ICS 43.020

CCS T 40

团　　体　　标　　准

T/GHDQ 103-2022

智能网联汽车服务平台信息安全技术要求

Intelligent Internet connected vehicle service platform technical requirements

2022-11-02 发布　　2022-11-03 实施

吉林省汽车电子协会　发 布

目　　次

前　言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国第一汽车集团有限公司智能网联开发院、启明信息技术股份有限公司联合提出。

本文件由吉林省汽车电子协会归口。

本文件由吉林省汽车电子协会组织实施。

本文件主要起草单位：启明信息技术股份有限公司、中国第一汽车集团有限公司智能网联开发院。

本文件主要起草人：刘磊、宋迎亮、蒋澈、张鸿彪、魏利、徐焕、曾宪宇、王鹏、郭彧、尤涛、陈明、李木犀。

本文件参与起草单位：中国汽车技术研究中心有限公司、东风汽车集团有限公司技术中心、吉林大学汽车仿真与控制国家重点实验室、中国汽车工程研究院股份有限公司、上汽通用五菱汽车股份有限公司、宇通客车股份有限公司、三六零数字安全科技集团有限公司、一汽解放汽车有限公司商用车开发院、一汽-大众汽车有限公司、中电信数智科技有限公司长春分公司、中电福富信息科技有限公司。

本文件参与起草人：李宝田、孙伟、周海鹰、李杰、全代勇、杨品章、陈炼松、杨军涛、田雪、高德志、王博、高深、李新坚。

本文件审查人：杨彦鼎（东风汽车集团有限公司技术中心）、夏国强（中国汽车工程研究院股份有限公司）、马文峰（一汽奔腾轿车有限公司）、马喜来（一汽解放汽车有限公司）、占锐（东风汽车集团有限公司技术中心）、孔晓霜（中国第一汽车集团有限公司创新技术研究院）。

本文件为首次发布。

引　言

随着智能化和网联化的快速发展，智能网联汽车的渗透率和保有量不断增加，面临的用车场景也越来越复杂，快速发展的技术和日益复杂的应用场景需要网联平台不断迭代升级。智能网联汽车信息安全事件也呈现复杂性和多样性的特点，可能会对个人、企业、甚至国家公共安全造成危害，需要强化智能网联汽车的安全保障。

为了保证智能网联汽车服务平台在提供相关汽车智能网联服务的同时，能够保障网联服务的安全可靠性，吉林省汽车电子协会联合各相关单位起草了系列标准。在本标准中，主要补充制定了智能网联汽车服务平台信息安全的相关技术要求。

智能网联汽车服务平台技术要求

1 范围

本文件规定了智能网联汽车服务平台信息安全技术要求，主要包括基础设施安全、平台安全、业务服务安全、开发运维安全。

本文件适用于智能网联汽车服务平台。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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/T 20271-2006 信息安全技术 信息系统通用安全技术要求

GB/T 25069-2022 信息安全技术术语

GB/T 32400-2015 信息技术 云计算 概览与词汇

GB/T 40861-2021 汽车信息安全通用技术要求

YDT 3752-2020 车联网信息服务平台安全防护技术要求

3 术语和定义

GB/T 20271、GB/T 25069、GB/T 31167、GB/T 32400界定的以及下列术语和定义适用于本文件。

3.1

智能网联汽车服务平台 Intelligent connected vehicle service platform

负责车辆及相关设备接入、管理、存储、计算和监控，为车主和企业提供各种应用服务。

3.2

虚拟机 Virtual Machine

虚拟机指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。

3.3

漏洞扫描 Vulnerability scanning

漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测（渗透攻击）行为。

3.4

容器镜像文件 Dockerfile

Dockerfile是一个包含用于组合映像的命令的文本文档。可以使用在命令行中调用任何命令。Docker通过读取Dockerfile中的指令自动生成映像。

4 智能网联汽车服务平台概述

智能网联汽车服务平台是面向汽车产业网联化、自动化、智能化需求，利用无线通信网络、互联网等信息通信技术，为车辆驾乘人员以及行业管理等提供的信息服务，支撑汽车和交通服务新模式新业态的信息服务平台。

