



# 中华人民共和国公共安全行业标准

GA/T 1168—2014

---

## 公安交通管理综合应用平台安全保护 通用技术要求

General technical requirements for the security protection of the traffic  
management integrated application platform

2014-06-23 发布

2014-06-23 实施

---

中华人民共和国公安部 发布

目 次

前言 ..... Ⅲ

引言 ..... Ⅳ

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 安全保护要求 ..... 2

    4.1 机房 ..... 2

    4.2 网络 ..... 3

    4.3 主机 ..... 5

    4.4 应用 ..... 6

    4.5 数据 ..... 8

5 安全管理系统 ..... 9

## 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部交通管理局提出。

本标准由公安部计算机与信息处理标准化技术委员会归口。

本标准起草单位：公安部交通管理科学研究所、国家道路交通安全产品质量监督检验中心。

本标准主要起草人：吴晓东、陈飞、季君、张捷、王健峰、刘榴、许卉莹、武红斌、邹伟、金永俊、孙巍、张军。

## 引 言

本标准描述公安交通管理综合应用平台及重要外挂系统应达到的安全保护技术要求,为公安交通管理综合应用平台及重要外挂系统安全建设和管理提供指导。

本标准旨在 GB/T 22239—2008 对信息系统安全等级保护第三级基本要求、GA/T 710—2007 对信息系统安全等级保护第三级基本配置要求,以及其他相关标准基础上,结合公安交通管理信息系统安全保护技术要求和特点,选取适用于公安交通管理综合应用平台的安全保护技术要素,并加以扩充和细化,从具体操作层面指导公安交通管理综合应用平台及重要外挂系统安全建设和管理。

# 公安交通管理综合应用平台安全保护 通用技术要求

## 1 范围

本标准规定了公安交通管理综合应用平台的安全保护通用技术要求。

本标准适用于公安交通管理综合应用平台的建设和管理,也适用于公安交通管理综合应用平台重要外挂系统的建设和管理。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB 50016—2006 建筑设计防火规范

GB 50174—2008 电子信息系统机房设计规范

GA 267—2000 计算机信息系统雷电电磁脉冲安全防护规范

GA/T 708—2007 信息安全技术 信息系统安全等级保护体系框架

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**局域计算环境 local area computing environment**

由一个或多个计算机系统(主机/服务器)组成的,以对信息系统中的数据信息进行存储、处理为主要目的、有明确边界的计算环境。一个局域计算环境可以由一个计算机系统组成,也可以由多个计算机系统经局域网连接组成。

[GA/T 708—2007,定义 3.4]

### 3.2

**用户环境 user environment**

由一个或多个终端计算机组成的,以提供用户使用信息系统中的数据信息为主要目的环境,也称独立用户/用户群。

[GA/T 708—2007,定义 3.7]

### 3.3

**网络系统 network system**

连接局域计算环境与局域计算环境及局域计算环境与用户环境的网络设备、设施所组成的系统。

[GA/T 708—2007,定义 3.9]

### 3.4

**安全域 security domain**

信息系统中执行相同安全策略的区域。在实施等级保护的信息系统中,安全域可以是具有相同安全等级的信息系统或子系统。

[GA/T 708—2007,定义 3.11]



### 3.5

#### 重要外挂系统 important plug-in system

公安交通管理部门建设应用的,通过公安交通管理综合应用平台提供的访问接口,能够写入、修改、删除公安交通管理综合应用平台数据的信息系统。

### 3.6

#### 网络边界 network boundary

公安交通管理综合应用平台及重要外挂系统安全域的网络环境至公安信息通信网其他网络环境的网络连接接口。

### 3.7

#### 关键服务器 pivotal server

公安交通管理综合应用平台及重要外挂系统的数据库服务器和应用服务器。

## 4 安全保护要求

### 4.1 机房

#### 4.1.1 场地选择

机房场地选择应符合以下要求:

- a) 远离产生粉尘、油烟、有害气体及生产或贮存具有腐蚀性、易燃、易爆物品的场所;远离水火灾火灾隐患区域;远离强振源和强噪声源;避开强电磁场干扰;
- b) 对于多层或高层建筑物内的机房,在确定主机房的位置时,要对设备运输、管线敷设、雷电感应和结构荷载等问题进行综合考虑和经济比较;采用机房专用空调的主机房,应具备安装室外机的建筑条件。

#### 4.1.2 防火

机房防火应符合以下要求:

