

# 适用于城市轨道交通 CBTC 系统的网络安全态势感知系统

刘懂懂<sup>1</sup> 周星宇<sup>2</sup> 朵建华<sup>1</sup> 王向阳<sup>1</sup> 韩 涛<sup>2</sup> 朱锁明<sup>2</sup>

(1. 宁波市轨道交通集团有限公司智慧运营分公司, 315101, 宁波; 2. 卡斯柯信号有限公司, 200072, 上海)

**摘 要** [目的]城市轨道交通 CBTC(基于通信的列车控制)系统面临复杂且多样化的网络安全问题。既有网络安全设备误报率高且与 CBTC 系统适配度低,对业务数据缺乏深度分析及多系统融合分析,无法主动感知网络安全威胁。为提高 CBTC 系统网络安全运营水平,有效保障 CBTC 系统的业务连续性,需构建适用于城市轨道交通 CBTC 系统的网络安全态势感知系统。[方法]结合相关标准中的通用技术要求,提出了适用于城市轨道交通 CBTC 系统的网络安全态势感知系统架构,阐述了该系统架构中前端数据源的数据内容及核心组件的具体功能。介绍了面向 CBTC 系统的日志规范化技术、安全威胁分析技术和态势可视化技术等关键技术。[结果及结论]适用于城市轨道交通 CBTC 系统的网络安全态势感知系统架构与 CBTC 系统架构高度适配,系统功能与 CBTC 系统运行场景高度融合;采用该系统,可实现业务高效联动,降低既有网络安全系统设备的误报率,提高 CBTC 系统网络安全水平,有效保障 CBTC 系统的业务连续性。

**关键词** 城市轨道交通;信号系统;网络安全态势感知

**中图分类号** U231.7

**DOI**:10.16037/j.1007-869x.2024.10.058

## Cybersecurity Situational Awareness System Applicable for Urban Rail Transit CBTC System

LIU Dongdong<sup>1</sup>, ZHOU Xingyu<sup>2</sup>, DUO Jianhua<sup>1</sup>, WANG Xiangyang<sup>1</sup>, HAN Tao<sup>2</sup>, ZHU Suoming<sup>2</sup>

(1. Smart Operation Branch of Ningbo Rail Transit Group Co., Ltd., 315101, Ningbo, China; 2. CASCO Signal Ltd., 200072, Shanghai, China)

**Abstract** [Objective] Urban rail transit CBTC (communication-based train control) systems face complex and diverse cybersecurity challenges. Existing cybersecurity tools feature high false alarm rates and poor adaptation to CBTC systems, lacking in-depth analysis of business data and integration across multiple systems, thus incapable to proactively detect cybersecurity threats. To enhance the cybersecurity operations of CBTC systems and ensure the continuity of CBTC system busi-

ness operations, it is necessary to develop a cybersecurity situational awareness system applicable for urban rail transit CBTC systems. [Method] Based on general technical requirements outlined in relevant standards, a cybersecurity situational awareness system architecture tailored to urban rail transit CBTC systems is proposed. The data content from front-end data sources and the specific functions of core components in the system architecture is expounded. Key technologies, including log normalization techniques, security threat analysis methods, and situational visualization techniques for CBTC systems are introduced. [Result & Conclusion] The cybersecurity situational awareness system architecture applicable for urban rail transit CBTC system is highly compatible with CBTC system architecture, and its functions are deeply integrated with CBTC operational scenarios. The implementation of this system enables efficient business coordination, reduces the false alarm rates of existing cybersecurity equipment, enhances the cybersecurity levels of CBTC systems, effectively ensuring the continuity of CBTC system business operations.

**Key words** urban rail transit; signaling system; cybersecurity situational awareness

## 1 CBTC 网络安全风险分析

目前,新建城市轨道交通线路普遍采用 CBTC(基于通信的列车控制)系统。CBTC 系统主要包括车载和轨旁 ATC(列车自动控制)、ATS(列车自动监控)、DCS(数据传输系统)以及 MSS(信号维护支持系统)等子系统,各个子系统之间通过网络互相联通,存在一定的安全风险。CBTC 系统一旦遭到严重的病毒破坏或网络攻击,可能会扰乱列车正常运行秩序,甚至会造成大面积运输瘫痪,从而对社会秩序和公共利益造成严重损害。因此,对 CBTC 系统的网络安全有着极高的要求。

CBTC 系统面临的网络安全问题呈现复杂且多样化特点,主要体现在以下几方面:

