|  |  |
| --- | --- |
| ICS |  |
| CCS | 点击此处添加CCS号 |

|  |
| --- |
| 11 |

北京市地方标准

DB XX/T XXXX—XXXX

车路云一体化路侧智能基础设施

第6部分：信息安全技术要求

P

Roadside infrastructure of Vehicle-Road-Cloud integration Part 6：Technical Requirements for Cybersecurity

（征求意见稿）

XXXX - XX - XX发布

XXXX - XX - XX实施

       发布

目次

[前言 II](#_Toc183619586)

[1 范围 1](#_Toc183619587)

[2 规范性引用文件 1](#_Toc183619588)

[3 术语和定义 1](#_Toc183619589)

[4 缩略语 2](#_Toc183619590)

[5 信息安全架构 3](#_Toc183619591)

[6 通用安全要求 3](#_Toc183619592)

[7 通信网络安全要求 7](#_Toc183619593)

[8 软件升级安全要求 8](#_Toc183619594)

[9 数据安全要求 9](#_Toc183619595)

[参 考 文 献 10](#_Toc183619596)

1. 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。

本文件是DB11/T 2328《车路云一体化路侧基础设施》的第6部分。

本文件由北京市经济和信息化局提出。

本文件由北京市市场监督管理局归口并实施。

本文件起草单位：

本文件主要起草人：

1. 引言

本系列文件通过提出车路云一体化路侧基础设施的组成及架构、建设要求、运维要求、信息安全要求等内容，为车路云一体化路侧基础设施设计、开发、集成提供参考，有效推动车路云一体化路侧基础设施的标准化建设。本系列文件拟分为7个部分。

车路云一体化路侧智能基础设施 第6部分：信息安全技术要求

* 1. 范围

本文件规定了车路云一体化路侧智能基础设施的信息安全技术要求，其中包括通用安全要求、通信网络安全要求、软件升级安全要求、数据安全要求的内容。

本文件适用于车路云一体化路侧智能基础设施中具备操作系统的路侧基础设施的信息安全的设计、实现和管理。

* 1. 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 15852 信息技术 安全技术 消息鉴别码

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32918 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 35275 信息安全技术 SM2密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2密码算法使用规范

GB/T 39786 信息安全技术 信息系统密码应用基本要求

YD/T 3957 基于LTE的车联网无线通信技术 安全证书管理系统技术要求

* 1. 术语和定义

下列术语和定义适用于本文件。

3.1

车路云一体化系统 Vehicle-Road-Cloud integration

采用无线通信和互联网技术，全方位实施车车、车路信息实时交互，并在全时空动态交通信息采集与融合的基础上开展车辆主动安全控制和道路协同管理，实现人、车、路的有效协同，从而形成安全、高效和环保的道路交通系统。

3.2

路侧计算单元 roadside computing unit

部署在道路、公路沿线或者场端，配合其他设施或系统完成交通信息汇聚、处理与决策的计算模块、设备或设施。

3.3

路侧通信单元 roadside communication unit

设置于道路路侧或龙门架等位置，具备无线或有线连接方式的产品或功能集成产品。

3.4

路侧感知单元 roadside sensing unit

设置于道路路侧或龙门架等位置，具备感知功能的传感器或传感器集，用于对道路交通运行情况、交通参与者、交通事件等检测识别，包括但不限于激光雷达、摄像头、毫米波雷达等产品。

3.5

路侧基础设施 roadside infrastructure

车路云一体化中的路侧计算单元、路侧通信单元、路侧感知单元等设备的统称。

3.6

路侧基础设施管理系统 roadside infrastructure management system

对路侧基础设施进行接入、认证、授权、审计日志收集、配置策略下发等统一管理的系统。

3.7

重要数据 important data

一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益或者个人、组织合法权益的数据，包括：

—— 军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据；

—— 车辆流量、物流等反映经济运行情况的数据；

—— 汽车充电网的运行数据；

—— 包含人脸信息、车牌信息等的车外视频、图像数据；

—— 涉及个人信息主体超过10万人的个人信息；

—— 国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。

[来源：汽车数据安全管理若干规定（试行），第三条]

