GY

中华人民共和国广播电影电视行业标准

GY/T 303.2—2016

智能电视操作系统
第2部分：安全

Smart TV operating system
Part 2: Security

2016－12－15 发布　　2016－12－15 实施

国家新闻出版广电总局　　发布

目　　次

前　言

GY/T 303《智能电视操作系统》已经或计划发布以下部分：

——第1部分：功能与架构；

——第2部分：安全；

——第3部分：应用编程接口；

——第4部分：硬件抽象接口；

——第5部分：功能组件接口；

——第6部分：可信执行环境接口；

——第7部分：符合性测试。

本部分为GY/T 303的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由全国广播电影电视标准化技术委员会（SAC/TC 239）归口。

本部分起草单位：国家新闻出版广电总局广播科学研究院、华为技术有限公司、中兴通讯股份有限公司、东方有线网络有限公司、深圳创维-RGB电子有限公司、上海联彤网络通讯技术有限公司、阿里云计算有限公司、深圳市海思半导体有限公司、中国科学院声学研究所、中国科学院信息工程研究所、陕西广电网络传媒（集团）股份有限公司、上海下一代广播电视网应用实验室有限公司、中国科学院软件研究所、北京数码视讯科技股份有限公司、北京永新视博数字电视技术有限公司、北京数字太和科技有限责任公司、上海兆芯集成电路有限公司、晨星软件研发（深圳）有限公司、腾讯科技(深圳)有限公司、华数数字电视传媒集团有限公司、深圳市茁壮网络股份有限公司、湖南国科微电子股份有限公司、北京海尔集成电路设计有限公司、创维数字技术股份有限公司、杭州国芯科技股份有限公司、上海高清数字科技产业有限公司、北京泰合志远科技有限公司。

本部分主要起草人：盛志凡、郭沛宇、解伟、刘金晓、王东飞、王继刚、万乾荣、郭晓霞、朱佩江、杨明磊、王强、王磊、张伟、张晶、王兴军、熊彬、孙鹏、王亚哲、李斌、王明敏、杨勋、贾庭兰、万倩、严海峰、汤新坤、何剑、方中华、孙明勇、丁送星、郭万永、张震宁、吴迪、徐其桓、周芸、叶建隆、梁志坚、龚克、郗望、郭永伟、郑力铮、张德岭、陈林锋、席岩、游昌海、董进刚、黄新军、来永胜、王旭升、赵良福、朱允斌、白伟、程伯钦、陈亚东、谢振雷、孙鹏、谢长弘、孟庆康、吴坚。

引　言

本部分的发布机构提请注意，声明符合本部分时，可能使用涉及本部分有关内容的相关授权的和正在申请的专利如下：

序号	标准章条号	专利名称
1	7	一种智能电视操作系统
2	7	一种智能电视系统
3	6.5、8.1	一种在智能电视操作系统中支持全媒体播放的方法及智能电视终端
4	8.2	一种用于智能操作系统的条件接收方法和系统
5	8.2	一种用于智能操作系统的条件接收方法和系统
6	8.1	一种用于智能操作系统的数字版权管理（DRM）方法和系统
7	8.1	一种支持数字版权管理（DRM）的媒体网关/终端实现方法及其设备

本部分的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本部分的发布机构保证，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本部分的发布机构备案，相关信息可以通过以下联系方式获得：

专利权利人	联系地址	联系人	邮政编码	电话	电子邮箱
国家新闻出版广电总局广播科学研究院	北京市西城区复兴门外大街2号	孟祥昆	100866	010-86098010	mengxiangkun@abs.ac.cn

请注意除上述专利外，本部分的某些内容仍可能涉及专利。本部分的发布机构不承担识别这些专利的责任。

智能电视操作系统
第2部分：安全

1 范围

GY/T 303的本部分规定了智能电视操作系统的安全体系、安全机制等相关技术要求。

本部分适用于智能电视操作系统的研发、生产和应用。

2 规范性引用文件

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

GY/T 255—2012 可下载条件接收系统规范

GY/T 277—2014 互联网电视数字版权管理技术规范

GY/T 303.1—2016 智能电视操作系统 第1部分：功能与架构

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本部分。

3.1.1

智能电视操作系统 television operating system; TVOS

运行在电视接收终端等终端之上，具备管理系统资源（包括硬件、软件及数据资源）、控制程序执行、支撑应用软件运行等功能的系统软件。

3.2 缩略语

下列缩略语适用于本部分。

API 应用程序编程接口（Application Programming Interface）

App 应用程序（Application）

CA 证书认证机构（Certification Authority）

DCAS 可下载条件接收系统（Downloadable Conditional Access System）

DRM 数字版权管理（Digital Rights Management）

DVB 数字视频广播（Digital Video Broadcasting）

HAL 硬件抽象层（Hardware Abstract Layer）

OS 操作系统（Operating System）

OTP 一次性写入(One Time Programming)

REE 富执行环境（Rich Execution Environment）

ROM 只读存储器（Read-Only Memory）
SELinux Linux强制访问控制安全系统（Security-Enhanced Linux）
SDK 软件开发工具包（Software Development Kit）
TApp 可信应用（trust application）
TEE 可信执行环境（Trusted execution environment）

4 概述

TVOS 安全由 TVOS 安全机制、基础安全能力和安全架构三部分组成。

TVOS 安全机制包括基于可信执行环境的安全计算机制、数字证书安全信任机制、基于安全芯片和硬件安全信任根的安全信任链校验机制、基于安全视频路径的媒体视频内容保护机制等。

TVOS 基础安全能力包括硬件安全、软件安全、网络安全、数据安全、应用安全等全方位安全防护能力。

TVOS 安全架构一方面定义了基于 TVOS 软件架构和安全机制构建和扩展 TVOS 基础安全能力的方式。基于 TVOS 软件架构和安全机制，相关硬件安全、软件安全、网络安全、数据安全和应用安全等安全模块分别置于相应的内核层、硬件抽象层、功能组件层、执行环境层和应用框架层，且位于 TVOS 不同软件功能层的硬件、软件、网络、数据和应用等安全模块通过相互协同，形成相应的硬件安全、软件安全、网络安全、数据安全和应用安全等基础安全能力；在相应的 TVOS 软件功能层，硬件、软件、网络、数据和应用等安全模块可灵活扩充，并与已有的安全模块协同，增强相应的 TVOS 基础安全能力，支撑 TVOS 安全功能的不断扩展。TVOS 安全架构另一方面定义了 TVOS 系统软件和应用软件在运行时进行安全隔离的方式。

