城市轨道交通信号系统的信息安全

龚一民　陈先宽　张国锋
浙江众合科技股份有限公司　浙江　杭州　310051

摘　要：近年来，随着我国社会水平的不断发展，城市基础设施也不断完善，城市轨道交通是最重要的城市基础设施建设项目之一，其投资风险大、投资周期长、投资多等多方面的特点。轨道交通信息化进程虽然取得了一定成绩，但系统中存在的信息安全风险管理还停留在浅层信息管理层面，浅层信息管理如何纳入深度学习管理，这已成为当前公交建设的重要任务之一。本文旨在识别轨道交通信息系统中存在的信息安全风险，并进行相关介绍，希望对判断轨道交通信息系统的安全起到重要作用。

关键词：城市轨道建设；信号系统；风险辨识；信息安全应用

引言

近年来，我国开展城市现代化建设，注重区域经济一体化和协调发展，城市交通网络建设为区域复合发展奠定了坚实基础，拉动了城市经济的强劲发展。城市轨道交通信号系统的建设是当前交通结构的重要组成部分，可以保证列车有序运行，保障列车运行安全。它是一个综合高效的自动化系统，该系统的影响直接影响到列车运行的效率，值得高度重视，不容忽视。随着科学技术的飞速发展，城市轨道交通信号系统的技术也在不断提高，特别是计算机信息技术的应用开辟了新的机遇。在未来的轨道信号系统建设中，我们将着眼于系统的智能化设计，以实现交互，做好高层次设计，完善轨道交通信号系统。

1 城市轨道交通信号控制系统的优点

（1）城市轨道交通信号系统是一个完全独立的系统，不需要与其他设备连接，可以独立工作，其独立性便于安装和调试。

（2）轨道交通信号控制系统不同于其他系统，它包括双向传输，还可以进行大量数据的传输。

（3）城市轨道交通信号系统中包含了一个非常有趣的结构——闭塞，通过路障的移动可以缩短两列列车之间的距离，有利于提高行车安全和行车速度。

（4）该系统可以远程控制列车，自动化程度高，可以在不依赖大量人力资源的情况下提高服务质量。

（5）该系统还有一个非常高的品质点，那就是它可以控制每辆列车之间的运动，保证运动的安全，提高列车运行效率[1]。

2 城市轨道交通信号系统运行中存在的风险

2.1 安全政策规范欠缺，安全意识薄弱

从当前的城市轨道交通领域来看，必须改进安全管理。从目前的工作可以看出，大部分地铁线路在信息安全管理和系统架构方面的安全问题还没有完全解决。同时，在实践中，项目的设计、开发、运维等方面缺乏行之有效的信息安全标准。它涵盖了各种主题，包括驾驶安全方面以及员工的安全意识。因此，企业和员工提高这方面的安全风险意识非常重要。

2.2 生产系统终端管理不完善

从城市轨道交通信号系统的工作情况来看，部分终端设备没有安装杀毒软件，没有及时进行更新。包括USB方面也没有落实好有效的封锁，从而导致了USB的违规使用问题。在这个通过USB设备进入病毒的时代，很容易危及整个系统设备，从而对系统性能产生不利影响。另外，一些终端设备后，还存在安装工作不需要的软件的问题，应及时解决。

2.3 不可抗拒风险

轨道交通信号系统运行中不可避免的风险主要体现在两个方面：主要软硬件的非常规后门、关键设备的运维风险：首先，从前者来看，信号系统的关键软硬件设备大都是国外的产品，也有国外的生产厂掌握着核心技术，因此，便加剧了非常规后门的风险。其次，从后者来看，我国目前在系统维护方面，同样十分依赖国外的厂商，基本上不具备自主的维护能力。对此，就这一问题而言，国外的连续外包服务可靠性其实是无法保障的，一旦出现了国外厂商的服务停止，便会导致设备的无法更新和无法维护[2]。

3 信息安全技术的种类

3.1 加密技术

当前，为了确保网络的安全性，需要采用密码技术。通常，不同的密码技术可以适应不同的用户不同的需要。密码技术，简而言之，就是将被加密的文件，用

一个以密钥为参数的一个加密函数进行转换，使它成为一个没有任何意义的文件，当对方成功地收到了该文件，再将该密码解密，就可以获得原来的内容，从而防止了文件数据信息的泄漏，也可以增加了文件数据信息的保密性和精确度。