- a) 采取区域隔离防火措施,将重要设备与其他设备隔离开;
- b) 当机房位于其他建筑物内时,在主机房和其他部位之间设置耐火极限不低于 2 h 的隔墙,隔墙上的门采用甲级防火门;
- c) 安装洁净气体灭火系统,并设置火灾自动消防系统,能够自动检测火情、自动报警、自动切断非消防电源,并自动灭火;不使用水、干粉或泡沫等容易产生二次破坏的灭火剂;
- d) 耐火等级不应低于 GB 50016—2006 民用建筑规定的二级要求。

#### 4.1.3 供配电

机房供配电应符合以下要求:

- a) 将计算机系统供电与其他供电分开,并配备应急照明装置;
- b) 配置 UPS 不间断电源,保证电压不足、供电中断时关键服务器等重要设备正常运行;
- c) 设置冗余或并行的电力电缆线路为计算机系统供电;
- d) 配备线路稳滤波装置,保证供电电源质量;
- e) 电源线和通信线缆隔离铺设,避免互相干扰。

#### 4.1.4 接地

机房接地应符合以下要求:

- a) 设等电位连接网络,机房内设备的金属外壳、机柜、机架、金属管、槽、屏蔽线缆外层、防静电接地、安全保护接地、浪涌保护器接地端等以最短的距离与等电位连接网络的接地端子连接,连接线采用多股铜质金属线,其截面积大于等于  $16 \text{ mm}^2$ ;
- b) 等电位连接网络采用铜排或铜带,其截面积大于等于  $35 \text{ mm}^2$ ;
- c) 交流工作接地和安全保护接地,接地电阻小于等于  $4 \Omega$ ;直流工作接地,接地电阻按计算机系统具体要求确定。

#### 4.1.5 防雷

机房防雷应符合以下要求:

- a) 所处建筑设置避雷装置;
- b) 设置电源防雷保安器,其冲击通流容量和限制电压按 GA 267—2000 的表 5 选取;
- c) 在建筑物屋顶敷设电源或信号线路时,穿金属管进行屏蔽保护,金属管进行等电位连接。

#### 4.1.6 电磁防护

机房电磁防护应符合以下要求:

- a) 采用接地方式,防止外界电磁干扰和设备寄生耦合干扰;
- b) 对关键设备和磁介质实施电磁屏蔽。

#### 4.1.7 空气调节

机房温度、相对湿度及空气含尘浓度应符合 GB 50174—2008 中 B 级以上电子信息系统机房规定的要求。

#### 4.1.8 环境和设备监控

机房环境和设备监控应符合以下要求:

- a) 在可能发生水患的部位设置漏水检测和报警装置;将强制排水设备的运行状态纳入监控系统;进入机房的水管分别加装电动和手动阀门;
- b) 配备综合监控系统,实现机房温湿度、电压、电流等的监控报警功能;
- c) 采取技术措施,实现主机的集中控制和管理。

#### 4.1.9 其他

机房还应符合以下要求:

- a) 设单独出入口,另设紧急疏散出口,标明疏散线路和方向,并设置疏散照明和安全出口标志灯;出入口控制系统能受相关系统的联动控制而自动释放电子锁;
- b) 主机房配置专用空气呼吸器或氧气呼吸器;
- c) 采取防鼠害和防虫害措施;
- d) 设置电子门禁系统、视频监控系统和入侵报警系统。

### 4.2 网络

#### 4.2.1 结构安全

结构安全应符合以下要求:

- a) 按照方便管理和控制的原则划分不同的子网或网段,并分配地址段;
- b) 网络边界处配备硬件防火墙设备;



- c) 实现关键网络设备的故障冗余,确保发生故障时可以自动切换;
- d) 绘制与当前运行情况相符的网络拓扑结构图;
- e) 建设骨干网络备用通信链路,实现通信链路的冗余备份。

#### 4.2.2 访问控制

访问控制应符合以下要求:

- a) 在硬件防火墙或核心交换机等关键网络设备上配置并启用访问控制策略,只允许网络管理员的计算机地址远程访问网络设备;
- b) 在硬件防火墙、核心交换机、操作系统或数据库管理系统中配置并启用访问控制策略,限制对数据库服务器和应用服务器的访问;
- c) 配备具备根据会话状态信息为数据流提供明确的允许或拒绝访问功能的网络设备,并配置相应策略,控制粒度为网段级;
- d) 配备具备按用户和系统之间的运行访问规则,决定允许或拒绝用户对受控系统进行资源访问功能的网络设备,并配置相应策略,控制粒度为单个用户。