3.8

安全启动 secure boot

对系统启动中的各个组件进行逐级验证，实现启动过程的完整性和真实性保证。

* 1. 缩略语

以下缩略语适用于本文件。

4G：第四代移动通信技术（the 4th Generation Mobile Communication Technology）

5G：第五代移动通信技术（the 5th Generation Mobile Communication Technology）

ACL：访问控制列表（Access Control List）

CVE：通用漏洞和风险（Common Vulnerabilities & Exposures）

CNNVD：中国国家信息安全漏洞库(China National Vulnerability Database of Information Security)

HTML：超文本标记语言（Hyper Text Markup Language）

IP：网际互联协议（Internet Protocol）

ID：身份标识号码（IDentity）

LTE-V2X：基于LTE的车用无线通信技术（LTE Vehicle to Everything）

MAC：媒体存取控制（Media Access Control）

PCB：印制电路板（Printed Circuit Board）

RFID：射频识别（Radio Frequency Identification）

SMS：短信息服务（Short Message Service）

TLCP：传输层密码协议（Transport layer cryptography protocol）

TLS：传输层安全协议（Transport Layer Security）

USB：通用串行总线（Universal Serial Bus）

URL：统一资源定位系统（Uniform Resource Locator）

WLAN：无线局域网络（Wireless Local Area Network）

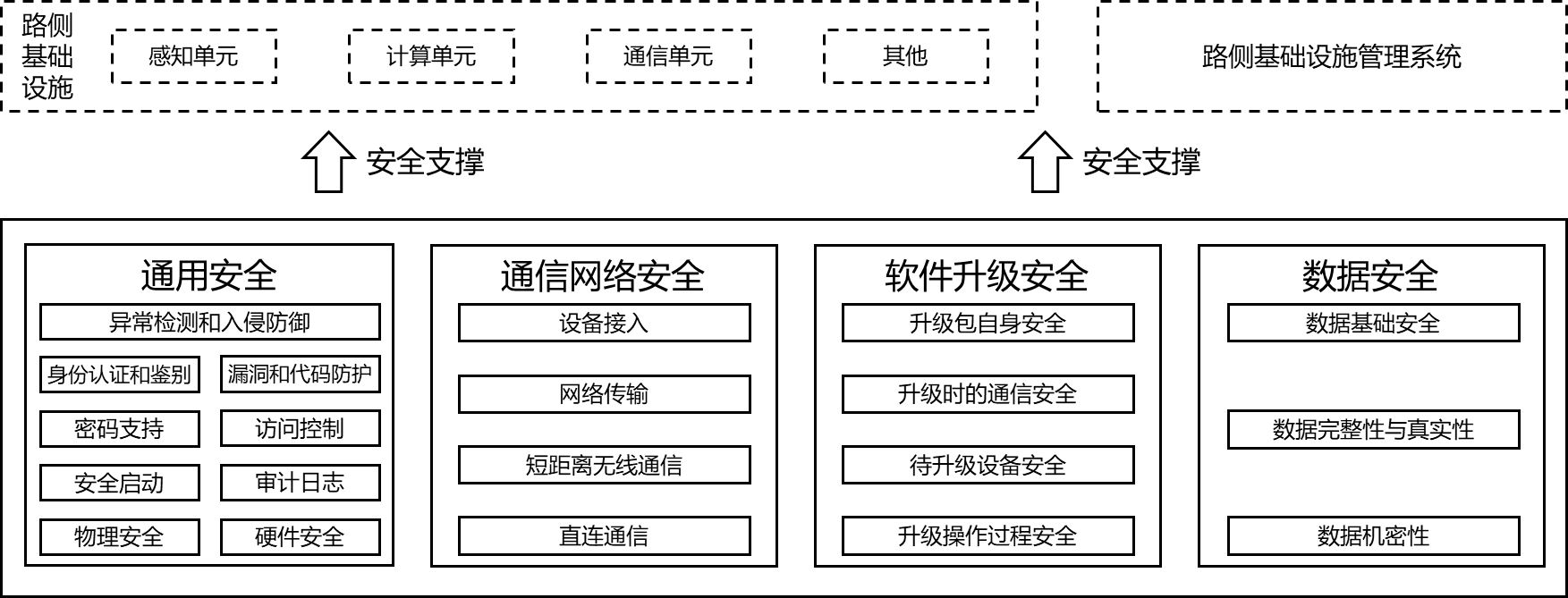
TCM：可信密码模块（Trusted Cryptography Module）

TPCM：可信平台控制模块（Trusted Platform Control Module）

TPM：可信平台模块（Trusted Platform Module）

* 1. 信息安全架构

