ICS 35.040
R07

JT

中华人民共和国交通运输行业标准

JT/T XXX—XXXX

交通运输行业信息系统安全等级保护基本要求

Basic requirement for security classified protection of transportation information system

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国交通运输部　发布

目 次

前　言

本标准按照GB/T1.1-2009给出的规则起草。

本标准由交通运输部科技司提出。

本标准由交通运输部信息通信及导航标准化技术委员会归口。

本标准起草单位：中国交通通信信息中心。

本标准主要起草人：李璐瑶、戴明、武俊峰、成瑾、肖榕、刘佳、王梓博、杜渐

交通运输行业信息系统安全等级保护基本要求

1 概述

1.1 目的

本标准规定了交通运输行业不同安全保护等级信息系统的基本保护要求，既应具备的最低安全能力，适用于指导分等级的信息系统的安全建设和监督管理。

1.2 范围

包括该技术指南适用的行业单位范围、系统范围、适用工作过程范围等。

1.3 术语

GB/T 5271.8 和 GB 17859-1999 确立的以及下列术语和定义适用于本标准。

安全保护能力 security protection ability 系统能够抵御威胁、发现安全事件以及在系统遭到损害后能够恢复先前状态等的程度。

1.4 引用文件

交通运输行业信息系统信息安全等级保护基本要求的编制主要依据以下标准：

《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）

《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）

《信息安全等级保护管理办法》（公通字[2007]43 号）

《关于开展全国重要信息系统安全等级保护定级工作的通知》（公通字[2007]861 号）

《信息安全等级保护备案实施细则》（公信安[2007]1360 号）

《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号）

《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技[2008]2071 号）

《计算机信息系统安全保护等级划分准则》（GB17859）

《信息安全技术 信息系统安全等级保护定级指南》（GB/T22240-2008）

《信息安全技术 信息系统安全等级保护实施指南》（GB/T25058-2010）

《信息安全技术 信息系统安全等级保护基本要求》（GB/T22239-2008）

《信息安全技术 信息系统安全等级保护测评过程指南》（送审稿）

《信息安全技术 信息系统等级保护安全设计技术要求》（征求意见稿）

《关于开展部重要信息系统定级备案工作的通知》

《关于进一步开展交通运输行业信息安全等级保护工作的通知》（厅科技字[2012]120 号）

2 编制原则

2.1 基本原则

交通运输行业信息系统管理、运营、支撑、服务交通运输行业业务，是我国重要的基础信息系统，建立与行业业务应用需求相适应的安全措施和方法，指导、规范、约束交通运输行业各应用信息系统信息安全建设，并以此为基础，建立交通运输行业信息系统信息安全保障体系，构建防护、监控、信任三

条安全基线，形成立体纵深防御、安全时效的信息安全保障技术体系，使交通运输行业整体信息安全防护能力达到较高水平。

交通运输行业信息系统安全建设，需要遵循以下总体要求：

1) 遵循交通运输行业信息安全等级保护的相关标准和规范要求；
2) 按照本指南进行设计，保障系统结构完整，安全要素全面覆盖；
3) 安全建设是一个逐步完善的过程，各单位应依据本指南进行统一规划，在建设时可以根据信息化的发展逐步建设与完善。
4) 以本要求为基本要求，各单位在安全体系建设时，可根据具体信息系统的特点，适当调整部分安全要素要求，但不得低于本技术要求。

2.2 总体目标

交通运输行业信息系统安全保障建设的基本思路是：以保护信息系统为核心，严格参考等级保护的思路和标准，从多个层面进行建设，满足交通运输行业信息系统在物理层面、网络层面、系统层面、应用层面和管理层面的安全需求，建成后的保障体系将充分符合国家标准，能够为交通运输行业相关业务的开展提供有力保障。

安全保障体系建设的要点包括：

2.2.1 构建分域的控制体系

交通运输行业信息系统基本要求，在总体架构上将按照分域保护思路进行，本方案将交通运输行业信息系统从结构上划分为不同的安全区域，以安全区域为单位进行安全防御技术措施的建设，各个安全区域内部还根据安全需求的不同进一步划分了子安全域和三级安全域，子安全域和三级安全域的边界也采用了与一级安全域形同的边界安全防护措施，从而构成了分域的安全控制体系。

