



Solarec

二次开发网络安全注意事项

文档版本 05

发布日期 2023-10-08

版权所有 © 海思技术有限公司2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HISILICON、海思和其他海思商标均为海思技术有限公司的商标。

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。

海思技术有限公司

地址：上海市青浦区虹桥港路2号101室 邮编：201721

网址：<https://www.hisilicon.com/cn/>

客户服务邮箱：support@hisilicon.com



前言

概述

本文旨在从网络安全的角度，重点分析基于SolarA² MCU解决方案交付包开发的产品，在被使用中可能面临的与本交付包中SDK软件包相关的网络安全的威胁，同时针对性的给出相应的解决方案。本文以SolarA²交付包为例进行描述。

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
SolarA ²	1.0.1



读者对象

本文档（本指南）主要适用于以下工程师：



- 技术支持工程师
- 客户开发工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 危险	表示如不可避免则将会导致死亡或严重伤害的具有高等级风险的危害。
 警告	表示如不可避免则可能导致死亡或严重伤害的具有中等级风险的危害。



符号	说明
 注意	表示如不可避免则可能导致轻微或中度伤害的具有低等级风险的危害。
须知	用于传递设备或环境安全警示信息。如不可避免则可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “须知”不涉及人身伤害。
 说明	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

修订记录

修订日期	版本	修订说明
2022-08-15	01	第1次正式版本发布。
2022-09-02	02	第2次正式版本发布。 刷新第1章，优化描述。
2022-09-07	03	第3次正式版本发布。 刷新第4章，优化缩略语描述。
2022-11-07	04	第4次正式版本发布。 刷新第1章，优化业务分层示意图； 刷新第2.1章，优化须知的具体描述； 刷新第2章，增加引用文档的具体名称。
2023-10-08	05	第5次正式版本发布。 新增2.3参数检查开关章节。



目 录

前言.....	i
1 简介.....	1
2 开发包使用安全注意事项.....	2
2.1 设备接口安全.....	2
2.1.1 概述.....	2
2.1.2 JTAG.....	2
2.1.3 UART.....	2
2.1.4 UART 升级功能.....	3
2.2 关键代码保护.....	3
2.3 参数检查开关.....	4
3 展望.....	6
4 缩略语表.....	7



插图目录

图 1-1 业务分层示意图.....	1
图 2-1 IDE 勾选方式开启参数检查.....	5



表格目录

表 2-1 关键代码保护权限说明..... 4

表 4-1 缩略语清单..... 7

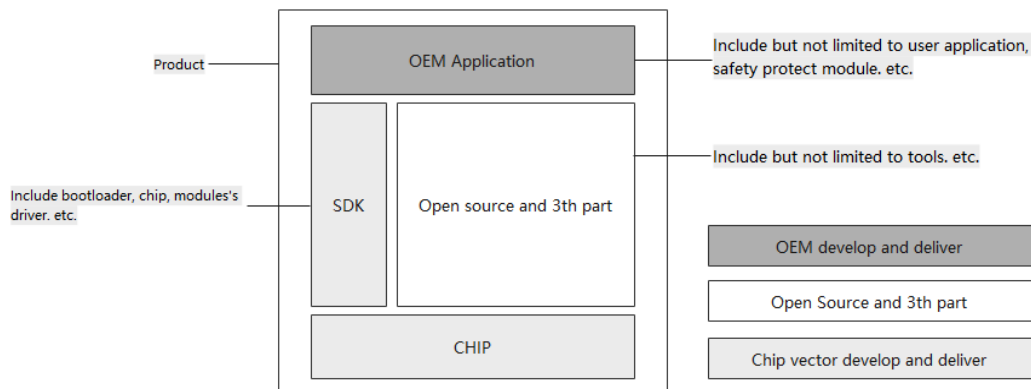


1 简介

本公司是全球领先的Fabless半导体设计公司，致力于向包含视频监控、机顶盒、智能家庭、电机控制等领域的全球设备商提供全面MCU 解决方案。网络互联和多媒体行业的迅猛发展极大地改善了人们的生活质量，促进了社会的进步，也带来了网络安全、隐私保护的挑战。作为产业链的重要一分子，本公司非常重视网络安全和用户隐私保护，希望与客户共同构筑产品的网络安全，保障最终消费者的权益。

众所周知一个产品的网络安全，需要产业链上的各方，包括MCU 供应商、设备商、运营商，甚至最终用户，共同努力来达成。本公司作为其中重要的参与方，主要提供MCU 及SDK开发包等基础组件。图1-1给出了典型产品应用中的业务分层。

