硬件项目安全管理设计方案

1 物理安全设计

1.1 设备物理安全

对于安防监控设备，如摄像头，应采用防暴、防水、防尘的外壳设计，能承受一定程度的冲击和破坏，适合在室外、公共场所等复杂环境中安装使用。安装位置应选择隐蔽且不易被破坏的地方，同时配备防盗支架，防止设备被盗。

智能交通系统中的交通信号控制器、车辆检测器等设备，应安装在坚固的机箱内，机箱具备防撬、防砸功能，并设置锁具，只有授权人员才能打开。设备安装区域应设置防护栏或警示标识，禁止无关人员靠近和触碰。

1.2 机房及存放环境安全

对于存放服务器、数据存储设备等关键设备的机房，应具备严格的 access 控制措施，采用门禁系统，只有授权人员才能进入。机房应配备消防系统，如火灾报警器、灭火器等，并定期进行消防演练，确保在发生火灾时能够及时灭火，减少损失。

机房的环境应保持稳定，温度、湿度应控制在适宜设备运行的范围内，避免因环境因素导致设备故障。同时，机房应具备防鼠、防虫、防雷等措施，保障设备的安全运行。

2 数据安全设计

2.1 数据采集安全

在安防监控系统中，采集视频数据时应确保设备的合法性和准确性，防止非法设备接入系统采集数据。对于涉及个人隐私的监控区域，如居民小区的楼道、住户窗户等，应合理设置监控范围，避免采集无关的隐私信息。

智能交通系统采集车辆信息、交通违法数据等时，应采用加密传输方式，确保数据在采集过程中不被篡改和窃取。同时，应建立数据采集审核机制，对采集的数据进行审核，确保数据的真实性和有效性。

2.2 数据存储安全

对安防监控视频数据、智能交通系统数据等重要数据，应采用加密存储方式，选择高强度的加密算法，如 AES、RSA 等，防止数据被非法访问和窃取。数据存储设备应具备冗余备份功能，定期进行数据备份，备份数据应存放在安全的地方，并进行加密处理。

建立数据存储访问控制机制，对数据存储设备的访问进行严格控制，只有授权人员才能访问和管理数据。同时，对数据的访问操作进行记录，以便进行审计和追溯。

2.3 数据传输安全

在数据传输过程中，采用加密传输协议，如 SSL/TLS 等，确保数据在网络传输过程中不被监听、篡改和窃取。对于安防监控系统的视频流传输，应采用专用的传输协议，并进行带宽控制，避免因数据传输占用过多带宽影响系统的正常运行。

建立数据传输完整性校验机制，对传输的数据进行校验，确保数据在传输过程中没有丢失或被篡改。当发现数据传输异常时，应及时中断传输，并发出告警信息。

（四）数据使用安全

对于存储和传输的敏感数据，如个人身份信息、车辆信息等，在使用过程中应严格遵守相关法律法规，不得随意泄露和滥用。建立数据使用授权机制，只有经过授权的人员才能使用相关数据，并且使用范围应受到严格限制。

对数据的使用情况进行记录和审计，定期检查数据使用记录，发现异常使用情况及时进行处理。同时，当数据不再需要使用时，应按照规定进行销毁，确保数据不会被非法利用。

3 网络安全设计

3.1 网络架构安全

采用分层网络架构设计，将安防监控系统、智能交通系统、智慧社区系统等划分为不同的网络区域，如前端设备区、数据传输区、后端处理区等，并在不同区域之间设置防火墙，实现网络隔离和访问控制。

防火墙应配置严格的安全策略，只允许必要的网络通信流量通过，阻止非法访问和攻击。同时，定期对防火墙的安全策略进行审查和更新，确保其有效性。

3.2 网络设备安全

对路由器、交换机等网络设备进行安全配置，修改默认用户名和密码，关闭不必要的服务和端口，防止黑客利用漏洞进行攻击。定期对网络设备的固件进行升级，修复已知的安全漏洞。

建立网络设备监控机制，对网络设备的运行状态、网络流量等进行实时监控，当发现异常情况时，及时发出告警信息，并采取相应的处理措施。

3.3 网络访问安全

采用强身份认证机制，如用户名密码 + 动态口令、USBKey 等，对访问网络的用户进行身份认证，确保只有授权用户才能访问网络。对不同用户设置不同的访问权限，实现精细化的访问控制。