车路云一体化路侧基础设施包括感知单元、计算单元、通信单元等，依托路侧基础设施管理系统，形成一套完整的车路云一体化路侧基础设施业务体系，为充分实现该业务体系的安全保障能力，从通用安全、通信网络安全、软件升级安全、数据安全等方面提出安全要求，为车路云一体化系统相关业务提供安全支撑。通用安全方面提出物理安全、硬件安全、安全启动、审计日志、身份认证和鉴别、访问控制、漏洞和代码防护、异常检测和入侵防范、密码支持等要求。通信网络安全方面提出设备接入、网络传输、短距离无线通信及直连通信等要求。软件升级安全方面提出升级包自身安全、升级时的通信安全、待升级设备安全及升级操作过程安全等要求。数据安全方面提出数据基础安全、数据完整性与真实性及数据机密性等要求。车路云一体化路侧基础设施信息安全架构见图1。



1. 车路云一体化路侧基础设施信息安全架构图
   1. 通用安全要求
      1. 物理安全

路侧基础设施应结合其应用及安全需求，采取防物理破坏、防雷、防水、防尘等措施。所处物理环境不应会对设施造成物理破坏，如挤压、强振动等。

路侧基础设施应具备可供长时间工作的稳定电力供应。

可参照GB/T 22239等级保护第二级以上相关要求。

* + 1. 硬件安全

硬件PCB应关闭非必要的接口，不应存在后门或隐蔽接口，调试接口应禁用或设置安全访问控制；

硬件PCB及芯片不可暴露用以标注端口和管脚功能的可读丝印；

用于存储重要数据的关键芯片及安全芯片，应减少暴露管脚；

可具备常见侧信道攻击（功耗差分分析、电磁差分分析、电流故障注入、电磁故障注入）的防范措施。

* + 1. 安全启动

路侧通信单元和路侧计算单元应具备安全启动功能。

可基于可信根对系统引导程序、系统程序等进行可信验证；可通过可信根实体对安全启动所使用的可信根进行保护，可信根实体包括OTP、TPM、TCM、TPCM等，可信根实体应当具备一次性写入不可修改特性。

安全启动覆盖范围至少包含从引导程序到系统内核。

* + 1. 审计日志

审计日志事件应包括但不限于：用户登录、用户操作、配置变更和信息安全事件等。

审计日志内容应包括但不限于：事件的时间、操作IP地址、主体标识、客体标识、类型和结果等。

审计日志中应禁止以明文形式存储密钥（不含公钥与证书）、口令等信息。

应具有访问控制机制，防止对审计日志进行非授权访问，避免受到非逾期的删除、修改或覆盖等。

审计日志应定期备份，审计日志保留时间不应少于6个月，如通过本地或集中方式进行备份。

* + 1. 身份认证和鉴别

路侧基础设施对用户的身份认证和鉴别功能，使用口令鉴别方式时，应支持首次登录时强制修改默认口令或设置口令，支持设置口令生存周期不长于3个月，支持口令复杂度检查、口令错误次数限制。