2.2.2 构建纵深的防御体系

针对交通运输行业信息系统分别从物理安全、网络安全、主机安全、应用安全通、数据安全及备份恢复等五大方面提出安全措施要求，保障交通运输行业业务应用的可用性、完整性和保密性保护，并在此基础上充分考虑各种技术的组合和功能的互补性，提供了多重安全措施的综合防护能力，从外到内形成一个纵深的安全防御体系，保障信息系统整体的安全保护能力。

2.2.3 保证一致的安全强度

将采用分级的办法，对于部署于同一安全区域的系统采取强度一致的安全措施，并采取统一的防护策略，使各安全措施在作用和功能上相互补充，形成动态的防护体系。

3 安全防护体系要求

3.1 总体防护层次

交通运输行业信息系统由部级、省级单位、市级单位三级单位构成，由于单位层级不同，在整个信息安全管理体系中发挥的职能与作用也不相同，应采用逐级递加的安全防护级别，不同级别系统安全保护等级不同。通过采用结构化的安全防护级别能够有效为三级单位构建一套覆盖全面、重点突出、节约成本、持续运行的结构化安全防御体系。

3.2 部级单位防护体系建设要求

部级（中交通信）通过对省级单位的信息采集、汇集实现船联网跨省级单位的船舶电子身份认证和数据交换等应用服务。

在业务系统受到破坏后，侵害的客体是公民、法人和其他组织的合法利益，即船舶运营业主、省级水运管理局，侵害的客观方面表现为：一旦信息系统的业务信息遭到入侵、修改、增加、删除等不明侵害（形式可以包括丢失、破坏、损坏等），会对船舶运营业主、两省一市的航运单位的合法权益造成侵害。侵害的客观表现为可以表现为无法客观、真实的对两省一市的船舶数据运营数据、航行数据、水上服务区、船舶加油站数据进行统计、分析、查询或敏感信息泄露等侵害，侵害的程度为严重损害，安全防护级别为第二级。

在系统服务受到破坏后，侵害的客体是社会秩序和公共利益，即船舶运营企业、两省一市，侵害的客观方面表现为：无法对两省一市辖区内的船舶实现跨省级单位的电子身份认证和数据交换服务，船舶运营业主无法实时了解其他省的航道信息，（如水位测量信息、实时天气信息、航行区域地理信息、航道障碍物信息、区域内河流、河运信息等）侵害的程度为严重损害，安全防护级别为第三级。

通过对业务信息安全等级（二级）、系统服务安全等级（三级）进行综合判定，确定市级单位安全保护等级为三级。

3.3 省级单位防护体系建设要求

省级单位包括 xxx 家单位，主要通过对 xxx 等应用服务，服务客体为公民、法人和其他组织。

在业务系统受到破坏后，侵害的客体是公民、法人和其他组织的合法利益，即船舶运营业主、省级水运管理局，侵害的客观方面表现为：一旦信息系统的业务信息遭到入侵、修改、增加、删除等不明侵害（形式可以包括丢失、破坏、损坏等），会对船舶运营业主、省级水运管理局的合法权益造成侵害。侵害的客观表现为可以表现为无法客观、真实的对省内船舶数据运营数据、航行数据、水上服务区、船舶加油站数据进行统计、分析、查询或敏感信息泄露等侵害，侵害的程度为严重损害，安全防护级别为第二级。

在系统服务受到破坏后，侵害的客体是公民、法人和其他组织的合法利益，即船舶运营业主、省级水运管理局，侵害的客观方面表现为：无法对辖区内的船舶实现跨市级单位的电子身份认证和数据交换服务，船舶运营业主无法实时了解省内其他城市航道信息，（如水位测量信息、实时天气信息、航行区域地理信息、航道障碍物信息、区域内河流、河运信息等）侵害的程度为严重损害，安全防护级别为第二级。

通过对业务信息安全等级（二级）、系统服务安全等级（二级）进行综合判定，确定市级单位安全保护等级为二级，鉴于省级单位重要性高于市级单位，省级单位的安全防护级别为加强型二级防护。