1) 无线通信的脆弱性问题。CBTC 系统通常依赖无线通信进行列车与地面之间的信息传输,但既有基于 Wi-Fi 无线通信技术在身份验证、加密和传输等方面可能存在高漏洞,容易遭受攻击。

2) 旧技术使用问题。部分 CBTC 系统可能仍采用旧的 Wi-Fi 技术,而旧技术的网络保护能力相对较弱,容易成为攻击者的目标。

3) 与外部网络连接问题。由于业务需要, CBTC 系统和外部 IT 网络存在联通需求,但通常缺乏适当的安全措施,这种不安全的连接可能导致来自其他网络的潜在渗透,进而对 CBTC 系统的安全性和可用性产生影响。

4) CBTC 系统设备本身的脆弱性问题。ATC 子系统设备大多是嵌入式板卡设备,其自身的处理能力偏弱,如果子系统内部发生异常数据交互行为,也会影响 CBTC 系统的正常运行。

为解决上述网络安全问题,新建城市轨道交通线路的信号系统按照等级保护三级的技术要求装备网络安全设备,主要包括:在边界增加入侵检测类设备和防火墙类设备,增加日志审计类设备用于收集各种日志,增加主机加固类设备,等等。经过调研分析发现,上述增加的设备现场运营效果欠佳,主要原因如下:

1) 目前等级保护三级的网络安全设备组成的安全防御系统缺乏对 CBTC 系统业务场景化的知识建模,没有从 CBTC 系统设备自身业务场景和脆弱性来进行系统性设计,与 CBTC 系统的适配程度较低,只是单点防御部署,无法有效发现真正的网络安全隐患和威胁。

2) 网络安全审计类设备大多是收集各个网络安全设备、主机操作系统以及网络设备上传的日志数据,缺乏关联融合分析,没有形成协同效应。

3) 缺乏对网络流量数据的深度分析。由于未对 CBTC 系统内部协议进行识别,网络安全设备通常只是从网络传输层分析业务流量数据,没有更贴近应用层面进行流量数据分析。

4) 缺乏主动感知预警和联动处置的能力。当检测到攻击事件后再采取相应措施,已经为时已晚<sup>[1]</sup>。

## 2 CBTC 网络安全态势感知系统架构

### 2.1 技术框架

文献[2]中明确定义了网络安全态势感知系统

的技术框架,包括前端数据源、核心组件以及其他要素等三部分。核心组件是实现网络安全态势感知的重要手段,其表现形式可以是平台、系统等。实现网络态势感知也依赖于应急处置、安全决策以及数据共享等其他要素。为了能更有效地进行网络安全态势感知,前端数据源需能覆盖网络安全态势感知范围内的通信网络、区域边界和计算环境<sup>[2]</sup>。本文基于以上技术要求,构建适用于城市轨道交通 CBTC 系统的网络安全态势感知系统(以下简称“态势感知系统”),实现由安全风险要素获取至安全风险感知预测、响应处置的安全运营体系。

### 2.2 前端数据源

态势感知系统整体架构如图 1 所示。

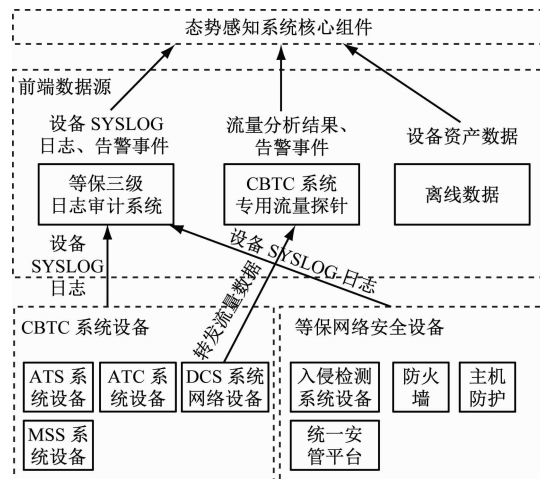


图 1 态势感知系统整体架构

Fig. 1 Overall architecture of situational awareness system

等级保护三级的网络安全设备是构建态势感知系统重要的前端数据源。近年来, CBTC 系统实施等级保护三级的方案也是按照分区域保护的思路进行的。根据 CBTC 系统特点,将 ATS 子系统冗余网及 ATC 子系统冗余网划入网络安全内区,而外部接口机与外部交换机连接的系统,如 ISCS(综合监控系统)等,统一划为网络安全外区,实现从结构上完成安全域的划分。在 CBTC 系统安全内区,通过增加入侵检测设备、审计类设备、防火墙类设备、日志审计系统、主机防护软件和统一安全管理平台等产品,建立安全防护技术体系,实现网络安全所需的访问控制、边界完整性检查、入侵防范、安全审计、集中安全管理以及主机安全等功能。上述网络安全设备提供给态势感知系统的数据内容和格式如表 1 所示。