路侧基础设施之间的身份认证和鉴别功能，应具备可用于通信识别的唯一标识，如采用设备ID、序列号、MAC地址或其组合等作为唯一标识；应基于唯一标识或结合密码技术进行身份认证和鉴别。

路侧基础设施与智能网联汽车的身份认证和鉴别功能，应符合7.4.1中的要求。

路侧基础设施接入路侧基础设施管理系统的身份认证和鉴别功能，应基于路侧基础设施唯一标识对其进行身份认证和鉴别；应具备对路侧基础设施进行周期性接入认证的能力，及时感知设备出现的认证异常。

路侧基础设施管理系统对用户的身份认证和鉴别功能包括：

* 1. 应对登录路侧基础设施管理系统的用户进行身份认证和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
  2. 应采用口令、密码技术、生物识别技术等两种或两种以上组合的鉴别技术对登录路侧基础设施管理系统的用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现；使用口令鉴别方式时，应符合6.5.1中的要求；
  3. 应对登录路侧基础设施管理系统的用户身份鉴别信息进行安全保护，保障用户鉴别信息存储的机密性和完整性，以及传输过程中的机密性和完整性；
  4. 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数，宜不超过5次，超过次数时，限制5分钟后再登录和当登录连接超时自动退出等相关措施。
     1. 访问控制

系统访问控制策略要求如下：

* 1. 应对不同的用户设置不同的账户和权限；
  2. 应依据访问数据的不同类型与安全级别进行不同的策略设计；
  3. 不同类型安全级别的访问控制应与用户身份认证鉴别功能绑定，如基于身份的用户鉴别安全机制，增加多级控制机制；
  4. 数据库系统与文件系统应设计用户鉴别和访问控制策略，并遵循最小授权原则对各类系统访问用户配置访问控制策略；
  5. 访问控制策略应使用白名单机制，明确定义允许的行为，其他一切行为都将被阻止；
  6. 应建立面向数据应用的安全控制机制，包括访问控制时效的管理和验证，以及应用接入数据存储的合法性和安全性取证机制；
  7. 应具备登录失败处理功能，如采用结束会话、限制非法登录次数和网络登录连接超时自动退出等措施，符合6.5.5 4)中的要求；
  8. 访问控制策略变更时，应进行评估，经审核批准后方可实施变更，并记录操作日志。
  9. 默认状态下应仅开启必要的服务和对应的端口，应明示所有默认开启的服务、对应的端口及用途，应支持用户关闭默认开启的服务和对应的端口；
  10. 非默认开放的端口和服务，应在用户知晓且同意后方可开启；如建立端口监测功能，对非法开启的端口进行感知、告警。
  11. 路侧基础设施硬件设备的外部接口、其他调试接口等应进行访问控制保护，禁止非授权用户访问。对USB设备、移动光驱等外部存储设备应进行严格的接入管控，默认状态下接入后无法使用。
  12. 在设备具备身份认证的基础上，访问控制可采用基于属性或者角色的访问控制策略对用户进行授权管理和访问控制；
  13. 可建立基于设备行为的数据存储安全监测与控制机制；

数据存储系统访问控制要求如下：

* 1. 应设计数据存储系统的访问控制策略和访问控制机制，对访问对象的访问范围和操作权限进行限定，确保不超出预定义的范围，且满足最小授权原则；
  2. 应使用存储访问控制模块部署数据用户身份标识与鉴别策略、数据访问控制策略，并执行相关安全控制措施；
  3. 不同类型安全级别的访问控制应与用户身份认证鉴别功能绑定，如基于身份的用户鉴别安全机制，增加多级控制机制。
     1. 漏洞和代码防护