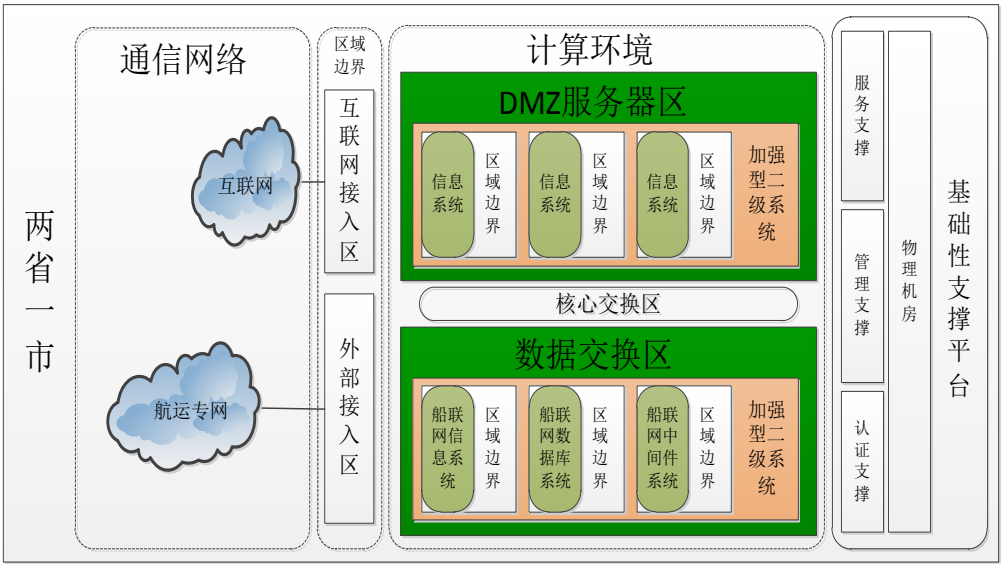

图 3.3 两省一市等级保护安全等级

3.4 市级单位防护体系建设要求

市级单位包括海口局、海事局、航道局等单位，主要采用船载智能终端通过在航道、航道沿岸、船闸、桥梁、水上服务区、船舶加油站、垃圾收集站、交叉点、港口等区域部署的 RFID 岸基设备接入船联网，为船舶提供身份认证、数据交换等服务，服务客体为公民、法人和其他组织。

在业务系统受到破坏后，侵害的客体是公民、法人和其他组织的合法利益，即船舶运营、海口局、海事局、航道局等单位，侵害的客观方面表现为：一旦信息系统的业务信息遭到入侵、修改、增加、删除等不明侵害（形式可以包括丢失、破坏、损坏等），会对公民、法人和其他组织的合法权益造成侵害。可以表现为船舶数据受到篡改或丢失、历史数据无法查询等后果，造成敏感信息泄露，侵害的程度为严重损害，安全防护级别为第二级。

在系统服务受到破坏后，侵害的客体是公民、法人和其他组织的合法利益，即船舶运营、海口局、海事局、航道局等单位，侵害的客观表现为：海口局、海事局、航道局等单位无法对辖区内的船舶进行有效管理，（如无法检测航道水位、闸口邻近船舶数量统计、船舶靠港码头信息等）。船舶运营业主无法实时了解航道信息，（如水位测量信息、实时天气信息、航行区域地理信息、航道障碍物信息、区域内河流、河运信息等）侵害的程度为严重损害，安全防护级别为第二级。