3.2 防火墙技术

防火墙技术，简而言之，就是一种可以允许商务交易，也可以禁止商务交易的网络通信安全技术，它可以提高网络的安全性，防止侵扰和病毒入侵。防火墙是两张网间的一道防栏杆，可以按照安全规划的战略来保护网后的安全。在我们的生活中，防火墙的地位与功能就像是一扇安全大门，起到了保护大门内部安全的作用。

4 信号系统内信息安全的设计

4.1 应用的访问控制和接入认证安全设计

在保护系统和应用系统的同时，将现有的用户名称/口令的存取控制机制提升为双重验证机制，实现了存取保护和使用控制两方面的保障。目前，该技术已十分成熟，并被大量地用于金融，安全等领域。在使用该技术的过程中，需要考虑到运行规则和习惯的要求，并对其进行优化，在突发事件下，可以通过调度人员对其进行临时调整。当前可用的生物鉴别技术有人脸鉴别，虹膜鉴别，指纹鉴别等。尤其对于一个远端装置来说，需要经过两个/多个系数的验证[3]。

4.2 数据的安全设计

其中的重要数据有：①访问验证/身份验证数据，例如：使用者名称/口令，私钥，密钥，生物资料等；②主要应用程序的组态资料，如行资料库、应用程式组态档案等；③用户名、操作权限等系统管理信息；④重要的商业资料，例如运营进度表，运营日志等。为确保重要信息的安全性，对信号系统的软件进行了密文保存和完整性检验。首先，该系统将密钥数据以密码方式保存，使得黑客在入侵过程中，无论是否入侵计算机、是否入侵存储媒体，都不能获得密钥，也不能从中获得任何有用的信息，从而对该信号系统造成更大的伤害。其次，由于该密钥信息在被保存时带有MAC代码，所以只能通过一般的MAC认证来获取密钥信息，从而对密钥信息的篡改和破坏进行预警。对重要的资料，利用媒体周期性的备份或异构的异构储存，在资料被篡改或破坏后，可以即时复原。

4.3 安全防护体系设计

目前，在城市轨道交通信号的系统设计中，因为其实质上是一种对数据传输系统的控制，所以在建立网络时，必须以独立的专用网方式来进行。其次，在进行信号系统的安全保护制度的设计时，也要充分运用工业控制防火墙，确保与其它网络系统之间的安全隔离，然后根据安全策略的设置，对各部分的数据进行有效的隔离和处理。然后，以系统的安全策略为依据，对数据信息的传输进行了合理的控制，划分出了不同的权限，并实现了良好的禁止。其次，对于与其它网络进行信号隔离的过程中，必须建立起一道安全的、安全的防火墙。这种防火墙的设定，是要保证信号系统具有很强的独立性，不容易受到其它因素的干扰，使其系统能够实现独立性，完善性，在信号传送时，保证流量数据信息，并在异常流量进入信号系统网络时，进行针对性的处理。信号系统的整个构建过程，其在网络边界的工控防火墙上的部署，就是根据最小通过性原则，一种响应的系统部署。在此基础上，根据不同的商业要求，对这份白名单做了一些改进。合理的开发几个IP，并对对应的端口进行合理的配置，并对其进行严格的监控[4]。

5 信息安全技术在轨道交通信号系统中的应用

5.1 通信网络安全数据传统

除在可靠的网络之间扩散外，还可能在不可信的网络内部扩散。这是怎么回事？事实上，由于传统的信息系统是以一种闭合的方式进行设计的，所以它具有很好的可靠性。其中，无线通信系统主要由综合接收网，无线通信系统等组成。针对低信度网络中的信息传递问题，本项目拟采用基于数字密码技术的动态验证技术，以保证信息传递的保密性和通信的正确性。密码体制主要有两种：aescc和aessccm。在这种情况下，可以通过缓存的密码算法来选择密钥的长度。密码系统的安全性能除了依赖于密码系统自身之外，还依赖于密码系统的可靠度。以技术方式参加密钥的发展，分发，更新，销毁，都要受到诸如ikve2，srp6这样的密钥交换协定的限制。