业务安全、内容安全、支付安全、安全启动和安全升级等 TVOS 安全功能可基于 TVOS 安全机制、基础安全能力和安全架构来构建，并可通过基础安全能力的提升和安全模块的增加而持续演进增强和扩展。

5 总体安全要求

5.1 一般要求

应符合GY/T 303.1—2016规定的软件架构、组件模型、软件模块和接口等相关要求。

TVOS所承载的应用软件程序只能是JAVA或WEB形态，不能以TVOS组件的插件形态出现。

5.2 基础安全能力要求

5.2.1 基础硬件

应基于安全芯片等底层硬件为 TVOS 的软件安全、网络安全、数据安全和应用安全的实现提供可信执行环境、安全存储区域、硬件层级密钥机制、硬件安全信任根、启动校验、硬件密码算法引擎、密码管理和安全视频路径等硬件安全能力。

5.2.2 基础软件

应能保障系统软件运行的安全，包括系统软件所控制的硬件、计算和数据等系统资源的安全。TVOS应具备如下的软件安全能力：

a) 访问控制

应具备对不同软件模块和应用访问相关数据和文件、调用相关软件模块和操作相关设备资源进行权限配置和管理的能力，使相应软件模块和应用只能按照所指定的安全访问控制权限访问相关数据、调用相关软件模块、操作相关设备资源，防止相应软件模块和应用获取安全敏感数据、执行未授权操作、调用未授权的软件模块，以及防止非授权入侵代码的执行等。应支持 SELinux 安全访问控制机制。

b) 资源访问权限管理

应具备对资源访问的权限进行控制和管理的能力，且能保存和查询应用资源访问权限的信息。应基于SELinux 权限控制机制，要求所有的主体对资源客体的访问必须经过明确的许可，访问主体对资源客体的资源访问权限应由相关安全策略所定义的安全上下文决定；所有客体与主体间均由一个唯一的安全上下文进行关联；在运行期间，特定的进程等访问主体与进程间通信通道、文件和网络主机等资源客体之间的访问控制关系不可自主修改。

c) 根权限

应具备对根权限进程进行跟踪的能力，保障只有进入根权限进程列表的进程才能以根权限模式运行。操作系统根权限不对应用层开放。

d) 数字签名安全校验

应具备基于数字签名技术对应用在安装或运行时进行安全校验的能力，支撑将安全信任链校验机制传递至应用软件。

e) 远程升级

应进行基于安全信任链校验机制的安全校验，只有通过安全校验的系统软件版本才允许在设备上进行远程升级。

f) 本地升级

应进行基于安全信任链校验机制的安全校验，只有通过安全校验的系统软件版本才允许在设备上进行本地升级。

5.2.3 基础网络

应能保障系统运行的网络通信安全，包括网络传输安全和网络入侵防范等。

应具备支持 IPSec 等协议的网络安全协议栈，以支撑防 DOS 攻击、防 ARP 欺骗、IP 地址黑白名单、服务端口接入控制名单（ACL）、网络流量管理统计以及虚拟专用网络（VPN）通道等功能。

5.2.4 基础数据

应能保障系统软件和应用软件运行所产生数据的安全。

应具备通过安全文件系统进行数据安全存储的能力，支持文件句柄随机分配、文件系统安全管理、文件系统内核模块校验、文件完整性校验、数据加解密算法以及关键数据的防回滚机制，确保用户数据不被恶意泄漏和篡改、实现对安全敏感信息的保护等。

5.2.5 基础应用

应能保障合法应用的安全运行、管理应用的安装，包括拒绝非法应用安装、管理应用的系统资源访问权限和控制应用的资源访问等。

应用软件应在进行基于安全信任链校验机制的安全校验，确保应用软件的合法性和完整性后，才能在TVOS上安装运行。

5.3 基本安全功能要求

5.3.1 内容安全

应基于基础安全能力和安全机制保障媒体内容文件安全，确保按照媒体内容许可授权要求安全地播放媒体内容。

5.3.2 业务安全

应基于基础安全能力和安全机制保障媒体内容流的安全，确保按照媒体内容流条件接收授权要求安全地播放媒体内容流。

5.3.3 支付安全

应基于硬件安全和安全机制保障支付相关信息输入和传输交换的安全，支撑支付应用安全地完成相关支付操作。

5.3.4 安全启动

应基于硬件安全和安全机制实现从芯片到引导程序至TVOS软件的安全启动，保障TVOS软件安全运行，防止对系统软件的篡改。

5.3.5 安全升级

应基于硬件安全和安全机制确保升级软件包的合法性和完整性，保障系统软件远程升级和本地升级的安全。

6 安全机制

6.1 可信执行环境（TEE）

TVOS TEE 基于 TVOS 可信安全硬件和可信安全软件实现，为 TVOS 提供可信安全计算环境。

TVOS 可信安全硬件支持安全芯片、安全内存访问控制、安全总线连接、安全中断、安全时钟、安全随机数、安全加解密引擎等功能，支持安全视频路径。

TVOS 可信安全软件包括安全 OS 和 TEE HAL。安全 OS 具备内存管理、安全时间、任务调度、中断、任务通信、加解密等功能，可支持内存隔离、版本防回滚、安全存储、TApp 动态加载；TEE HAL 支持 DRM TApp、DCAS TApp 和支付 TApp 等。

6.2 硬件安全信任根

硬件安全信任根作为内置于安全芯片不可改写安全存储区域中的安全信息，应为系统安全启动、系统软件安全升级、应用软件下载安装的安全信任链校验机制信任根。

6.3 数字证书安全信任机制

数字证书安全信任机制应支持基于 X.509 规范进行分级的安全信任校验，每级安全信任校验应采用对应层级的数字证书。

6.4 安全信任链校验机制

安全信任链校验机制应采用数字证书安全信任机制，对信任链路中各环节的软件合法性和完整性进行校验，信任链路自底向上从安全芯片开始，包括启动加载软件和操作系统，至应用软件。