基于图 1 所示的车联网“云-管-端”架构，车联网信息服务平台位于“云端”，其体系架构依据行业应用情况。

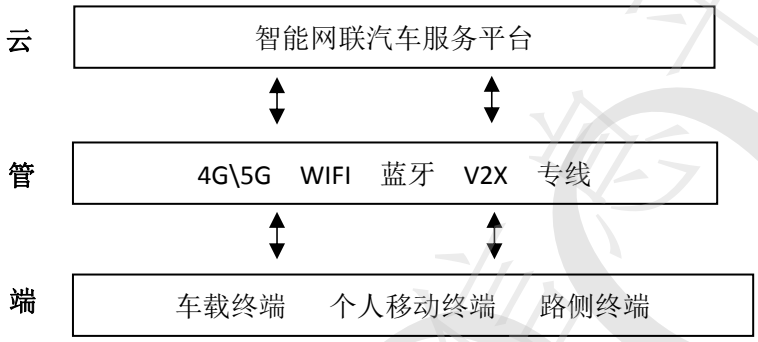

图 1 端管云架构

平台架构分为基础设施、基础平台、业务服务三层。

开发运维过程包括需求、设计、开发、测试、发布、运维六个部分。

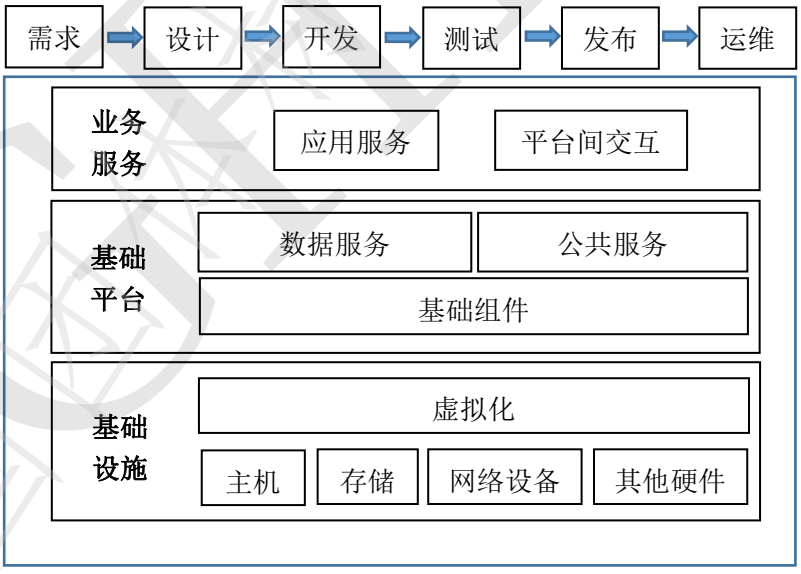

图 2 智能网联汽车服务平台架构

5 基础设施安全

5.1 物理设施安全防护要求

5.1.1 机房场地选择

机房场地选择符合以下要求：

a) 机房场地选择在具有防震、防风和防雨等能力的建筑内；

b) 机房场地避免设在建筑物的顶层或地下室，否则加强防水和防潮措施。

5.1.2 物理访问控制

机房出入口配置电子门禁系统，控制、鉴别和记录进入的人员。

5.1.3 防盗窃和防破坏

防盗窃和防破坏符合以下要求：

a) 将设备或主要部件进行固定，并设置明显的不易除去的标识；

b) 将通信线缆铺设在隐蔽安全处；

c) 设置机房防盗报警系统或设置有专人值守的视频监控系统。

5.1.4 防雷击

防雷击符合以下要求：

a) 将各类机柜、设施和设备等通过接地系统安全接地；

b) 采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。

5.1.5 防火

防火符合以下要求：

a) 机房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，灭火系统应为二氧化碳或卤代烷；

b) 机房及相关的工作房间和辅助房采用具有耐火等级的建筑材料；

c) 对机房划分区域进行管理，区域和区域之间设置隔离防火措施。

5.1.6 防水和防潮

防水和防潮符合以下要求：

a) 采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

b) 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；

c) 安装渗水检测设备，对机房进行防水检测和报警。

5.1.7 防静电

防静电符合以下要求：

a) 采用防静电地板或地面并采用必要的接地防静电措施；

b) 采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。

5.1.8 温湿度控制

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。

5.1.9 电力供应

电力供应符合以下要求：

a) 在机房供电线路上配置稳压器和过电压防护设备；
b) 提供短期的备用电力供应，至少满足设计负荷工作 6 小时以上；
c) 设置冗余或并行的电力电缆线路为计算机系统供电。

5.1.10 电磁防护

电磁防护符合以下要求：

a) 电源线和通信线缆隔离铺设，避免互相干扰；
b) 对关键设备实施电磁屏蔽。

5.2 服务器安全防护要求

5.2.1 身份鉴别

身份鉴别符合以下要求：

a) 对登录服务器的用户进行身份标识和鉴别；用户身份标识具有唯一性，不同用户不能共用身份标识；