通过对业务信息安全等级（二级）、系统服务安全等级（二级）进行综合判定，确定市级单位安全保护等级为二级。

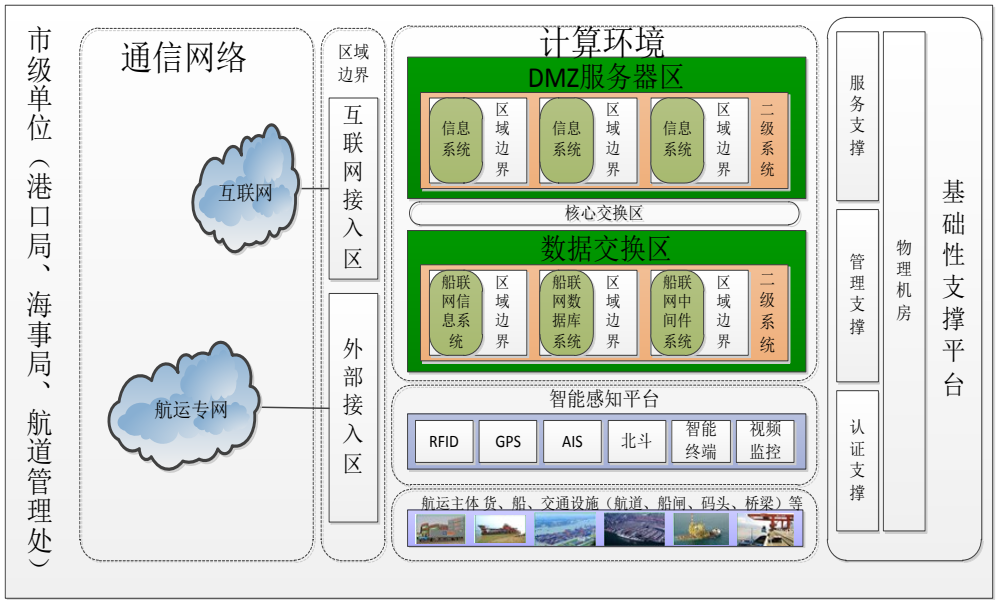

图 3.4 市级单位等级保护安全等级

4、基本技术要求

4.1 物理安全基本要求

4.1.1 物理位置的选择

本项要求包括：

a） 交通运输行业重要信息系统机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；

1） 应具有机房或机房所在建筑物符合当地抗震要求的相关证明；

2） 机房外墙壁应没有对外的窗户。否则，窗户应做密封、防水处理。

b） 交通运输行业重要信息系统机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。

1） 机房场地不宜设在建筑物顶层，如果不可避免，应采取有效防水措施。机房场地设在建筑物地下室的，应采取有效的防水措施；

2） 机房场地设在高层建筑物高层的，应对设备采取有效固定措施；

3） 如果机房周围有用水设备，应当有防渗水和疏导措施。

c） 交通运输行业重要信息系统配套的各种户外感知节点、数据采集终端等需要配备防雷击的装置，部署位置不再易塌陷地区或容易遭受水灾的位置。

4.1.2 物理访问控制

本项要求包括：

机房出入口应安排专人值守，控制、鉴别和记录进入的人员；

1） 机房出入应当安排专人负责管理；

2） 没有门禁系统的机房应当安排专人在机房出入口控制、鉴别和记录人员的进出；

3） 有门禁系统的机房，应当保存门禁系统的日志记录，采用监控设备将机房人员进出情况传输到值班点，并应记录外来人员进出机房的情况。

需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围；

1） 来访人员进入机房，应有审批流程，并记录带进带出的设备、进出时间、工作内容，并监控其在限定的范围内工作，并有专人陪同；

2） 机房出入口应进行视频监控，监控记录至少保留 3 个月。

应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；

1） 机房应当按照消防要求和管理要求进行合理分区，区域和区域之间设置物理隔离装置；

2） 机房应当设置专门的过渡区域，用于设备的交付或安装；

3） 重要区域包括：主机房、辅助区、支持区等功能区域。

重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

交通运输行业重要信息系统配套的各种户外感知节点、数据采集终端需配置防止非法人员操作的相关装置。

4.1.3 防盗窃和防破坏

本项要求包括：

a） 应将主要设备放置在机房内；

b） 应将设备或主要部件进行固定，并设置明显的不易除去的标记；

1） 主要设备应当安装、固定在机柜内或机架上；

2） 主要设备、机柜、机架等应有明显且不易除去的标识，如粘贴标签或铭牌。

c） 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；

通信线缆可铺设在地下、管道或线槽中。

d） 应对介质分类标识，存储在介质库或档案室中；

e） 应利用光、电等技术设置机房防盗报警系统；

f） 应对机房设置监控报警系统。

1） 应至少对机房的出入口、操作台等区域进行摄像监控；

2） 监控录像记录至少保存 3 个月。

g） 交通运输行业重要信息系统配套的各种户外感知节点、数据采集终端需具备防盗装置。（F）

4.1.4 防雷击

本项要求包括：

a） 机房建筑应设置避雷装置；

1） 机房或机房所在大楼，应设计并安装防雷击措施，防雷措施应至少包括避雷针或避雷器等；

2） 应具有经国家防雷检测部门年检合格的相关证明。

b） 应设置防雷保安器，防止感应雷；

c） 机房应设置交流电源地线。

d） 交通运输行业重要信息系统配套的各种户外感知节点需具备防雷击装置。（F）

4.1.5 防火

本项要求包括：

a） 交通运输行业重要信息系统机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；

1） 应至少达到 GB50174-2008 中 A 类电子信息系统机房设计规范的消防要求；

2） 机房的火灾自动消防系统应向当地公安消防部门备案。

b） 交通运输行业重要信息系统机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；

机房设备区域与其他区域的隔离材料应参照 GB50016-2006 要求，应达到耐火等级二级。

c） 交通运输行业重要信息系统机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

