1.1.1 系统安全保密方案

1.1.1.1、系统安全保密概述

涉密系统安全保密建设是一个复杂的系统工程，无论是对已建计算机信息系统进行安全保密改造，还是新建一个涉密系统，都必须进行安全保密设计，提供安全保密。进行涉密系统安全保密方案设计，首先要进行系统分析，以了解、掌握涉密系统的详细情况；然后，根据涉密系统的实际情况分析网络的脆弱性和面临的威胁，并进行风险分析，确定安全保密的防护重点；依据国家有关信息安全保密标准、法规和文件进行安全保密系统设计，明确所采用的安全保密技术、措施和产品，提供恰当的配置方案，并规范整个涉密统的安全保密管理；最后，提出安全保密建设的实施计划和经费概算。

1.1.1.2、系统分析

（1）硬件资源、存储介质、软件资源、信息资源等系统资源的情况；

（2）涉密系统的用户和网络管理人员的情况；

（3）网络结构图（含传输介质的情况）及相关描述；

（4）应用系统的情况，如应用系统的名称、功能、所处理信息的密级、用户范围、访问权限、安全保密措施等。

1.1.1.3、脆弱性分析和威胁分析

涉密系统安全保密应分析网络的脆弱性，结合涉密系统的实际情况分析所面临的威胁。例如，如果网络中采用了公共网络进行数据传输，就存在通信数据被窃听的威胁。除此之外，可能还存在如下威胁：

（1）非法访问

（2）电磁泄漏发射

（3）通信业务流分析

（4）假冒

（5）恶意代码

（6）破坏信息完整性

（7）抵赖

（8）破坏网络的可用性

（9）操作失误

（10）自然灾害和环境事故

（11）电力中断

1.1.1.4、风险分析

涉密系统安全保密应对涉密系统进行风险分析。根据脆弱性分析和威胁分析的结果，分析利用这些薄弱环节进行攻击的可能性，评估如果攻击成功所带来的后果，根据涉密系统所能承受的风险确定涉密系统的防护重点。

对于涉密系统，信息的保密性就是安全保密防护的重点；对于重要的涉密系统，如果日常工作对涉密系统的依赖性特别强，一旦网络瘫痪后果非常严重，难以承受，就必须考虑建立比较完善的应急处理和灾难恢复中心。

1.1.1.5、安全保密系统设计

涉密系统安全保密应根据脆弱性分析、威胁分析和风险分析的结果，依据国家有关信息安全保密标准、法规和文件进行涉密系统的安全保密系统设计，应该提出安全保密系统设计的目标、原则、安全策略和安全保密功能结构。

1.1.1.6、安全保密技术和措施

涉密系统安全保密应提供实现安全保密系统所采用的安全保密技术和措施。通常包括；

（1）物理安全防护措施

（2）备份与恢复

（3）计算机病毒防治

（4）电磁兼容

（5）身份鉴别

（6）访问控制

（7）信息加密

（8）电磁泄漏发射防护

（9）信息完整性校验

（10）抗抵赖

（11）安全审计

（12）安全保密性能检测

（13）入侵监控

（14）操作系统安全

（15）数据库安全

1.1.1.7、安全保密产品的选型原则

涉密系统安全保密应提出安全保密产品的选型原则，通常包括：

（1）安全保密产品的接入应该不明显影响网络系统运行效率，并满足工作的要求。

（2）涉密系统中使用的安全保密产品原则上必须选用国产设备。

（3）安全保密产品必须通过国家主管部门指定的测评机构的检测。

（4）涉及密码技术的安全保密产品必须获得国家密码主管部门的批准。

（5）安全保密产品必须具有自我保护能力。

1.1.1.8、安全保密管理措施

安全保密管理在涉密系统的安全保密中占有非常重要的地位，即使有了较完善的安全保密技术措施，如果管理的力度不够，将会造成很大的安全隐患。因此，涉密系统安全保密方案应特别强调不能忽视安全保密管理，并提供安全保密管理的具体措施，如安全保密管理机构、管理制度、管理技术和涉密人员的管理。

1.1.1.9、系统安全

1.1.1.9.1、平台安全体系

规章制度：当平台上线运行后，为了保障平台的安全，防止安全事件发生，除了平台在设计和实现上必须考虑安全外，使用方还须制定相应的规章和制度来配合。主要有平台使用操作规范，平台离线数据使用规范，平台设备管理规范等等，这些规范将在系统运行上线后一一制定和实施。

安全架构：平台在设计和开发时已考虑平台的安全，从用户使用的程序对象上来保障平台的安全。平台的安全架构应用多层安全设计模式（MLS：Multi-Level Security），多层安全架构是一种计算机应用系统安全架构模式，它将系统中的元素从安全角度划分成多个不同的层次和方面，然后在这些层次和方面应用各自的安全机制来保障整个系统的安全。平台的安全架构划分成以下几个层次：设备安全、数据安全、应用安全和网络安全。

安全风险管理：平台应对平台在运行使用中发生的各种安全风险或已经发生的安全事件进行管理。安全风险管理分为：安全风险甄别、安全风险报警、安全风险处理、安全事件追溯等几个方面。

1.1.1.9.2、平台安全架构

执勤信息系统平台的安全架构采用应用多层次安全设计模式（MLS：Multi-Level Security）。多层安全架构是一种计算机应用系统安全架构模式，它将系统中的元素从安全角度划分成多个不同的层次和方面，然后在这些层次和方面应用各自的安全机制来保障整个系统的安全。平台的安全架构划分成：设备安全、数据安全、应用安全、网络安全、操作系统安全等五个层次。

1.1.1.9.3、设备安全管理

（1）设备接入安全

平台中有多种不同类型的设备硬件，包括录像机、可视对讲、门禁、警戒雷达、高压电网、声光报警器、智能枪弹柜、分布式节点、信息发布终端、融合通信等。对于各种数字设备，平台使用统一认证的方式来进行接入控制，对于各种模拟设备，使用相应的规章制度进行接入和管理控制。

（2）设备管理安全

在平台的应用中，会对设备进行管理和设置，为了保证设备管理的安全，平台统一使用武警部队相关标准文件及规范要求提供的应用界面来对设备进行管理和设置，在进行设备的管理和设置前，使用系统自身的数字证书来登录设备系统，防止通过其他途径来对设备进行管理和设置。

上述设备安全手段，由各设备厂商提供。执勤信息系统平台支持这些安全手段的应用。

（3）网络安全管理

网络安全主要指平台在网络上交换数据时对数据的安全保护。平台运行在武警专网上，武警专网是封闭性网络，只有本系统内部人员使用，再匹配采购人单位已有的网络安全措施，其网络安全性已有十分安全的保障。平台对于重要的数据信息，通过建立可信传输信道并进行数据加密的方式进行传输，确保数据安全。

1.1.1.9.4、数据安全管理

（1）数据加密

在高安全级别应用情况下，系统采用在网络层采用 IPSec 或在传输层采用 TLS

对重要业务数据、指令数据、用户数据进行安全加密，并通过兼容采购单位现有的加密机等设备，确保数据在传输过程的安全。

（2）数据完整性保护

平台采用数字摘要、数字时间戳等技术防止信息的完整性被破坏，即防止恶意篡改系统数据。数字摘要可采用信息摘要 5（MD5）、安全哈希算法 1（SHA-1）、安全哈希算法 256(SHA256)等算法。

