

符合等级保护三级要求的城市轨道交通综合监控系统信息安全设计

徐启禄¹ 高月鑫²

(1. 青岛地铁集团有限公司, 266061, 青岛; 2. 同方股份有限公司, 100083, 北京 // 第一作者, 高级工程师)

摘要 网络安全等级保护(简称“等保”)2.0 和城市轨道交通综合监控系统(ISCS)建设的国家标准已经实施, ISCS 信息安全按照等保三级进行建设已成为趋势。根据国家标准有关等保的要求, 分析了目前 ISCS 信息安全现状和存在的问题。围绕“一个中心、三重防护”要求, 提出了 ISCS 信息安全的设计方案, 并从 ISCS 网络安全架构、信息安全功能设置等方面给出了实施建议。

关键词 城市轨道交通; 综合监控系统; 信息安全; 等级保护
中图分类号 F530.7; TN915.08

DOI:10.16037/j.1007-869x.2021.09.017

Information Security Solution for Urban Rail Transit ISCS Complying with Third-level Classified Protection Standard

XU Qilu, GAO Yuexin

Abstract The national standards of internet safety classified protection 2.0 and urban rail transit ISCS (integrated supervisory control system) have been implemented, and it has become a trend to construct the ISCS information security in accordance with the classified protection level 3. In line with the requirements of national classified protection standards, current situation and existing problems of ISCS information security are analyzed. Design scheme of ISCS information security centering ‘one center, triple protection’ is put forward, and implementation suggestions in terms of ISCS network security architecture and information security function settings are provided.

Key words urban rail transit; ISCS (integrated supervisory control system); information security; classified protection

First-author's address Qingdao Metro Group Co., Ltd., 266061, Qingdao, China

《交通运输信息化“十三五”发展规划》提出: 推进交通运输“互联网+”, 要求充分利用信息技术改造传统交通运输业^[1]。《中华人民共和国网络安全法》明确规定, 对于涉及公共通信、金融、交通等的

关键基础设施行业, 需在其等级保护(以下简称“等保”)制度的基础上, 实施重点保护。2019 年 12 月 1 日, 与等保 2.0 相关的 GB/T 22239—2019《信息安全技术网络安全等级保护基本要求》等国家标准正式实施。等保 2.0 相比等保 1.0 更加注重全面主动防御、感知预警、动态防护、安全检测、应急响应等, 且定级对象扩展至基础信息网络、工业控制系统、云计算平台以及大数据等平台系统^[2]。

城市轨道交通综合监控系统(ISCS)深度集成了电力监控系统(PSCADA)、环境与设备监控系统(BAS)等系统, 互联信号、通信、自动售检票等系统, 对城市轨道交通的多个专业、系统进行集中监控和联动, 是支撑城市轨道交通可靠、安全运行的关键系统之一, 一旦被人入侵干扰将造成灾难性后果。新形势、新政策也对 ISCS 的信息安全提出了更高的要求, 必须构建一个完善的安全体系架构。

1 ISCS 的信息安全级别

根据国家标准的相关要求“综合监控系统的信息安全应符合现行国家标准《工业控制系统信息安全》规定”“且宜按信息系统安全等级保护标准第三级进行设计、工程实施和验收”^[3]。等保 2.0 新规要求“应在工业控制系统与企业其他系统之间部署访问控制设备, 配置访问控制策略”^[4]。

虽然上述标准中并未强制要求 ISCS 必须满足等保三级标准, 但是, 考虑到 ISCS 的集成度越来越高, 对城市轨道交通的安全稳定运行已经不可或缺。建设、设计、集成、运营等相关各方已经基本形成一致的认识, 即 ISCS 信息安全应满足等保三级的标准。

2 ISCS 信息安全建设现状及安全问题分析

等保三级对系统安全保护环境提出了很多具

体明确的要求,但是现阶段 ISCS 信息安全建设还存在诸多问题。

1) 没有正确的信息安全观。ISCS 从业人员存有 ISCS 处于内部局域网环境、信息安全与我无关的态度,导致 ISCS 信息安全建设从设计、工程实施乃至运营管理都得不到重视,并且缺乏管理制度的约束。理念决定行动,如果没有树立正确的信息安全理念,就会导致缺乏相关信息安全预防措施。

2) 缺乏集中安全管理与审计。由于缺乏信息安全观,因此也没有在技术层面上对设备、应用系统等账号认证方式进行限制,存在大量弱口令。存在一个账号多人使用的情况,因此不知道何人何时做了何操作;尤其是在对第三方运维人员管理方面,因为没有有一个集中管理平台对工作人员、用户的账号、认证、授权、审计等进行管理,因此难以实现统一的信息安全管理。由于缺乏有效的网络准入和资源访问控制机制,在 ISCS 网络任意节点都可访问全线系统资源,因此无法对 ISCS 内的网络行为进行识别与监测。