图 1-1 业务分层示意图



CHIP 和 SDK部分由本公司提供，这部分的网络安全由本公司负责；

OEM Application部分是客户开发的，其网络安全由客户负责；

Open Source and 3th part部分主要是开源软件和第三方组件，其网络安全由客户、开源社区及第三方负责。



2 开发包使用安全注意事项

2.1 设备接口安全

2.1.1 概述

- 硬件接口指各种通用标准的物理接口，包括JTAG、UART等，带有调试功能的接口在安全设计时尤其需要重点关注。
- 硬件接口攻击是近端攻击者首选的攻击方式，而利用现有硬件接口及其协议、软件漏洞进行攻击，可以认为是攻击成本最小的一类硬件攻击方式。因此，硬件接口安全设计的基本原则是攻击面最小化。
- 正式发货版本中所有用于生产、开发调试、维修的接口要求默认禁用且不可激活。

2.1.2 JTAG

JTAG的安全防护设计有以下两种方案，根据产品的安全需求选择合适的方案：

- 直接去掉JTAG信号链路。无法通过工具或焊接等方式从外部连接JTAG口。
- 通过func_jtag_enable选项控制JTAG口开关。
0：禁用JTAG功能。
1：开启JTAG功能。(默认值)

须知

func_jtag_enable选项的地址请参考对应MCU 技术参考指南手册。

2.1.3 UART

UART的安全防护设计有以下两种方案，根据产品的安全需求选择合适的方案：

- 直接去掉调试UART信号链路。无法通过工具或焊接等方式从外部连接调试UART口。



- 通过uartX_enable选项控制UART口开关。
0: 禁用UART功能。
1: 开启UART功能。(默认值)

须知

- uart0_enable用于控制UART0。uart1_enable用于控制UART1。
- uartX_enable选项的地址请参考对应MCU 技术参考指南手册。

2.1.4 UART 升级功能

为保证安全性，禁止发货版本开启UART升级功能。

- 通过uart0_boot_enable选项控制UART升级功能开关。
0: 禁用UART升级功能。
1: 开启UART升级功能。(默认值)

须知

uart0_boot_enable选项的地址请参考对应MCU 技术参考指南手册。

2.2 关键代码保护

为保护客户的程序代码安全性，建议发货版本开启关键代码保护功能。

- 通过protection_level选项控制关键代码保护功能开关。
0: 开启关键代码保护功能。
1: 禁止关键代码保护功能。(默认值)

须知

- 关键代码保护可防止通过JTAG访问Flash数据。开启关键代码保护同时请保证uart0_boot_enable被设置为0，关闭UART升级功能。防止通过UART升级功能替换版本。
- func_jtag_enable为1时protection_level配置才有效。func_jtag_enable为0时JTAG口关闭，protection_level为0或1都无法通过JTAG访问MCU。
- protection_level的地址请参考对应MCU 技术参考指南手册。



表 2-1 关键代码保护权限说明

模块	protection_level=0	protection_level=1（默认值）
程序存储区 (main_rgn0)	JTAG无读写权限	JTAG有读写权限
用户数据存储区 (main_rgn1)	JTAG有读写权限	JTAG有读写权限
SYSRAM	JTAG只有读权限	JTAG有读写权限
寄存器	JTAG只支持将 protection_level从0->1。 protection_level从0->1 时，会清除程序存储区 (main_rgn0)中所有数据。	JTAG有读写权限

- 用户数据存储区 (main_rgn1) : Flash的最后一个Sector（最后一个Sector大小请参考对应MCU 技术参考指南手册），可用于存储用户参数。
- 程序存储区 (main_rgn0) : Flash中除最后一个Sector外的其他区域，用于存储客户程序代码。
- 默认代码只运行在程序存储区 (main_rgn0)。protection_level=0时JTAG有SYSRAM读权限，出于安全考虑，请不要配置程序在SYSRAM中运行。

2.3 参数检查开关

SDK支持模块级的入参合法性校验。开启入参合法性检查的版本可提高产品的安全性，但会占用更大的FLASH空间，对应的API会增加参数校验的执行时间。为提升安全性，请在正式发货版本中开启入参合法性校验特性。

