知从.木牛

ZC.MuNiu

知从木牛 Cybersecurity 英飞凌 TC3XX 产品手册

知从®木牛基础软件平台

知从木牛 Cybersecurity 英飞凌 TC3XX 产品手册

知从®木牛基础软件平台

1 开发背景

智能网联汽车在全球范围内蓬勃发展，由此带来的汽车网联化逐渐成为未来汽车的重要发展方向。联网所带来的信息安全问题在网联化汽车上同样存在，车厂和设计开发人员将不得不在整车电子电气架构上实施高要求的信息安全措施。2009 年欧洲的奥迪和宝马等汽车制造商发布了 Security Hardware Extension(SHE)标准（图 1），2011 年由一些主要的 Tier 1 和汽车半导体公司发布基于 SHE 规范的 HSM 硬件规范，2016 年 SAE 针对车辆的生产、运行、维护和报废的整个生命周期。发布了提供了车辆网络安全的流程框架和指导 SAE J3061.2020 即将发布的 ISO 21434 是基于 SAE J3061 制定的、针对车辆整个生命周期的标准。这将是和 ISO 26262 功能安全一样的重量级的标准。

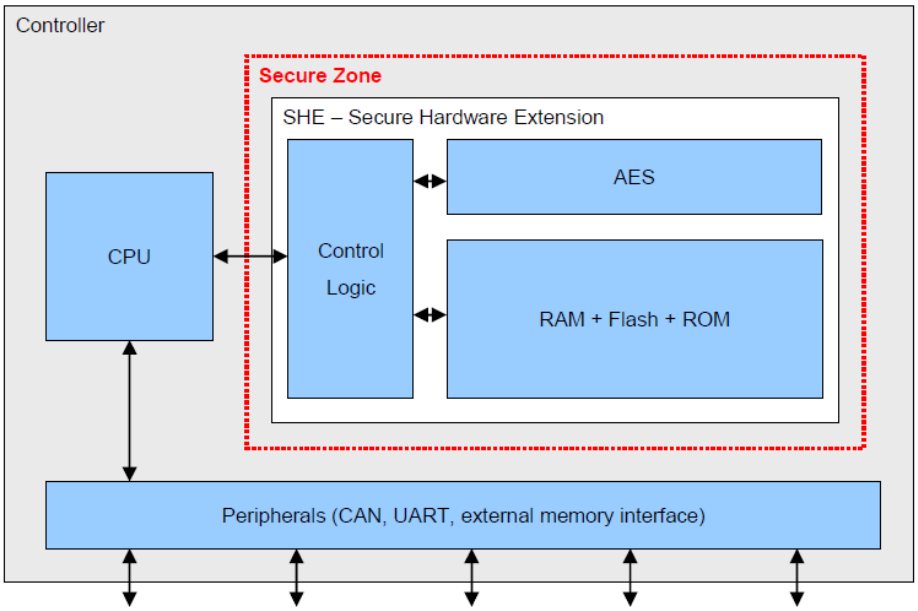

图 1 Secure Hardware Extension

2018 年底，知从科技开始投入资源开发满足 SHE 标准并能兼容 AUTOSAR 4.2.2/4.4.0 的 HSM 内核和接口函数，经过不懈努力，终于 2020 年 9 月发布了基于英飞凌 TC3xx 的第一款信息安全软件库--木牛 Cybersecurity Lib。

2 产品概述

知从科技针对英飞凌 TC3xx 系列(如 TC39x,TC38x 和 TC37x 等)所开发的木牛 Cybersecurity Lib 包括硬件加密模块(HSM)的内核固件(zHSM CORE)和客户应用接口函数(SHE CD)。内核固件除了满足常规的 SHE 功能(密钥注入、对称加解密、消息认证码生成与校验、随机数生成和安全启动等)，还可扩展多种算法，如 HASH 和 ECC256 等。SHE CD 接口函数除了满足支持 AUTOSAR4.2.2 的需求外，还可升级到更高版本的 AUTOSAR 4.4.0,甚至可以作为一个单独的复杂驱动，和非 AUTOSAR 环境集成。

简而言之，木牛 Cybersecurity Lib 灵活地适用于所有 AURIX 2G 产品，具有高扩展性，可以根据不同的客户项目要求进行升级配置和再开发，最终满足不同客户的信息安全需求。