3) 互联接口网络无隔离。ISCS 的互联网络环境复杂,互联接口之间没有有效的安全隔离措施,ISCS 与互联专业接口直接由终端到终端互联,网络协议、端口任意开放。

ISCS 集成的子系统(PSCADA、BAS 等)为传统工业控制系统,一方面这些系统的设计目的在于实现各种实时控制功能,基本不考虑信息安全问题;另一方面这些系统相对比较封闭,一般被认为受到外界入侵的风险较小。但 ISCS 互联的子系统(ATS(列车自动监控)、PIS(乘客信息系统)、AFC(自动售检票)等)为不同种类的 IT 系统,使得 ISCS 的开放性大为提高。在 PSCADA、BAS 系统与 ISCS 控制层纵向间无隔离的情况下,这些子系统会完全暴露来自 ISCS 病毒、木马、网络攻击的威胁下。

4) 终端主机无防护。为了保证系统稳定,ISCS 各种主机(服务器、工作站、前置机(FEP)等)在投运后,操作系统一般不进行漏洞补丁修补。漏洞会被入侵者用以获取系统的完全访问权限;外接设备、移动存储设备等介质携带的病毒也会利用漏洞进行二次传播,造成网络内的主机成片感染,甚至造成寄生、蠕虫、勒索等危害严重的病毒泛滥。国内的 ISCS 及相关系统已经出现过多次病毒入侵等信息安全事故。

3 ISCS 信息安全方案设计

ISCS 存在的信息安全问题涉及到制度约束、管理与审计、网络通信安全、工控系统、主机安全等多个方面,因此,进行 ISCS 信息安全方案设计时,需通过梳理 ISCS 业务流程,分析以上关键保护点,然后分层分域设计安全机制及策略。要确保 ISCS 信息安全方案技术与管理有机结合,相互支撑,实现技管并重。

3.1 ISCS 信息安全设计要点

在管理层面应制定管理、检查制度和信息安全事件应急响应制度,通过制度的学习和执行强化信息安全观念,通过规章制度和定期监督检查约束信息安全行为,保障信息安全保护能力不断提高。

在技术层面,依据等保 2.0 新标准的三级防护规范要求:“通过第三级的安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计加以实现”^[5],即“一个中心”管理下的“计算环境、区域边界、通信网络的三重防护”体系框架,实施多层隔离和保护,防止某薄弱环节影响整体安全;重点对操作人员使用的终端、业务服务器等计算节点进行安全防护,控制操作人员行为,把住攻击发起源头,防止发生攻击行为;同时分析 ISCS 应用系统业务流程,制订访问控制安全策略,并由安全网关依据安全策略自动执行,扎牢网络漏洞。

ISCS 信息安全设计遵循“分层分域、边界控制,内部监测、集中管控”的原则。

“分层分域、边界控制”即划分安全管理中心、ISCS 中央级/车站级、车站级 PSCADA、车站级 BAS 等安全区域,区域边界部署防火墙,实现协议层、细粒度的访问控制。

“内部监测、集中管控”即在中心级构建安全管理中心子系统,结合审计设备、终端管理、4A(Authentication 身份验证、Account 账号管理、Authorization 授权控制、Audit 安全设计)堡垒机等,实现网络内设备状态的集中监测,并能够进行全局日志分析、安全策略统一下发。