b) 身份鉴别信息具有复杂度要求并定期更换；
   口令复杂度要求：至少包含大、小写字母，数字，特殊字符至少四种中的三种；位数至少 8 位；
c) 具有登录失败处理功能，可采取结束会话、限制登录失败次数和自动退出等措施；
d) 远程管理时，采取数据加密措施防止鉴别信息在网络传输过程中被窃听。

5.2.2 访问控制

访问控制符合以下要求：

a) 建立安全的访问控制机制，防止匿名用户未授权访问；禁止未登录用户访问用户登录后的资源；
b) 及时删除或停用多余的、过期的账户，避免共享账户的存在；
c) 允许对访问服务器的地址范围进行限制；

5.2.3 安全审计

安全审计符合以下要求：

a) 审计范围应覆盖服务器上的每个用户；
b) 审计记录应包括事件的日期、时间、类型、主体标识和结果等；
c) 保护审计记录，有效期内避免受到非授权的访问、篡改、覆盖或删除等；
d) 审计日志保存周期不得少于 6 个月。

5.2.4 入侵防范

入侵防范符合以下要求：

a) 遵循最小安装的原则以减小攻击面，关闭不需要的系统服务和端口，仅安装需要的组件和应用程序，保持系统补丁及时得到更新；
b) 通过设定终端接入方式（堡垒机）或网络地址范围对通过网络进行管理的管理终端进行限制。

5.2.5 恶意代码防范

安装防恶意代码软件，并定期进行升级和更新防恶意代码库。

5.3 网络安全防护要求

5.3.1 网络架构

网络架构符合以下要求：

a) 车载终端通过 APN 专线与服务平台进行通信，避免公网通信的安全隐患；
b) 提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。

5.3.2 访问控制

访问控制符合以下要求：

a) 在网络边界或区域之间设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
b) 删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
c) 对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。

5.3.3 安全审计

安全审计符合以下要求：

a) 对网络系统中的网络设备运行状况、网络流量、管理员和运维人员行为等进行日志记录；
b) 审计记录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；
c) 所有网络设备的系统时间应保持一致；
d) 对审计记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等。

5.3.4 网络安全监测要求

网络安全监测符合以下要求：

a) 对网络系统中的网络设备运行状况、网络流量、管理员和运维人员行为等进行监测，识别和记录异常状态；
b) 监测是否对平台服务存在以下攻击行为：端口扫描、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；
c) 当监测到攻击行为时，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。