3 应用领域

木牛 Cybersecurity Lib 主要应用于有信息安全需求的控制器。 如图 2 ，本产品适应于汽车电子电气架构里的： 动力域控制器， 车身域控制器， 安全域控制器和信息域控制器。

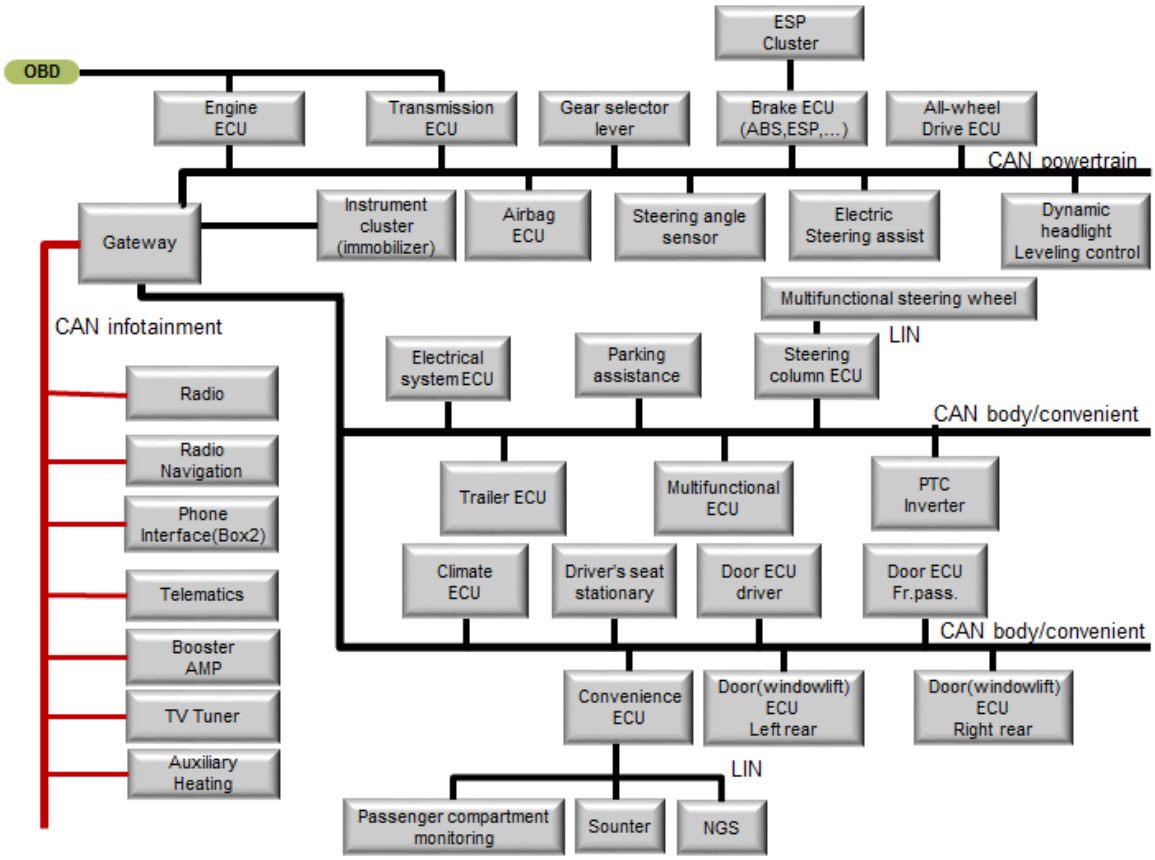

图 2 汽车电子电气架构

用户通过将木牛 Cybersecurity Lib 集成到基于 TC3xx 的汽车电控单元中，可以满足 SHE 标准里所规定的汽车电控单元所具有的信息安全功能。

4 软件模块及功能

木牛 Cybersecurity Lib 的软件主要分为两部分(图 3)：

1) HSM 硬件加密模块固件(zHSM CORE）
2) Tricore 主核的 SHE 复杂驱动(zSHE CD）

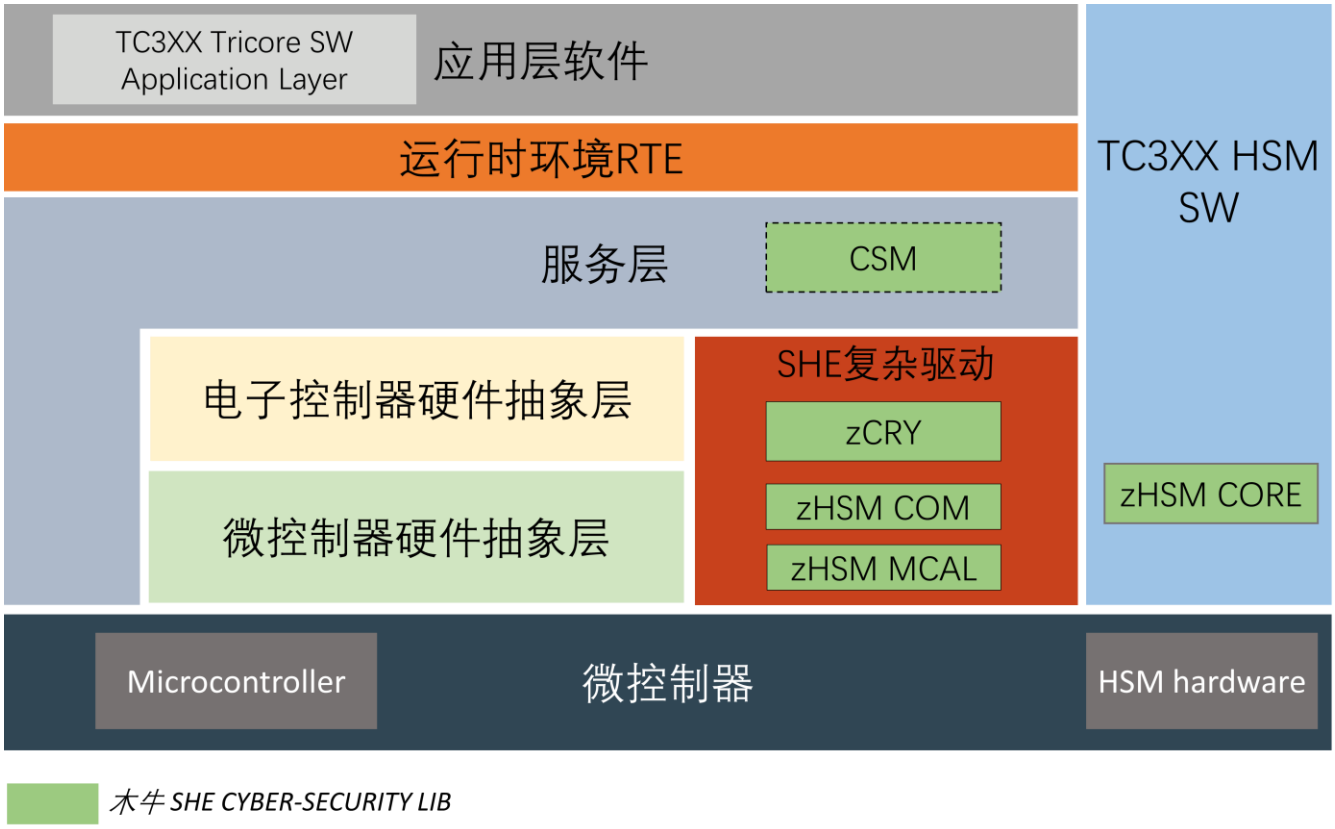

图 3 木牛 Cybersecurity Lib 的 AUTOSAR 集成

zSHE CD 包含和 CSM 的接口 zCRY 模块，和 HSM 通讯的 zHSM COM 和 zHSM MCAL 模块三个子模块，各模块的功能介绍如表 1。

表 1 软件模块功能说明

软件模块	模块组件	AUTOSAR Layer	功能定义
zHSM CORE (加密内核)	zHSM CORE	N/A	使用了 HSM 内部的硬件加速器，如随机数生成器、AES-128 等（如图 4）
zSHE CD （主核）	1) zCRY 2) zHSM COM 3) zHSM MCAL	SHE CD	微处理器 Hsm 驱动、与 Hsm 核的通信驱动、Crypto Interface 等
CSM （主核）	CSM	SERVICE	用户信息安全管理的接口函数