（3）数据备份

针对于系统数据库，提供人工与自动备份策略，将数据库数据备份为数据文件，在系统中提供数据文件导出与还原功能。

1.1.1.9.5、应用安全管理

平台的应用安全主要包括用户的登录认证和权限控制。

平台建立以用户、角色、权限为基础定义的权限管理和控制模式，拥有统一的权限列表，权限列表包括平台中的各种操作权限和按照设备为基本对象的访问权限，权限列表是开放和可配置的，可根据平台功能的改进来进行设置和修改，还可以根据平台中管理的设备和功能的增加进行更新；角色是权限列表中一组权限的集合，表示视频监控业务中一类用户使用模式，平台为角色设置和分配具体的权限；用户是具体操作平台的使用者，平台为具体的用户指定角色，一个用户在平台中可以拥有多个角色，当用户登录平台后，其登录时的角色就是用户在操作和使用平台的权限。用户在平台中进行任何操作之前，平台都会对其操作进行权限验证，只有该用户拥有该权限时，才被运行进行操作。

（1）角色管理

角色管理：支持角色的增删改查功能，分配角色具有的系统权限、设备权限，添加角色用户。

角色的批量删除功能：可以对角色进行批量的删除。

（2）用户密码加密

由于系统运行网络环境较为复杂，采用密码模式（resource owner password credentials）作为授权获取机制时，如果直接使用通过在 URL 中附带明文密码的方式，在通信报文在被人截取的情况下，容易导致密码泄露。

因此，在传输过程中，针对用户密码要采用加密的方式进行。系统使用 RSA 对密码进行加密和解密操作，用户密码在系统中以 SHA256 加密的方式保存在数据库中，每次登录前，客户端从服务器端获取公钥和随机值，公钥用于加密明文；随机值可以加强每一次操作的安全性，随机值也加入明文中一并加密，服务端对随机值进行校验，校验后从缓存中销毁，这样就算被别人拿到加密后的密文再次发起请求，由于随机值已失效，请求也是无效的。服务端通过自己的私钥对请求解密，采用 SHA256 加密后对和数据库中的密码做比较验证。

服务可以定期更换公私钥的方式来进一步提升安全性。

(3) 密码强度限制

系统用户设置、修改密码时采用弱口令检查机制。弱口令的规格需要结合项目的实际情况制定，建议满足如下要求：

1. 口令长度至少 8 个字符；

2. 口令至少同时包含字母和数字；

3. 口令不能和帐号或者帐号的倒写一样；

若设置的口令不符合上述规则，对用户提出警告。

1.1.1.9.6、操作系统安全管理

（1）身份鉴别

对登录操作系统的用户进行身份标识和鉴别，操作系统管理用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。口令长度不得小于 8 位，且为字母、数字或特殊字符的混合组合，用户名和口令不得相同，禁止明文存储口令；

（2）访问控制

实现操作系统和数据库系统特权用户的权限分离；严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；

（3）入侵防范

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.

1.1.1.9.7、安全风险管理

平台的安全风险管理分为安全风险甄别、安全风险报警、安全报警处理、安

全事件追溯几个方面。

（1）.安全风险甄别：平台建立安全审计机制，将平台中的所有用户主要操作进行日志记录，并对这些日志进行安全分类和安全审计，系统管理员可根据其以往经验或随着平台运行而积累的经验对这些安全审计记录进行安全级别设置，甄别安全风险，设置报警条件。

（2）.安全风险报警：根据系统管理员甄别的安全风险，平台对系统产生的安全审计日志进行检查，如符合报警条件，平台将产生安全风险报警，及时提醒系统管理员进行风险处理。

（3）.安全报警处理：平台提供应用界面对平台产生的安全报警进行处理，包括通知安全负责人、提醒进行有安全风险操作的用户、记录安全报警处理意见等。

（4）.安全事件追溯：对于已经发生的安全事件，平台提供安全审计日志分析查询功能，帮助系统管理员追溯可疑用户的操作记录，找出产生安全事件的原因，确定安全事件的责任人。

1.1.1.10、平台涉密安全

安全防护体系：按照《军队计算机信息系统安全保密防护要求及检测评估方法》《军队后勤安全防护体系》等有关要求，构建安全防护体系，在网络安全、数据安全、系统安全、应用安全等方面，采取相应的安全技术防护手段。在研发测试阶段，负责本项目测试过程中的保密安全监督和检查，直接对测试项目经理负责，并受安全保密办公室的指导，有权停止测试，并对出现的保密安全问题采用相应的预案，从而保证项目的保密性、安全性测试是检测系统的安全机制、保密措施是否完善且没有漏洞。主要是为了验证系统的防范能力。测试的方法是测试人员模拟非法入侵者，采用各种方法冲破防线。例如，以系统的输入作为突破口，利用输入的容错性进行正面攻击；故意使系统出错，利用系统恢复的过程．窃取口令或其他有用的信息；想法设法截取或破译口令；利用浏览非保密数据，获取所需信息等等。

1.1.1.11、保密措施

1.1.1.11.1、保密管理体系

本公司按照国家和上级保密工作要求，结合本公司维修、保修、技术保障及军品研制项目或产品工作实际，参照体系标准要求，建立文件化保密管理体系：管理手册、程序文件。各部门按照体系的要求开展保密管理活动，并运用过程方法和 PDCA 循环来持续改进保密管理工作，以确保国家秘密的安全，保持并不断提高体系运行的有效性。

1.1.1.11.2、保密文件要求

本公司保密管理体系文件包括：

a) 管理手册

b) 程序文件

c) 作业指导文件

d) 记录。

e) 与保密工作有关的外来文件。

1.1.1.11.2.1、保密管理手册

《保密管理手册》确定了公司保密管理体系的范围，规定了应控制的要求，包括对形成文件的程序的引用，反映了公司保密管理体系的总体框架和思路，通过对公司保密方针、保密工作目标等内容的描述，规定保密管理具体内容，展示了公司保密管理体系总的原则和意图，并明确规定了公司各层级机构及人员的职责和权限。

支持性文件：《文件控制及管理评审程序》。

1.1.1.11.2.2、文件控制

公司建立《文件控制及管理评审程序》，对保密管理体系所要求的文件进行控制，以确保文件充分、适宜、有效。

a) 保密管理手册、程序文件由公司主要负责人批准实施。

b) 当发放新版或修改文件时，应及时收回失效或作废的文件，确保文件的更改和现行修订状态得到识别，确保在使用时可获得适用文件的有关版本。

c) 为防止作废文件被使用，作废文件应加上作废标识，只能作为参考资料。

d) 识别过程中需要保存的文件和资料，应及时整理归档，按各程序文件及《保密工作档案管理程序》的相关规定执行。

1.1.1.11.2.3、记录控制

建立《保密工作档案管理程序》，通过对记录的标识、贮存、保护、检索、保存期限和处置的有效控制，使保密工作的实施过程有完整的管理绩效证据，并能清楚地证明过程满足规定要求的程度。

所有档案记录应清晰、准确、完整，保存方式应便于存取和检索，保存环境应适宜，以防止损坏、变质、丢失。档案记录不允许涂改，更正应采用划改的方法，并有更正人签名或盖章。