系统应遵循最小安装的原则，仅安装运行需要的组件或应用程序；安装运行需要的组件或应用程序,应使用最新的公开版本。

应通过设定接入方式、网络地址范围等方法对通过网络进行管理的终端进行限制。

应能及时发现可能存在的已知公开漏洞，不应存在权威漏洞库（如：NVDB、CNVD、CVE、CNNVD）公开的6个月及以前的高危以上漏洞，并在经过管理者充分测试评估后，针对高危漏洞应于5日内完成修补或采取风险缓解措施。

宜通过代码混淆、代码加密、代码签名等技术，保护代码免受恶意攻击。

* + 1. 异常检测和入侵防御

入侵检测要求如下：

* 1. 应具有实时获取受保护网段内的数据包的能力用于检测分析各类恶意攻击；
  2. 应监视整个网络或某一指定网口的报文流量和字节流量，如在流量入侵检测之外部署主机入侵检测程序，对智能设备的Linux、Windows等操作系统搜集包含但不限于进程、文件、登录信息等基础安全数据。
  3. 应提供攻击检测与防护能力，如具备对关键网络节点的监测，检测、阻断各类网络攻击行为。

异常分析要求如下：

* 1. 应对收集的网络攻击事件日志、异常流量事件、设备运行异常日志等数据进行分析，发现安全事件；
  2. 应具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力；
  3. 可具有把不同的事件进行关联，发现低危害事件中隐含的高危害攻击的能力。

入侵防御要求如下：

* 1. 当检测到入侵时，应自动采取响应动作以发出安全警告；
  2. 在监测到网络上的非法连接时，应具备阻断能力；
  3. 管理员可对被检测网段中指定的目的设备指定不同的响应方式；
  4. 告警可采取屏幕实时提示、邮件通知、短信通知、系统日志等一种或几种方式组合；
  5. 可具备与防火墙进行联动的能力，可按照设定的联动策略自动调整防火墙配置。

管理控制要求如下：

* 1. 应提供管理、配置入侵检测系统的能力；
  2. 应按照安全事件的严重程度将事件分级，以便从大量的信息中捕捉到危险的事件；
  3. 安全事件数据库中的内容可包括事件的定义和分析内容、详细的恢复处置方案、可采取的对策等；
  4. 可具备策略模板、支持策略的导入和导出；
  5. 可具有远程配置终端入侵检测策略的能力。

检测报告要求如下：

* 1. 应保存检测到的安全事件并记录安全事件信息，日志内容符合6.4.2中的要求。如包括解决方案建议；
  2. 管理员可通过管理界面实时查看安全事件，并生成安全事件的检测结果报告，报告格式如WORD、HTML、PDF等。
     1. 密码支持

路侧基础设施应使用符合GB/T 39786相关要求的密码算法，宜采用国家密码管理主管部门批准的国产商用密码算法。具体要求如下：

* 1. 身份鉴别、数字签名、密钥交换宜采用SM2算法，遵循GB/T 32918、GB/T 35275及GB/T 35276相关要求，为了保证本文件有更好的兼容性和可扩展性，可支持RSA-2048及以上算法。
  2. 数据的完整性保护宜采用基于SM4分组密码算法或者SM3密码杂凑算法的消息鉴别码（MAC）机制，遵循GB/T 15852相关要求。为了保证本文件有更好的兼容性和可扩展性，可支持SHA-256及以上算法。
  3. 数据的对称加解密计算宜采用SM4分组密码算法，遵循GB/T 32907相关要求。为了保证本文件有更好的兼容性和可扩展性，可支持AES-128及以上算法。

路侧基础设施所采用的各种密码设备，如安全芯片、密码模块、服务器密码机、数字签名验证服务器、时间戳服务器等，应遵循密码相关国家和行业标准，并得到国家密码管理主管部门认证核准。

路侧基础设施设备所使用的密钥必须在国家密码管理主管部门批准的密码设备内生成。路侧基础设施设备所涉及的密钥存储、分发、导入或导出、使用、备份与恢复、归档、销毁等密钥全生命周期管理应符合GB/T 39786相关要求。

