文章编号：1005-8451（2015）02-0028-05

高速铁路自然灾害及异物侵限监测系统信息安全架构设计和研究

姚洪磊[1]，刘江川[2]，王　彤[1]
（1.中国铁道科学研究院　电子计算技术研究所，北京　100081；
2. 大西铁路客运专线有限责任公司　工程部，太原　030027）

摘　要：为提高高速铁路自然灾害与异物侵限监测系统（简称：灾害监测系统）安全，保障系统稳定运行，通过分析灾害系统监测面临的安全风险和安全需求，设计了灾害监测系统安全体系架构，结合具体模型和数据处理流程，重点从物理安全、网络安全、主机安全、应用安全和数据安全等不同方面对灾害监测系统软件的安全系统进行设计。应用结果表明，在不降低软件性能条件下，安全架构及设计方案对提高软件安全性有明显效果，可有效地提高灾害监测系统自身安全性。

关键词：高速铁路；灾害监控；信息安全设计；安全架构
中图分类号：U29-39　　**文献标识码：**A

Information security design and research for High-Speed Railway Nature Disaster and Foreign Invasion Monitor System

YAO Honglei[1], LIU Jiangchuan[2], WANG Tong[1]
(1.Institute of Computing Technologies, China Academy of Railway Sciences, Beijing　100081, China;
2.Engineering Department, Atlantic Railway Passenger Dedicated Co.Ltd, Taiyuan　030027, China)

Abstract: In order to improve the information security of High-speed Railway Nature Disaster and Foreign Invasion Monitor System, ensure operational stability of the System, the paper designed Information Security System, combined with specific models and data processing of the System. The design was focused on the physical security, network security, host security, application security and data security for the software of High-speed Railway Nature Disaster and Foreign Invasion Monitor System. The application results showed that the software security architecture and design solutions could improve software security without reducing the performance of the software, effectively improve information security of the System.

Key words: high-speed railway; disaster monitoring; information security design; security architecture

我国高速铁路建设迅猛发展，截至2013年底，我国高速铁路运营里程已达到11 000 km。高速列车的运行与旅客生命财产息息相关，随着列车运行速度的不断提高，风、雨、雪自然灾害和异物侵限事件对于高速列车运行安全影响增大，在高速铁路建设同步建设高速铁路灾害监测信息系统，以防止或减轻各类灾害及异物侵限对高速铁路列车行车安全的危害，为列车运行安全提供技术保障。

高速铁路自然灾害与异物侵限监测系统（以下简称：灾害监测系统）为列车安全运行等方面提供有力保障的同时，也需要考虑自身运行的安全，在进行安全设计时，根据信息安全相关技术要求[1]，除了在保障系统安全、稳定运行以及在安全管理方面建立相应管理规范和规章制度外，本文主要从技术角度分析灾害监测系统面临的安全风险和安全需求，从物理安全、网络安全、主机安全、应用安全和数据安全5个方面对安全架构进行设计。

1　灾害监测系统介绍

灾害监测系统对高速铁路沿线风、雨、雪及上跨铁路的道路桥梁的异物侵限实现有效、准确、实时的监测，为调度指挥及维护管理提供报警、预警信息，有效防止或减少灾害对高速铁路列车运行安全的影

收稿日期：2014-10-08
基金项目：中国铁道科学研究院基金项目(1052DZ1301)。
作者简介：姚洪磊，助理研究员；刘江川，高级工程师。

响。灾害监测信息系统中，铁路局中心系统由数据处理中心和前端应用两级结构组成，汇总处理风、雨、雪及异物侵限监测、报警信息，并与列车调度指挥系统（CTC）、防洪管理系统、综合视频监控系统、其它铁路局中心系统及省气象局气象观测网相关系统进行信息交换和共享，为高速铁路动车组运行安全提供技术保障[2]，灾害监测系统结构如图 1 所示。