d） 交通运输行业重要信息系统配套的各种户外感知节点、数据采集终端需采用耐火材料制作。（F）

4.1.6 防水和防潮

本项要求包括：

a） 水管安装，不得穿过机房屋顶和活动地板下；

1） 与机房设备无关的水管不得穿过机房屋顶和活动地板下；

2） 机房屋顶和活动地板下铺有水管的，应采取有效防护措施。

b） 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

c） 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；

d） 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

e） 交通运输行业重要信息系统配套的各种户外感知节点、数据采集终端需具备在雨天正常工作的功能。

4.1.7 防静电

本项要求包括：

a） 交通运输行业重要信息系统**主要设备**应采用必要的接地防静电措施；

b） 交通运输行业重要信息系统机房应采用防静电地板。

机房的防静电活动地板应符合 GB6650《计算机机房用活动地板技术条件》。

4.1.8 温湿度控制

交通运输行业重要信息系统机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

1） 开机时机房温度应控制在 22℃-24℃；

2） 开机时机房相对湿度应控制在 40%-55%；

3） 停机时机房温度应控制在 5℃-35℃；

4） 停机时机房相对湿度应控制在 40%-70%。

4.1.9 电力供应

本项要求包括：

a） 应在交通运输行业重要信息系统机房供电线路上配置稳压器和过电压防护设备；

b） 应提供短期的备用电力供应，至少满足**主要设备**在断电情况下的正常运行要求；

1） 机房应配备 UPS；

2） UPS 实际运行供电时间不少于备用供电系统启动时间的 2 倍。

c） 应设置冗余或并行的电力电缆线路为计算机系统供电；

d） 应建立备用供电系统。

1） 应配备或租用发电机；

2） 发电机供电时间应不小于 24 小时。

e）交通运输行业重要信息系统配套的各种户外感知节点、数据采集终端需配有自供电系统。

4.1.10 电磁防护

本项要求包括：

a） 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；

1） 机房或机房所在的大楼必须有接地措施，并且接地电阻必须小于 1 欧姆；

2） 机房验收报告应提供合格的检测结果。

b） 电源线和通信线缆应隔离铺设，避免互相干扰；

电源线和通信线缆应铺设在不同的桥架或管道，避免互相干扰。

c） 应对关键设备和磁介质实施电磁屏蔽。

4.2 应用安全基本要求

4.2.1 身份鉴别

本项要求包括：

交通运输行业重要信息系统应采用统一的身份认证登录控制模块对登录用户进行身份标识和鉴别；

交通运输行业重要信息系统应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

1） 管理用户通过受控本地控制台管理应用系统时，应采用一种或一种以上身份鉴别技术；

2） 管理用户以远程方式登录应用系统，应采用两种或两种以上组合的鉴别技术进行身份鉴别。

交通运输行业重要信息系统应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

交通运输行业重要信息系统应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

交通运输行业重要信息系统应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

4.2.2 访问控制

本项要求包括：

交通运输行业重要信息系统应提供访问控制功能，依据安全策略控制用户对文件、数据库表以及各种感知节点等客体的访问；

交通运输行业重要信息系统访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；

交通运输行业重要信息系统应由授权主体配置访问控制策略，并严格限制默认账户的访问权限；

交通运输行业重要信息系统应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；

交通运输行业重要信息系统应具有对重要信息资源设置敏感标记的功能；

交通运输行业重要信息系统应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

4.2.3 安全审计

本项要求包括：

