工具软件

网络安全二次开发注意事项

文档版本　　00B01

发布日期　　2018-03-20

商标声明

 、HISILICON、海思和其他海思商标均为深圳市海思半导体有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受海思公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，海思公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

深圳市海思半导体有限公司

地址：深圳市龙岗区坂田华为基地华为电气生产中心　　邮编：518129

网址：http://www.hisilicon.com

客户服务电话：+86-755-28788858

客户服务传真：+86-755-28357515

客户服务邮箱：support@hisilicon.com

前　言

概述

本文档主要针对工具软件进行免责声明。

产品版本

与本文档相对应的产品版本如下。

产品名称	产品版本
Hi3559A	V100
Hi3559C	V100
Hi3519A	V100
Hi3516C	V300
Hi3516E	V100

读者对象

本文档（本指南）主要适用于工具软件交付的客户。

修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

修订日期	版本	修订说明
2018-03-20	00B01	第一次临时版本发布。

目 录

插图目录

表格目录

1 概述

1.1 简介

终端芯片工具软件包，主要针对各产品对工具主要诉求，持续累积海思工具交付能力，为内外部客户提供整体工具解决方案，提高开发与运维效率。

仅提供给客户用于提高效率、提升服务质量、减少风险等目的，在芯片二次开发业务中使用的软件，属于外部调测类工具。所有工具推荐在非商用环境下使用，否则，可能会产生网络安全相关风险。