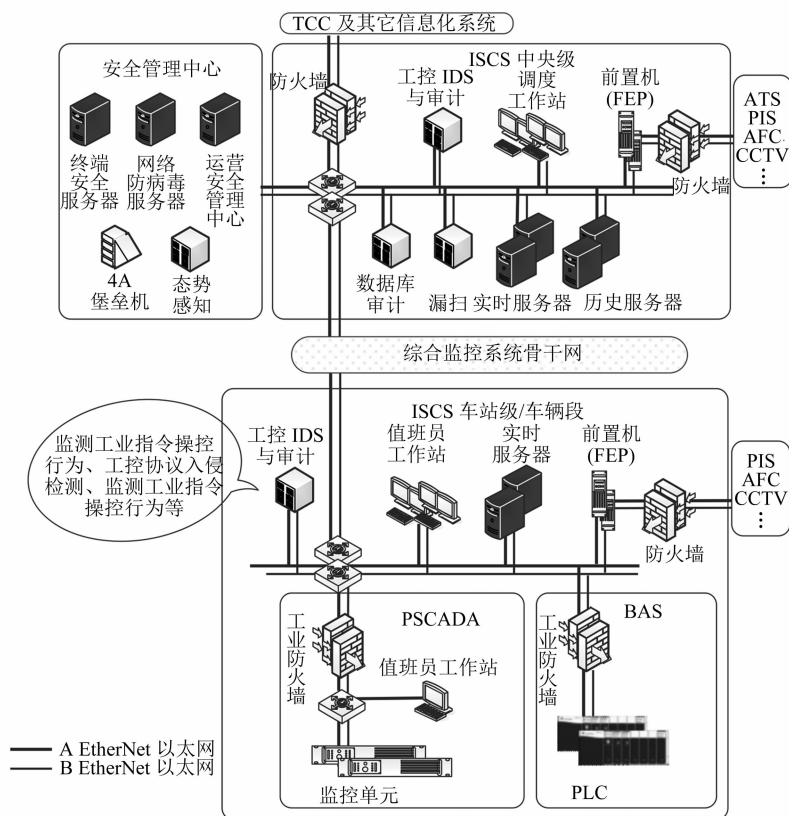
基于上述技防原则的 ISCS 信息安全构架如图 1 所示。

3.2 建设安全管理中心

安全管理中心是 ISCS 安全管理的核心。等保三级明确要求:安全管理中心实现系统管理、审计管理、安全管理、集中管控,且划分特定的管理区

域。因此,在 ISCS 控制中心需建设安全管理中心,从技术层面提供系统安全的监察和管理手段。安

全管理中心可利用 ISCS 的网管中心设备进行适当扩容后构建,使其兼具网管和信息安全管理的功能。



注: IDS——入侵检测系统; TCC——线网指挥中心; CCTV——视频监控系统; PLC——可编程逻辑控制器。

图1 城市轨道交通 ISCS 信息安全构架

安全管理中心系统包括 4A 堡垒机、安全审计与监测、工控异常检测、动态态势感知等子系统。

1) 4A 堡垒机:通过 4A 堡垒机对被授权人员(运维人员)在系统内的维护行为进行解析、分析、记录、汇报^[6];监督管控运维人员对设备 IP 地址、用户名、口令等信息的记录,控制运维人员能运维哪些设备、执行哪些操作命令,避免运维人员非法或无意执行高危操作,并对运维人员的操作进行实时监控和事后审计,解决管理运维人员操作难、乱、不可追溯等问题。

2) 安全审计与监测:需要对 ISCS 内的网络行为的安全性进行感知及预警。通过对网络流量、数据库访问等进行分析、记录并挖掘展示,对 ISCS 网络行为进行审计、管控,一方面是审计系统内部发起的行为操作是否合规,包括系统内中央级与车站级、与控制层等方向;二是系统外部对 ISCS 发起的访问是否具有威胁。

审计设备对 ISCS 内网络、数据库提供全面的行为监控,对网络、数据库访问进行合规性管理;对 ISCS 业务网络进行安全审计,采集、分析和识别网络数据流,监视网络系统的运行状态,记录网络事件,发现安全隐患。

安全管理中心还可以集中监视全线网络设备和主机设备的健康状态,同时收集全线主机设备、操作系统、应用平台、数据库等的日志信息,实现对各设备审计数据集中汇总和分析的功能。全面掌控系统状态,满足等保对集中管控的要求。

3) 工控异常检测:ISCS 平台作为 PSCADA、BAS 系统控制命令的来源,在 ISCS 网络内对该类工控指令的合规性检测是非常重要的。通过工控异常检测系统可检测工业指令操控行为、异常报文、工控漏洞攻击、工控协议入侵等行为,监测工控网络中的敏感操控,预警 ISCS 网络内对 PSCADA、BAS 系统存在威胁的网络故障与异常行为,保护

PSCADA、BAS 等工控系统的安全运行。

4) 动态态势感知:动态态势感知平台从主机端、网络层、流量审计等获取 ISCS 的安全日志、流量分析、漏洞信息、资产状态、僵尸蠕虫数据,完成安全事件信息的采集、聚合、过滤、关联,实现对 ISCS 安全态势的动态感知。通过大数据分析 & 可视化展示等手段,展示安全威胁实时预警、监控数据实时汇总、报表统计等信息,对网络风险和系统健康态势集中呈现、分析、预测、处理。