限制远程访问网络的权限，对于需要远程访问网络的用户，应采用加密的 VPN 通道，并对 VPN 接入进行严格的身份认证和访问控制。同时，定期对远程访问记录进行审计，发现异常访问及时处理。

4 应用安全设计

4.1 软件安全开发

在软件开发过程中，采用安全开发生命周期（SDL）方法，在需求分析、设计、编码、测试等各个阶段都融入安全因素。对代码进行安全审计和漏洞扫描，及时发现和修复软件中的安全漏洞。

使用安全的编程语言和开发框架，避免使用存在安全隐患的函数和方法。在软件发布前，进行全面的安全测试，包括渗透测试、漏洞扫描等，确保软件的安全性。

4.2 应用程序安全

应用程序应具备防 SQL 注入、防 XSS 攻击、防 CSRF 攻击等安全防护功能。对用户输入的数据进行严格的验证和过滤，防止恶意数据注入应用程序。

采用会话管理机制，对用户的会话进行有效管理，设置合理的会话超时时间，防止会话被劫持。同时，对敏感操作进行二次验证，如修改密码、删除数据等，确保操作的安全性。

5 保密方案设计

项目虽按公开级管理，但公司全体参研、参试及服务人员在现场调试、交付、运维期间，须无条件遵守公司所现行保密制度及安全保卫规定，并履行以下义务：

人员范围限定：公司须提前 3 个工作日向甲方提交《现场人员名单及保密审查表》，所有人员须通过公司所政治审查及保密培训，取得临时出入证后方可进入指定工作区域；未经甲方书面批准，严禁更换或新增人员。

场所活动限制：公司人员仅限在甲方划定的调试机房、会议室及指定通道内活动，严禁进入与项目无关的涉密场所；携带的电子设备、存储介质须接受甲方安检，禁止携带具备无线通信功能的设备进入调试区域。

信息隔离与禁传：在任何场合均不得查看、询问、记录、拍摄、复制、谈论与项目无关的国家秘密、商业秘密或内部敏感信息；禁止通过电话、网络、社交媒体、会议、论文、宣传材料等任何形式对外披露项目技术方案、性能指标、实验数据、图片视频及现场情况。

资料管理：公司在项目过程中形成的纸质及电子文档须统一编号、双人双锁管理，每日离场前交甲方保密办清点封存；调试日志、截屏、脚本等仅用于项目排故与验收，禁止挪作他用或带离现场。

违规追责：如公司人员违反上述规定，甲方有权立即终止其现场资格，并按《保密违法行为处理办法》追究公司违约责任；造成泄密的，依法移送国家保密行政管理部门处理，公司承担全部法律责任及经济赔偿。

公司须在合同签订前与甲方签署《专项保密承诺书》，并确保所有现场人员逐人签字确认。

5.1 系统保密设计

5.1.1 保密信息

项目需要保密的信息内容主要是指所有单位提供给我方的项目相关信息以及资料、建设信息等资料。

未经用户允许，不会将由用户提供的有关采购合同或任何合同条文、规格、计划、图纸、模型、样品或资料提供给与履行采购合同无关的任何其他人。即使向与履行采购合同有关的人员提供，也会注意保密并限于履行合同必须的范围。

承诺对项目技术文件以及由建设相关单位提供的所有内部资料、技术文档和信息予以保密；未经建设相关单位书面许可，不以任何形式向第三方透露公司项目以及项目的任何内容；将按照建设相关单位的要求签订相关的保密协议。

将加强项目资料的保密管控，严格针对项目全生命周期涉及的纸质、声音、影像、图像、电子等各种形态资料及其载体的保密管控措施，记录资料由生成到销毁整个生命周期内的使用日志，并根据实际工作情况及时对制度进行调整，资料保密管理制度的建立和修订需得到军队单位方的同意后方可实行。

将加强项目在建设相关单位工作场所使用设备，特别是笔记本电脑、移动设备、存储介质等便携设备使用的保密管理。对接入军队系统网络内使用的设备，严格遵守军队关于终端安全管理、移动存储介质管理等要求，遵守服务笔记本电脑专网专用，还将制定此类便携式设备保密使用管理规定。便携式设备保密使用管理规定的建立和修订需得到军队单位方的同意后方可实行。

服务期间，所有服务于项目的计算机、移动设备、存储介质等设备损坏或报废，我司将严格按照军队单位相关规定进行处理；服务期满后，所有服务项目的计算机、移动设备、存储介质等设备按照军队单位相关规定进行处理。