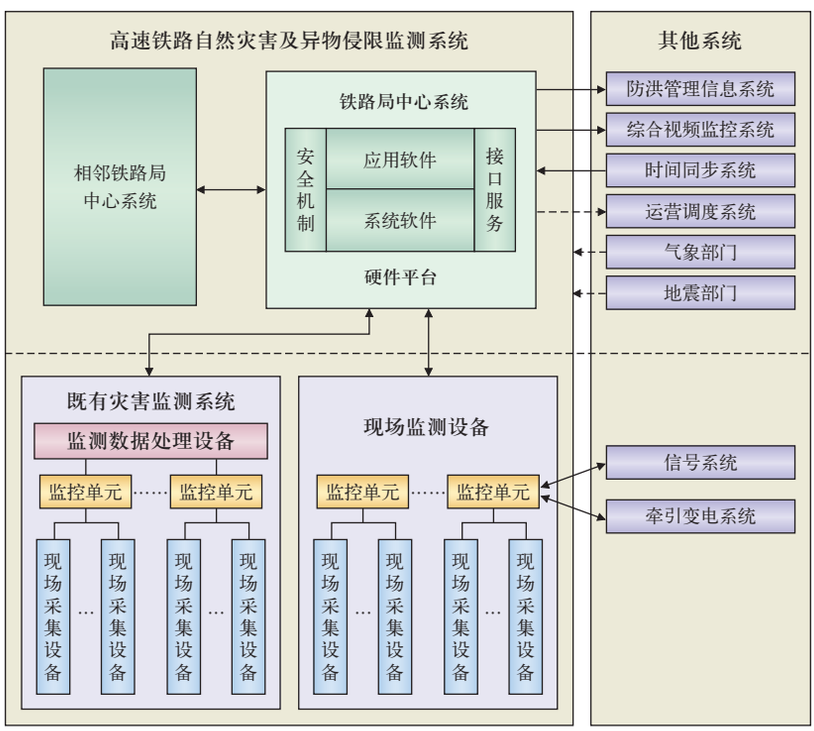

图1　灾害监测系统结构

2　安全风险及安全需求分析

2.1　安全风险

灾害监测系统及其承载的网络面临以下几个方面的安全风险[3~4]：

（1）监测系统漏报和误报的安全风险，包括由于监测点采集设备接口接触不良、传感器设备故障或宕机、服务器故障或宕机、网络数据流量超过设定阈值等导致灾害监测系统的漏报和误报，引起影响列车运行的安全事故；

（2）故障导致灾害监测系统中断运行的安全风险，包括由于应用软件或进程发生异常、应用服务器或数据库服务器运行状态异常等导致灾害监测系统停止运行的安全风险；

（3）人为因素导致灾害监测系统中断运行的安全风险，包括由于软件或操作系统升级、服务器升级或更换、网络设备升级或更换等人为操作导致监测数据传输中断或采集设备上报不及时的安全风险；

（4）自然环境威胁引起的安全风险，包括灾害监测信息系统现场采集、传输、铁路局中心设备和计算网络设备设施可能遭受水灾、火灾、雪灾等环境事故等造成的安全风险；

（5）病毒和恶意攻击安全风险，包括非授权的接入对网络的入侵或攻击、包含恶意攻击、堵塞式攻击、终端或服务器的病毒感染、外部用户的非法接入等。

（6）有缺陷的设计、实现和维护可能导致应用系统存在安全隐患和漏洞而影响应用系统可用性的安全风险；

2.2 安全需求

（1）针对监测系统漏报和误报的安全风险，需要在灾害监测系统具备监测点及传感器状态检测功能，可以对各数据采集节点的运行状态进行实时检测，同时采用双缓冲机制和负载均衡技术降低误报和漏报的风险；

（2）针对故障导致灾害监测系统中断运行的安全风险，需要在铁路局中心机房内部署机房环境监控系统，对核心服务器的运行状态、重要性能指标、网络设备性能、应用软件或进程的状态进行监控并及时报警；

（3）针对人为因素导致灾害监测系统中断运行的安全风险，需要建立完备的备份机制，在对服务器或软件进行升级时，需保证灾害监测系统的零时和无缝切换；

（4）针对自然环境威胁引起的安全风险，需加强对户外监控采集设备的防雷和防水保护，加强铁路局中心机房环境的防雷、防火、防盗、防电磁泄露等保护；

（5）针对病毒和恶意攻击导致的安全威胁，应加强灾害监测系统网络边界的安全防护，并建立有效的防病毒机制；

（6）针对应用软件可能存在的安全缺陷，需在应用软件研发和设计时从数据校验、资源控制、通

信保密、访问控制和安全审计等方面考虑应用系统的安全性。

3 安全架构设计

安全架构指提供系统软硬件方面整体安全性的所有服务和技术工具的总和，安全设计涉及系统的各组成部分，具体内容包括物理安全、网络安全、主机安全、应用安全和数据安全，灾害监测系统安全架构如图 2 所示。