#### 4.2.3 设备注册及边界检查

设备注册及边界检查应符合以下要求:

- a) 按照公安信息通信网联网设备及应用系统注册管理要求,对公安信息通信网内设备进行设备注册;
- b) 未经批准,不得擅自注销或删除公安信息通信网内设备一机两用监控软件;
- c) 按照公安信息通信网边界接入平台安全要求,对与公安信息通信网以外的网络数据交换实施统一接入和管理;
- d) 防止无法安装一机两用监控软件的公安信息通信网内设备违规连接外部网络。

#### 4.2.4 入侵防范

入侵防范应符合以下要求:

- a) 在硬件防火墙设备中配置禁用常见攻击端口、防范拒绝服务攻击等安全策略;
- b) 配备入侵检测或防御设备;
- c) 当检测到攻击行为时,记录攻击源 IP 和攻击的类型、目的、时间,在发生严重攻击事件时提供报警。

#### 4.2.5 网络设备防护

网络设备防护应符合以下要求:

- a) 对登录网络设备的用户进行身份标识和鉴别,禁止网络设备采用默认用户登录;
- b) 登录网络设备的用户身份标识具有不易被冒用的特点,口令复杂度满足大写字母、小写字母、数字和特殊字符四者中三者以上组合,不包含用户名,长度至少 10 位以上要求;
- c) 每季度至少更换一次网络设备用户口令;
- d) 当登录网络设备进行远程管理时,采取措施防止用户身份鉴别信息在网络传输过程中被窃取;
- e) 启用网络设备登录失败处理功能,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。

#### 4.2.6 安全审计

安全审计应符合以下要求:



- a) 启用硬件防火墙、入侵检测、入侵防御、核心交换机、路由器等网络设备安全审计功能,对运行状况、网络流量、用户行为等进行日志记录;
- b) 审计记录包括事件的日期、内容、用户、类型、事件是否成功及其他与审计相关的信息;
- c) 采取设置访问权限、数据备份等措施保护审计记录,避免受到未预期的删除、修改或覆盖;
- d) 审计记录集中存储到安全管理系统,保存 3 个月以上;
- e) 提供对审计记录数据进行统计、查询、分析和生成审计报表的功能。

#### 4.2.7 冗余设计

冗余设计应符合以下要求:

- a) 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;
- b) 提供关键网络设备、通信线路的硬件冗余,保证系统的高可用性。

### 4.3 主机

#### 4.3.1 身份鉴别

身份鉴别应符合以下要求:

- a) 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;对同一个操作系统或数据库系统进行管理和操作的不同用户,分别创建不同的操作系统或数据库系统用户;
- b) 为同一服务器上的操作系统和数据库系统的用户分配不同的用户名称,用户名称具有唯一性;
- c) 对操作系统和数据库系统进行远程管理时,采取措施防止鉴别信息在网络传输过程中被窃取;
- d) 操作系统禁止采用默认用户登录,登录界面中不显示上次登录用户名称;数据库系统禁止缺省用户名和密码登录;
- e) 操作系统和数据库系统用户身份标识具有不易被冒用的特点,口令复杂度满足大写字母、小写字母、数字和特殊字符四者中三者以上组合,不包含用户名,长度至少 10 位以上要求;
- f) 启用登录失败处理功能,可采取结束会话、多次非法登录后锁定用户和自动退出等措施;
- g) 为应用系统创建专用的数据库系统用户,未经授权,不使用应用系统专用用户连接到数据库系统进行数据库操作;
- h) 同一服务器上的应用系统,需要连接不同数据库系统时,采用不同的数据库用户名称;
- i) 同一安全域内的操作系统和数据库系统用户设置不同的密码;
- j) 建立系统用户清单和说明文档,每季度对用户使用情况进行检查和清理,删除或锁定多余的、过期的用户,避免共享用户的存在。

#### 4.3.2 访问控制

访问控制应符合以下要求:

- a) 在操作系统和数据库系统中配置并启用访问控制功能,制定访问控制策略,控制用户对系统资源的访问;
- b) 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;
- c) 实现操作系统特权用户和数据库系统特权用户的权限分离;
- d) 制定操作系统和数据库系统端口使用清单并归档保存,采取措施禁用未使用的端口;
- e) 对安装 Windows 操作系统的关键服务器,启用系统防火墙功能,设置系统入站、出站等规则。