保密工作记录应确定保存期限。作为档案的记录保存期应满足法律法规的要求，保密管理体系运行相关记录一般保存不少于 5 年，有明确保存期要求的按规定执行。

1.1.1.11.3、职责、权限和沟通

1.1.1.11.3.1、公司保密组织机构及职责分工

领导职责：对所负责的保密管理体系实现过程所策划的要求负有领导责任，对保密体系实现过程中的重大事项进行决策，并监督其执行，协调落实，保证所需的资源。

归口管理职责：对所负责的保密管理体系实现所策划的要求负有制定和完善规章制度，以及组织、策划、监督检查、效果评价和针对不足采取相应措施、持续改进的责任。

参与实施职责：按照保密管理体系要求和相关国家保密法规和要求实施体系管理，确保过程满足策划要求。

1.1.1.11.3.2、各级保密组织机构

公司保密工作组织机构包括保密委员会、保密办公室。

a）保密委员会是本公司保密管理的最高机构，成员由主要负责人，分管保密工作负责人及各部门的负责人组成。

b）保密办公室负责保密日常管理工作，保密办公室为公司办公室属下部门，并指定一名人员负责公司保密管理工作，均须通过培训和考核并获得保密工作资格证书。

保密委员会职责

a）贯彻执行党和国家以及上级机关制定的保密工作方针、政策、法规和《武器装备科研生产单位保密资格审查管理办法》的有关规定。

b）每年召开例会不少于 2 次，研究、部署、总结保密工作，及时解决重要问题。

c）

审查公司保密管理手册、程序文件和工作计划，对落实情况进行监督检查。

d）确定保密委员会成员职责分工，定期检查职责履行情况。

e）组织、协调、指导重大保密工作事项。

f）审批公司产生的国家秘密范围和期限。

g）审批公司涉密人员和保密要害部位。

h）组织查处一般泄密事件，协助国家安全机关、保密工作部门查处重大泄密事件。

i）总结推广保密工作先进经验，表彰、奖励保密工作先进集体和个人。

j）向上级保密主管部门请示、报告重要保密工作事项，组织完成上级交办的保密工作。

保密工作机构职责

保密办公室机构设在公司办公室下，在保密委员会领导下独立行使保密管理职能：

a）向保密委员会或保密工作领导小组提出工作建议，组织落实保密委员会的工作部署。

b）制定保密制度。

c）组织指导涉密人员的审查界定和保密教育培训。

d）组织保密检查工作。

e）监督指导定密工作。

f）组织协调保密审查工作。

g）监督指导重要涉密活动的保密管理工作。

h）组织确定和调整保密要害部位。

i）监督指导计算机和信息系统、通信及办公自动化设备的保密管理工作。

j）监督指导保密防护措施的实施。

k）查处违反保密法律法规的行为和泄密事件。

l）提出保密责任追究和奖惩建议。

m）本体系所规定的其他职责。

各部门保密工作职责

a）贯彻落实公司保密工作部署和要求。

b）落实本部门及业务相关范围内的保密管理安全防范措施。

c）组织对本部门员工进行日常保密教育、培训。

d）对本部门保密工作进行监督、检查。

各级人员保密职责

法定代表人或主要负责人责任

a）对公司保密工作负全面领导责任。

b）保证党和国家有关保密工作的方针政策和法律法规在本单位的贯彻执行。

c）保证《武器装备科研生产单位保密资格审查认证标准》在本单位的实施，及时解决保密工作中的重要问题，监督检查领导责任制的落实。

d）为保密工作提供人力、财力、物力等条件保障。

公司分管保密工作负责人责任

a）对公司保密工作负具体领导责任。

b）及时研究和部署保密工作。

c）对保密工作落实情况组织监督检查。

d）为保密工作机构履行职责提供保障。

部门负责人或项目负责人责任

a）对本部门或本项目的保密工作负直接领导责任。

b）掌握本部门或本项目的保密工作情况。

c）采取具体措施组织落实公司保密工作部署。

d）对保密措施落实情况进行监督检查。

涉密人员及一般人员责任

a）对本职岗位的保密工作负直接责任。

b）本职岗位的保密要求。

c）按规定履行保密工作职责。

安全保密管理员职责

主要负责公司涉密计算机的日常安全保密管理工作，包括用户账号管理以及安全保密设备和系统所产生日志的审查分析。

兼职保密员职责

a）按照公司保密工作布署，协助保密办公室领导做好日常保密管理工作。

b）了解国家保密法律、法规、方针、政策，熟知公司保密管理体系文件及相关专项制度并贯彻实施。

c）对涉密人员、部位、载体实施日常监督管理。

d）及时向保密办公室领导提出保密工作建议，报告重要情况和泄密事件。

e）完成领导交办的工作。

1.1.1.11.4、保密管理要求

1.1.1.11.4.1、涉密载体管理

a）国家秘密载体应当按有关规定标明密级和保密期限。

b）制作、收发、传递、使用、复制、保存、维修和销毁国家秘密载体（含纸介质、磁介质和光盘等各类物品）及其过程文件资料，应当符合国家有关保密管理规定。

c）密品研制、生产、试验、运输、使用、保存、维修、销毁，应当符合国家有关保密管理规定。

d）严格控制国家秘密载体的接触范围。

e）国家秘密载体应当存放在密码文件柜中。

f）涉密人员辞职、解聘、调离涉密岗位，应当在离岗前清退保管和使用的国家秘密载体。

1.1.1.11.4.2、要害部门、部位管理

a）单位日常工作中经常产生、传递、使用和管理国家秘密的内设机构，应当确定为保密要害部门。

b）单位集中制作、存放、保管国家秘密载体及重要密品研制、实验的专门场所，应当确定为保密要害部位。

c）保密要害部门部位的确定，应当按有关规定履行审批程序。

d）保密要害部门部位应当采取严格的保密防护措施报警装置，设置安全值班人员。

e）涉及保密要害部门、部位的新建、改建工程项目要符合安全保密要求，所采取的保密防护措施应当经单位保密工作机构组织的审核，与工程建设同计划、同设计、同建设、同验收。

1.1.1.11.4.3、计算机管理

a）涉密计算机应当与国际互联网和其它公共信息网络实行物理隔离；禁止使用非涉密的计算机、存储介质存储和处理涉密信息；涉密信息的远程传输应当按国家有关部门要求采取密码保护措施；未经保密办公室审批，禁止对涉密计算机格式化或重装操作系统，禁止删除涉密计算机的移动存储介质及外部设备等日志记录。

b）应当建立信息设备和存储介质台帐；涉密信息设备和存储介质的维修、报废应当符合国家有关保密管理规定。

c）信息设备和存储介质应当具有标识，涉密的应当标明密级，非密的应当标明用途；涉密信息设备和存储介质中的涉密信息应当标明密级。

d）涉密计算机应当制定文档化的安全保密策略，并根据环境、系统和威胁变化情况及时调整更新；每 3 个月形成文档化的安全保密审计报告；每 12 个月根据系统综合日志，进行一次风险自评估，形成文档化的风险分析报告，对存在的风险应当及时采取补救措施。

e）涉密计算机应当按照存储和处理信息的相应密级进行管理和防护；涉密计算机应当选择通过国家相关主管部门授权测评机构检测的安全保密产品，并正确配置和使用；涉密计算机应当采取身份鉴别、访问控制和安全审计等技术保护措施，及时升级病毒和恶意代码样本库，进行病毒和恶意代码查杀，及时安装操作系统、数据库和应用系统的补丁程序；涉密计算机中的信息输出应当相对集中，有效控制；未经保密办公室审批，涉密计算机用户终端禁止安装或拆卸硬件设备和软件。

f）应当拆除涉密便携式计算机中具有无线联网功能的硬件模块；涉密计算机禁止使用具有无线功能的外部设备；未经单位保密工作机构审批，涉密便携式计算机不得存储涉密信息。

g）在涉密计算机内使用的存储介质应当采取绑定或有效的技术措施；禁止使用无标识的存储介质；禁止在低密级计算机上使用高密级存储介质；禁止在低密级存储介质上存储高密级信息；信息交换应当符合国家有关保密管理规定，并配备中间转换机。

h）

涉密信息设备和传输线路的电磁泄漏发射防护措施应当符合国家有关保密管理规定。

i）涉密计算机和存储介质携带外出应当履行审批手续，确保仅存有与外出工作相关的涉密信息，带回时应当进行保密检查。

j）当配备涉密计算机安全保密管理员，涉密计算机安全保密管理人员应当通过安全保密培训，持证上岗，并按照涉密人员管理。

k）要建立防止涉密信息上国际互联网和其它公共信息网络的控制措施,对外发布信息应当经过保密审查；从国际互联网和其它公共信息网络下载信息、程序和软件工具等到涉密计算机中应当加强管理与控制。