在信任链路中，各环节软件必须被数字签名，且能使用预置在信任链路前一环节软件中的密钥逐级进行安全校验，其中，启动加载软件应使用硬件安全信任根进行校验。只有信任链路中各环节软件都通过安全校验，安全信任链路才建立。

安全信任链校验机制应保障信任链路中启动加载软件、操作系统和应用程序的来源合法性和完整性。

6.5 安全视频路径

TVOS安全视频路径应包括安全解密/解扰、安全解码、安全缓存、安全显示或输出保护等环节，涵盖加密视频内容从解密/解扰开始直至最终显示的保护路径各环节。

视频内容在TVOS安全视频路径的任一环节及各环节之间的传输都在TVOS TEE可信执行环境下获得安全保护。

7 安全架构

7.1 基础安全架构

TVOS基础安全架构包括REE和TEE两部分，如图1所示。

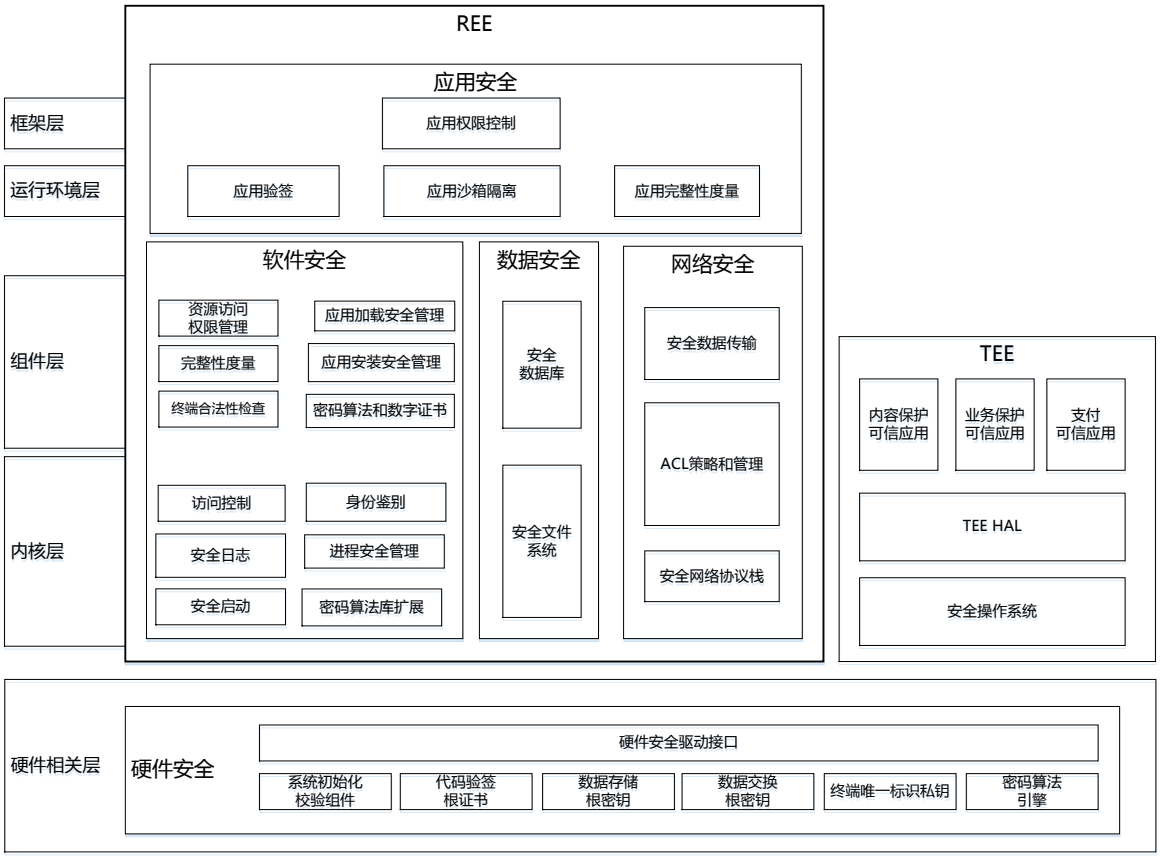

图 1 基础安全软件架构

TVOS硬件安全基础能力应为软件安全、网络安全、数据安全和应用安全等基础安全能力的构建提供支撑；软件安全、网络安全和数据安全等基础安全能力应基于硬件基础安全能力构建，并共同为应用安全基础安全能力的构建提供支撑；应用安全基础能力应基于软件安全、网络安全和数据安全等基础安全能力构建。

7.2 沙箱隔离安全架构

应基于TVOS软件架构和基础安全架构对每个TVOS应用进行沙箱隔离，为每个TVOS应用构建一个相应的应用沙箱。每个TVOS应用沙箱应由一个相应的TVOS应用进程构建，该应用进程由相应的TVOS应用及其所调用的TVOS应用框架层相关功能接口单元实例、相应的应用执行环境和所调用的相关功能组件客户端实例界定。TVOS应用沙箱可根据需要采用TVOS基础安全能力和安全机制进行安全加固。

应基于TVOS软件架构和基础安全架构对每个TVOS功能组件进行沙箱隔离，为每个TVOS功能组件构建一个相应的组件沙箱。每个TVOS组件沙箱应由一个相应的TVOS组件进程构建，该组件进程由相应的TVOS功能组件服务端及其所调用的其他功能组件客户端实例和硬件抽象层相关功能接口单元实例界定。TVOS组件沙箱可根据需要采用TVOS基础安全能力和安全机制进行安全加固。