1.2 版本交付内容说明

基础版本基于 C/C++，Java 语言开发。版本交付的工具产品如表 1-1 所示。

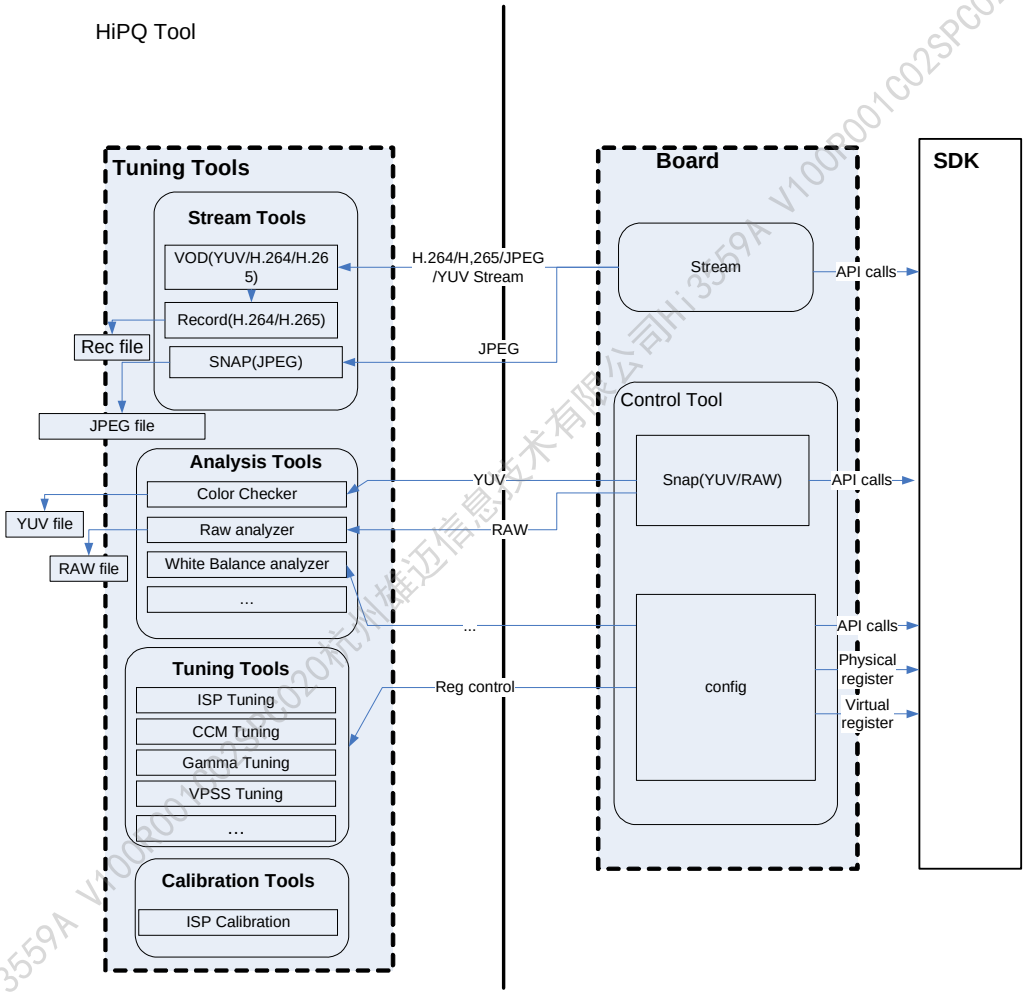
表1-1 版本交付的工具产品

工具名	工具类别	备注
HiBurn	外部调测类工具	量产/烧写类工具
HiLoader	外部调测类工具	镜像制作
HiAQ	外部调测类工具	音频质量调试工具
HiPQ	外部调测类工具	图像质量调试工具
CASignTool(Linux/Windows)	外部调测类工具	安全工具