开启模块参数检查方式包括IDE勾选方式和用户编码方式。

- IDE勾选方式

通过HiSpark IDE中MCU配置器->配置信息->MACRO，找到模块参数检查开关，如[图 IDE勾选方式开启参数检查](#)所示。勾选参数检查使能的模块，点击生成代码，即可开启模块参数检查；去掉模块参数检查勾选，点击生成代码，即可关闭模块参数检查。

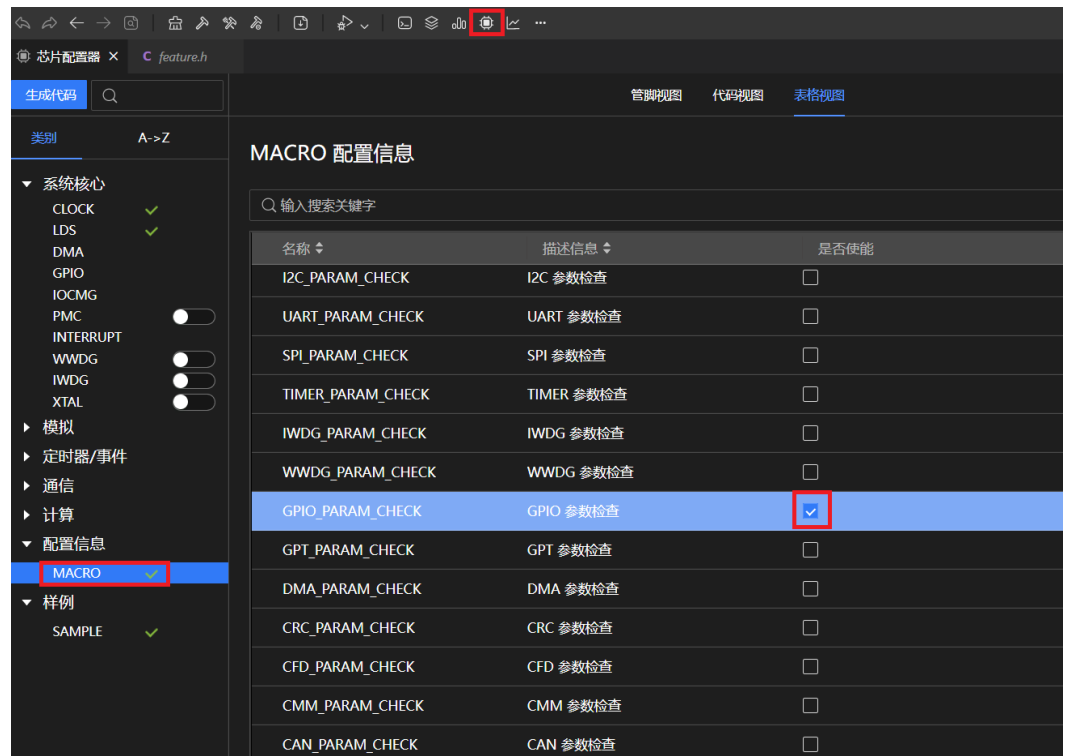
- 用户编码方式

用户可在user\feature.h文件中定义想要开启参数检查的模块宏名称，参数检查宏名称统一格式为XXX_PARAM_CHECK（XXX代表模块名称，全大写），以GPIO模块为例，开启参数检查宏示例代码如下。关闭模块参数检查删除用户在user\feature.h文件中的宏定义即可。

```
#define GPIO_PARAM_CHECK 1
```



图 2-1 IDE 勾选方式开启参数检查





3 展望

客户有必要基于特定的安全威胁分析采用相对应的安全措施。以下的一些安全原则可供客户参考。

1. 适度的安全

安全设计是基于特定的安全危险场景分析，考虑到性能、成本、业务影响，决策采用最合适的安全措施。

2. 最小授权

根据职责的需要，给用户、维护人员、网络单元、程序、进程等授予最小的权限和资源。这样能减少潜在的安全风险。

3. 主动协同防御

及时识别恶意攻击源，并在攻击造成显著危害前自动删除恶意用户和网络之间的连接。也可以降低连接的带宽和服务质量，以尽量减少负面影响。

4. 纵深防御

纵深防御原则涉及到对威胁的多重防御。例如，当一个防御层不够时，另一个防御层将防止造成一个完整的破坏。



4 缩略语表

表 4-1 缩略语清单

英文缩写	英文全称	中文全称
UART	Universal Asynchronous Receiver/ Transmitter	通用异步收发器
JTAG	Joint Test Action Group	联合测试工作组