TVOS应用和TVOS功能组件模块应遵循上述TVOS沙箱隔离安全架构，如图2所示。

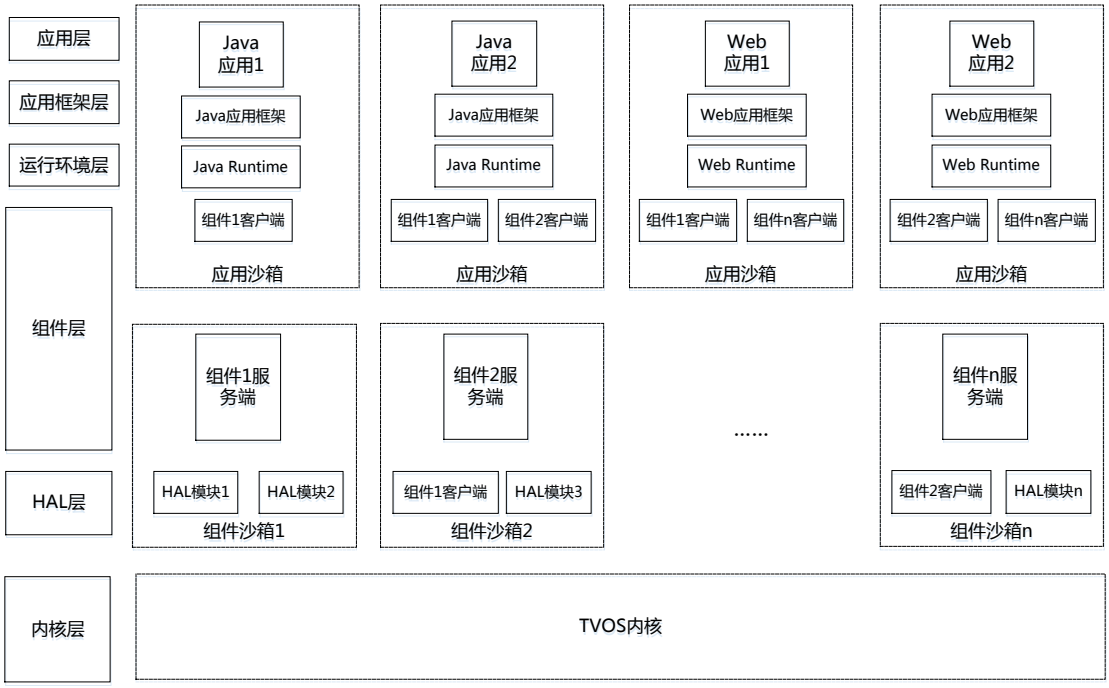

图 2　沙箱隔离安全架构

8　基本安全功能

8.1　内容安全

TVOS 内容安全应基于 TVOS 安全机制和硬件信任根建立 DRM 的安全信任链，通过使用密钥安全存储与管理机制、授权信息安全解密与存储管理机制以及安全视频路径保护措施，实现基于硬件安全的终端内容安全授权、安全解密、安全解码和安全播放与输出。TVOS 内容安全应符合 GY/T 277—2014 的要求。

TVOS 内容安全应能通过 TVOS DRM 组件与 DRM APP 和 DRM TApp 及媒体引擎组件协同实现。DRM APP 为 JAVA 形态或 WEB 形态。内容安全的功能实现参见附录 A。

8.2　业务安全

TVOS 业务安全应基于 TVOS 安全机制和硬件信任根建立 DCAS 的安全信任链，通过 DCAS 根密钥派生、密钥安全存储管理、数据解密和安全存储、安全视频路径保护措施等，实现基于硬件安全的终端业务条件接收安全授权、安全解密解扰、安全解码和安全播放。TVOS 业务安全应符合 GY/T 255—2012 的要求。

TVOS 业务安全应能通过 TVOS DCAS 组件与 DCAS App 和 DCAS TApp 及媒体引擎组件和数字电视组件协同实现。DCAS APP 为 JAVA 形态或 WEB 形态。业务安全的功能实现参见附录 B。

8.3　支付安全

TVOS 支付安全基于 TVOS 安全机制和硬件信任根建立支付安全信任链，通过安全支付组件与安全支付

App 和安全支付 TApp 的协同工作，实现基于二维码扫描支付方式的订单签名，基于安全 UI 的用户账号与密码获取、以及基于安全 UI 的支付校验码输入与验证，支撑安全支付 APP 和安全支付 TApp 完成相关安全支付操作。支付安全的功能实现参见附录 C。

8.4 安全启动

应基于硬件安全和安全机制安全信任链校验机制对启动加载软件、操作系统和应用程序逐级进行安全校验，只有全部通过安全校验后，系统才能安全启动，设备方能进入正常工作状态。

安全启动以安全芯片为基础，TVOS 系统实例与安全芯片硬件一一绑定；安全启动的信任链以安全芯片为起点，经终端 Bootloader 引导程序至 TVOS 内核和文件系统，信任链的每一环节只有通过数字签名校验后方可启动。

安全启动流程通常为：系统上电后，SoC 的 ROM 将加载 Bootloader 引导程序，然后再加载 TVOS TEE 部分并创建安全区内存，再后加载 TVOS REE 部分并创建普通区内存，每一级软件的装载和引导都应通过数字证书信任机制合法性和完整性的安全校验，只有在任意一个环节的安全校验通过后，该环节方可启动，该环节的后一环节方可进入校验状态，只有全部环节都通过安全校验后，系统方可启动，任何一步的验证失败都将导致系统启动失败。安全启动的实现参见附录 D。