2 图像质量调试工具

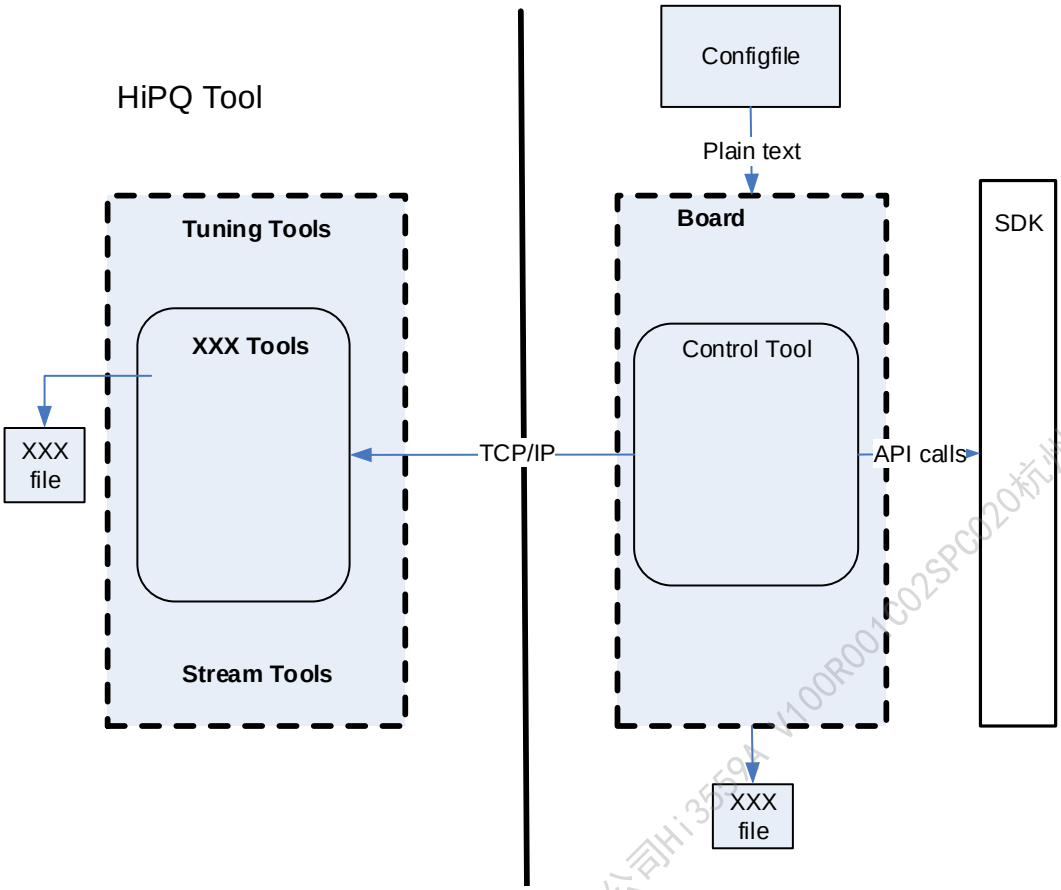
2.1 基本架构

图2-1 图像质量调试工具基本架构图



2.2 安全攻击及威胁

图2-2 图像质量调试工具与外围交互图



图像质量调试工具分为服务端与客户端的可执行程序，两端使用局域网内的 TCP/IP 与 HTTP 协议传输数据。网络搭建时：

- **调试部分服务端**从明文配置文件中读取服务端口号之后监听，服务端在运行过程中会存取过程中的二进制文件（XXX.bin 文件与 XXX.raw 文件）。
- **调试部分客户端**启动时指定发送端口号后进行命令与数据的交互，客户端在运行过程中会存取从服务端获取的数据（raw 数据、yuv 数据、isp 参数数据）。

点播部分服务端从明文配置文件中读取默认媒体部分参数，固定 80 端口启动监听，客户端运行过程中会存储录像文件（XXX.h264 文件与 XXX.h265 文件）与抓拍文件（XXX.jpg）。

2.3 安全维度

2.3.1 登录控制

使用图像质量调试工具需基于 MPP 搭建环境（包括单板准备，boot 烧录，kernel 烧录，rootfs 烧录，网络设置等）后运行。运行前需配置调试部分的监听端口号，端口号以明文方式保存在图像质量调试工具运行目录下的 config.cfg 文件中。修改其[Default]字段中的 Port 参数，默认监听 4321 端口，修改方式见《图像质量调试工具使用指南》的 1.3.2.3 章节。点播部分固定占用 80 端口，运行前需检查是否有别的进程占用 80 端口监听。

2.3.2 权限控制

图像质量调试工具客户端登录时，需输入要登录单板 IP 与端口号（点播部分占用 80 端口，登录时无需输入）。

2.3.3 存储安全

图像质量调试工具在运行过程中，根据不同应用条件，会存取中间文件至单板或 PC。服务端中间文件存取路径可配置，配置项均以明文方式保存在**图像质量调试工具运行目录**下的 config.cfg 文件中。客户端中间文件，如 XXX.yuv\XXX.raw 等，需选择存取路径，而一些数据报告等中间文件，如 XXX.jpg 等，默认存取为客户端运行的当前目录下。