交通运输行业重要信息系统应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；

应用系统应能够对每个业务用户的关键操作提供记录，例如用户登录、用户退出、增加用户、修改用户权限等操作。

交通运输行业重要信息系统**应保证无法单独中断审计进程，**无法删除、修改或覆盖审计记录；

审计进程应作为应用系统整体进程中的一部分，并且不能单独中断。

审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；

审计记录应至少保存 6 个月。

交通运输行业重要信息系统应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

4.2.4 剩余信息保护

本项要求包括：

交通运输行业重要信息系统应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

交通运输行业重要信息系统应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

4.2.5 通信完整性

交通运输行业重要信息系统应采用**密码技术**保证通信过程中数据的完整性。

通过互联网、信息专网、无线短程通信网、GPRS 网、卫星网等网络进行通信时，应采用密码技术保证通信过程中数据的完整性。

4.2.6 通信保密性

本项要求包括：

a) 在通信双方建立连接之前，交通运输行业重要信息系统应利用密码技术进行会话初始化验证；

通过互联网、信息专网、无线短程通信网、GPRS 网、卫星网等网络进行通信时，建立通信连接之前，应用系统应利用密码技术或可靠的身份认证技术进行会话初始化验证。

b) 交通运输行业重要信息系统应对通信过程中的**整个报文或会话过程或关键报文**进行加密。

通过互联网、信息专网、无线短程通信网、GPRS 网、卫星网等网络进行通信时，应对整个报文或会话过程或关键报文进行加密。

4.2.7 抗抵赖

本项要求包括：

a) 交通运输行业重要信息系统应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；

原发证据包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录。

b) 交通运输行业重要信息系统应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

接受证据应用系统操作与管理记录至少应包括操作时间、操作人员及操作类型、操作内容等记录。

4.2.8 软件容错

本项要求包括：

交通运输行业重要信息系统应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；

交通运输行业重要信息系统应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

4.2.9 资源控制

本项要求包括：

当交通运输行业重要信息系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

用户在登录应用系统后在规定的时间内未执行任何操作，应自动退出系统。

交通运输行业重要信息系统应能够对系统的最大并发会话连接数进行限制；

交通运输行业重要信息系统应能够对单个账户的多重并发会话进行限制；

交通运输行业重要信息系统应能够对一个时间段内可能的并发会话连接数进行限制；

交通运输行业重要信息系统应能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额；

交通运输行业重要信息系统应能够对系统服务水平降低到预先规定的最小值进行检测和报警；

交通运输行业重要信息系统应提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。

4.2.10 自身抗攻击性

本项要求包括：

a）交通运输行业重要信息系统需具备一定的抗攻击抗渗透能力，采用的容器没有已公布的安全漏洞，自身没有 SQL 注入漏洞、跨站漏洞、缓冲区溢出漏洞等。

4.3 主机安全建设基本要求

4.3.1 身份鉴别

本项要求包括：

交通运输行业重要信息系统配套的主机应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

1） 口令应符合以下条件：数字、字母、符号混排，无规律的方式；

2） 口令的长度至少为 10 位；

3） 口令至少每季度更换 1 次，更新的口令至少 5 次内不能重复；

4） 如果设备口令长度不支持 10 位或其他复杂度要求，口令应使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。