8.5 终端管控

TVOS终端管控应基于TVOS安全机制和硬件信任根建立终端管控的安全信任链，实现对智能电视终端信息和参数的查询、统计、设置、监控和上报等功能。

TVOS 终端管控应能通过 TVOS 终端管控组件与终端管控 App 及其他组件协同实现。终端管控组件应能对所接收的终端管控指令逐一进行数字签名校验。

8.6 安全升级

TVOS 的安全升级包括操作系统的安全升级和应用的安全升级。

操作系统的安全升级应进行基于安全信任链校验机制的安全校验，只有通过安全校验的操作系统版本才允许进行升级。操作系统的升级禁止回滚。

应用软件的安全升级应进行基于安全信任链校验机制的安全校验，只有通过安全校验的应用软件版本才允许进行升级。安全应用的升级禁止回滚。

安全升级的实现参见附录 E。

附 录 A
（资料性附录）
内容保护功能实现

TVOS 通过 DRM 应用、DRM 组件、媒体引擎组件、DRM TApp 的协同工作实现 DRM 功能，如图 A.1 所示。

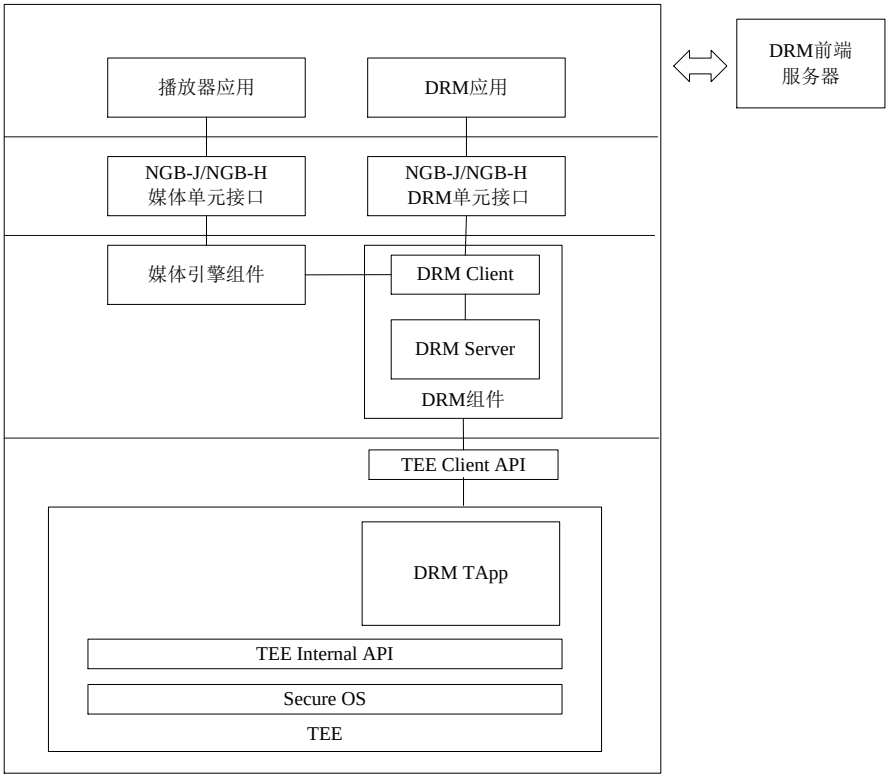

图 A.1 DRM 功能实现

DRM 功能实现方法如下：

a) 播放器应用播放 OTT 内容时，通过应用框架层的媒体单元接口将媒体内容的 URl 发送给媒体引擎组件，由媒体引擎组件获取播放文件列表和 DRM 相关信息；
b) 媒体引擎组件将 DRM 相关信息发送给 DRM 组件，由 DRM 组件根据 DRM 应用标识启动相应的 DRM 应用和 DRM TApp，并将 DRM 相关信息通过 TEE Client API 转发到 TEE 中的 DRM TApp；
c) DRM TApp 首先判断内容授权情况，如内容没有授权则通知 DRM 应用向 DRM 服务器获取内容授权，并将获取到的许可证返回 DRM TApp；
d) 媒体引擎组件创建 TEE 与 REE 的共享缓冲区，将加密媒体内容存储到共享缓冲区中；
e) DRM TApp 解析许可证，获取内容密钥，使用内容密钥解密加密媒体内容，将解密后的媒体内容存储在安全存储区，并将安全存储区的地址通过 DRM 组件发送给媒体引擎组件；
f) 媒体引擎组件将安全存储区地址发送给底层硬件音视频解码器，对解密后的媒体内容进行解码，并通过 HDCP 保护输出。