1.1.1.11.4.4、通信及办公自动化设备管理

a）处理涉密信息的办公自动化设备禁止连接国际互联网和其它公共信息网络；禁止连接内部非涉密计算机；禁止使用非涉密办公自动化设备存储和处理涉密信息。

b）通信设备的使用应当符合国家有关保密管理规定，重要涉密场所禁止使用无线通信设备；办公自动化设备应当建立台帐，并指定专人管理；禁止使用具有无线互联功能的办公自动化设备处理涉密信息；涉密办公自动化设备的维修、报废应当符合国家有关保密管理规定。

1.1.1.11.4.5、宣传报道管理

a）涉及军品事项的宣传报道、展览、公开发表著作和论文等，应当经过保密审查；需报主管部门审批的，应当履行报批手续。

b）接受涉及军品事项的新闻媒体采访，应当履行审批手续，不得涉及国家秘密。

1.1.1.11.4.6、涉密会议管理

a）涉密会议应当在具备安全保密条件的场所召开。

b）与会人员身份确认和涉密载体的发放、清退、销毁应当指定专人负责，使用和管理应当符合相关保密要求。

c）会议使用的扩音等技术设备应当符合保密要求；会议场所禁止带入手机等移动通信工具，必要时应当设置手机信号干扰器；禁止带入具有无线上网功能的便携式计算机；未经批准禁止带入具有摄录功能的设备。

1.1.1.11.4.7、外场维修管理

a）单位应当指定专人负责保密管理工作。

b）对无线通信设备和具有摄录功能的设备等应当采取严格控制措施。

c）对涉密载体和密品的管理应当采取安全保密防护措施。

1.1.1.11.4.8、协作配套管理

a）承担涉密协作配套任务的单位，应当严格执行合同保密条款，遵守保密协议；

b）在合同签订、合同履行和合同文本中，严格控制背景、用途等涉密内容，不得泄露配套项目研制必需的技术要求以外的涉密信息。

1.1.1.11.4.9、保密检查

a）单位应当每 6 个月组织保密检查，对发现的问题，及时整改。

b）单位保密工作机构应当每 3 个月对涉密部门负责人进行保密检查，保密委员会或保密工作领导小组年度内应当组织对单位负责人的保密检查。

c）涉密部门和涉密人员应当每月进行保密自查。

d）发现泄密事件应当按有关规定及时报告和采取补救措施，并报告查处情况。

支持性文件：《保密检查及失泄密事件查处程序》。

1.1.1.11.5、考核与奖惩管理

a）应当严格执行保密责任追究制度。

b）保密责任落实情况应当纳入年度绩效考核内容。

c）对保密工作做出突出成绩的单位和个人应当给予表彰和奖励。

d）对违反保密法律法规的行为，应当视情给予处罚；泄露国家秘密的，应当按照有关规定作出处理。

1.1.2 试验验证方案

1.1.1.12、平台软件测试

1.1.1.12.1、平台软件测试的基本要求

软件测试是一项综合性的工程，需要由项目组的专职机构安排专业的人员进行测试，并组织系统用户、程序员、测试人员、录入人员共同参与，测试的环境尽可能使用系统运行时环境，并保证足够的业务数据量，听取用户的意见，进行系统的进一步优化，尽可能保证测试环境和生产环境的仿真。

测试结果将按有关的说明作记录。任何被发现的问题以及它们对系统其它任何部分可能会产生的影响，都将作记录。这些问题必须告知责任者，并被跟踪至圆满解决。由任何修改而导致的被影响部分将被确认并重新测试。硬件和软件的配置也将予以考虑和记录。

软件测试应该是对系统有针对性的、综合性的测试，根据 CMM2 软件开发测试方法论标准，我们对软件测试的范围由五大领域组成。

1.性能测试

性能测试包含两方面含义：a) 计算机系统或子系统实现其功能的能力； b) 对计算机系统或子系统执行其功能的能力的度量，例如，响应时间、事务处理能力等[GB/T 11457－1995]。

性能的要求及测评应遵循“GB/T 16260-1996 信息技术—软件产品评价—质量特性及使用指南”和“GB/T 17544-1998 信息技术－软件包－质量要求和测评”的规定。主要是测试一个应用在重负荷下的表现，例如测试一个 Web 站点在大量的负荷下，何时系统的响应会退化或失败。性能测试记录表如下表所示：

指标	要求值	测试结果	备注
用户响应时间 (User response times)			
系统响应时间 (System response times)			
外部接口响应时间 (External interface response times)			
CPU 利用率 (Central processor unit (CPU) utilization)			
内存利用率 (Memory utilization)			
系统吞吐量 (Throughput rates)			

表格.性能测试记录图

2.功能测试

功能是指程序中的一个算法的实现，利用该实现，用户或程序可以完成某一

工作任务的全部或部分内容[GB/T 17544－1998]。功能测评应遵循“GB/T 16260-1996 信息技术—软件产品评价—质量特性及使用指南”和“GB/T

17544-1998　信息技术－软件包－质量要求和测评”的规定。

主要对有图形界面（GUI）的应用程序上作的黑盒测试，而不是模块级的。与模块级的测试一样，GUI 功能测试也是通过输入不同的数据序列后得到的应用反馈，来检测该应用程序是否具有功能完备性（即，是否可用），当然也可以人工逐个地敲键盘输入测试。

现在的应用程序,尤其是与各行业应用与服务结合得越来越深入的应用系统，随着其业务的复杂和开发能力的加强，使现在的应用系统在功能上面（尤其体现在 GUI 应用程序上）越来越复杂，这就需要一个独立的机构来对某些已经标准化的软件进行功能测试。

功能测试需要编写具体的测试用例，并针对测试用例进行测试，记录测试结果和编制测试分析报告，测试报告中关于功能测试则需要按照下表（系统总体功能测试记录表）进行总体评价。

指标	测试评价	备注
成熟性：解决对前代版本的问题及回避由缺陷引起的功能障碍		
许可缺陷性：在发生缺陷或者接口问题下维持一定水平的性能		
恢复性：错误发生时恢复到指定水平的性能		

3.可用性

对“用户友好性”的测试。显然这是主观的，且将取决于目标最终用户或客户。用户面谈、调查、用户对话的录像和其他一些技术都可使用。程序员和测试员通常都不宜作可用性测试员。可用性测试总体评价记录表如下表（总体可用性测试记录表）所示。

指标	测试评价	备注
理解性：软件系统用户对自己的动作直接有关的系统反应要容易理解		
学习性：在系统的多种学习阶段中用户为吸收知识所花的时间最少化		
操作性:软件系统允许用户根据工作习惯调整系统的流程及工作环境		
个性化：能根据用户需求或用户对已分配的工作的熟练度变更软件系统		
错误容差:		