2.3.4 交互安全

图像质量调试工具的网络环境仅支持运行在局域网内，使用 TCP_IP 协议实现网络传输。

2.3.5 数据传输安全

图像质量调试工具传输数据时，使用简单标示等识别是否为工具发出的数据包。数据包的完整性使用简单算法校验仅供初步识别是否有网络丢包。

2.4 安全面

2.4.1 管理

工具仅供在产品开发过程使用，产品中不推荐使用。

2.4.2 控制

工具仅供开发过程中使用，涉及的端口号在产品中需关闭或者删除，用户需要保护此端口号与单板 IP、中间敏感信息等的存取，如 bin 功能，不能包含在产品中。

2.4.3 使用环境

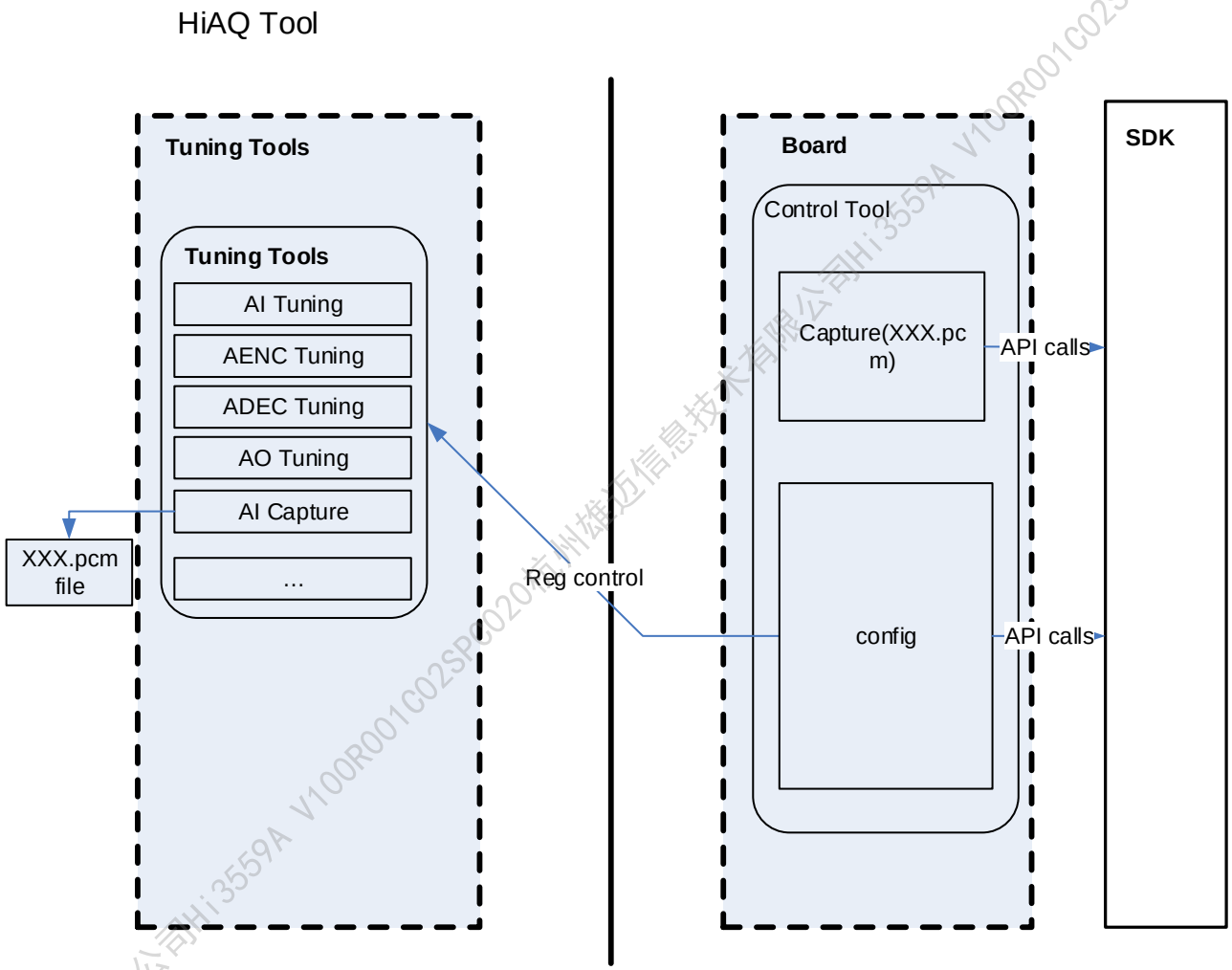
工具仅限于局域网内使用。

3 音频质量调试工具

3.1 基本架构

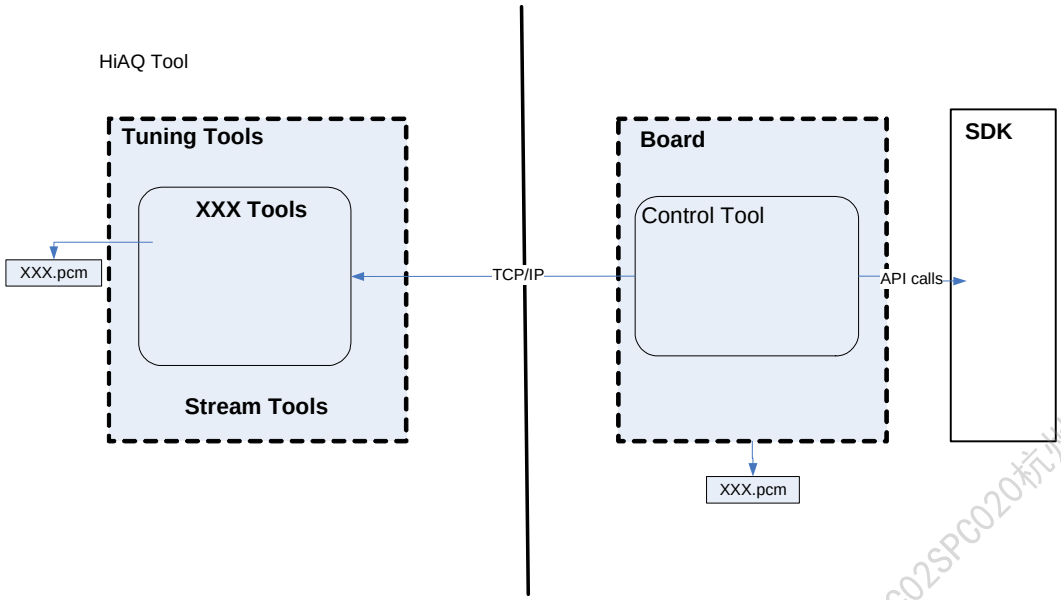
音频质量调试工具的基本架构如图 3-1 所示。

图3-1 音频质量调试工具基本架构图



3.2 安全攻击及威胁

图3-2 音频质量调试工具与外围交互图



音频质量调试工具分为服务端和客户端的可执行程序，两端使用局域网内的 TCP/IP 协议传输数据。网络搭建时：

- **调试部分服务端**从明文配置文件中读取服务端口号之后监听，服务端在运行过程中会写出过程中的二进制文件（XXX.pcm 文件）。
- **调试部分客户端**启动时指定发送端口号后进行命令与数据的交互，客户端在运行过程中会存取从服务端获取的数据（XXX.pcm 数据）。

3.3 安全维度

3.3.1 登陆控制

使用音频质量调试工具需基于 MPP 搭建环境（包括单板准备，boot 烧录，kernel 烧录，rootfs 烧录，网络设置等）后运行。运行前需配置调试部分的监听端口号，端口号以运行 HiAQTool.sh 文件的入参。使用方法：./HiAQTool.sh 端口号。

3.3.2 权限控制

音频质量调试工具客户端登录时，需输入要登录单板 IP 与端口号。

3.3.3 存储安全

音频质量调试工具在运行过程中，根据不同应用条件，会存取中间文件至单板或 PC。服务端中间文件存取路径为程序运行目录。客户端中间文件，如 XXX.pcm 等，需选择存取路径。