证书管理应由专门负责发放和管理数字证书的CA提供，作为车路云一体化应用中受信任的第三方电子认证服务提供者，应具有合法的电子认证服务许可证资质，承担公钥体系中公钥的合法性检验的责任，为车路云一体化应用提供具有法律效力的认证服务。为路侧基础设施提供证书认证服务的CA，应提供基于SM2密码算法的证书服务，遵循密码相关国家和行业标准要求。

路侧基础设施设备使用的X.509数字证书应采用获得电子认证服务主管部门许可的第三方ＣＡ颁发的数字证书，数字证书以及CRL格式应遵循GB/T 20518。路侧基础设施设备使用的V2X数字证书应遵循YD/T 3957。

* 1. 通信网络安全要求
     1. 设备接入

不应存在未在产品手册中声明的无线通信服务。

应能够对非授权设备私自联到内部网络的行为进行检查或限制。

可对外部的通信连接进行身份鉴别和授权管理，在未经授权的网络设备接入时，具备发现和告警的功能，拒绝接入并记录日志。

* + 1. 网络传输

基于公共互联网的通信过程应采取安全传输协议，如TLCP、TLS 1.2及以上等，保障通信数据的机密性、完整性和真实性。

应具有针对网络传输的访问控制功能，如根据源地址、目的地址、源端口、目的端口和协议等进行检查。

采用的通信协议不应存在后门，应及时进行安全更新。

* + 1. 短距离无线通信

当路侧基础设施与外界通过蓝牙、WLAN、Zigbee等方式进行短距离无线通信时，应具备启用与关闭短距离无线连接的管理功能，如手动打开、关闭短距通信连接，并对已建立无线连接的状态进行管理。

* + 1. 直连通信

发送端应采用基于数字证书的签名机制保证直连通信消息的真实性、完整性和抗抵赖性。

接收端应验证所接收到的其它直连通信设备发送的数据消息的证书有效性、及签名有效性，并且只对通过验证的数据进行进一步的处理；未通过验证的消息将被丢弃。

* 1. 软件升级安全要求
     1. 升级包自身安全

升级包的开发者使用第三方组件应识别其涉及公开漏洞库中已知的漏洞并安装补丁，不应存在由权威漏洞平台6个月前公布且未经处置的高危及以上的安全漏洞。

升级包应采用签名认证机制保证数据的真实性和完整性。

升级包发布后不应包含调试功能及调试信息，不应包含敏感信息（如个人信息、明文密钥、明文口令等）的接口。

可使用构建工具链提供的堆栈保护、自动引用计数等代码安全机制，提升升级包的安全性。

可使用安全机制防止升级包被逆向分析。

* + 1. 升级时的通信安全

待升级设备应从安全合规的指定站点下载和安装升级包。

升级前，待升级设备与升级服务系统之间应经过严格的双向认证和授权，当身份认证成功后，待升级设备与升级服务系统之间才能进行业务数据的通信交互；发生身份鉴权失败、有加密要求的数据内容校验失败等情况，应终止该响应操作。