表 1 网络安全设备提供给态势感知系统的前端数据源内容和格式

Tab.1 Source content and format of the front-end data provided to situational awareness system by cybersecurity equipment

网络安全设备	前端数据源内容	数据格式
入侵检测设备	恶意攻击、入侵行为告警信息	SYSLOG (标准系统日志格式)
审计类设备	DCS 网络设备运行状况、网络流量、用户行为等日志	SYSLOG
防火墙	非授权访问、阻止病毒等日志	SYSLOG
主机防护设备	恶意代码防范, 以及阻止病毒、木马等日志	SYSLOG

除此之外,还需要有针对性地增加 CBTC 系统专用流量探针设备。该设备通过采集 CBTC 网络流量和对 CBTC 系统内各子系统间协议的深度分析,实现网络流量监测和威胁识别。态势感知系统的核心组件实时获取流量探针设备的分析结果,以便后续进行场景化关联分析。

### 2.3 核心组件

态势感知系统核心组件如图 2 所示。

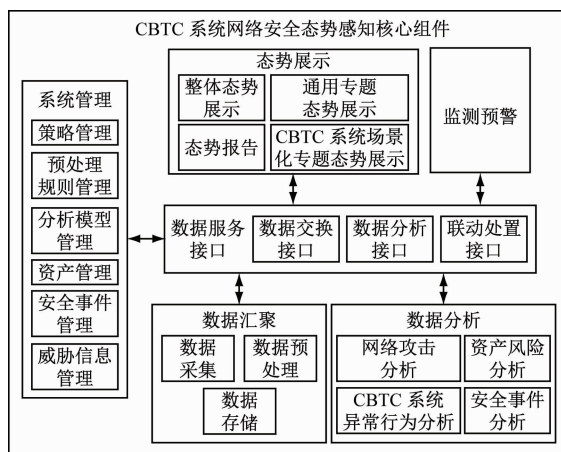


图 2 安全态势感知系统核心组件

Fig.2 Core component of cybersecurity situational awareness system

态势感知系统核心组件由数据汇聚、数据分析、态势展示、监测预警、数据服务接口以及系统管理等组件构成,各组件功能如下:

1) 数据汇聚组件。根据 CBTC 系统业务需求,从前端数据源采集数据,通过日志可视化范化技术,将采集的数据经筛选、补全、标记等预处理后进行存储,用于后续的关联数据分析。

2) 数据分析组件。基于内置的 CBTC 系统业

务规则分析模型,通过数据服务接口调用相关数据,进行网络攻击分析、CBTC 系统设备资产风险分析、基于 CBTC 系统设备脆弱性的异常行为分析以及安全事件分析。

3) 态势展示组件。主要通过数据服务接口调用相关数据进行多维度评估和展示。

4) 监测预警组件。主要基于设定的监测策略和预警规则进行预警,便于后续的安全决策和应急处置。

5) 数据服务接口组件。主要对态势感知系统内数据采集、交换、分析和应用等数据处理活动进行解耦,完成前端数据源与内部不同模版以及其他外部设备间的数据交互。

6) 系统管理组件。主要进行策略管理、预处理规则管理、分析模型管理、资产管理、安全事件管理和威胁信息管理。

## 3 态势感知系统关键技术

### 3.1 日志规范化技术

通常不同线路的 CBTC 系统提供的前端数据源日志信息分别来自不同厂商、不同类型的产品,因此将异构日志转换为统一的、可识别的日志,是场景关联分析的前提和基础。

传统的日志规范化技术一般采用正则表达式编写日志。如果日志格式稍有变化,正则表达式就可能会失效,进而造成日志无法识别和范化。为解决上述问题,态势感知系统首先采用机器学习方式对海量日志进行学习和识别,分析日志语法结构;然后基于聚类算法对日志自动聚类、合并,形成多个包含相似数据内容的日志集;最后根据日志集内日志数量的大小对日志集进行排序。

为满足 CBTC 系统安全运维人员的范化需求,态势感知系统操作界面设计采用了可视化范化技术,运维人员可在该界面编写正则表达式,并通过界面显示提取结果,运用鼠标将提取结果拖曳至相应的范化字段,直接完成字段对应;态势感知系统根据运维人员的操作自动生成范化解析脚本,并开始生效工作。可视化范化技术显著降低了范化工作的复杂度,提升了日志范化的效率,使态势感知系统更易用且高效。