5.1.2 保密责任

项目集成建设采取尽可能的措施对所有来自军队单位的信息严格保密，包括执行有效的安全措施和操作规程；

建设单位不可把秘密以任何方式泄露给第三方。

建设单位在收到信息后对保密信息的保密期限为长期保密。

5.1.3 保密措施

为避免泄密，我们制定全面的保密措施，涉及到项目实施过程中的各个阶段，包括：项目启动阶段保密措施、项目需求阶段保密措施、项目实施阶段保密措施。

5.1.4 项目启动阶段

5.1.4.1 制定项目保密制度

建立切实可行的保密规章制度，编制《军队系统信息安全日常综合服务项目保密管理制度》保密手册，完善必要的人防、物防、技防等保障措施，做到严格管理、责任到人、严密防范、确保安全。组织项目组成员学习，牢固树立保密观念，克服麻痹思想和侥幸心理，切实增强保密意识、责任意识，确保保密工作不出任何纰漏。

5.1.4.2 切实加强领导

成立保密工作领导小组，明确保密工作第一责任人，将项目相关载体的管理纳入日常的保密工作范围。

5.1.4.3 项目人员配备

按照德才兼备原则选配项目核心人员，并保持核心人员的相对稳定。项目核心人员岗前必须接受保密教育培训，签订保密责任书。

项目人员在岗期间应严格遵守保密法律法规和保密纪律，自觉接受保密检查、监督和管理，认真履行保密义务；调动或退休、辞职离岗，严格办理清理移交手续，并签订保密承诺书。

5.1.4.4 签订保密协议

对于本建设项目，从项目立项、需求、开发、实施均要同步做好保密工作，建立防范机制，相关人员均签订保密协议。

5.1.5 项目需求阶段

5.1.5.1 需求资料管理

需求调研过程中，军队单位提供的信息及资料、报价单等信息资料最好以纸质方式提供，在收到项目相关资料后，应如数查清，并放置于有保密措施的地方。在物品使用时，不得让非项目人员拿到。在项目结束后，根据客户的要求，如数寄回客户或烧毁。

在办公环境内，不能将有关项目的资料置于表面，避免无关人员看到项目相关物品。若项目人员不在存放项目资料的桌子、文件柜等附近时，应把项目资料放进桌子和文件柜等并锁好，项目人员要把钥匙妥善保管，不能随意放于桌子和文件柜外。

5.1.5.2 需求调研会议

需求调研会议选择具备保密条件的场所，并根据工作需要，限定参加人员，确定内容是否传达及传达范围；

召开涉及秘密事项的会议，应切实注意做好安全防护措施，并规定保密纪律，对与会人员进行保密教育；

会场内严禁使用无线话筒或无线扩音设备，会场中严禁使用移动电话；

严禁与会议无关的人员进入会场，严格控制列席会议人员，对需列席会议的人员，应提前报有关领导审定；

凡规定不准记录的会议，与会人员不得记录，不得录音；

会议期间印发的秘密文件一律标明密级、编号，发放签收，必要时会后收回；

会议内容及决定事项不得对外透露和传播；

会议结束后，要对会议室进行保密检查，有无遗失文件、笔记本等。要把应回收的文件如数收回，妥善处理。

5.1.5.3 需求人员管理

限定涉密信息的知悉范围，只对必须知悉的相关人员告知其内容，各人对自己因工作掌握或了解的保密信息负有保密义务，不打听与自己工作无关的信息。

5.1.6 项目实施阶段

所有参与项目人员具有严格的保密意识，禁止向第三方泄露建设项目中工作的任何信息，包括目标系统建设情况、网络安全情况、网络安全漏洞、内部人员信息、系统测试过程和结果等，禁止现场拍照、录像；

所有参与项目人员必须经过岗前培训，整个过程按照建设方案和建设计划进行工作开展；

在系统建设过程中，跨网数据导入只能使用光盘，且光盘仅作为数据传输介质，不能作为数据存储介质，在数据传输完毕后，光盘须做销毁处理；

所有系统建设、测试、试运行相关数据不得导出，测试类工具具有自主知识产权，入网前经过防病毒等安全检测；

所有调试、配置工具禁止使用摄像头、麦克风、蓝牙、无线网卡等设备，若含有内置摄像头则使用不透明胶带遮盖；

所有建设、测试、试运行记录和报告在保密计算机上处理和存储，由保密专员统一管理；

在清除试运行环境相关数据时，须采取专用数据擦除软件进行数据随机填写擦除，或采用安全擦除与低级格式化相结合的方式进行。