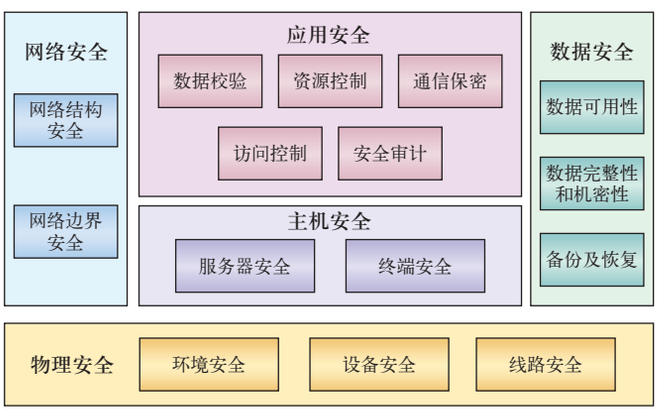

图2 灾害监测系统安全架构

4 设计方案

灾害监测系统安全设计可按照物理安全、网络安全、主机安全、应用安全和数据安全进行设计。

4.1 物理安全设计

灾害监测系统物理安全设计可从环境安全、设备安全和线路安全 3 个方面进行设计。

4.1.1 环境安全

环境安全包括环境条件安全和基础设施安全。保障环境条件安全应考虑火灾、水灾、爆炸以及其他形式的自然或人为灾害，系统监测设备如雨量监测设备、风速监测设备等一般位于户外，并安置于自然灾害频发地段，应充分考虑各个监测点的地面环境，监测设备应有专门的防雷电和防水等措施；

保障基础设施安全需要部署机房环境监控系统，使机房温度、湿度的变化在设备运行所允许的范围之内。所有的网络设备（包括交换机、路由器、服务器、防火墙等）都需设置物理保护，不能随意让人接触，相关主机和设备都应统一编号，定期进行维护；机房供电线路上应配置稳压器和过电压防护设备。

4.1.2 设备安全

在灾害监测系统中，设备选型上选用高可靠性硬件设备，数据库服务器采用双机热备方式配置，以确保主机的高可用性，数据存储采用逻辑卷镜像的双智能存储，以确保数据的高安全性，应用服务器采用负载均衡方式配置以确保业务的高连续性。

4.1.3 线路安全

线路安全包括电缆安全、光缆安全和供电安全。电源电缆是提供设备电力供应的保证，在灾害监测系统建设中，通信设备的电源线和通信线路设计采取地下暗线布放方式；光缆安全根据不同的环境采取不同的防护措施，在白蚁和昆虫啃啮地段采用防蚁光缆，在特殊地段如水底采用水底光缆接头盒，同时在设计施工时需考虑防止机械损伤、防强电、防雷电和防潮。

4.2 网络安全设计

4.2.1 网络结构安全

网络结构安全是指在网络结构设计上避免单点故障，灾害监测系统在网络结构上使用双星型网络冗余结构，如图 3 所示。

网络在结构上分为主用和备用链路，监控单元通过防灾专网接入车站的主备链路接入层交换机，各车站主备链路接入层交换机通过防灾专网主备用专用通道与铁路局中心核心交换机互联；既有防灾系统监控数据处理设备与铁路局中心系统、相邻铁路局中心系统间、中国铁路总公司复示终端与铁路局中心系统间、行车调度与工务终端间网络通信链路均采用上述主备链路通信方式来避免单点故障。

4.2.2 网络边界安全

网络边界安全包含系统内部不同区域间的边界安全和灾害监测系统与外部系统间的边界安全。

系统内部不同区域间的边界包括铁路局中心系统与相邻铁路局中心系统间、既有防灾系统与铁路局中心系统、中国铁路总公司复示终端与铁路局中心系统、行车调度与工务终端间的网络边界，此类边界安全防护采用的设计方案如下：