5.4 虚拟化安全防护要求

5.4.1 虚拟机安全

虚拟机安全符合以下要求：

a) 虚拟机之间、虚拟机与宿主机之间需进行隔离；
b) 虚拟机部署防病毒软件；
c) 保证虚拟机迁移过程中数据和内存的安全可靠，保证虚拟机的完整性和迁移前后安全配置环境的一致性；
d) 保证虚拟机操作系统的完整性，保证虚拟机操作系统不被篡改，且保证虚拟机实现安全启动；
e) 对虚拟机镜像文件进行完整性校验，保证虚拟机镜像不被篡改；
f) 提供最新版本的虚拟机镜像和补丁版本；
g) 定期进行漏洞扫描。

5.4.2 虚拟网络安全

虚拟网络安全符合以下要求：

a) 支持对虚拟网络的逻辑隔离，在虚拟网络边界处实施访问控制策略；
b) 对虚拟机网络出口带宽进行限制。

5.4.3 镜像和快照保护

镜像和快照保护符合以下要求：

a) 针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；
b) 提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改。

6 平台安全

6.1 组件安全

6.1.1 身份鉴别

身份鉴别认证符合以下要求：

a) 对组件的用户进行身份标识和鉴别；管理组件的用户身份标识具有唯一性；
b) 身份鉴别信息应有复杂度要求并定期更换；
c) 口令复杂度要求：至少包含大、小写字母，数字，特殊字符至少四种中的三种；位数至少 8 位；
d) 应启用登录失败处理功能，可采取结束会话、限制非法登陆次数和自动退出等措施；
e) 远程管理时，采取数据加密措施防止鉴别信息在网络传输过程中被窃听。

6.1.2 访问控制

访问控制符合以下要求：

a) 建立安全的访问控制机制，防止匿名用户未授权访问；
b) 建立安全的访问控制机制，禁止未登录用户访问用户登录后的资源；
c) 及时删除或停用多余的、过期的账户，避免共享账户的存在；
d) 在组件权限配置能力内，根据用户业务需要，配置其所需的最小权限。

6.1.3 安全审计

安全审计符合以下要求：

a) 审计范围应覆盖使用的组件上的每个用户；
b) 审计记录应包括事件的日期、时间、类型、主体标识和结果等；
c) 保护审计记录，有效期内避免受到非授权的访问、篡改、覆盖或删除等。

6.1.4 开放接口安全

开放接口安全符合以下要求：

a) 组件有与外部组件或应用之间开放接口的安全管控措施,接口协议操作通过接口代码审计、黑、白名单等控制措施保证交互符合接口规范；
b) 对关键接口的调用情况进行技术监控，如调用频率、调用来源等；
c) 用开放接口生成的业务应用在供用户下载之前也应通过安全检测。

6.1.5 监控预警

监控预警符合以下要求：

a) 部署相关系统平台能够对各类安全事件进行分析并通过声光等方式实时报警；

b) 核查监测范围是否能够覆盖网络所有关键路径；
c) 防止漏洞利用攻击和突破；
d) 报警时生成相应监控日志，并对关键管理人员进行邮件通报。

6.2 数据管理安全

6.2.1 数据采集

数据采集符合以下要求：
a) 对数据源的真实性进行验证；
b) 在确认真实数据源的基础上，对数据源进行身份验证；
c) 根据数据敏感度进行分类分级。分为一般数据、重要数据和敏感数据。

1）一般数据指在车联网信息服务运行过程中，车联网各主体间进行信息交互时的一般性、能公开获取或能在一定范围内公开的数据；

2）重要数据是指在车联网信息服务运行过程中，车联网各主体间进行信息交互时的数据，通过这些数 据能一定程度标识或识别到特定的车联网信息服务的主体、对象或其垂要特征；

3）敏感数据是指在车联网信息服务运行过程中，车联网各主体间进行信息交互时的数据，通过这些数 据能唯一标识或识别到特定的车联网信息服务主体、对象或其敏感特征，符合国家相关法律条款。