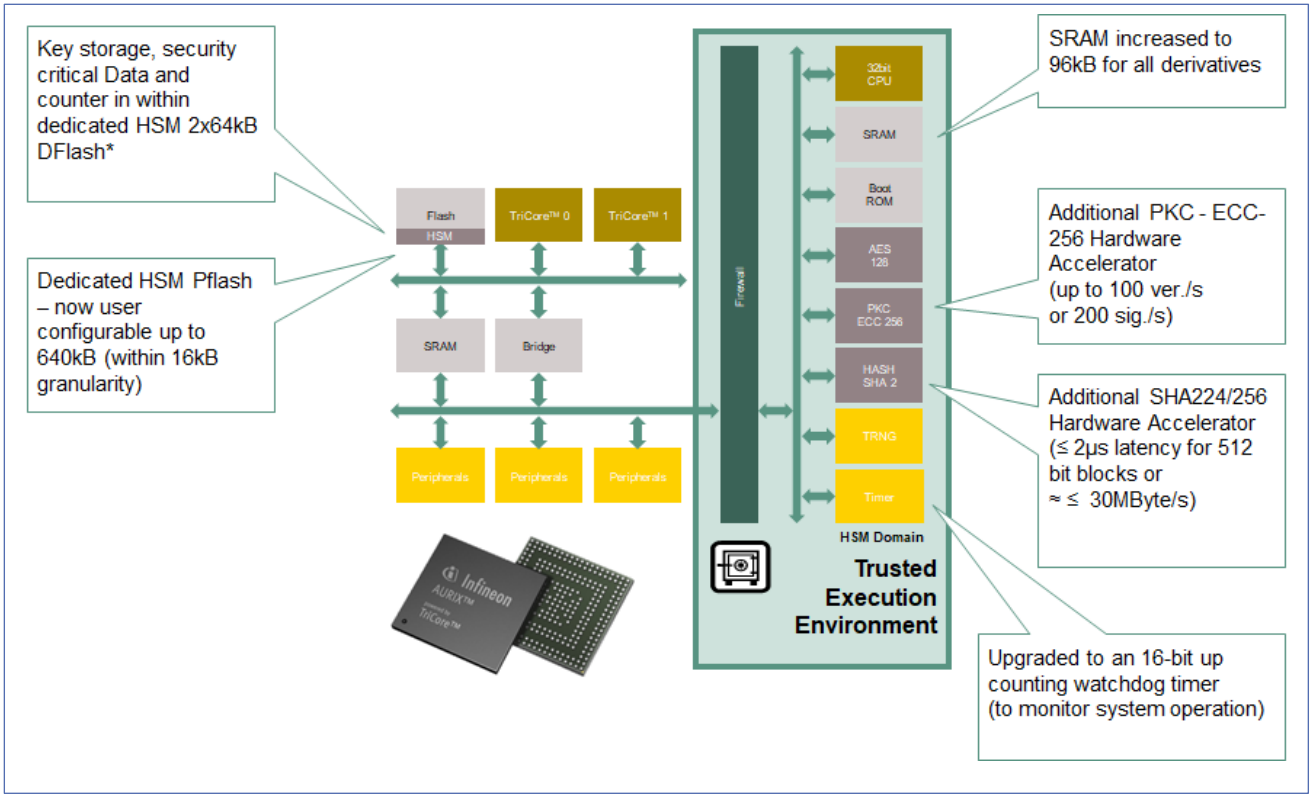

图 4 TC3xx HSM 资源

木牛 Cybersecurity Lib 支持 SHE 标准，和标准的 SHE 相比，Cybersecurity Lib 在功能上有一些扩展，主要功能及区别见表 2 和 3。

表 2 木牛 Cybersecurity Lib 的主要功能

Features		SHE standard	木牛 Cybersecurity Lib
AES 128 密码模式	ECB	✓	✓
	CBC	✓	✓
AES 128 消息认证码	CMAC	✓	✓
随机数生成器	伪随机数	✓	✓
	硬件随机数	/	✓
安全启动		✓	✓
非易失性密码槽		**10**	**>50**
可易失性密码槽		✓	✓
支持可用于消息认证密钥		/	✓
安全消息认证		/	✓