3.3.4 交互安全

音频质量调试工具的网络环境仅支持运行在局域网内，使用 TCP_IP 协议实现网络传输。

3.3.5 数据传输安全

音频质量调试工具传输数据时，使用简单标示等识别是否为工具发出的数据包。数据包的完整性使用简单算法校验，仅供初步识别是否有网络丢包。

3.4 安全面

3.4.1 管理

工具仅供在产品开发过程使用，产品中不推荐使用。

3.4.2 控制

工具仅供开发过程中使用，用户需要保护端口号，单板 IP，中间敏感信息的存取。

3.4.3 使用环境

工具仅限于局域网内使用。

4 安全工具

4.1 安全维度

CASignTool 在加解密模块（Crypto）及非 Boot 签名模块中，提供了以下三种加密方式和模式。

- 加密方式：
  - AES
  - TDES
  - SM4
- 加密模式：
  - CBC
  - ECB
  - CTR（不用于国密）

AES-CBC 的加密方式最为安全，建议客户选择使用。

此外，CASignTool 在加解密模块支持了国密算法（加密算法为 SM3/SM4，签名算法 SM2）。国密算法在提供给国外客户使用时，默认关闭。

4.2 安全面

4.2.1 控制

工具仅供开发过程中使用，用户需要保护端口号，单板 IP，中间敏感信息等的存取。

4.2.2 使用

交付的工具不涉及联网及获取客户的隐私数据；最终产品不含交付工具。

5 量产/烧写及其他工具

5.1 安全攻击及威胁

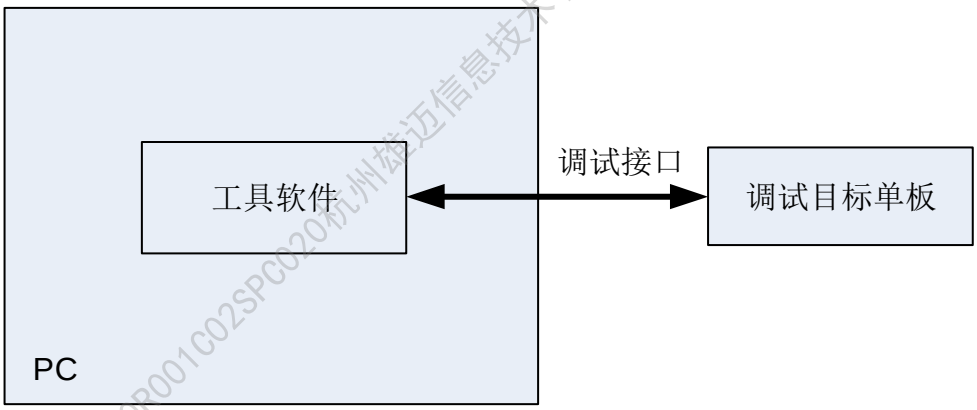
工具软件均为 PC 上运行的单机软件。部分工具只和运行系统上的文件系统相关。部分调试工具或者烧写工具需要通过调试接口和目标单板进行通信，主要涉及的接口在如表 5-1 中呈现：

表5-1 工具与通信方式

工具	通信方式
Hiburn	串口、USB、I2C、JTAG、网口

调试工具和烧写工具的组网结构一般如图 5-1 所示。

图5-1 调试工具和烧写工具的组网



如表 5-1 所述，目标单板的调试接口包括 JTAG、串口、I2C、USB、网口等。通过调试端口可以打印调试信息，甚至可以访问 CPU 的内部寄存器和设备中的任何信息。这些都是黑客对设备的硬件、软件、配置参数进行分析重要手段。

例如，使用 JTAG，黑客可以完成对设备程序运行的跟踪、调式、执行任意代码、读取和更改 Flash 上存储的软件和敏感配置数据、寻找设备的安全弱点和攻击方法。在获取

到设备的弱点和攻击方法后，黑客通常会将其公布在 Internet 网上，为产品带来安全威胁。

研发单板允许研发过程保留调试端口用于调试，但正式发货产品需删除调试端口的设计，建议不保留接口插座。

5.2 安全面

5.2.1 管理

工具仅供在产品开发过程使用，产品中不允许使用，如果使用发生的问题，我司不予处理。

5.2.2 控制

工具仅供开发过程中使用，用户需要保护端口号，单板 IP，中间敏感信息等的存取。

5.2.3 使用

交付的工具不涉及联网及获取客户的隐私数据；

最终产品不含交付工具。

5.3 其他使用安全注意事项

5.3.1 JTAG 接口

恶意者可通过 JTAG 接口，篡改系统和配置，恶意破坏系统。

建议客户采用以下措施：

- 产品出厂时，将 JTAG 接口从物理上删除。
- 芯片提供 JTAG disable 功能，从芯片层面直接永久关闭 JTAG。

5.3.2 PC 调试工具

- 所有的客户研发调测类工具仅支持客户在产品开发或生产过程中进行各种功能、效果调试，请勿放置到正式的产品中。
- 所有服务运维类工具仅提供给指定合作方使用，不可供外部访问。

5.3.3 调试接口

研发单板允许研发过程保留调试端口用于调试，但正式发货产品需删除调试端口的设计，至少不能保留接口插座。

5.3.4 镜像安全

配套的调试用的镜像不能编译到最终的产品中。

6 结论

综合以上章节，总结网络安全如下：

- 工具包中提供的工具属于外部调测类工具或者生产装备类工具，仅供开发过程中使用。
- 用户开发的产品数据保护需产品开发者保护。
- 工具的软件包中包含：可执行文件与配置文件。量产相关软件包中，请删除与工具所有的可执行文件与配置文件，并删除文档中关于工具描述。
- 所有工具都是非商用工具，只用于产品开发，若未遵循，一切后果与我司无关。

7 缩略语

表7-1 缩略语清单

缩写	全称
MPP	Media Process Platform
ISP	Image Signal Processor
JTAG	Joint Test Action Group