#### 4.3.3 安全审计

安全审计应符合以下要求:

- a) 实现关键服务器操作系统和数据库系统的安全审计,制定安全审计策略,并采取措施实现集中审计;
- b) 审计范围覆盖关键服务器的每个操作系统用户和数据库用户;
- c) 审计内容包括用户行为、系统资源异常使用和重要系统命令使用等事件;
- d) 审计记录包括时间、类型、主体标识、客体标识和结果等;
- e) 采取设置访问权限、数据备份等措施保护审计记录,避免受到未预期的删除、修改或覆盖等;
- f) 审计记录集中存储到安全管理系统,保存 6 个月以上;
- g) 提供对审计记录数据进行统计、查询、分析和生成审计报表的功能。

#### 4.3.4 入侵防范

入侵防范应符合以下要求:

- a) 操作系统遵循最小安装原则,仅安装需要的组件和应用程序;
- b) 通过设置升级服务器等方式保持系统补丁及时得到更新;
- c) 能够检测到对关键服务器进行入侵的行为,能够记录入侵的源 IP 和攻击的类型、目的、时间,并在发生严重入侵事件时提供报警。

#### 4.3.5 恶意代码防范

恶意代码防范应符合以下要求:

- a) 操作系统安装防恶意代码软件,并及时更新;
- b) 每天在系统空闲时段对操作系统进行恶意代码检查;
- c) 实现防恶意代码软件的统一管理和监控。

#### 4.3.6 资源控制

资源控制应符合以下要求:

- a) 在操作系统或数据库系统中,通过 IP 和 MAC 地址设定用户环境计算机接入许可安全策略;
- b) 设置用户环境计算机的操作超时锁定;
- c) 设置单个用户对系统资源的最大使用限度;
- d) 对关键服务器进行监视,监视服务器的 CPU、硬盘、内存、网络等资源的使用情况;
- e) 能够监测到系统的服务水平降低至预先规定的最小值并报警;
- f) 整理操作系统默认共享资源,取消无用的默认共享及相应服务。

#### 4.3.7 冗余

应实现关键服务器的故障冗余。

### 4.4 应用

#### 4.4.1 身份鉴别

身份鉴别应符合以下要求:

- a) 提供专用的登录控制模块对登录用户进行身份标识和鉴别;
- b) 提供用户身份标识唯一性检查功能,应用系统中不存在重复用户身份标识;
- c) 提供用户有效期限限制和用户 IP 地址验证功能;
- d) 提供密码、公安数字证书和指纹等用户身份认证功能;
- e) 采用密码身份认证方式时,用户密码采用不可逆算法加密存储,提供图片验证码验证、密码强



度检测及控制和定期强制更换密码功能；

- f) 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、暴力破解密码锁定和自动退出等措施；
- g) 提供对用户长期未使用、密码修改不及时检查和报警功能；
- h) 提供对同一用户多点同时登录应用系统的异常情况检测和限制功能。

#### 4.4.2 访问控制

访问控制应符合以下要求：

- a) 提供访问控制功能,依据安全策略控制用户对应用系统各项功能、文件、数据库表等客体的访问；
- b) 对象包括与资源访问相关的主体、客体及它们之间的操作；
- c) 限制默认账户的访问权限；
- d) 授予不同用户完成各自任务所需的最小权限,并在它们之间形成相互制约的关系；
- e) 核心业务模块访问数据时,提供图片验证码验证功能；
- f) 提供高频访问预警和阻断功能；
- g) 提供跨站脚本攻击、跨站请求漏洞和 SQL 注入防御功能；
- h) 调用 Web 应用层功能时,提供动态密钥验证功能；
- i) 调用数据库层存储过程时,提供动态密钥验证功能。

#### 4.4.3 安全审计

安全审计应符合以下要求：

- a) 提供覆盖到应用系统每个用户的安全审计功能,对应用系统版本升级、后台任务运行、高频访问、越权访问、规定时段外访问等重要安全事件进行审计；
- b) 审计记录的内容包括事件日期、时间、发起者信息、类型、描述和结果等；
- c) 采取设置访问权限、数据备份等措施保护审计记录,避免受到未预期的删除、修改或覆盖；
- d) 提供对审计记录数据进行统计、查询、分析和生成审计报表的功能；
- e) 审计记录集中存储到安全管理系统,保存 2 年以上。