发生用户误错时用最少的努力能修正误错		
工作适合性:软件系统环境在用户执行工作当中不加重困难而支持用户		

4.可靠性测试

可靠性指在规定的一段时间和条件下，软件维持其性质水平的能力有关的一组属性[GB/T 17544－1998]。主要测试软件在运行过程是否稳定可靠，并且具有容错性，可恢复性等。可靠性测试总体评价记录表如下表（可靠性测试记录表）所示：

指标	测试评价	备注
适合性：依据用户的目的提供适合的功能及适合程序的体现能力		
正确性：提供文件的正确信息及适合程序的体现能力		
相互运用性：与不同程序之间的数据交换能力		
安全性：防止没认可的人或者系统的存取访问保护信息与数据的能力		
遵守性：是否按照有关功能性及接口标准、规定、管理等		

5.兼容性测试

测试软件在一个特定的硬件/软件/操作系统/网络等环境下的性能如何。兼容性测试的几个方面：与软件无需采用有别于为该软件准备的活动或手段就可能适应不同的规定环境有关的软件属性；使软件遵循与可移植性有关的标准或约定的软件属性；与软件在该软件环境中用来替代制定的其他软件的机会和努力有关的软件属性。兼容性测试总体评价记录表如下表（兼容性测试记录表）所示：

指标	测试评价	备注
操作系统兼容性：软件对各类操作系统平台的适应性。有些软件需要在不同的操作系统平台上重新编译即可运行，有些软件需要重新开发或是改动较大，才能在不同的操作系统平台上运行，对于两层体系和多层体系结构的软件，还要考虑前端和后端操作系统的可选择性。		

数据库兼容性：		

软件是否提供对其他常用数据格式的支持。例如办公软件是否支持常用的DOC、WPS 等文件格式，支持的程度如何，即可否完全正确的读出这些格式的文件。		
应用软件兼容性：主要考察两项内容：一是软件运行需要哪些其他应用软件的支持，二是判断与其他常用软件，是否造成其他软件运行错误或软件本身不能正确实现其功能。		

1.1.1.12.2、平台软件测试方法

目前较为流行和普遍采用的软件测试方法有“黑盒测试”和“白盒测试”：

1、黑盒测试（功能测试/数据驱动测试）

在已知软件功能设计内容的前提下，由测试人员依据有关技术文档，着重测试和检验软件实现的功能是否符合要求，这种测试对软件或程序模块的内部结构与技术实现细节并不关心，而仅关心测试的软件或程序模块是否能正常运行，输入的数据、边界值等是否能被准确地接受，输出的结果是否正确，操作界面、操作效果、以及运行效果等是否达到了预定的目标。黑盒测试适用于各个阶段的测试活动。

黑盒测试方法主要是为了发现以下几类错误：

- 是否有不正确或遗漏了的功能
- 在接口上，输入能否正确地接受， 能否输出正确的结果
- 是否有数据结构错误或外部信息（例如数据文件）访问错误
- 性能上是否能够满足要求
- 初始化是否正确

2、白盒测试（结构测试/逻辑驱动测试）

在已知软件或程序模块的内部结构与技术实现细节的情况下，由测试人员利用程序的内部逻辑结构与有关文档的信息，设计并准备测试用例与模拟数据，注重检测程序模块的逻辑路径、不同点的执行状态、模块接口、执行效果等。这种测试虽然难度较大、过程复杂，但测试效果显著。白盒测试适用于软件编码阶段的单元测试活动中。

白盒测试主要对程序模块进行如下检查：

- 对程序模块的所有独立的执行路径至少测试一次；

- 对所有的逻辑判定，取“真”与取“假”的两种情况都能至少测试一次；
- 在循环的边界和运行界限内执行循环体；
- 测试内部数据结构的有效性等等。

1.1.1.12.3、平台软件测试类型

对本项目平台软件的测试，主要应包括以下 8 个类型的测试内容：

1.功能测试

着重测试软件系统、子系统、模块的功能是否达到了软件需求规格说明书中的功能要求。

2.接口测试

主要测试各子系统之间、模块之间、程序之间（或与系统外界的模块之间）的接口逻辑关系、检查数据衔接关系是否符合软件概要设计和详细设计说明书中的接口要求。

3.数据存取测试

通过测试活动，检查和分析有关的数据存取效果是否达到了数据库设计和功能设计的要求。例如输入数据能否被响应或保存，加工过程中的中间数据和输出的数据结果是否及时准确等。

4.运行时间测试

在进行软件测试活动的过程中，实时地记录操作界面应答、数据加工、数据查询等方面的系统响应时间，同时记录测试的运行环境、处理范围和数量，为界定软件系统的运行效率提供依据。

5.约束条件测试

在系统的数据收集（接受）、数据处理（事务处理）、数据访问等环节，涉及到许多约束或限制条件，在测试活动中，要预先有针对性地设计和准备这些约束和限制条件的内容，并对此进行测试，以保证软件系统体现出业务上需要的逻辑关联性、监控与制约关系。

