发现可疑的目标并进行阻断，充

分保证信号系统的信息安全。

4) 信号系统的主机、终端类设备包括工作站和服务器，工作站大多采用 Windows 系统，容易以主机作为网络的突破口被黑客利用。因此，采用工控主机卫士，以软件形式部署在控制中心、车站、车辆段、停车场等关键场所的工作站和服务器，代替杀毒软件建立恶意代码入侵防护体系，从而达到系统整体网络安全的目标。

5) 应用和数据安全是对进出数据库的访问过程进行解析，还原访问中的细节，给出完整、详细的结果，最后将其通过可视化的方式呈现，同时对信号系统的安全防护进行漏洞扫描。

6) 为实现信号系统安全管理，运营单位应建立专门的信息安全管理机构，制定完善的安全管理制度，采用规划(p1an)、实施(do)、检查(check)、处置(act)模型，建立、运行、监视和改进安全管理体系。基于等级保护的信号系统信息安全被动防御模型如图 3 所示。

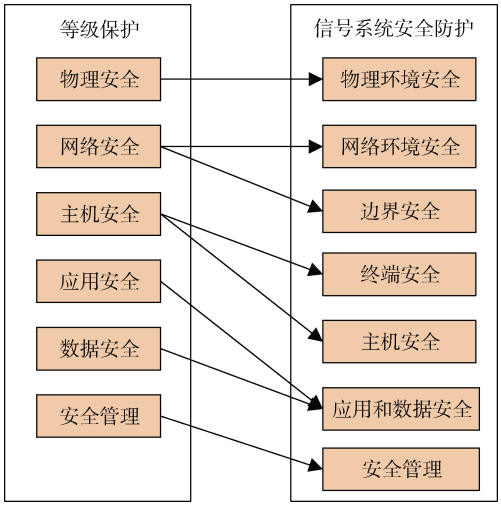

图 3　基于等级保护的信息安全被动防御模型

Figure 3　Information security passive defense model based on hierarchical protection

3.3　信息安全主动防御模型

主动防御从安全技术、安全策略、安全保障 3 个维度出发，致力于保障信号系统的信息安全。

1) 安全技术维由 5 类安全服务构成，将加密机制、访问控制机制、数据完整性机制、数字签名机制、鉴别交换机制、路由控制机制、业务流填充机制结合，互相交叉，为信号系统提供安全服务。

2) 安全策略维包含预警、保护、检测、响应、恢复、反击六大环节，通过检测和预警发现威胁，然后在保护和反击中不断提高系统的安全性，再利用响应和恢复完善安全策略。在 6 大环节的持续流动过程中，不断循环螺旋上升，逐渐实现信号系统的信息安全目标。

3) 安全保障维是从“以人为本”出发，通过合理的手段去管理和规范人的行为。从管理机构、制度、人员、培训等方面进行全面梳理，并设置相应的组织体系，完善管理方案，结合信息系统日常的定期运维管理，共同保障信号系统能够长时间持续地安全稳定运行。信号系统信息安全的主动防御模型如图 4 所示。

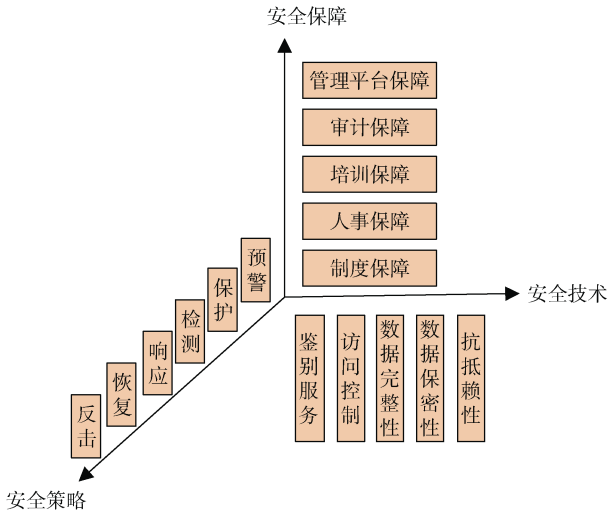

图 4　信号系统信息安全主动防御模型

Figure 4　Active defense model of signal system information security

4　信息安全主被动防御体系分析

信号系统信息安全的主被动防御体系具有主动性和立体型两大特点。基于等级保护的信号系统信息安全的被动防御与主动防御模型分工明确、协同合作、互相补充、共同作用，构成了立体的信号系统信息安全防护体系。被动防御与 3 个维度的主动防御模型关系如表 1 所示。