#### 4.4.4 通信完整性

采用密码技术保证通信过程中数据的完整性。

#### 4.4.5 通信保密性

通信保密性应符合以下要求：

- a) 在通信双方建立连接之前,应用系统利用密码技术进行会话初始化验证；
- b) 采用加密技术对通信过程中的重要数据进行加密；
- c) 采用系统备案方法,保障数据在可信应用节点间交换；
- d) 应用系统间数据交换采用 Web 服务技术,避免数据库间的直接数据交换；
- e) 应用系统中间件启用 SSL 技术,加强用户环境计算机浏览器到 Web 应用服务器通讯信道的安全性。

#### 4.4.6 抗赖性

抗赖性应符合以下要求：

- a) 能够为数据原发者或接收者提供数据原发证据的功能；



- b) 能够为数据原发者或接收者提供数据接收证据的功能。

#### 4.4.7 软件容错

软件容错应符合以下要求：

- a) 提供数据有效性检验功能,通过人机接口或通信接口保证输入的数据格式及长度符合系统设定要求;
- b) 在故障发生时,应用系统能够继续提供一部分功能并实施必要的措施。

#### 4.4.8 资源控制

资源控制应符合以下要求：

- a) 提供自动结束会话功能,通信一方在一段时间内未做任何响应,另一方能够自动结束会话;
- b) 提供对应用系统最大并发会话连接数进行限制的功能;
- c) 提供对单个用户多重并发会话进行限制的功能;
- d) 提供对一个时间段内并发会话连接数进行限制的功能;
- e) 提供对应用系统服务水平降低到预先规定的最小值进行监测和报警的功能。

#### 4.4.9 代码安全

代码安全应符合以下要求：

- a) 在应用系统程序代码中嵌入由公安部信息中心提供的安全管理程序,封闭不必要的访问端口;
- b) 不在应用系统程序中设计违反或绕过安全规则的入口和文档中未说明的入口;
- c) 对用户提交数据进行检查,替换或删除具有恶意代码攻击嫌疑的字符和字符串并记录日志;
- d) 简化应用系统程序错误提示信息,避免泄露系统配置等影响安全的信息;
- e) 应用系统上线前,采用白盒和黑盒测试技术,进行安全测试;
- f) 采用代码混淆技术提高应用系统的安全性;
- g) 采取措施防止应用系统程序代码被非授权或无意存取及修改;
- h) 删除应用系统程序中不执行的代码;
- i) 对应用系统版本和编译版本进行一致性检查,上线版本和编译版本不一致的禁止上线运行。

### 4.5 数据

#### 4.5.1 数据保护

数据保护应符合以下要求：

- a) 在操作系统内,针对具体用户对保存用户重要数据的目录和文件的读取、写入、运行、修改、列表等权限进行设置,防止未经授权的用户越权访问;
- b) 采用加密或其他有效措施保证系统管理数据、鉴别信息和重要业务数据存储和传输保密性;
- c) 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是否受到破坏,并在检测到完整性错误时采取恢复措施。

#### 4.5.2 数据文件删除

删除重要数据文件时,应采取技术措施防止数据文件被非法恢复。

#### 4.5.3 备份与恢复

备份与恢复应符合以下要求：

- a) 实现关键服务器操作系统、数据库数据的本地备份和恢复;
- b) 在实施本地数据备份时,文本数据完全备份至少每周一次;
- c) 实现异地容灾备份功能,利用通信网络将关键数据定时批量传送至备用场地;
- d) 数据省级集中管理的,实现应用级异地容灾备份。

## 5 安全管理系统

按照公安信息通信网综合安全管理平台技术要求,建立公安交通管理综合应用平台安全管理系统。

---

中华人民共和国公共安全  
行业标准  
公安交通管理综合应用平台安全保护  
通用技术要求  
GA/T 1168—2014

\*

中国标准出版社出版发行  
北京市朝阳区和平里西街甲2号(100029)  
北京市西城区三里河北街16号(100045)

网址 [www.spc.net.cn](http://www.spc.net.cn)

总编室:(010)64275323 发行中心:(010)51780235

读者服务部:(010)68523946

中国标准出版社秦皇岛印刷厂印刷  
各地新华书店经销

\*

开本 880×1230 1/16 印张 1 字数 17 千字  
2014年9月第一版 2014年9月第一次印刷

\*

书号: 155066·2-27272 定价 18.00 元

如有印装差错 由本社发行中心调换  
版权专有 侵权必究  
举报电话:(010)68510107



GA/T 1168-2014