6.安全性测试

对软件系统抵御非法操作能力的测试，包括：非法用户的登录、未经授权功能模块的使用、非法窃取数据或越权访问数据等方面。

7.强度测试

测试软件系统中某些敏感和关键部分，能否经得起超负荷运行。例如设计和准备占用最大存储量或其它资源的测试用例来测试系统的承受能力。

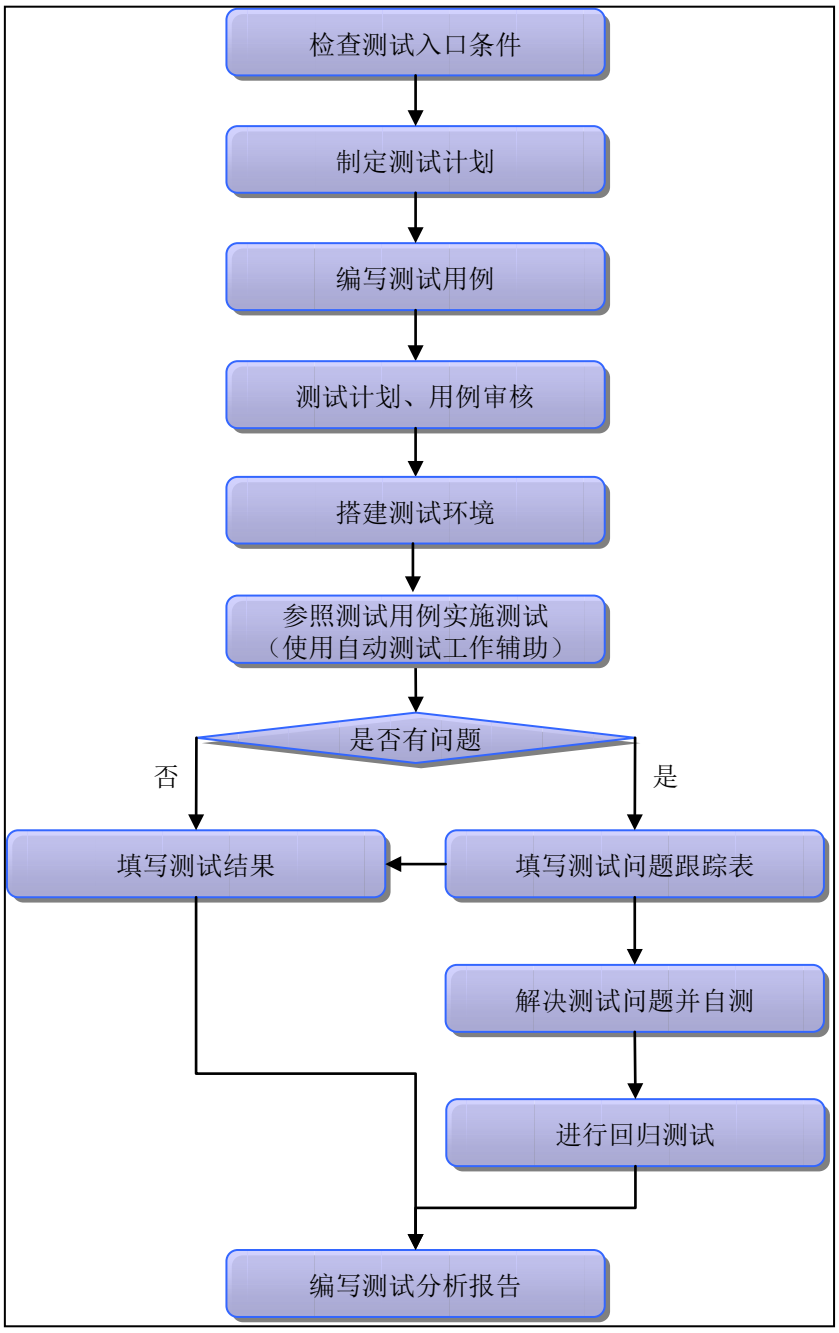
8.文档核查

在软件测试活动安排和实施过程中，必须结合软件开发各阶段产生的技术文档（包括业务需求资料和项目开发计划），来制定各种测试计划、测试用例和测试数据，以保证测试活动的针对性和有效性。通过测试发现的软件问题，往往不一定是程序问题，很可能涉及到前面阶段的软件设计或需求分析工作，为此，必须在测试活动中，对各种相关的技术文档进行再一次的核查，以体现测试的完整性。

在实际开发过程中，可以根据用户的实际要求，结合开发和测试的具体情况，扩充或调整某些测试类型，例如增加界面测试、可靠性测试等。

1.1.1.12.4、平台软件测试流程

软件测试基本工作流程如下图，此基本工作流程适合于各类单项测试工作：



图示.软件测试流程

为保证相关人员能够完全掌握系统的各类技术、使用及维护方法，项目组应具有针对性地制定出培训计划，必须提供内容全面的、面向多层次人员（领导、主要负责人、业务人员、技术人员等）的培训，以保障系统正常运行。

1.1.1.12.5、测试实施阶段

测试阶段分为单元测试，集成测试，系统测试，用户验收测试。下面针对不同的测试阶段介绍的测试组织，测试方法。

单元测试	
测试目的	测试程序功能模块的输入、输出、处理过程和运行状态的正确性，检查是否符合设计要求和编程规范。
测试范围	包括系统的全部功能模块
测试方法	文档检查：检查所提交的文档是否完整，格式是否符合规范，同时进一步了解模块的输入、输出及处理过程 程序代码走查：检查程序结构是否和文档相一致，算法是否合理，同时检查源代码的书写是否符合规范，执行策略是否合理、高效。 运行测试：运行所测模块，并根据需要输入相应的数据，包括实际业务数据、错误数据和非正常操作，检查模块对输入的响应
测试组织	以软件开发小组中的编码人员为主，软件测试小组协助
涉及角色	开发人员、测试人员
测试环境	单元测试环境使用软件开发环境
测试实施要点	对系统关键点，如平台建设，单元测试要求代码覆盖 100%，路径覆盖 100% 测试管理工具：Mercury TestDirector Enterprise,辅助进行测试
相关文档	详细设计文档、编程规范、单元测试计划、单元测试报告

集成测试	
测试目的	在单元测试的基础上，按照集成测试的计划，依据软件设计的要求，对系统各部分进行组装测试。测试各子系统之间的接口关系和数据衔接是否正确，组装后的子系统、全局数据结构、系统运行效果是否达到预先设计的要求。
测试内容	项目各子系统内部。各个子系统之间的集成测试
测试方法	对于系统接口测试，在通过建立接口 stub 进行 通过各应用系统开发商提供的适配器及模拟系统进行测试
测试组织	以软件开发小组中的编码人员为主，软件测试小组协助
涉及角色	开发人员、测试人员
测试环境	独立于开发的测试环境；
测试实施要点	集成测试方面一个关键点是，在子系统可以集成的时候尽早进行集成测试，因此项目组可能需要进行多个集成测试。在每个迭代周期中都需要安排集成测试 在继续复杂的测试之前，先进行冒烟测试。使用测试例数量不多的测试用例集来检验系统，确定是否可以继续后续的复杂测试。可以选择一组针对重要需求的基本功能测试的测试用例集作为冒烟测试用例集。
相关文档	概要设计、详细设计文档、集成测试计划、集成测试报告
系统测试	

测试目的	对软件的整体功能、性能、特性的有效性测试，并对软件配置与相关技术文档的内容进行复查，以测试被测软件是否满足需求分析说明书中的内容，以及软件配置及运行环境的效果确认
测试内容	包括整个系统功能测试和性能测试 在集成测试的基础上，模拟实际的运行环境，进一步按软件需求分析说明书定义的全部要求,对软件系统内的所有部分、与外部系统及数据连接进行整体性测试。
测试方法	对于平台功能测试，依据需求规格说明书，通过正交矩阵分析方法，建立完整的系统测试用例及数据 对于业务功能，在功能点测试的基础上，建立流程测试用例，模拟实际业务流程进行测试 性能测试采用测试工具模拟系统压力情况，获取性能测试指标
测试组织	软件测试小组负责测试，用户参加测试
涉及角色	开发人员、测试人员、用户
测试环境	独立于开发的系统测试环境；
测试实施要点	用户参与系统测试用例的编写，评审，并参与系统测试的执行。系统测试阶段系统开发已经结束，用户参与测试能更及时发现系统需求定义方面存在的缺陷。
相关文档	概要设计、详细设计文档、集成测试计划、集成测试报告
用户验收测试	
测试目的	以用户为主组织和准备现实业务中的实际用例和数据，在用户点的实际运行环境中，对软件系统的功能需求和非功能需求进行全面的复查和测试
测试内容	系统功能验收测试；系统性能验收测试 具体包括：功能是否符合需求分析说明，实际运行环境下的新系统能否达到预期的效果，系统的可靠性、安全性等性能是否有保障，用户对新系统的掌握和使用是否符合上岗要求等
测试方法	同系统测试
测试组织	用户主导测试，系统开发商，各应用系统开发商参加。
涉及角色	用户测试组，系统开发商，各应用系统开发商，产品提供商
测试环境	独立于开发的系统测试环境；
测试实施要点	用户验收测试前，完成对用户的操作培训；使参与测试人员熟悉系统实现功能及操作。 测试环境要与实际运行环境一致，可以考虑与试点运行结合进行。 验收测试时涉及到的厂商较多，对测试的组织与协调提出更高的要求，需要提前规划，明确各方职责。
相关文档	

	软件分析与设计说明书、用户手册、验收测试计划、验收测试报告、用户使用报告等

1.1.1.12.6、测试原则

测试是寻找软件问题、发现错误的主要手段，也是开发方和用户方沟通的重要途径之一。软件中所有程序都必须经过严格的测试和确认后，才能提交给用户验收。要根据各个子系统的特点，制定以下原则用以指导整个测试工作。