表 1　被动防御与主动防御的关系对照

Table 1　Mapping between passive defense and active defense

主动防御	物理安全	网络安全	主机安全	应用安全	数据安全	管理安全
安全技术维		√	√		√	
安全策略维		√	√	√	√	
安全保障维	√		√	√	√	√

4.1　网络安全域的划分

参考划分域的原则，是在满足信号系统业务和功能等特性的同时，还需保证系统整体运行的可用性，

信号系统的安全域划分如下：

1) Inside 区域：包括深灰网、浅灰网的设备，如应用服务器、数据库、网关服务器、终端等；

2) Outside 区域：主要包括 ISCS、CLOCK 等外部系统的接口机和外部 3 层交换机。

3) DMZ 区域：主要包括对外提供服务的通信前置机和 3 层交换机。

安全域划分如图 5 所示。

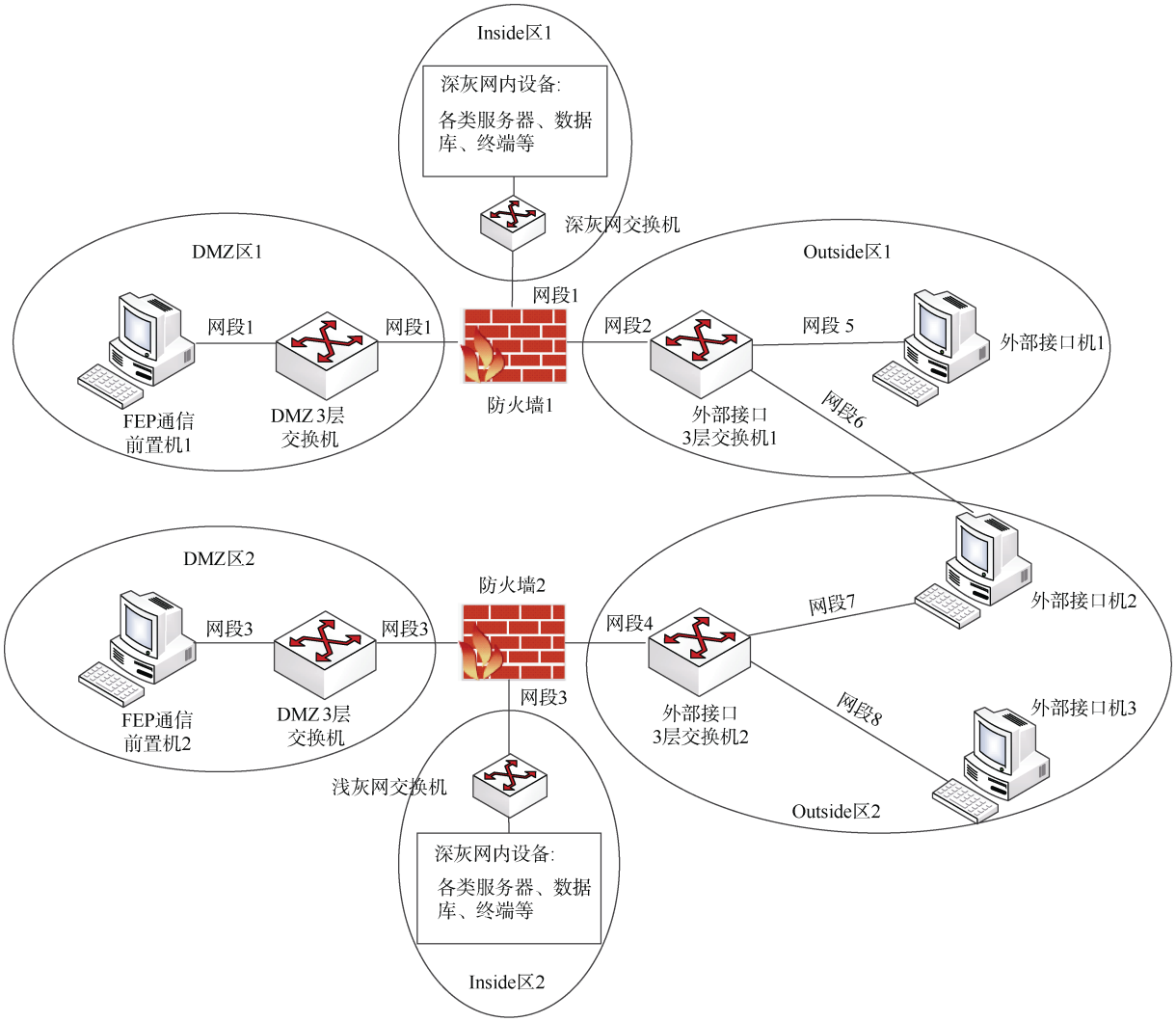

图 5 信号系统网络安全域的划分

Figure 5 Schematic of signal system network security domain division

4.2 网络安全防御系统

保护是整个安全防御系统的第一层屏障，主要利用工业防火墙和陷阱机实现。在信号信息网络 Inside 区域、Outside 区域、DMZ 区域的各个边界处，布置工业防火墙来实现隔离控制，监控数据包，防止非法活动。将陷阱机隐藏安装在防火墙后，利用模拟漏洞方式，诱导黑客入侵访问，引开黑客对各类服务器的攻击，以达到加强保护的目的。