（1）在网络出口、服务器区域及其他重要网段等各边界部署防火墙类边界隔离设备，对网络边界或区域逻辑隔离，实现网络层的访问控制；

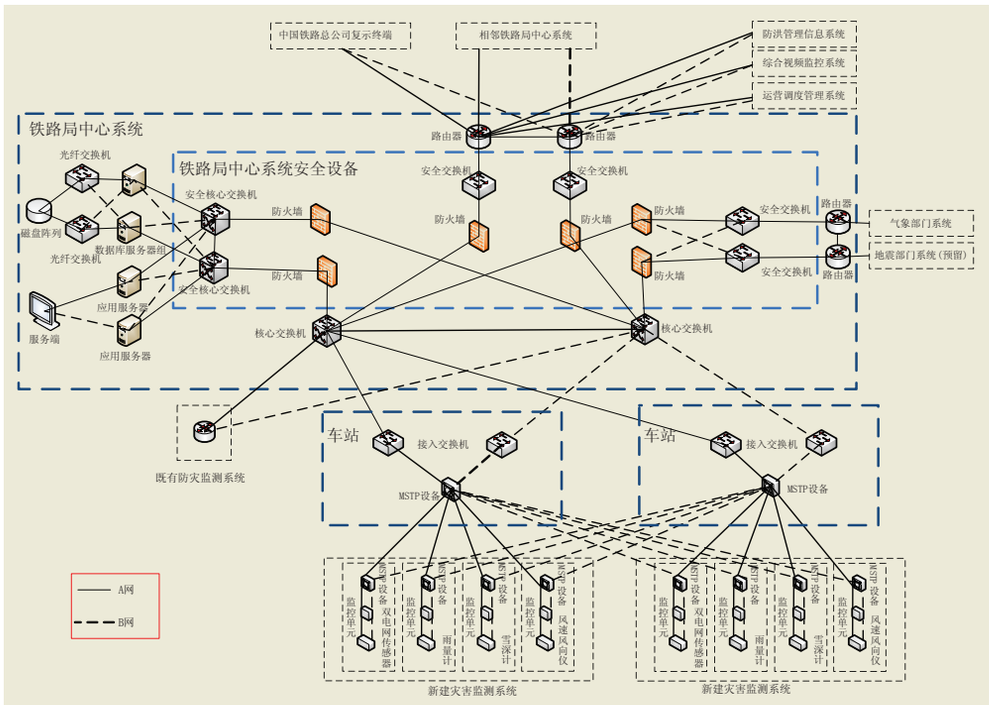

图3　灾害监测系统双星型网络结构

（2）在网络边界部署防病毒网关，在服务器、终端设备上安装防病毒系统（要求与防病毒网关具有不同的恶意代码库），同时在铁路局中心部署防病毒升级服务器，保持系统补丁及时得到更新，支持病毒库的统一管理；

（3）在网络中的关键点部署入侵检测系统（IDS）或入侵防御系统（IPS）实时监控和分析网络数据流及网络行为，即时发现各种恶意和可疑行为，提供及时的报警及响应。

与外部系统间的边界包括铁路局中心系统与综合视频监控系统间、省气象局气象观测网间、时钟同步系统、防洪管理系统、CTC 系统等外部系统的边界。为保证防灾专网和其他信息系统网络的相对独立，可采用网闸方式对各业务系统网络进行有效隔离。网闸是通过阻断各业务系统网络的直接连接，将原始数据以非网络连接的方式传送，使隔离机制传输具有不可编程性，使通过网闸的任何数据都不具有攻击和有害特性，在较高程度上保证了不同业务系统间的边界安全。

4.3　主机安全设计

主机安全是指铁路局中心灾害监控系统中的主机、桌面终端的安全，具体包括操作系统、中间件和数据库系统的安全。

（1）选择相对安全的操作系统、中间件和数据库系统，对主机系统进行必要的加固；对关键服务器和工作站均采用服务器版本的操作系统；

（2）应将主要服务器的性能指标纳入机房监控系统的监测范围，监测指标包括服务器的 CPU 利用率、内存、磁盘空间、重要进程运行状态、数据库运行状态等，防止因服务器宕机或应用服务停止造成的应用系统不可用。

（3）对操作系统、应用系统和数据库系统的用户进行有效管理，禁止缺省口令和弱口令。

（4）操作系统应遵循最小安装原则，仅安装需要的组件和应用程序，保持系统补丁及时得到更新。

（5）采用漏洞扫描技术对操作系统进行加固，在铁路局中心防灾专网中部署主机漏洞扫描设备，对专网中的主机和数据库进行自动发现、识别，根据其类型采取相应的漏洞扫描手段进行扫描，发现系统在安全策略配置上的漏洞和不合理处，并提供全面的报表和查询功能，在漏洞扫描的基础上对主机进行安全评估和加固。由于主机扫描时会产生大量的会话，为避免影响防火墙性能，不建议漏洞扫描产品跨骨干网和跨防火墙操作，一般部署于铁路局中心防灾内部局域网。