- 制定规范和完整的测试计划，严格按计划组织测试，排除测试活动的随意性。
- 预先组织和准备好各种测试用例和测试数据，以保证测试活动的顺利开展。
- 测试输入数据应与对应的预期输出结果配套。
- 测试用例中不仅有合理的输入条件，还要有不合理的输入条件。
- 妥善保存各种测试文档及测试用例与数据，为以后软件重测和维护提供方便。
- 对每一个测试结果要做全面的分析和检查。

1.1.1.12.7、测试准备

1、培训测试人员

有关软件的业务培训

软件测试方法、测试技术、测试规程、测试工具的培训

系统软件需求分析、软件设计、软件开发、软件操作方面的培训

测试用例和测试数据的设计和组织方面的培训

测试活动中的文档编写、质量记录、测试报告方面的培训。

2、编写测试计划

初步确定软件编码阶段的“单元测试”计划含在“软件开发小组”的工作计划中，测试小组重点是制定以下三种测试活动的计划。

编写“集成测试计划”

编写“系统测试计划”

编写“验收测试计划”

3、建立测试环境

测试环境的建立是测试准备的重要环节，要求做到：

测试环境必须与开发环境分开。

测试环境应尽可能模拟用户的使用环境，这样做有利于尽早发现被测软件在今后用户的使用环境下效果如何。

准备和安装好测试环境用的硬件设备，硬件设备的规模和数量应略大于测试小组的人员规模，并配置必须的输出设备。

安装和调试好测试环境用的系统软件，按照测试工作的计划，在测试活动开始之前，必须要以开发环境的系统软件为依据，对操作系统、数据库系统、网络通讯、开发工具等系统软件进行安装和调试，其中包括测试用的工具软件等。

对测试环境实施配置管理，安排专人对测试环境的软、硬件配置项进行初始状态记录，并为今后的配置管理做好准备。

4、收集有关文档和资料

收集和核对软件开发各阶段所产生的技术文档，及其它相关的技术资料。若发现文档欠缺或内容有问题，需及时通过项目经理去协调解决。

5、设计和准备测试用例

能否有针对性地编制实用、有效的测试用例与测试数据，取决于对视频监控业务、系统软件功能、平台产品，数据库结构等方面的理解和把握程度，这是软件测试中最难做的部分。针对软件的不同阶段的测试活动，需设计和准备侧重点不同的测试用例与测试数据。

1.1.1.12.8、测试执行

测试人员应按既定的测试步骤，选用测试实例和测试数据进行测试，根据测试情况，编写“测试日志”。根据测试中发现问题填写“测试问题报告单”。

实行封闭式完整测试，一次测试过程中不允许对软件编码作任何修改和调整，以保证当前测试的有效性。

测试全过程中的软件项和测试项均纳入配置管理。

1.测试问题跟踪

所有测试问题通过缺陷跟踪工具 clearquest 进行建立问题，问题分析与分配，开发修改，回归测试直到关闭整个过程跟踪。

测试问题按照问题严重级别进行分类，分为：致命问题，严重问题，一般问题，建议；

测试组长每天通过 Clearquest 工具汇总测试问题，生成测试情况报表，向项目组进行汇报， 项目根据问题严重级别、紧急程度安排修改。

2.测试结果分析

- 对于“集成测试”、“系统测试”和“验收测试”这三种测试活动所产生的测试结果，必须采用统计分析方法和技术进行处理。
- 每一次整体的测试过程完成后，必须对测试结果提出分析意见，确定测试结论，形成测试分析报告，并按修正的结果对应地修改相关的文档。
- 测试分析报告需要对测试范围、测试方法、测试实例与数据、测试进度和测试结果进行综合评价，具体指标有：
- 指出各项测试结果与预期结果之间的差异并分析差异的原因。
- 指出未被充分测试的特性或特性组合，并说明原因。
- 对致命问题和重大问题的排错与修改情况进行综合考察和评价。
- 对有关文档资料的齐全性进行审定，并对重要文档（特别是用户操作说明书）内容的适用性进行评价。

测试小组归纳已解决和尚未解决的问题，对照测试计划中所规定的“通过准则”确定此次测试是否通过。

1.1.1.12.9、测试组织与实施

1.测试模型

坚持使用 V 模型的测试规则，能够显著地节省时间和成本，并且可以保证提交高质量和高可靠性的应用系统。针对应用系统开发测试过程中的每一个环节，V 模型都可以进行有计划的测试工作，从而确保实现每个阶段的阶段成果。

- 用户验收测试：

在应用系统上线前进行，通过测试来测试系统的功能是否已经达到了业务的需求，系统的性能是否满足系统的需求。用户验收测试中的功能测试部分建议由甲方委派技术骨干组建的测试团队进行，系统的性能验收测试根据本项目技术人员的配备情况考虑由第三方测试机构进行。

- 系统功能和性能测试

这里说的系统功能和性能测试是指应用系统提交给用户进行验收测试前进行的测试。由开发商完成。

功能测试是为了测试应用系统已经满足了软件需求规格说明书中所定义的需求。

性能测试是为了测试系统是否可以承受预定的负载和满足业务需求。由专门的测试人员使用压力测试工具进行测试

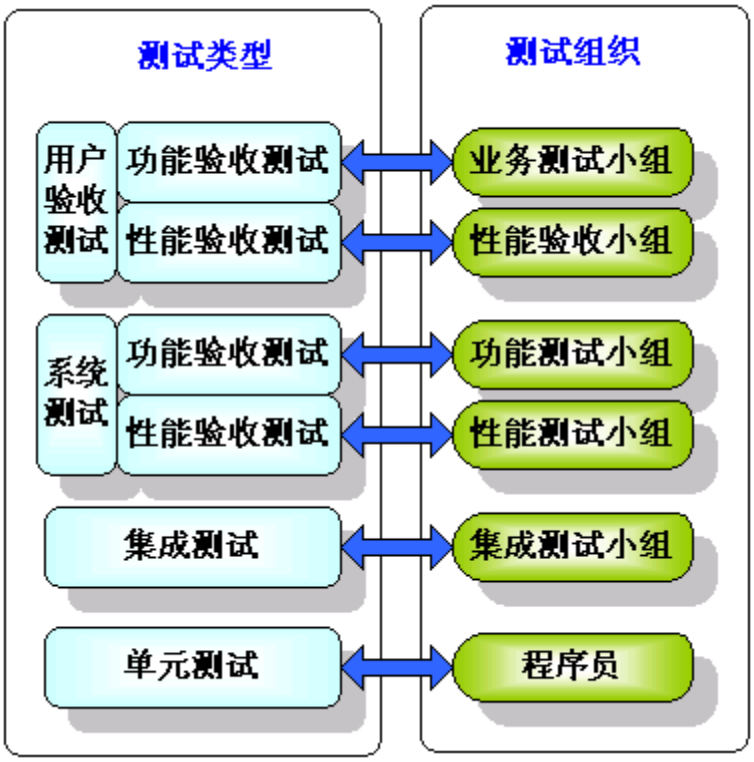
■ 集成测试

测试集成后的系统是否符合系统架构设计要求。集成由开发人员和测试人员共同完成。

■ 单元测试

测试每个模块是否符合详细设计要求。由程序员负责测试数据和方式。

2、测试人员组成



（1）业务测试小组

在开发商完成系统测试后，将系统提交给业务测试小组进行测试。业务测试小组针对业务需求对系统进行认真的测试，测试系统是否满足了业务的需求。

业务测试要求测试人员对视频监控领域的业务非常熟悉。所以业务测试小组建议由甲方抽调部分业务人员组建而成。人员数量将根据项目的规模确定，对于本项目，根据美电贝尔的经验，业务测试人员需要6～12名才能保证测试的进度和质量。