检测和预警是整个安全防御系统的核心。检测由工控漏洞扫描平台、陷阱机和取证系统相互作用，如检测异常、发现漏洞。工控漏洞扫描平台模仿黑客的动作行为，定期对控制中心、车辆段、车站等重要场所的各个服务器、工作站及端口处的已知漏洞进行扫描，对存在漏洞或漏打补丁的对象及时采取补救措施；陷阱机是一种蜜罐系统，采用诱骗入侵的原理，在系统中记录网络中非法入侵的行为，起到了复测的效果；取证系统通过事后分析技术，发现新的病毒、新的攻击方式或者新的漏洞。除此之外，取证机也可以通过记录进出的流量监视网络活动，检测内部网络是否受到入侵威胁。

响应和恢复是攻击时和攻击后的关键。取证机记录所监视的所有目标进出网络的数据包，采用在线检测和离线分析相结合的方式，获取相应的证据；分析机通过读取取证机上的数据内容进行事后统计分析和数据还原，以此发现新的病毒、新的攻击手段和工具，得出详细报表，生成新的数据库，依次交替完成对新的病毒和攻击的检测。同时，在完成检测的基础上，以防御策略为指导，采用各种安全措施、防御技术优化系统，达到及时修补漏洞和升级系统的目标。信号系统信息安全防御系统的物理架构如图 6 所示。

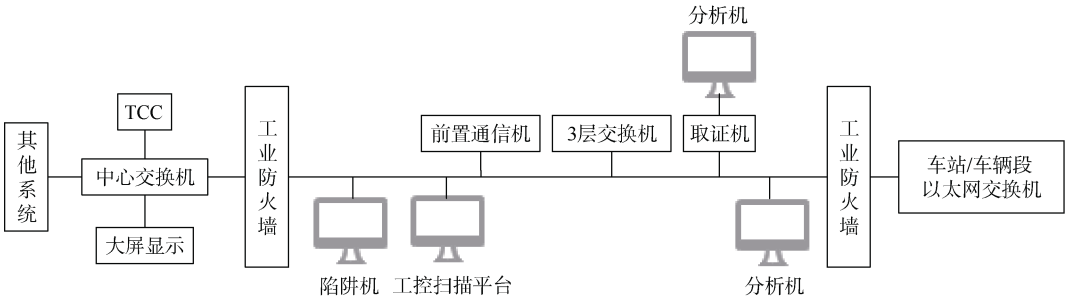

图 6　信号系统信息安全防御系统的物理架构

Figure 6　Physical architecture of signal system information security defense system