附 录 B
（资料性附录）
业务保护功能实现

B.1 基于JAVA的功能实现

DTV 基于 JAVA 的应用在接收到频道切换指令或节目播放指令的处理流程如图 B.1 所示。

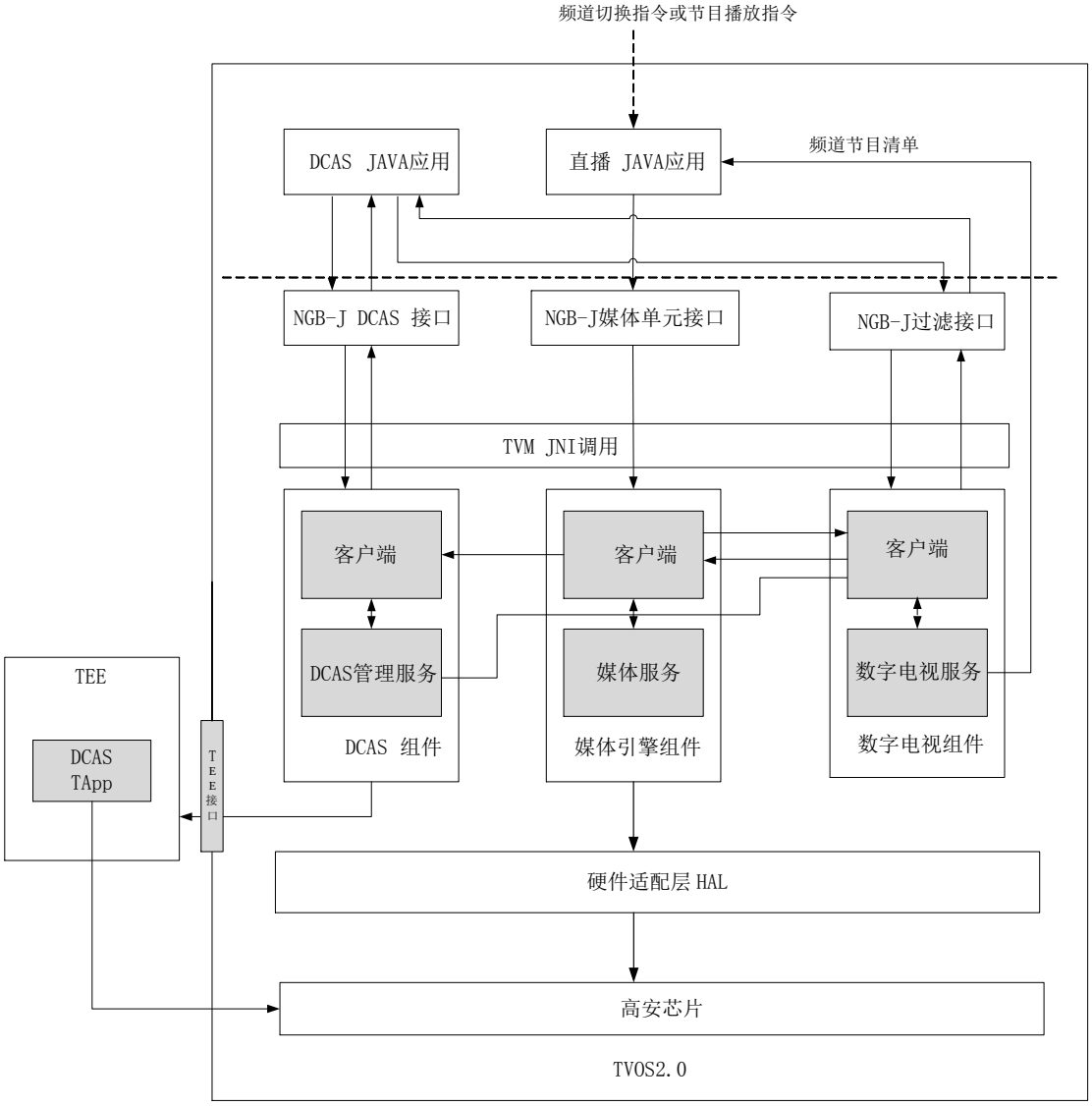

图 B.1 基于 JAVA 的系统处理流程

基于 JAVA 的 DTV 直播实现步骤如下：

a) 用户使用直播应用观看节目，切换到某个频道；直播应用调用 NGB-J 媒体单元的相应接口，并将频道的 DVB 三要素（original network id、transport stream id、service id）传给 NGB-J 媒体单元。

b) NGB-J 媒体单元将 DVB 三要素传递给媒体播放组件。
c) 媒体播放组件根据 DVB 三要素从 DTV 组件获取 freeCAMode 标识，判断频道是否加扰，如果是加扰频道，则获取 casId、ecmPid、emmPid、streampath。
d) 如果频道是非加扰的，则媒体播放组件直接调用底层驱动正常播放；如果是加扰的，则媒体播放组件创建播放的 PipeLine，并将 audioPid、videoPid 和 casId、ecmPid、emmPid、streampath 一起传给 DCAS 组件。
e) DCAS 组件根据 casId 选择相应的 DCAS 应用，并通过 DCAS API 将 audioPid、videoPid、casId、ecmPid、emmPid、streampath 传给 DCAS 应用。
f) DCAS 应用进行相关初始化，并根据 ecmPid 和 emmPid 通过 NGB-J Section 单元调用 DTV 组件获取 ecm Data 和 emm Data，同时 DCAS 应用将 streampath、audioPid、videoPid 和 casId 传给 DCAS 组件，DCAS 组件将这些参数通过 TEE Client API 送到 Secure OS 中的 TApp 模块。
g) DCAS 应用将获得的 ecm Data、emm Data 传给 DCAS 组件，DCAS 组件将 ecm data、emm data 通过 TEE Client API 送到 Secure OS 中的 TApp 模块。
h) TApp 模块在 Secure OS 中解析 ecm data、emm data 获得 EK2、EK1、ECW 并设置给高安芯片，实现加扰频道的解扰。

B.2 基于WEB的功能实现

DTV 基于 WEB 的应用在接收到频道切换指令或节目播放指令的处理流程如图 B.2 所示。

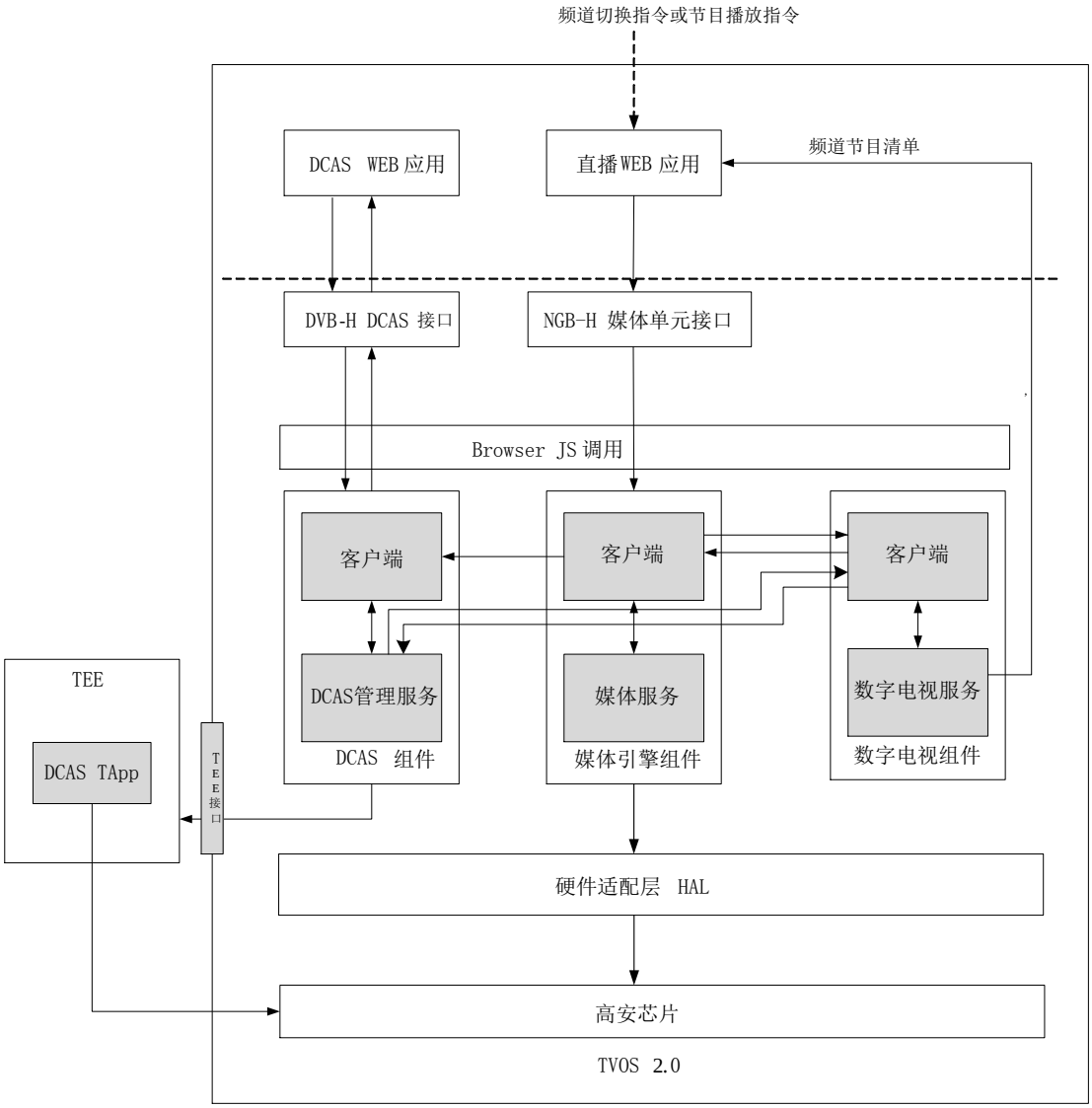

图 B.2 基于 WEB 的系统处理流程

基于 WEB 的 DTV 直播实现步骤如下：

a) 用户使用直播应用观看节目，切换到某个频道；直播应用调用 NGB-H 媒体单元的相应接口，并将频道的 DVB 三要素（original network id、transport stream id、service id）传给 NGB-H 媒体单元。

