TMIS 安全问题及解决方法

胡蔷

TP3 B

摘 要：分析了TMIS建设中遇到的安全问题，探讨了相应的解决措施。
关键词：铁路 信息 系统 安全 措施 方法

Security Problems of TMIS and Solution to them

HU Qiang
(Information Technology Department of Railway Administration Huhhot,Huhhot,010050)

Abstract: It was analyzed the security problem which may exist in the structure of TMIS , gave solution to them
Keyword: Railway Information System, security problem, solution

1 引言

TMIS 是一个构筑在计算机数据通信网上的应用系统，这一系统中传输数据的安全性直接影响到铁路运输的生产组织和正常运营。影响系统安全性的因素主要有以下几个方面。

2 影响 TMIS 安全的因素

2.1 系统工作环境

系统工作环境遭到破坏的因素主要有 2 个方面：自然不可抗拒力（如洪水、地震、火灾等）；人为的破坏。因此，TMIS 计算机运行环境必须考虑如何避免这两种因素的影响。

2.2 数据完整性

由于数据本身丢失或被窃取、失密、编（解）码或处理错误可能会造成数据错误或不完整。其后果表现为信息丢失；信息处理无法及时进行；密码失密导致货物被冒领等。

胡 蔷 呼和浩特铁路局信息技术处 工程师 010050 呼和浩特市

2.3 数据传输中断及网络入侵

对于TMIS 而言，网络设备故障或者是人为入侵，影响数据的传输，造成铁路运输生产无法正常进行，严重的恶意入侵甚至可能导致系统遭到破坏。

2.4 操作失误和权限控制失误

操作失误的原因来自 TMIS 操作人员业务不熟练或者操作权限管理的失控，后者容易为恶意入侵者造成可乘之机。

2.5 业务管理漏洞

除技术和设备上的问题外，由于 TMIS 中涉及到有价的信息流和物流，管理上的漏洞也可能造成直接的物质损失，具体表现为站车交接过程中货物的遗失、监守自盗和冒领等。为此，必须在技术上采取有效安全手段的同时辅之以各种管理措施来提高系统的安全可靠程度。

2.6 计算机病毒入侵

计算机病毒在TMIS 上的扩散可能导致主机系统丧

员缺乏计算机基础知识的实际情况，对他们进行基本操作、基本原理的培训，从而杜绝违章操作，减少人为因素造成的设备故障或损坏。

（2）加强维护管理人员的培训：目前站段主机房值班人员中，有相当一部分人员来自其它生产岗位，有的只经过简单的专业培训，有的甚至未经过专业培训。针对这些实际情况，应适当增加办培训班的次数，使他们尽快熟悉业务，掌握技术。

3.3 设立地区性 TMIS 设备维修站

针对站段计算机维修人员少、技术力量薄弱的问题，设立地区性维修站，这样做不但可以解决设备维修时由站段到路局的设备运输问题，还可以集中技术人员和维修设备，提高设备维修水平。

3.4 健全激励考评机制

通过制定实施《维修人员工作量量化考核办法》，把维修人员的工作量与奖惩挂钩，加大考核力度，激发有关人员的工作热情。同时严格落实设备操作规程及各项制度，确保设备的正确使用，强化日常设备的保养，减少故障的发生。

4 结束语

提高 TMIS 设备的维护和维修水平，可以提高站段 TMIS 设备的可靠性、安全性、经济性和综合效益，更好地为铁路运输服务。

（收稿日期：2002-08-20）

失运行能力，客户端的病毒程序则可能造成数据不完整或破坏操作系统。这一方面的威胁主要来自于非法软件的复制，操作人员非工作性的操作（如游戏、安装其他程序），下载基础数据的病毒感染等。

2.7 其他

由于密钥、条码在信息系统中广泛使用，这些新技术本身也存在新的管理问题。密钥失控导致错误、条码由于破损而无法正确阅读等。所以在考虑运用新技术的同时必须为技术运用后的安全问题提供解决措施。