交通运输行业重要信息系统配套的主机应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；

交通运输行业重要信息系统配套的主机应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性；

1） 应为操作系统的不同用户分配不同的用户名，确保用户名具有唯一性；

2） 应为数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。

交通运输行业重要信息系统配套的主机应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

1） 通过本地控制台管理主机设备时，应采用一种或一种以上身份鉴别技术；

2） 以远程方式登录主机设备，应采用两种或两种以上组合的鉴别技术进行身份鉴别。

交通运输行业重要信息系统感知节点配套的终端能够在感知接入时提供自身身份鉴别的机制。

交通运输行业重要信息系统感知节点配套的终端采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

4.3.2 访问控制

本项要求包括：

交通运输行业重要信息系统配套的主机应启用访问控制功能，依据安全策略控制用户对资源的访问；

交通运输行业重要信息系统配套的主机应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；

交通运输行业重要信息系统配套的主机应实现操作系统和数据库系统特权用户的权限分离；

交通运输行业重要信息系统配套的主机应严格限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令；

1） 系统无法修改访问权限的特殊默认账户，可不修改访问权限；

2） 系统无法重命名的特殊默认账户，可不重命名。

交通运输行业重要信息系统配套的主机应及时删除多余的、过期的账户，避免共享账户的存在；

交通运输行业重要信息系统配套的主机**应对重要信息资源设置敏感标记；**

交通运输行业重要信息系统配套的主机应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

4.3.3 安全审计

本项要求包括：

交通运输行业重要信息系统配套的主机审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；

系统不支持该要求的，应以系统运行安全和效率为前提，采用第三方安全审计产品实现审计要求。

交通运输行业重要信息系统配套的主机审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；

审计内容至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。

交通运输行业重要信息系统配套的主机审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

交通运输行业重要信息系统配套的主机应能够根据记录数据进行分析，并生成审计报表；

交通运输行业重要信息系统配套的主机应保护审计进程，避免受到未预期的中断；

交通运输行业重要信息系统配套的主机应保护审计记录，避免受到未预期的删除、修改或覆盖等。

审计记录应至少保存 6 个月。

4.3.4 剩余信息保护

本项要求包括：

交通运输行业重要信息系统配套的主机应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

交通运输行业重要信息系统配套的主机应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

4.3.5 入侵防范

本项要求包括：

交通运输行业重要信息系统配套的主机应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

针对重要服务器的入侵行为检测可通过网络级或主机级入侵检测系统等方式实现。

交通运输行业重要信息系统配套的主机应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；

应能够在程序启动时对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施，如不能正常恢复，应停止有关服务，并提供报警。