b) NGB-H 媒体单元将 DVB 三要素传递给媒体播放组件。

c) 媒体播放组件根据 DVB 三要素从 DTV 组件获取 freeCAMode 标识，判断频道是否加扰，如果是加扰频道，则获取 casId、ecmPid、emmPid、streampath。

d) 如果频道是非加扰的，则媒体播放组件直接调用底层驱动正常播放；如果是加扰的，则媒体播放组件创建播放的 PipeLine，并将 audioPid、videoPid 和 casId、ecmPid、emmPid、streampath 一起传给 DCAS 组件。

e) DCAS 组件根据 casId 选择相应的 DCAS 应用，并通过 DCAS API 将 audioPid、videoPid、casId、ecmPid、emmPid、streampath 传给 DCAS 应用。

f) DCAS 应用进行相关初始化，并根据 ecmPid 和 emmPid 通过 DCAS 组件调用 DTV 组件获取 ecm Data 和 emm Data，同时 DCAS 应用将 audioPid、videoPid 和 casId 传给 DCAS 组件，DCAS 组件将这些参数通过 TEE Client API 送到 Secure OS 中的 TApp 模块。

g) DCAS 应用将 ecm Data、emm Data 传给 DCAS 组件。

h) DCAS 组件将 ecm data、emm data 通过 TEE Client API 送到 Secure OS 中的 TApp 模块。

i) TApp 模块在 Secure OS 中解析 ecm data、emm data 获得 EK2、EK1、ECW 并设置给高安芯片，实现加扰频道的解扰。

附 录 C
（资料性附录）
安全支付功能实现

TVOS 通过支付应用、应用框架层支付 SDK、支付组件和 Payment TApp 的协同工作实现支付功能，如图 C.1 所示。

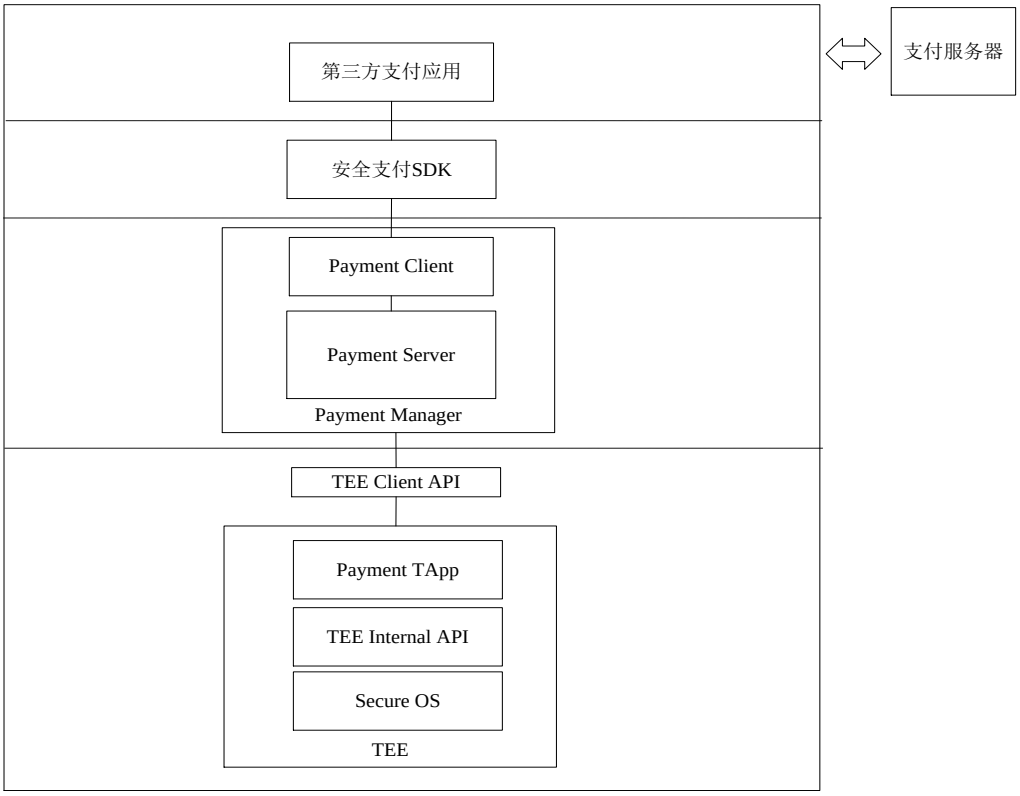

图 C.1 支付功能实现

安全支付实现方法如下：

a) 用户通过第三方支付应用购买商品，点击支付按钮发起支付请求；
b) 第三方支付应用产生唯一订单号并发送给安全支付 SDK 进行订单号签名；
c) 支付组件通过 TEE Client API 向 TEE 中的支付可信应用发送订单号签名请求，由支付可信应用使用支付安全密钥对订单号生成签名，并将签名逐级返回安全支付 SDK；
d) 安全支付 SDK 使用附带签名的订单号向支付服务器发起支付二维码获取请求；
e) 支付服务器验证支付客户端身份和订单签名，生成支付二维码发送给第三方支付应用；
f) 用户使用手机扫描二维码，向支付服务器发起支付请求，支付服务器完成支付流程并返回结果给用户。