3 安全措施

通过前面对可能威胁系统安全性的因素分析，提出以下的解决措施。

3.1 环境安全

在系统环境建设时，必须依据国家、铁道部及IT行业的标准。设计中应考虑提供照明、动力系统峰值调整、双路后备电源、灾难发生后的隔离等措施，保证系统在运行时，有平稳的动力、良好的温度和湿度。还应考虑针对突发灾难性事件的措施，包括防火，防雷电，防静电，防水和抗干扰设计等。

3.2 数据安全

为了保证数据的完整性和一致性，在硬件设备上考虑TMIS的各联网节点中采用主备计算机双机备份，存储设备的磁盘镜象和RAID5技术。

对涉及系统运行的核心数据本身进行加密操作是保证数据安全的重要手段。要对站间交换的数据及上报的财务数据进行加密，其标准应满足铁道部要求或遵循DES等行业标准。

系统的数据存取权限必须严格分级控制。对于电子数据的存取采取操作人员身份认证和读写权限的多级控制。对重要数据的处理采用联机事务处理（OLTP）技术，支持事务提交及事务失败后的回滚(rollback)。

3.3 网络安全

网络安全措施包括网络传输安全，网络访问控制和网络设备备份措施。

站间交换及汇总上报数据的传输采用加密技术，避免明码传输。对于基于socket的C/S应用程序的请求应答使用特殊服务端口。

所有网络节点的局域网和广域网均采取隔离措施，LAN上的所有主机应采用内部虚拟IP，并透过代理服务器(Proxy Server)访问WAN。LAN和WAN之间必须设置防火墙(Firewall)，限制WAN上可访问LAN上有关主机的外部IP。

系统数据通信网必须留有一定的备用设备，对系统的数据通道需留有冗余路由。有条件的车站，可以使用双数据通信线路，以保证系统通信设备发生故障时能够尽快更换。此外，对于系统的路由设备，建议尽量采用模块化的结构，以保证系统故障时能通过相关模块的更新来提高系统的可靠性。

3.4 应用系统的安全

应用系统安全措施主要包括操作人员身份认证，业务操作权限控制，操作维护日志管理，密钥管理和应用系统版本控制等方面。对操作人员进行身份合法性验证，可以采取口令认证，IC卡认证和数字签名(Digital Certification)等方式进行交叉验证。对系统各级作业人员的操作权限进行严格划分，各类人员只能完成其业务权限内的操作。

对所有涉及系统数据增加、修改和删除等更新操作，必须严格地记录系统操作日志，记载操作动作，内容，更新前后数据的状态，操作日期时间和操作人员，并以流水方式记录操作日志，禁止对操作日志的修改，使操作日志成为TMIS的“黑匣子”，以便在系统发生故障后，能够明确划分责任。

由于系统的认证过程均采用密码认证，所以密码、密钥的生成，分发需要统一管理。建议系统建设中对密码、密钥采用X.400或DES标准，并由路内密码管理机构统一管理其分配。

版本控制包括应用程序及相关参数的版本发行，版本使用周期和版本测试等方面，从而使整个系统的应用软件保持一致的版本。

3.5 安全措施

业务安全措施是对技术安全手段的必要补充。具体包括：防伪，安全条例，计算机系统安全技术审查和定期审核等。

对TMIS有价票据需要采用特殊的票底，票底需要有专门底纹，并按铁道部规定制作打印其字体、字型和条码。在车站交接班管理以及代理点管理中要严格票卷管理，建立票据领用制度。

为保证系统的安全性及可靠性，对TMIS的安全检查和系统维护必须制定有关条例，并严格依据条例进行工作。

对TMIS各子系统的建设和实施上线必须执行系统安全技术审查，未通过安全技术审查的禁止上线运行。此外，系统投产运行后，对系统安全需要建立定期审核（如年检）制度，对上线后的系统如不满足安全审核要求，需要限期整顿。

4 结束语

综上所述，加强系统的安全，提高系统的可靠性并非单一的技术措施可以达到的，需要加强管理并采用多种措施以确保系统的安全。

（收稿日期：2002-08-20）