基于AUTOSAR架构的CP轻量化技术

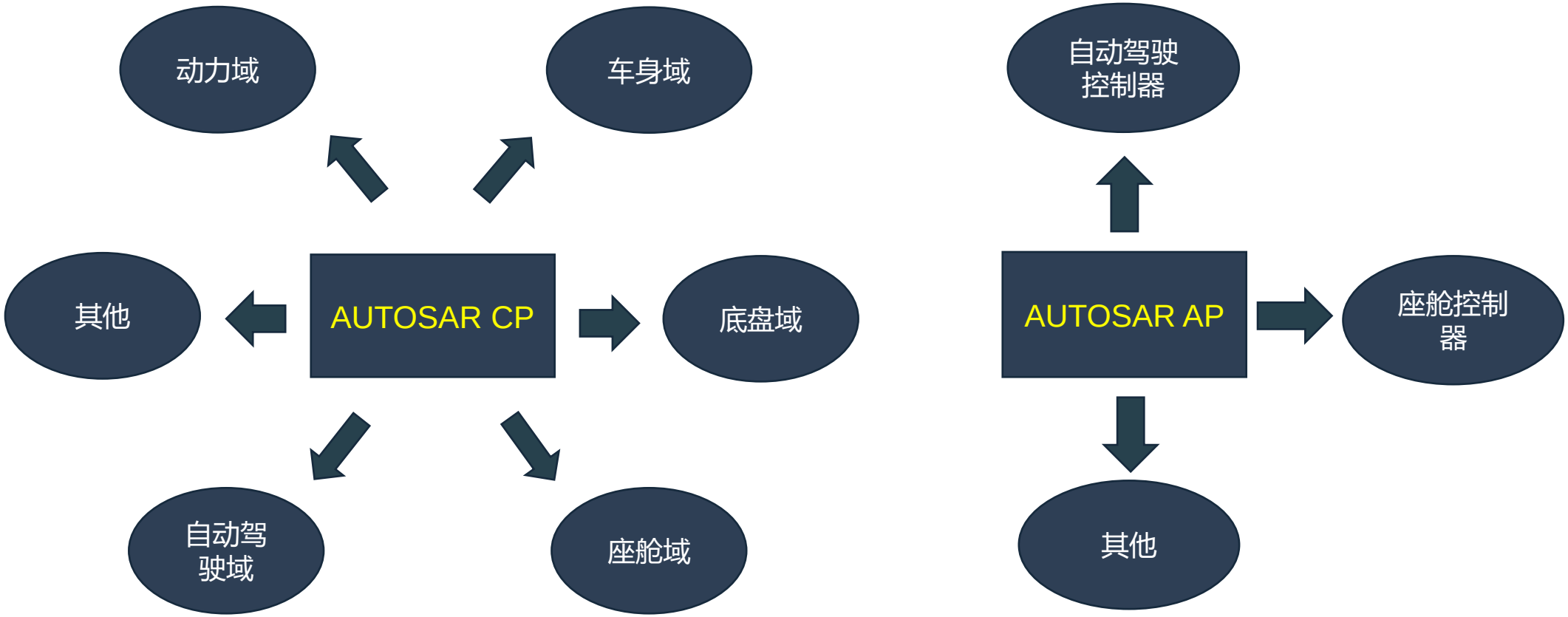
曹守营

2025-03-18

2025第六届软件定义汽车论坛暨AUTOSAR中国日

上海

AUTOSAR应用场景



AUTOSAR应用场景

- 应用算法比较复杂
- 芯片资源相对丰富
- 对功能安全有需求
- 对信息安全有需求

MPC57xx S32K14x S32K3XX

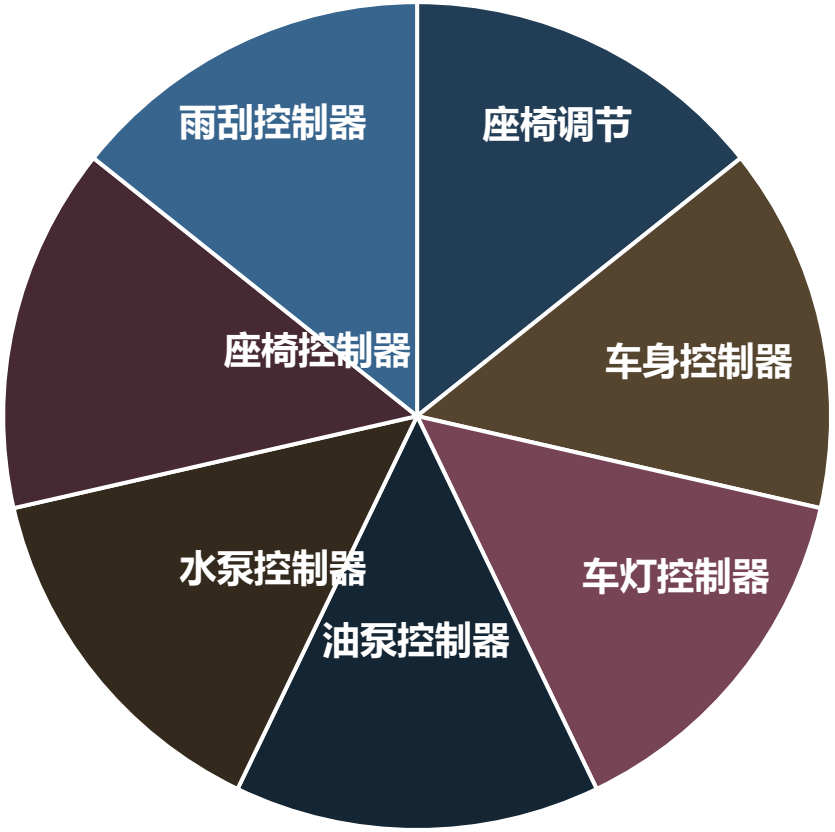
TC234/264/275 TC364/377/387/397