6.2.2 数据存储

数据存储符合如下要求：
a) 采用密码技术支持的保密性保护机制对存储数据的保密性提供保护,针对敏感级数据支持密钥管理机制对敏感数据进行加密；
b) 能够检测到数据在存储过程中完整性受到破坏，防止数据被篡改、删除和插入等操作。在数据完整性遭到破坏时，提供授权用户可察觉的告警信息，并在检测到完整性错误时采取必要的恢复措施；
c) 设置数据访问规则，非授权用户不能访问和更改数据的访问权限。

6.2.3 数据传输

数据传输符合以下要求：
a) 保证数据传输的保密性（如鉴别信息，指用于鉴定用户身份是否合法的信息，重要和敏感数据等）；
b) 保证数据传输的完整性,能够检测到数据在传输过程中完整性受到破坏，并能够在检测到完整性遭到破坏时采取必要的措施恢复或重新获取数据。

6.2.4 数据使用

数据使用符合以下要求：
a) 对数据的使用进行授权和验证；
b) 保证数据使用的目的和范围符合国家相关法律法规的要求；
c) 对敏感数据的使用进行审计，并形成审计日志；
d) 支持敏感数据使用过程中的动态脱敏。

6.2.5 数据共享

数据共享符合以下要求：

a) 制定共享方案，并进行共享方案可行性评估与风险评估，确定制定数据共享风险控制措施；
b) 进行数据共享前的网络安全能力评估，保证数据共享的安全实施；
c) 保证数据在不同数据设备之间共享不影响业务应用的连续性；
d) 数据共享中应做好数据备份及恢复相关工作。

6.2.6 数据备份与恢复

数据备份与恢复符合以下要求：

a) 提供本地数据备份与恢复功能，进行定期备份，或提供多副本备份机制；
b) 提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；
c) 提供重要数据处理系统的热冗余，保证系统的高可用性；
d) 备份数据与原数据具有相同的访问控制权限和安全存储要求；
e) 提供身份认证等安全认证措施，保证仅授权用户知情或控制下才能执行本地和远程备份和恢复数据的操作。

6.2.7 数据销毁

数据销毁符合以下要求：

a) 建立数据销毁策略和管理制度，明确销毁对象和流程：并建立数据销毁审批机制，设置销毁相关监督角色，监督操作过程；
b) 能够提供手段协助清除数据因不同设备间共享、业务终止、自然灾害、合同终止等遗留的数据，对日志的留存期限符合国家有关规定；
c) 提供手段清除数据的所有副本；
d) 保证文件、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消除；
e) 提供手段禁止被销毁数据的恢复。

6.3 容器安全防护

6.3.1 镜像安全

镜像安全符合以下要求：

a) Dockerfile 不要存储密码等敏感信息；
b) Dockerfile 不要添加不必要的应用，如 SSH、Telnet 等；
c) 避免以超级用户身份运行容器；
d) 定期扫描及时发现容器镜像中的安全漏洞并采取防范措施；
e) 开启信任机制，保证容器镜像从镜像仓库到用户端的完整性；
f) 避免私有仓库暴露在公网中；
g) 需要对 Docker 容器运行时的各项性能指标进行实时监控。

6.3.2 容器虚拟化安全

容器虚拟化安全符合以下要求：

a) 限制每个容器的磁盘使用量；
b) 使用内存限制机制来防止一个容器消耗所有主机资源的拒绝服务攻击；

c） 限制容器能力，只保留需要的系统功能。

6.3.3 容器网络安全

容器网络安全符合以下要求：

a） 按需配置网络访问控制；

b） 对容器之间的通信流量进行限制。

7 业务服务安全

7.1 应用服务安全

7.1.1 运营管理安全

身份鉴别符合以下要求：

a） 对用户进行身份标识和鉴别；用户身份标识具有唯一性，不同用户不能共用身份标识；

b） 身份鉴别信息具有复杂度要求并定期更换，更换时间间隔应不超过三个月；采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现；