5　结语

在信号系统信息化、网络化高速发展的背景下，从系统网络结构出发，结合系统特点及信息安全需求与现状，研究信号系统信息安全防御技术。采用基于等级保护的被动防御体系和基于安全技术、安全策略、安全管理的三维主动防御体系结合的防御理念，加强系统的防御能力，对信号系统的信息安全体系的完善有一定的理论和实践意义。但该模型尚欠经济性分析论证，下一步可从信息安全评估方面，考虑实现防御利益最大化的最佳组合策略，部署信息安全防御体系。

参考文献

[1] 张峰. 基于策略树的网络安全主动防御模型研究[D]. 成都: 电子科技大学, 2004.
ZHANG Feng. Policy tree based proactive defense model for network security[D]. Chengdu: University of Electronic Science and Technology of China, 2004.

[2] 林旺群, 王慧, 刘家红, 等. 基于非合作动态博弈的网络安全主动防御技术研究[J]. 计算机研究与发展, 2011, 48(2): 306-316.
LIN Wangqun, WANG Hui, LIU Jiahong, et al. Research on active defense technology in network security based on non-cooperative dynamic game theory[J]. Journal of computer research and development, 2011, 48(2): 306-316.

[3] 陈安观. 列车调度指挥系统(CTC/TDCS)网络信息安全主动防御体系设计方案研究[J]. 铁路通信信号工程技术, 2017, 14(3): 32-34.
CHEN Anguan. Active defense system design scheme of CTC/TDCS system network information security[J]. Railway signalling & communication engineering, 2017, 14(3): 32-34.

[4] 倪国栋. 铁路综合视频监控系统信息安全防护应用研究[J]. 铁道通信信号, 2018, 54(2): 53-56.

[5] 陶伟. 城市轨道交通信号系统信息安全问题研究[J]. 城市轨道交通研究, 2018, 21(S1): 20-23.
TAO Wei. Research on the information security for urban rail transit signal system[J]. Urban mass transit, 2018, 21(S1): 20-23.

[6] 包正堂. 列控系统信息安全风险主动防御研究[D]. 北京: 北京交通大学, 2017.
BAO Zhengtang. Active defense of security risk in train control system[D]. Beijing: Beijing Jiaotong University, 2017.

[7] 何坚安. 蜜罐技术在信息安全防御中的应用与研究[J]. 网络安全技术与应用, 2020(8): 29-31.
HE Jian'an. Application and research of honeypot technology in information security defense[J]. Network security technology & application, 2020(8): 29-31.

[8] 李朝阳, 彭道刚, 吕政权, 等. 基于改进ADT的综合能源系统信息安全风险分析[J]. 浙江电力, 2020, 39(12): 122-128.
LI Zhaoyang, PENG Daogang, LYU Zhenquan, et al. Information security risk analysis of integrated energy system based on improved ADT[J]. Zhejiang electric power, 2020, 39(12): 122-128.

[9] 高锐, 魏光辉, 赵弘洋. 城市轨道交通车地无线通信安全风险研究[J]. 电子产品可靠性与环境试验, 2014, 32(5): 43-48.
GAO Rui, WEI Guanghui, ZHAO Hongyang. Information security of train-ground wireless communication system in urban rail transit[J]. Electronic product reliability and environmental testing, 2014, 32(5): 43-48.

[10] 信息安全技术 信息系统安全等级保护基本要求: GB/T 22239—2008[S]. 北京: 中国标准出版社, 2008.

[11] 信息系统安全等级保护实施指南: GB/T 25058—2010[S]. 北京: 中国标准出版社, 2011.

[12] 中华人民共和国计算机信息系统安全保护条例[S]. 北京, 1994.

（编辑：傅依萱）