（2）性能验收小组

在开发商完成系统性能测试后，将系统提交给性能验收测试小组进行性能测试。性能验收小组针对事先预定的性能指标需求和业务负载需求对系统的性能进行测试，以测试系统是否满足了性能的需求。

性能测试是比较专业的测试，牵涉到多方面的技术，需要测试人员具有多个领域的技术了解。主要有：

- 网络技术
- 操作系统
- 数据库
- 中间件
- 测试方法、测试规划
- 测试工具
- 系统调优

因此，建议性能验收小组由专业的第三方测试机构担当。

（3）功能测试小组

由开发商组建功能测试小组，完成系统的功能测试。在开发商完成功能测试后，系统才能提交用户进行验收测试。

（4）性能测试小组

由开发商组建性能测试小组，完成系统的性能测试。性能测试是软件测试中的重中之重，并且测试难度比较大。在开发商提交应用软件系统给用户进行性能验收前，必须先通过开发商自身的性能测试，并提交性能测试方案、用例、分析报告给用户。

（5）集成测试小组

由开发商组建集成测试小组，完成集成测试。

（6）程序员

程序员负责单元测试，单元测试一般以白盒测试方法进行测试。

1.1.1.12.10、测试工具

以下列出在测试中使用的主要工具：

测试阶段	工具	工具用途
单元测试	JUnit	针对 Genaral

		Java 应用的自动测试框架。对关键模块进行单元测试
	HttpUnit	针对 Web 应用的自动测试框架。
	Cactus	针对 J2EE 应用的自动测试框架。
	Profile	对关键模块进行单元级别的性能评价
集成测试	JUnit	对关键模块进行功能回归测试；对集成版本进行集成测试
	FindBugs	Java Bytecode 检查软件，能够发现数十种常见的代码缺陷
	Checkstyle	集成化代码审查软件
	Hammurapi	源代码风格检查软件
	Profile	对比不同模块的性能；测试集成版本总体性能指标
	CruiseControl	自动化创建、Email 通知等功能
系统测试	Robot	GUI 系统功能测试
		VU 系统性能测试
	TestDirect	测试管理
	WinRunner	功能测试
	LoadRunner	性能测试
	E-Test	基于 Web 的性能及功能测试

1.1.1.13、系统联调验证

1.1.1.13.1、联调验证定义

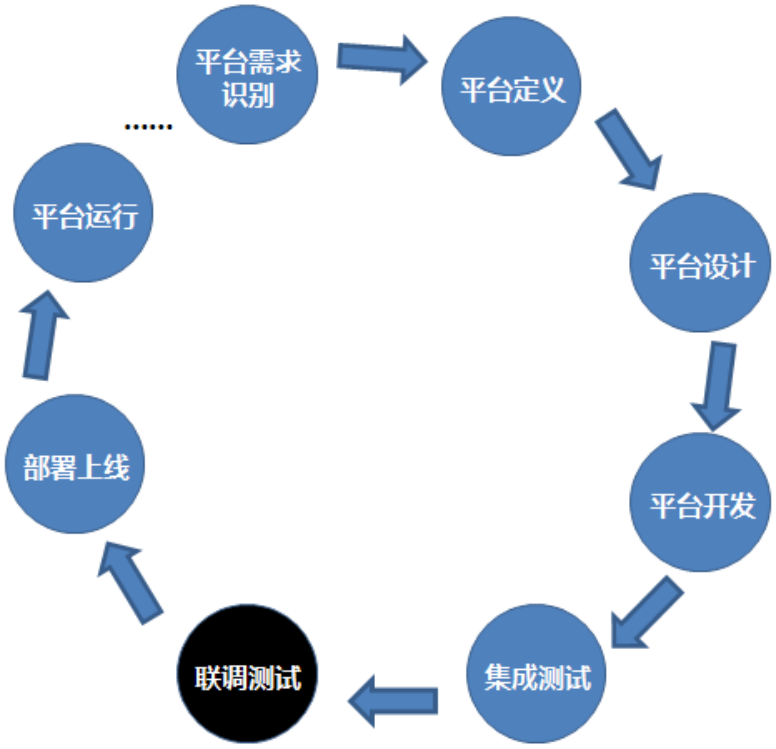
联调验证是指执勤信息系统平台软件通过各种接口，实现与其他系统或设备的业务交互，而需要在上线前进行的各系统间的协同验证。验证工作由执勤信息系统平台软件供应方主导、组织和执行，由设备供应方共同参与。

系统调联调验证对于平台软件能否按期投入试运行并尽快达到理想状态是至关重要的，经验告诉我们，如果仅仅在安装全部完成后进行调试，往往会将工程的验收一拖再拖，因此我们调试工作和安装是交叉进行的，安装一套设备调试一套设备，当各系统的安装基本结束，调试工作也已完成了一半。

完成系统安装后，验证工程师和维护工程师即可对系统进行调试，验证系统在实际环境下的运行情况。若发现问题，立即通知开发人员进行修正。验证工程师和维护工程师需要编写系统调试报告。

联调验证等同于系统间接口的 UAT 验证，联调验证中的需要软件平台提供商和平台支撑硬件设备提供商共同参与，采购方业务责任人员需对整个联调验证的业务功能进行验证和确定。

联调验证在整个平台软件生命周期中的阶段和位置如下图所示：



联调验证的发起应在集成验证阶段结束后、系统部署上线开始前。

通过联调验证，可以最大限度的暴露并解决问题，以确保执勤信息系统平台上线后能够正常使用，满足执勤信息系统的业务需求，保证各硬件设备和业务系统能够通过勤信息系统平台软件实现正常的执勤管理业务。

1.1.1.13.2、联调验证范围

系统安装完成后，按照系统要求的基本功能、性能逐一验证。

联调验证由连通性验证、功能性验证、性能验证三部分组成。

1.1.1.13.2.1、连通性验证

连通性验证是指系统集成商在进行联调验证执行前，对所有需要调用的执勤系统支撑设备、业务系统的基本功能所进行的简单验证。连通性验证强调设备和系统能否被正常调用，而不进行业务层面验证。

连通性验证的目的是为了保证在联调验证执行阶段，平台软件能够顺利连接，能够正常调用需要接入的设备或系统的功能接口，连通性验证包含网络连通性验证及功能连通性验证两部分工作。

连通性验证之前应完成以下工作：

1、 确保联调验证环境搭建完毕

2、 网络策略开通完毕

3、 设备或系统提供方完成设备或系统部署

4、 执勤信息系统平台完成服务部署

1.1.1.13.2.2、功能验证

功能性验证是指执勤信息系统平台按照已编写完成的验证用例进行验证验证，尽可能的发现潜在问题。功能性验证重在全面覆盖业务场景。

功能性验证是联调验证的重点，是执勤信息系统平台正常使用的保障。

功能性验证之前应完成以下工作：

1、完成连通性验证

2、完成验证设计，包括验证用例和验证数据的编写审核

1.1.1.13.2.3、性能验证

性能验证是指执勤信息系统平台按平台性能需求，利用工具进行平台并发、视频延时、响应时间、报警延时等性能指标进行验证，以验证平台是否满足客户需求。

1.1.1.13.3、验证组织机构

验证的具体组织机构如下所示：