操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

持续跟踪厂商提供的系统升级更新情况，应在经过充分的测试评估后对必要补丁进行及时更新。

4.3.6 恶意代码防范

本项要求包括：

a） 交通运输行业重要信息系统配套的主机应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；

1） 原则上所有主机应安装防恶意代码软件，不支持的主机操作系统除外；

2） 未安装防恶意代码软件的主机，应采取有效措施进行恶意代码防范。

b） 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；

c） 交通运输行业重要信息系统配套的主机应支持防恶意代码的统一管理。

交通运输行业重要信息系统感知节点配套的终端应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

4.3.7 资源控制

本项要求包括：

a） 交通运输行业重要信息系统配套的主机应通过设定终端接入方式、网络地址范围等条件限制终端登录；

b） 交通运输行业重要信息系统配套的主机应根据安全策略设置登录终端的操作超时锁定；

c） 交通运输行业重要信息系统配套的主机应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况；

d） 交通运输行业重要信息系统配套的主机应限制单个用户对系统资源的最大或最小使用限度；

e） 交通运输行业重要信息系统配套的主机应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

重要服务器的 CPU 利用率、内存、磁盘存储空间等指标超过预先规定的阈值后应进行报警。

4.4 数据安全基本要求

4.4.1 数据完整性

本项要求包括：

交通运输行业重要信息系统应能够检测到**系统管理数据**、鉴别信息和重要业务数据在传输过程中完整性受到破坏，**并在检测到完整性错误时采取必要的恢复措施；**

交通运输行业重要信息系统应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

4.4.2 数据保密性

本项要求包括：

a) 交通运输行业重要信息系统应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性；

通过互联网、信息专网、无线短程通信网、GPRS 网、卫星网等网络传递系统管理数据、鉴别信息和重要业务数据应采取加密方式。

b) 交通运输行业重要信息系统应采用加密或其他保护措施实现**系统管理数据**、鉴别信息和**重要业务数据**存储保密性。

4.4.3 备份和恢复

本项要求包括：

a) 交通运输行业重要信息系统应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放；

1） 备份每天产生的所有重要信息，并场外存放备份介质；

2） 每季度对备份数据至少进行一次抽样性恢复测试。

b) 交通运输行业重要信息系统应提供异地数据备份功能，异地容灾备份建设地点距离主系统需 300 公里，利用通信网络将关键数据定时批量传送至备用场地；

c) 交通运输行业重要信息系统应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；

d) 交通运输行业重要信息系统应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

3） 对主要的网络设备、通信设备建立备份机制，有备机备件；

4） 对主要的通信线路有冗余备份线路，主备通信线路应采用不同运营商；

5） 主要的网络设备、通信线路在发生故障时可以主备自动切换，不影响业务运行。

4.5 网络安全基本要求

4.5.1 结构安全

本项要求包括：

应保证**主要网络设备**的业务处理能力具备冗余空间，满足业务高峰期需要；

主要网络设备的业务处理能力至少为历史峰值的 3 倍。

应保证**网络各个部分的带宽**满足业务高峰期需要；

应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；

业务终端和业务服务器应放置在不同的子网内，并建立安全的访问路径。

应绘制与当前运行情况相符的网络拓扑结构图；

应绘制完整的网络拓扑结构图，有相应的网络配置表，包含设备 IP 地址等主要信息，与当前运行情况相符，并及时更新。

应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；

应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；

应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。

应对所有业务确定重要性、优先级，制定业务相关带宽分配原则及相应的带宽控制策略，根据安全需求，采取网络 QoS 或专用带宽管理设备等措施。

无线网络与业务系统处置区域需要进行区域隔离；

4.5.2 访问控制

本项要求包括：

应在网络边界部署访问控制设备，启用访问控制功能；

应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，**控制粒度为端口级；**

网络边界访问控制设备应设定过滤规则集。规则集应涵盖对所有出入边界的数据包的处理方式，对于没有明确定义的数据包，应缺省拒绝。

应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；

应在会话处于非活跃一定时间或会话结束后终止网络连接；

管理终端连接网络设备，应在会话处于非活跃的时间超过 5 分钟或会话结束后终止网络连接。

应限制网络最大流量数及网络连接数；

重要网段应采取技术手段防止地址欺骗；

应禁用网络设备的闲置端口，采用非虚拟 IP 设备地址绑定等方式防止地址欺骗。

应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户；

应限制具有拨号访问权限的用户数量。

原则上不应通过互联网对重要信息系统进行远程维护和管理。

无线网络接入到内部网络的区域需设置边界访问控制设备，并配备严格的访问控制策略。

4.5.3 安全审计

本项要求包括：

应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；

审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

应能够根据记录数据进行分析，并生成审计报表；

应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等；

无线网络接入到内部网络的区域需设置审计设备。

4.5.4 边界完整性检查

本项要求包括：

应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；

应能够对内部网络用户私自联到外部网络的行为进行检查，**准确定出位置，并对其进行有效阻断。**

能够检查网络用户终端采用双网卡跨接外部网络，或采用电话拨号、ADSL 拨号、手机、无线上网卡等无线拨号方式连接其他外部网络。

4.5.5 入侵防范

本项要求包括：

应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；

当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

4.5.6 恶意代码防范

本项要求包括：

应在网络边界处对恶意代码进行检测和清除；

如果部署了主机恶意代码检测系统，可选择安装部署网络边界部署恶意代码检测系统。

应维护恶意代码库的升级和检测系统的更新。

4.5.7 网络设备防护

本项要求包括：

应对登录网络设备的用户进行身份鉴别；

应删除默认用户或修改默认用户的口令，根据管理需要开设用户，不得使用缺省口令、空口令、弱口令。

应对网络设备的管理员登录地址进行限制；

网络设备用户的标识应唯一；

主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；

1） 通过本地控制台管理网络设备时，应采用一种或一种以上身份鉴别技术；

2） 以远程方式登录网络设备，应采用两种或两种以上组合的鉴别技术进行身份鉴别。

身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

1） 口令应符合以下条件：数字、字母、符号混排，无规律的方式；

2） 管理员用户口令的长度至少为 10 位；

3） 管理员用户口令至少每季度更换一次，更新的口令至少 5 次内不能重复；

4） 如果设备口令长度不支持 10 位或其他复杂度要求，口令应使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。

应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

应实现设备特权用户的权限分离。