4.4　应用安全设计

灾害监测信息系统无论是采用 B/S 结构还是 C/S 结构，都要防止应用系统中用户数据的丢失、修改或滥用。应用系统安全设计可以从数据校验、资源控制、通信保密、访问控制、安全审计 5 个方面进行考虑。

4.4.1　数据校验

在对应用系统设计时应考虑对数据的有效性进行验证，如通过人机接口（程序界面）输入或通过

通信接口输入的数据格式或长度是否符合系统设定要求，防止个别用户数据畸形数据而导致系统出错（如：SQL 注入攻击）。

4.4.2 资源控制

在应用系统设计时应考虑当通信一方在一段时间未做任何相应，另一方应能自动结束会话，并且该时间应能进行配置，同时应考虑采取措施对最大的并发会话连接数进行限制，该数据应能进行配置。

4.4.3 通信保密

在应用系统设计时，与外部信息系统的通信应采用加密协议，如 SSL、HTTPS 等安全协议。

4.4.4 访问控制

在应用系统设计时，应考虑具备管理员权限的用户可以通过应用程序灵活定制某个用户对应用系统数据库表、进程、功能模块等的访问控制权限。

4.4.5 安全审计

在应用系统设计时，应考虑具备审计功能，对登录日志、操作日志、应用系统日志、异常事件等应能进行记录和审计，发生安全事件时应能进行报警。

4.5 数据安全设计

灾害监测系统的数据安全应根据系统的特点，从数据的可用性、数据完整性和保密性、数据备份和恢复等方面进行设计：

4.5.1 数据可用性

数据的误报和滥报：灾害监测系统处理的数据主要为采集监测点的报警类数据，该类数据具有访问不确定、随机性较大，数据量大的特点，采用双缓冲机制处理抖增类数据，接收到此类数据时，先将其放置在缓冲区中进行预处理，对重复数据和异常数据进行过滤和筛选，再将其复制至另一缓冲区进行正式处理后上报上级系统，最大可能防止数据的误报和滥报。

数据的漏报：（1）可能是攻击或 DDoS 攻击而导致服务器充斥大量要求回复的信息，消耗网络带宽或系统资源导致网络或系统不堪负荷以至于瘫痪而停止提供正常的网络服务，监测点无法及时将监测数据上报至铁路局中心系统，设计时可以考虑在铁路局中心防灾系统专网内部署主机入侵检测系统，防止恶意攻击；（2）服务器、操作系统、应用软件的升级或更换导致服务不可用，设计时可考虑采用负载均衡方法，当其中一套应用服务（包含应用服务器、数据库服务器等）暂时不可用时，另一套应用服务依然可用，实现升级过程中的无缝和零时切换，避免监测数据的漏报。

4.5.2 数据完整性和保密性

对数据库中存储和传输的数据应有完整性校验措施，可采用 MD5 算法对存储和传输数据进行完整性校验；对数据库中的敏感数据采用加密算法进行加密存储。

4.5.3 备份和恢复

通过专用的备份恢复软件，结合利用网络备份手段对灾害监测信息系统的重要主机、数据库服务器进行备份，并制定相应的备份恢复策略；对重要服务器采用 RAID 方式冗余磁盘阵列提供容错恢复。

5 结束语

本文的安全架构设计方案从环境安全为灾害监测系统安全提供了物理基础，从网络安全保障了通信数据的传输，从主机安全保障了系统的运行环境，从应用安全加强了系统安全审核机制，从数据安全方面加强了系统对数据的过滤。由于系统加强了对无效、非法以及重复数据的过滤，在提高安全的同时也提高了系统的处理性能。随着灾害监测系统在各行业的进一步应用，结合特定应用场景的安全架构设计是后续的研究方向。

参考文献：

[1] 中华人民共和国国家质量监督检验检疫总局，中国国家标准化管理委员会 .GB/T 22239–2008， 信息安全技术—信息系统安全等级保护基本要求 [S]. 北京：中国标准出版社，2008.

[2] 王 瑞，喻麒睿，王 彤 . 高速铁路灾害监测系统优化升级 [J]. 中国铁路，2013（10）：17-20.

[3] 李晓宇，张 鹏，戴贤春 . 高速铁路自然灾害及异物侵限监测系统运用及管理优化研究 [J]. 中国铁路，2013（10）：21-25.

[4] 张卫军 . 防灾监控系统在高速铁路中的应用 [J]. 铁道通信信号，2010，46（6）：80-81.

责任编辑 方 圆