待升级设备与升级服务系统之间传输的数据内容应通过密码技术，如TLCP或TLS 1.2及以上等安全通信协议，实现机密性和完整性保护。

* + 1. 待升级设备安全

待升级设备应保证自身的计算环境安全。

应使用由合规的密码设备产生的安全密钥，以便建立安全通信和对服务器的安全访问。

应对外部输入的来源（如用户界面、URL等来源）进行校验。

在接收到升级包后，应立即对其执行真实性和完整性检查，并对未通过验证的升级包执行有效处置。

应支持权限管理并遵守最小授权原则，对不同的应用软件基于实现特定功能分配不同的接口权限，尽量避免使用root用户执行软件升级。

在遭遇如断电或连接中断时，应支持升级失败后的自动回滚，或或支持断点续传功能，防止设备功能失效。

应在升级成功后完成功能自检和审核，保证自身健康性和过程可审核。

应建立ACL，对升级包的读写执行权限予以明确，以便升级包的存储、解析、执行被认证、授权和审核。

* + 1. 升级操作过程安全

升级过程启动前，应确认网络连接、计算环境等基础运行条件，避免升级中断或失败。

在车流高峰期应避免执行软件升级。

升级启动时应执行自检机制，并校验软件完整性。

升级过程若需要采集和处理敏感信息，应采取安全措施确保敏感信息不被其他应用窃取。

升级过程正常退出时，应擦除缓存中的升级包镜像和文件中的敏感信息。

升级过程中途失败时，应确保将系统恢复到最近的可用版本或将系统置于安全状态。

不论升级成功与否，都应对升级过程记录日志，并采取适当的访问控制机制管理日志读取和写入的权限。

若待升级设备无法继续存储或更新日志时，应对日志文件进行安全转储。

可考虑升级启动前安全检查机制、升级启动后自检机制、升级失败回滚机制、数据及隐私保护机制、升级过程日志记录与存储等方面的测试，以提高升级操作过程的安全性。

* 1. 数据安全要求
     1. 数据基础安全

路侧基础设施涉及的数据应进行分类分级，根据不同的数据类别进行相应的安全性保护。

应分别从数据采集、数据存储、数据传输、数据加工、数据提供、数据销毁等数据全生命周期进行相应的安全性保护，在数据不同阶段进行数据完整性、真实性、机密性保护。

根据数据类别及各类业务对数据的使用需要，确定数据存储所必需的最短时间期限。

* + 1. 数据完整性与真实性

数据采集阶段可按照6.5.2中的要求对采集设备进行身份认证和鉴别，保证采集数据来源的真实性。

数据采集阶段可采用数据校验等机制，如基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制的密码技术，保证采集数据的完整性。

数据传输阶段可采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术实现传输数据的完整性保护。

数据存储阶段应采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术确保重要数据存储过程中的完整性，并在检测到完整性错误时采取必要的恢复措施。

* + 1. 数据机密性

数据传输阶段应采用密码技术实现关键数据、鉴别数据和其他重要数据传输的机密性，在进行加密时应采用如AES-128以上、SM4同等或以上强度的加密算法。

身份鉴别如采用密码技术，鉴别数据应采用安全机制（如安全芯片、密码模块等）进行保护。

重要数据应存储在安全区域或以密文形式存储。

重要数据应采用安全机制防止泄漏，如采用加密、脱敏等方法。

数据传输过程中，应对数据发送方和接受方实施身份认证，在建立连接前，利用密码技术进行初始化会话验证，必要时采用经认证的安全传输协议或标准安全协议服务或安全协议服务（TLCP或TLS 1.2及以上），避免来自基于协议的攻击和破坏。

数据保存应依据国家及行业主管部门有关规定以及个人信息主体约定的时限等，针对不同类型的数据设定保存期限，并应采取技术手段，在车路云一体化系统中去除待删除的数据。



参 考 文 献

1. GB 40050-2021 网络关键设备安全通用要求
2. GB 44495—2024 汽车整车信息安全技术要求
3. GB 44496—2024 汽车软件升级通用技术要求
4. GB/T 40861-2021 汽车信息安全通用技术要求
5. GB/T 44464—2024 汽车数据通用要求
6. GB/T 40856-2021 车载信息交互系统 信息安全技术要求及试验方法
7. YD/T 3594-2019 基于LTE的车联网通信安全技术要求
8. YD/T 3707-2020 基于LTE的车联网无线通信技术 网络层技术要求
9. YD/T 3709-2020 基于LTE的车联网无线通信技术 消息层技术要求
10. YD/T 3755-2020 基于LTE的车联网无线通信技术 支持直连通信的路侧设备技术要求
11. YD/T 3751-2020 车联网信息服务 数据安全技术要求