附 录 D
（资料性附录）
系统安全启动

TVOS 安全启动包括安全芯片到引导程序的信任构建、引导程序到 TVOS TEE 部分的信任构建和 TVOS TEE 部分到 TVOS REE 部分的信任构建三个步骤。安全芯片到引导程序的信任构建由 ROM 固化代码从 Flash 存储器读取 BL_KEY1 和使用 BL_KEY0 对 BL_KEY1 的签名，通过预埋在安全芯片 OTP 区域中的 BL_KEY0 验证 BL_KEY1 的合法性，验证成功后加载引导程序和使用 BL_KEY1 对引导程序的签名，通过 BL_KEY1 验证引导程序的合法性，验证成功后将系统控制权交给引导程序；引导程序到 TVOS TEE 部分的信任构建由引导程序加载 Secure OS 镜像和使用 BL_KEY1 对 Secure OS 镜像的签名，通过 BL_KEY1 验证 Secure OS 镜像的合法性，验证成功后将系统控制权交给 Secure OS；TVOS TEE 部分到 TVOS REE 部分的信任构建由引导程序装载 TVOS 内核及系统镜像和使用 BL_KEY1 对 TVOS 内核及系统镜像的签名，通过 BL_KEY1 验证 TVOS 内核及系统镜像的合法性，验证成功后将系统控制权交给操作系统。上述验证过程任何一步的验证失败则导致系统启动失败。TVOS 安全启动流程如图 D.1 所示。

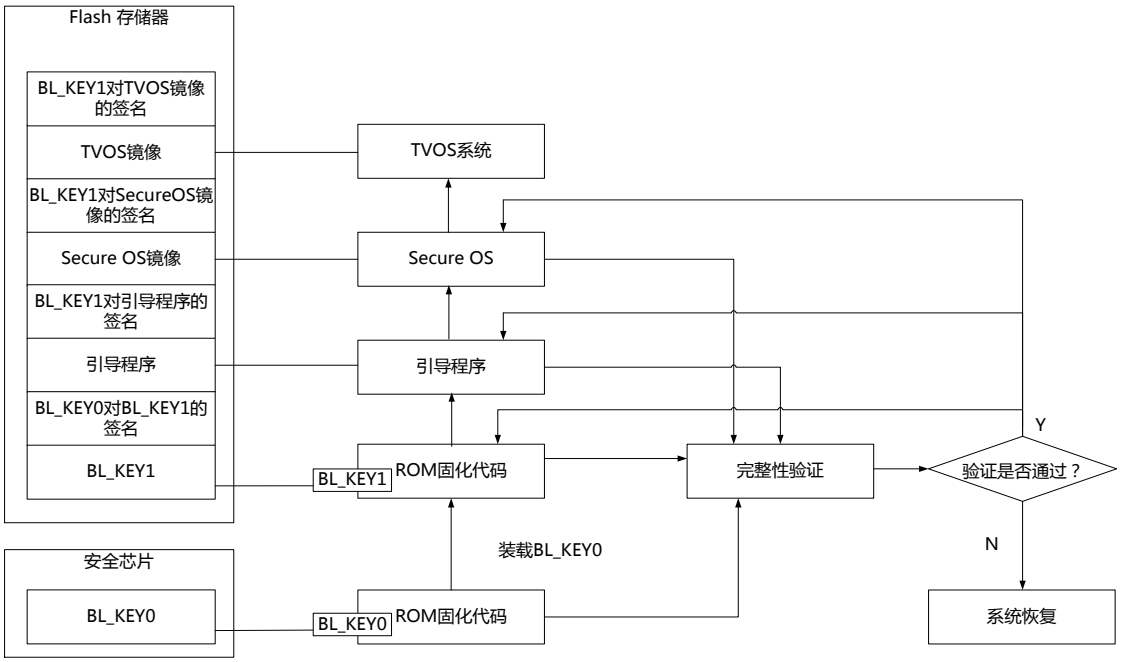

图 D.1 系统安全启动流程

附 录 E
（资料性附录）
系统安全升级

TVOS 的安全升级依靠模块的签名和校验来保证。所有的升级文件，包括系统升级、内置应用升级和第三方应用升级都需要按照运营商的要求签名保证安全，升级软件时必须校验签名，通过以后才能进行升级。运行在终端的程序各分区也要按照运营商的要求进行签名，并在程序启动时进行签名校验，如果校验不通过则自动重启终端。

应用软件通过内置软件模块检测升级，升级触发应按照服务器前端配置的参数来决定 TVOS 终端是否需要升级。为了保证系统安全升级，所制定的升级参数需要保证唯一性排他性。

TVOS 终端在升级前检查终端程序是否符合运营商制定的安全签名规范，保证终端能在安全的环境下正确启动运行程序。终端上电后，先启动引导模块。引导模块需要进行签名校验，校验通过后根据升级标志判断是否进入系统升级模块。升级有两种模式，OTA 下载（通过 cable）和 IP 下载。所有的升级流必须经过签名后才能下发，进入升级后先下载数据，下载完成后先校验签名才进行擦写和程序烧录。如果不需要升级就校验应用程序签名,校验通过后再启动应用程序。升级过程中，若有断电或信号故障，不能损坏升级模块，当模块重新上电或恢复信号后，重新进行系统升级功能。系统升级完成后，不要影响模块升级前的参数设置。

系统安全升级流程如图 E.1 所示。

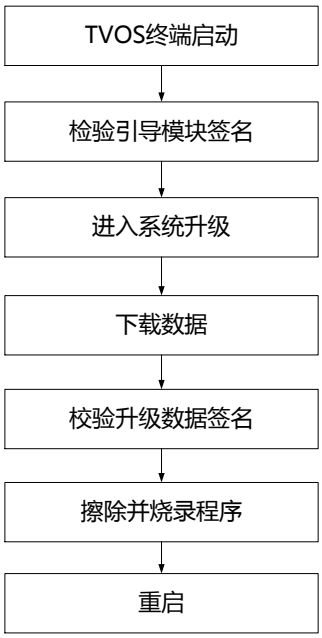

图 E.1 系统安全升级流程

中 华 人 民 共 和 国
广播电影电视行业标准
智能电视操作系统
第 2 部分：安全
GY/T 303.2－2016
*
国家新闻出版广电总局广播电视规划院出版发行
责任编辑：王佳梅
查询网址：www.abp2003.cn
北京复兴门外大街二号
联系电话：（010）86093424　　86092923
邮政编码：100866