需具有口令复杂度限制功能，并在设置密码、修改密码、重置密码的时候进行密码复杂度校验：

1） 口令复杂度要求：口令复杂度要求：至少包含大、小写字母，数字，特殊字符至少四种中的三种；位数至少 8 位；

2） 不能使用和用户名相同的密码；

3） 避免使用默认口令，如果使用，则在用户首次登录时，强制用户修改密码；

4） 非前台客户密码，强制定期更改密码，并根据系统实际使用情况环境设置密码更新周期频率；

5） 系统在设置密码、修改密码、重置密码时，对口令复杂度、强度在服务端进行校验；

6） 在设置密码、修改密码、重置密码时，给予用户或客户明确提示“不建议将密码设置成与常用软件、网站相同或相似的用户名和密码组合”；

7） 修改后的密码不能与前 5 个密码一致，若一致，则提示（或拒绝）用户。

c） 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自动退出等措施；

d） 对于客户身份鉴别类等敏感信息，采取应用层即时数据加密措施加密传输，防止数据被非法截获；

e） 重要操作时，系统应在服务器端对用户输入数据的合法性和有效性进行校验，防止水平越权（如用户 A 通过修改账号 ID 越权对用户 B 的账号进行操作）；

f） 防止垂直越权：重要操作时，对用户权限进行校验，防止垂直越权操作。

1） 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；

2） 在为用户授权时，服务器端按照权限规则对权限进行校验，互斥的权限不能共存于一人如：

用户不能同时拥有操作和审核的权限；

3） 在重要操作（如账号增删改、授权、业务操作、业务审批）时，系统在服务器端对当前用户的权限进行校验，防止垂直越权。

7.1.2 移动终端访问安全

移动端访问服务平台符合以下要求：

a) 移动端登录需手机号、密码、验证码、生物识别；
b) 对于客户身份鉴别类等敏感信息，采取应用层即时数据加密措施加密传输，防止数据被非法截获；
c) 重要操作（如远控等操作）增加个人识别码验证，如 PIN 码等；
d) 建立安全的访问控制机制，禁止未登录用户访问用户登录后的资源。

7.1.3 设备接入安全

接入控制符合以下要求：
a) 采用安全证书进行双向身份认证，保证只有授权的设备节点可以接入；
b) 定期更换设备通信秘钥；
c) 只有授权的用户才能进行设备配置和操作。

7.1.4 安全审计

安全审计符合以下要求：
a) 审计范围覆盖到用户在业务应用中的关键操作、重要行为、服务调用情况等重要事件；
b) 对审计记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等；
c) 定期针对审计日志进行人工审计。

7.2 平台间安全

7.2.1 访问控制

访问控制符合以下要求：
a) 平台间访问需要进行安全证书认证和访问密钥；
b) 认证信息需要定期更换。

7.2.2 数据校验

对各触点端和其他平台传入的数据进行有效性校验。

7.2.3 通信传输安全

通信传输安全符合以下要求：
a) 采用校验技术或密码技术保证通信过程中数据的完整性；
b) 采用密码技术保证通信过程中数据的保密性。

7.2.4 隐私保护

隐私保护符合国家个人信息保护法相关要求。加到引用文件里。

8 开发运维安全

8.1 开发安全

8.1.1 安全的开发工具

安全的开发工具符合以下要求：
a) 所有开发团队使用经过安全检查的开发工具；
b) 使用稳定的无安全隐患的开发工具。

8.1.2 禁用不安全的函数和 API

保证使用的所有函数和 API 是安全的，并禁用确定为不安全的函数和 API。

8.1.3 代码静态扫描

使用代码安全扫描工具对源代码执行静态分析，保证代码安全。

8.1.4 源码保护

源码保护符合以下要求：

a) 对源代码分级，按实际业务种类进行分级处理；
b) 进行源码访问控制，设置访问权限。

8.2 测试安全

8.2.1 动态程序分析

动态程序分析符合以下要求：

a) 为保证程序功能按照设计方式工作，有必要对软件程序进行运行时验证；
b) 使用运行时工具（如 AppVerifier）以及其他方法（如模糊测试）来实现所需级别的安全测试覆盖率。