3.3 建设安全的区域边界

根据 ISCS 与互联、集成子系统的网络结构逻辑的不同,划分不同安全区,将 ISCS 作为一个整体安全域,从外部系统接入(水平方向)到内部集成子系统(垂直方向)部署边界防护体系,实现对系统内外间的隔离防护:部署中央级与互联系统边界防火墙;部署中央级与其他信息系统边界防火墙;部署车站级与互联系统边界防火墙;部署车站级与集成子系统边界防火墙。

防火墙可以过滤进出网络的数据、管理进出访问网络的行为、封堵高危端口、记录通过防火墙的信息内容和活动、对网络攻击进行检测和告警^[7];通过强制性访问控制机制实现对源及目标计算节点的身份、地址、端口和应用协议等的可信验证。边界防护是 ISCS 信息安全的界墙,建设和加强入侵防护是 ISCS 网络安全防护的关键工作,同样也是等保三级对于访问控制和边界完整性检查的基本要求。

在水平方向,与外部的互联系统间设置防火墙,对接口通信协议的内容进行分析检测,实现协议层、端口细粒度的访问控制,拒绝外部非法连接,隔离来自外部的安全威胁;在垂直方向,与集成子系统间部署工业防火墙,用来隔离来自 ISCS 控制层的安全威胁。工业防火墙可以对工业协议(Modbus/TCP、Ethernet/IP、IEC104 等)内容、指令进行深度解析检测和非法阻断,满足等保 2.0 标准对工业控制系统安全通信网络技术隔离手段的基本要求。

3.4 加固计算环境安全

主机安全涉及系统内部所有主机设备及系统用户。ISCS 主机主要涉及工作站、服务器等,它们直接参与监视、控制各互联、集成子系统的终端设备。安全的计算环境是 ISCS 信息安全的基础。终端也是安全威胁发起的源头,恶意代码防范、非法外联管理、访问控制、安全日志、漏洞信息、资产状态、合规检查等都是终端设备的基础防护。

为主机配置的用户安全策略,包括登陆失败、超时退出、口令复杂度等策略,设置限制登陆访问地址并结合 4A 堡垒机安全审计系统实现统一的信息安全策略;部署终端安全管理软件,实现对全线主机准入控制、非法外联控制、外设及移动存储介质的集中管理,尤其对不可信的移动存储介质,保证进不来、数据拷贝不走,还可对主机设备的漏洞补丁进行统一更新;部署网络防病毒软件,对 ISCS 全线主机实现防恶意代码的统一管理,有效防范来自 U 盘、网络共享等各种途径的恶意代码入侵,并且终端的相关安全信息会及时反馈给系统中心,管理员能够及时了解网络内安全状态、分析安全事件,并能够远程操控设置终端安全策略。

3.5 安全的通信网络

在网络构架方面,规划设计网络时需做好网络带宽用量分析、IP 分配及预留、核心网络设备性能选择,以及通信链路、关键硬件设备(服务器、FEP、交换机等)冗余部署,保证系统可靠性。对于业务数据、安全管理,需为其在网络交换传输中单独划分通信通道。

ISCS 平台在车站与控制中心间的通信传输采用私有协议,在保证平台数据实时性传输的前提下,实现可控范围的数据完整性校验及加密;工业控制通信协议(Modbus TCP、IEC 104 等)多采用明文传输,采用 SSL(安全套接字协议)安全协议在传输层对网络连接进行加密,在保持现有通信协议功能、效率、可靠性基础上,实现通信加密和双向认证^[8],满足通信传输中完整性、保密性的要求。

4 ISCS 等保的测评认证

ISCS 信息安全方案实施完成后,需要经过信息安全等级保护的测评认证。等保测评涵盖了定级、备案、建设整改、等级测评等流程,是对 ISCS 安全保护状况的综合评价。

根据测评认证的要求,在 ISCS 的安全设计上,应注意以下几点:

1) 重点加固:应针对 ISCS 等保建设的原则方向,结合 ISCS 业务特点,针对性地进行安全加固,而不是一味堆砌安全设备和安全软件。

2) 适度安全:信息安全防护是为业务生产系统服务的,要基于 ISCS 的安全需求进行整改。不顾安全成本、违背业务需求一味进行信息安全建设,

(下转第 82 页)