表 3 木牛 Cybersecurity Lib 的 SHE 功能说明

主要功能	解释说明
SHE 对称密钥加解密	对称式 AES-128，支持 ECB 和 CBC 加密模式对称加密
SHE CMAC 消息认证码 生成与校验	对称式 AES-128 消息认证码
SHE CMAC 安全消息认证码 生成与校验	支持安全 CMAC 验证，使应用程序能够检查安全相关数据的完整性
SHE 明文密钥装载	存储 128 位密钥到 HSM 的 RAM, 不涉及安全协议
SHE 密钥导出	对导出 RAM 密钥进行包装(加密和身份验证)
SHE 基于安全协议的密钥装载	使用安全协议将 128 位密钥存储在 HSM 非易失性存储器中
SHE 随机数生成	使用 AES 生成伪随机数,种子由 TRNG 生成
SHE 安全启动	验证应用程序启动代码的 CMAC.
SHE 调试模式	使用安全协议启用对 HSM 调试接口的访问
SHE 状态获取	获取 SHE 状态.
SHE 命令取消	取消当前正在执行的操作.
SHE 错误报告	除了 CSM 返回代码之外，还可以通过 AUTOSAR 机制报告 SHE 错误
SHE 超时处理	如果 HSM 响应时间超过预定义的限制，则报告错误
应软件更新支持 (Cipher 和 MAC)	在应用软件的更新过程中也可以使用密码和 MAC 功能
硬件随机数	支持生成真随机数
AES 加密扩展 (OFB, CFB, CTR, XTS,GCM)	支持额外的 AES 模式
密钥扩展	支持扩展更多的非易失性密钥

5 配置环境

配置环境	
硬件 (支持芯片)	INFINEON SAK-TC3XX
编译器选择	TASKING 6.3R1 HighTec 4.9.3.0
评估硬件	TriBoard TC3xx
调试器	Lauterbach (Trace32 XXXXX) Isystem (IC5XXX) PLS (UDE 5.X)
配置工具	Muniu_v5.0.5
配置环境	Win10 64bit/Win7 64bit

编译器选项	
Tasking 编译选项	--core=tc1.6.2 -t -Wa-gAHLs --emit-locals=-equ,-symbols -Wa-Ogs -Wa--error-limit=42 $(ISO_OPTION) --eabi-compliant --integer-enumeration --language=-comments,-gcc,+volatile,-strings --switch=auto --align=0 --default-near-size=0 --default-a0-size=0 --default-a1-size=0 □O<*variants*> --tradeoff=4 -g --source -D_TASKING_C_TRICORE_=1
Tasking 链接选项	-o "$(ELFDIR)/$(PROJNAME).elf" -o "$(ELFDIR)/$(PROJNAME).hex":IHEX --hex-format=s -t -D__CPU__=$(CPU_USED) -Cmpe:vtc $(LTC_OPTIMIZATION) --error-limit=42 -M -mcrfiklsmnoduq
HighTec 编译选项	-save-temps=obj $(ISO_OPTION) -ansi -fno-asm -ffreestanding -Wundef -Wp,$(ISO_OPTION) -fno-short-enums -fpeel-loops -falign-functions=4 -frecord-gcc-switches -fsection-anchors -funsigned-bitfields -ffunction-sections -fno-ivopts -fno-peephole2 -nostartfiles -O3 -g3 -W -Wall -Wuninitialized $(TRIBOARD_DEFINE) -mtc162 -D_GNU_C_TRICORE_=1 $(CALLFUNCTION) -I "$(PRODDIR)/tricore/include/machine"
HighTec 链接选项	-o "$(ELFDIR)/$(PROJNAME).elf" -Wl,-Map="$(ELFDIR)/$(PROJNAME).map" -nostartfiles -Wl,--allow-multiple-definition -Wl,--cref -Wl,--oformat=elf32-tricore -Wl,--mcpu=tc162 -Wl,--mem-holes -Wl,--extmap="a" -L"$(PRODDIR)/tricore/include “

6 证书

中华人民共和国国家版权局

计算机软件著作权登记证书

证书号：软著登字第6700633号

软件名称：知从木牛信息安全库软件
[简称：信息安全库]
V1.0

著作权人：上海知从科技有限公司

开发完成日期：2020年03月14日

首次发表日期：2020年06月03日

权利取得方式：原始取得

权利范围：全部权利

登记号：2020SR1895504

根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。

中华人民共和国国家版权局
计算机软件著作权
登记专用章

No. 07119009

2020年12月25日

木牛软件著作权登记证书

上海市软件行业协会

软件产品证书

经评估,知从木牛信息安全库软件[简称：信息安全库]V1.0 符合《进一步鼓励软件产业和集成电路产业发展的若干政策》和《软件产品评估规范》的有关规定，评估为软件产品，特发此证。

申请企业：上海知从科技有限公司
软件类别：应用软件
证书编号：沪ZC-2021-0019
有 效 期：五年

上海市计算机软件评测重点实验室
（上海计算机软件技术开发中心）
二〇二一年十一月二十五日

木牛软件 CYBERSECURITY 产品证书