### 3.2 安全威胁分析技术

CBTC 系统面临的安全威胁包括已知威胁和未知威胁。态势感知系统需要采用多层次的分析技

术来保证精准、高效地感知潜在的威胁。

1) 感知已知威胁。根据 CBTC 系统安全分析经验,构建了开放式知识规则分析引擎,内置安全分析场景规则,运维人员也可通过可视化方法新增或编辑关联分析规则。知识规则分析引擎针对由前端数据源提供的安全日志和流量分析结果等数据进行实时关联融合分析,并结合各类场景数据,及时发现已知的攻击、威胁。前端数据源提供的大多是事件日志格式数据,这些数据经统一规范化后,由知识规则分析引擎使用决策表及交叉决策表与预置规则进行匹配关联,具体的匹配模式包括场景关联以及统计关联。

2) 感知未知威胁。对于未知威胁的感知,首先使用基于机器学习的异常行为检测方法,从海量日志和流量结构数据中选择属性特征进行学习,构建实体行为基线模型;然后通过实际值与预测值的偏差分析识别异常行为;最后进一步计算置信度,根据计算结果,将超出置信度阈值的异常行为判断为安全威胁事件。

### 3.3 低代码态势可视化技术

态势可视化的目的是生成 CBTC 系统网络安全综合态势图,使分析结果数据可视化、态势可视化。态势感知系统通过直观、易理解的图形化界面,结合低代码报表、大屏开发和图形组态技术,使网络安全态势的展示更加高效、便捷,便于运维人员从更高层面观察和感知问题<sup>[3]</sup>。

态势感知系统利用低代码开发平台,通过图形化拖曳、参数化配置等方式,快速构建出网络安全态势的可视化展示界面。这种开发方式可以大大减少代码编写量,提高开发效率,适合态势感知系统产品化以及工程化的要求<sup>[4]</sup>。

## 4 结语

本文设计了适用于城市轨道交通 CBTC 系统的网络安全态势感知系统,详细阐述了该系统架构中前端数据源的数据内容及核心组件功能,分析了

安全态势感知系统的关键技术,包括面向 CBTC 系统的日志规范化技术、安全威胁分析技术以及态势可视化技术。态势感知系统与 CBTC 系统架构高度适配,两者业务高度融合,实现了高效业务联动,降低了既有网络安全系统设备的误报率,提高了 CBTC 系统网络安全运营水平,有效保障了 CBTC 系统的业务连续性。

## 参考文献

- [1] 周献飞,徐浩,焦建林,等. 电力监控系统网络安全态势感知研究与建设[J]. 供用电, 2020, 37(3): 64.  
ZHOU Xianfei, XU Hao, JIAO Jianlin, et al. Research and construction of network security situational awareness in electric power monitoring system [J]. Distribution & Utilization, 2020, 37(3): 64.
- [2] 国家市场监督管理总局, 国家标准化管理委员会. 信息安全技术 网络安全态势感知通用技术要求: GB/T 42453—2023 [S]. 北京: 中国标准出版社, 2023:3.  
State Administration for Market Regulation, Standardization Administration of the People's Republic of China. Information security technology—General technical requirements for network security situation awareness: GB/T 42453—2023 [S]. Beijing: Standards Press of China, 2023:3.
- [3] 王慧强,赖积保,朱亮,等. 网络态势感知系统研究综述[J]. 计算机科学, 2006, 33(10): 5.  
WANG Huiqiang, LAI Jibao, ZHU Liang, et al. Survey of network situation awareness system [J]. Computer Science, 2006, 33(10): 5.
- [4] 陶源,黄涛,张墨涵,等. 网络安全态势感知关键技术研究及发展趋势分析[J]. 信息网络安全, 2018(8): 79.  
TAO Yuan, HUANG Tao, ZHANG Mohan, et al. Research and development trend analysis of key technologies for cyberspace security situation awareness [J]. Netinfo Security, 2018(8): 79.

· 收稿日期:2024-05-20 修回日期:2024-06-22 出版日期:2024-10-10

Received:2024-05-20 Revised:2024-06-22 Published:2024-10-10

· 通信作者:刘懂懂,高级工程师, liudongdong\_nbjd@163.com

· ©《城市轨道交通研究》杂志社,开放获取 CC BY-NC-ND 协议

© Urban Mass Transit Magazine Press. This is an open access article under the CC BY-NC-ND license

欢迎订阅《城市轨道交通研究》

服务热线 021—56830728 转 821