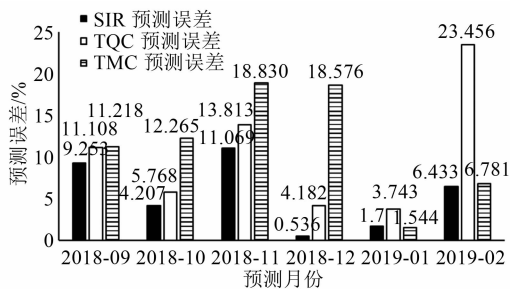


图7 西安地铁2号线2018年9月—2019年2月不同分类方法的客流量预测误差对比图

自然季节性和制度节性是影响季节性波动最主要的因素。TMC和TQC分类方法的季节分组只体现了自然季节性,而本文所采用的方法根据两者叠加的结果进行分组,更为准确。

综上所述,基于月客流残差的季节指数预测方法具有较高的预测精度和较好的稳定性。

4 结语

本文通过对月客流残差分析,提出了基于月客流残差的季节分类方法,以季节指数调整客流达到提高预测精度的目的。通过对三种分类方法进行对比分析,本文提出的分类方法在月度客流预测中精度较高,基本满足对客流量的预测需求。

(上接第76页)

反而会导致ISCS业务运行更加复杂,影响业务平台的可靠性、实效性,会起相反的作用。

3) 问题整改:测评认证是在技术与管理共用情况下的一个综合安全评定。问题整改是落实等级保护工作的关键,适合业务系统的整改策略,要充分利用各安全组件,严格按照网络安全等级保护标准要求、测评要求及时、规范地进行问题整改。

5 结语

根据等保2.0三级防护规范和实施指南要求,通过部署安全管理中心、加固计算环境安全、增强边界安全隔离、进行安全审计等措施,可以显著提升ISCS信息安全防护能力,满足等保三级要求。本文介绍的方案已在ISCS信息安全建设项目中进行实施,并通过了第三方机构的信息安全三级评测及CNAS的认证。当然,ISCS的等保三级安全设计还是较新的课题,等级保护也只是现代信息系统安全应达到的底线,还需要根据后续的实际运行情况不断进行改进。

通过该分类方法计算出的季节指数用于预测时,能更好地适应城市轨道交通客流的季节性变化趋势,从而使运营公司及时调整相关运能运力,制定更加经济合理的月度或年度运营计划。

考虑到影响城市轨道交通客流季节性因素的多样性,后续需要对网络、不同线路和站点的季节区间进行对比分析。

参考文献

- [1] 王夏秋,张宁,王健. 基于季节指数的城市轨道交通月度客流预测方法[J]. 城市轨道交通研究,2018(10): 25.
- [2] 赵钰棠,杨信丰,杨珂. 基于支持向量机的地铁客流量预测[J]. 都市快轨交通,2014(3): 35.
- [3] 吉海兵,吕效国,周培,等. 加权季节性指数法及其应用[J]. 数学的实践与认识,2010(12): 80.
- [4] 何俊,刘会茹,张彦群. 不变季节指数法的应用[J]. 黄冈师范学院学报,2008(3): 25.
- [5] 邓明,张荷观. 利用虚拟变量对季节指数的估计[J]. 统计与决策,2007(4): 15.
- [6] 王跃军,刘万春,王正平,等. 基于季节指数修正因子的交乘趋向预测方法[J]. 军民两用技术与产品,2006(4): 43.
- [7] 郑薇,王灿强,李维德. 基于季节指数调整与HGWO-SVR算法的农产品价格预测模型[J]. 统计与决策,2018(19): 33.
- [8] 周华任,李浩然,孙学金,等. 一种基于季节指数的灰色马尔科夫气温预测模型[J]. 数学的实践与认识,2016(4): 167.

(收稿日期:2019-10-17)

参考文献

- [1] 中华人民共和国交通运输部. 交通运输信息化“十三五”发展规划[R]. 北京:中华人民共和国交通运输部,2016.
- [2] 杨雪飞. 浅谈等级保护2.0的新变化和等保工作的误区[J]. IT经理世界,2019(1): 51.
- [3] 中华人民共和国工业和信息化部电子工业标准化研究院. 城市轨道交通综合监控系统工程技术标准:GB/T 50636—2018[S]. 北京:中国建筑工业出版社,2018.
- [4] 国家标准化管理委员会. 信息安全技术网络安全等级保护基本要求:GB/T 22239—2019[S]. 北京:中国标准出版社,2019.
- [5] 国家标准化管理委员会. 信息安全技术网络安全等级保护安全技术要求:GB/T 25070—2019[S]. 北京:中国标准出版社,2019.
- [6] 徐世亮,操屹. 浅析构建国土资源网上交易系统安全防护体系[J]. 江西通信科技,2013(2): 45.
- [7] 单联春. 防火墙与入侵检测系统联动构建网络安全堡垒[J]. 有线电视技术,2005(10): 80.
- [8] 高锐强,朱虹,贾立东,等. 基于SSL安全协议实现工业控制通讯协议加密及认证的研究[J]. 化工设计通讯,2019(1): 121.

(收稿日期:2020-12-10)