8.2.2 隐私数据保护

不能用生产数据中的隐私数据进行测试。

8.3 发布安全

8.3.1 渗透测试

渗透测试是对软件系统进行的白盒安全分析，由专业安全团队通过模拟黑客操作执行。

8.3.2 漏洞扫描

漏洞扫描符合以下要求：

a) 扫描虚拟机 VMs、主机映像、容器和类似的组件的全部内容，以发现操作系统、应用程序平台和商业软件的漏洞。还应根据行业最佳实践标准的安全配置加固指引，对操作系统和应用程序平台的配置开展扫描；
b) 在运行之前，对容器镜像、小程序、APP 等进行深度的漏洞扫描；
c) 对镜像模板文件、镜像软件、镜像恶意文件、镜像敏感文件、镜像开源许可、阻断镜像构建进行漏洞扫描。

8.4 运维安全

8.4.1 漏洞和风险管理

漏洞与风险管理符合以下要求：

a) 取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；
b) 定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

8.4.2 网络和系统安全管理

网络与系统安全管理符合以下要求：

a) 划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
b) 指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
c) 建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
d) 制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；
e) 详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；
f) 指定专门的部门或人员对日志、检测和报警数据等进行分析、统计，及时发现可疑行为；
g) 严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；
h) 严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；
i) 严格控制远程运维的开通，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；
j) 保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略行为。

8.4.3 访问控制

访问控制符合以下要求：

a) 由授权主体配置访问控制策略，并严格限制默认用户的访问权限；
b) 严格限制各用户的访问权限，按安全策略要求控制用户对业务、数据、网络资源等的访问。

8.4.4 恶意代码防范管理

恶意代码防范管理符合以下要求：

a) 提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；
b) 定期验证防范恶意代码攻击的技术措施的有效性。

8.4.5 配置管理

配置管理符合以下要求：

a) 记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；
b) 将基本设备信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

8.4.6 变更管理

变更管理符合以下要求：

a) 明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；
b) 建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；
c) 建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

8.4.7 备份与恢复管理

备份与恢复管理符合以下要求：

a) 识别需要定期备份的重要业务信息、系统数据及软件系统等；
b) 规定备份信息的备份方式、备份频度、存储介质、保存期等；
c) 根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

8.4.8 安全监控

监控符合以下要求：
a) 容器/主机内进程行为监控；
b) 容器/主机内文件行为监控；
c) 容器/主机内网络行为监控；
d) 容器系统调用监控；
e) 需部署相关系统平台能够对各类安全事件进行分析并通过声光等方式实时报警；报警时生成相应监控日志，并对关键管理人员进行邮件通报；
f) 监测范围需能够覆盖网络所有关键路径。

8.4.9 安全事件处置

安全事件处置符合以下要求：
a) 及时向安全管理部门报告所发现的安全弱点和可疑事件；
b) 制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；
c) 在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；
d) 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

8.4.10 应急预案管理

应急预案管理符合以下要求：
a) 规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；
b) 制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；
c) 定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；
d) 定期对原有的应急预案重新评估，修订完善。

8.4.11 风险处理

a) 恶意镜像禁止运行；
b) 容器内恶意行为阻断。

8.4.12 日志安全

日志安全符合以下要求：
a) 在考虑业务系统稳定运行的前提下，保证日志记录完整，满足安全管理要求；
b) 日志记录中禁止包含业务的敏感信息，避免因日志分析导致业务敏感数据泄密。

参 考 文 献

[1] GB/T 22239-2019信息安全技术网络安全等级保护基本要求
[2] GB/T 31167-2014信息安全技术云计算服务安全指南