对网络设备，主要设备及安全设备进行检查，以确保其安全。对网络设备的操作信息进行常规的采集和检查，比如交换机、数据流和运行状态信息，对管理员登录、事件列表和改变硬件配置进行控制，对处理器、内存利用率和端口状况进行检查。而对企业内部网络进行的安全检测，则是对企业内部网络网络的运行状况、非法访问端口、恶意扫描等方面的检测。铁路信号采用了ICT技术，预警和网络安保体系得到了进一步的改进。将其划分为三个层次：网络安全性，通信完整性，网络安全性。以上所提到的方法，主要是针对某些非法使用者，当他们进入本地网路时，由于密码体制的干扰而不能进入本地网路。在进行数据和信息的传递时，必须保证其安全。所以，必须在传送协议中加入安全性协议。

安全连接、数据传输和连接释放都是安全的。而建立安全连接，最大的作用就是避免某些非法用户进行连接[5]。

通常，安全层在接到请求后，都会进行一次验证，如果对方的身份没有问题，那么就会与对方建立联系，如果对方没有问题，那么就会被拒绝。为了保证资料的安全性和完整性，必须保证资料的安全性和完整性，必须保证资料的安全性和完整性。在确保资料完整的前提下，不会产生任何的差错。释放安全连接说明这一个层级是可以随时做好安全连接释放工作的，但不需要进行特别的防护。在实际应用中，应用最广泛、最可靠的技术之一就是使用失效分析技术。该方法是在发生了故障以后，一步一步地寻找可能产生故障的原因，进行分析，确定故障和事件之间的关系。该故障诊断系统不但可以完成对故障的检测，分析故障产生的原因，并给出相应的解决方法，而且可以在解决了故障之后，对全部的信号装置都可以进行监控和诊断，从而避免相同的故障的再度出现。适时判断信号设备的工作状况进行表述，根据信号设备的故障概率修正健康指标，评估和计算未来信号设备事故，确定信号设备故障的严重程度，模拟风险监控。通过对信号设备运行状态的评估，及时发现缺陷并进行风险评估，根据评估结果确定风险因素。评估系统的管理层必须提交验证报告，其中必须包括系统审查、技术规范、安全证书等。

5.2 ATS中的网络安全

ATS系统是列车正常运行专线的核心技术，是铁路客运专线的核心技术，也是铁路客运专线的核心技术。然而，对ATS系统造成的危害主要表现在以下两个方面：一是系统的测试、维护和修改工作必须在实际操作中不断地改进和改进；然而，由于工作人员有可能错误地连接设备，或是做了一些违法的事情，导致系统被病毒侵入，从而导致系统失效，从而对列车的正常运营和列车的调度和控制的安全造成了严重的影响；另外就是，尽管ATS网络系统属于一个相对封闭的私人网络，但该技术的实施的依据是它要对所有的网络用户开放，而且可以通过网络来进行资源共享。因此，要想有效地防止对ATS网络系统造成的风险，就要在调度中心、车站之间等处使用防火墙技术和入侵检测系统，并且在系统中添加实名认证和漏洞评估子系统。这种方式不但可以有效的控制系统的整体权限以及对资源的存取，而且还可以防止任何的病毒侵入，从而达到保护系统的目的。

6 结束语

二十一世纪是一个信息化的年代，自动化、智能化技术得到了很好的发展，并在各个主要的产业中得到了很好的运用，在城市轨道交通的信号体系中，应该顺应时代的发展要求，对其进行技术创新，将现代化的计算机信息技术运用到极致，引导其朝着智能、完全自动化的方向发展，运用大数据技术，对其进行高效的信息采集、分析，从而达到数据的共享。随着我国铁路建设和运营水平的不断提高，可以强化对城市轨道交通信号系统新技术发展的研究，让它的技术变得更为完善，方便推广和应用，这对于引起一次城市轨道交通技术变革，与时代发展的需要相一致，还可以为智慧城市轨道交通的实现打下坚实的基础，因此，它有着非常重要的意义。

参考文献

[1]张宝全，黄祖源，周枫.智能电网信息安全威胁分析及防御研究[J].软件导刊，2020，17(2):189-191,194.

[2]孙守胜.城市轨道交通信号系统新技术发展前景[J].电子技术与软件工程，2020(24)：33-34.

[3]徐鑫,焦凤霞.基于通信的列车控制系统（CBTC）互联互通测试方案设计与实现[J].铁路通信信号工程技术，2020，15(11)：58-62.

[4]杨春妮,陈帅.城市轨道交通信号系统的风险分析[J].通讯世界,2020(3):11-12.

[5]樊亚丽.城市轨道交通信号系统能力分析及优化措施[J].轻松学电脑,2020,000(026):P.1-1.