RH850 RL78/U2A/U2B

SPC58NN

特殊场景

- 应用算法相对简单
- 芯片资源相对较少
- 需要和其他控制器通信
- 需要诊断和存储等功能
- 可能对功能安全有要求
- 可能对信息安全有要求



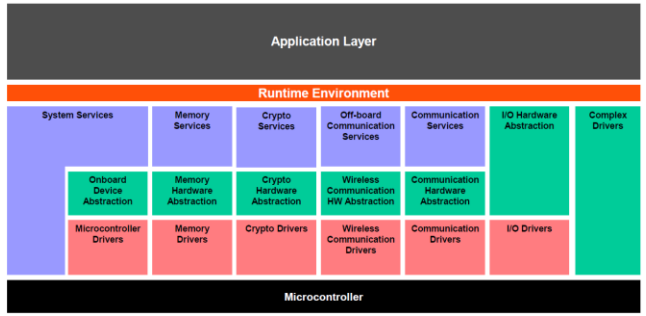
Infineon TLE989x

NXP S32Mx

RENESAS RH850

AUTOSAR价值

AUTOSAR特点



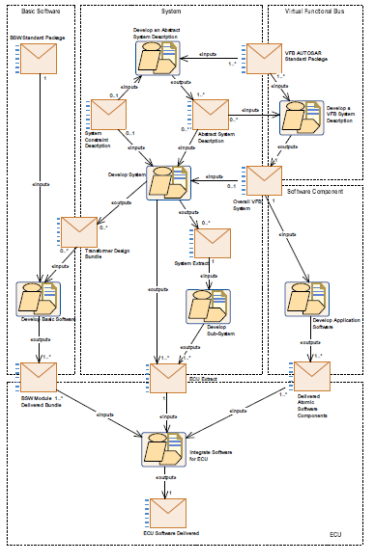
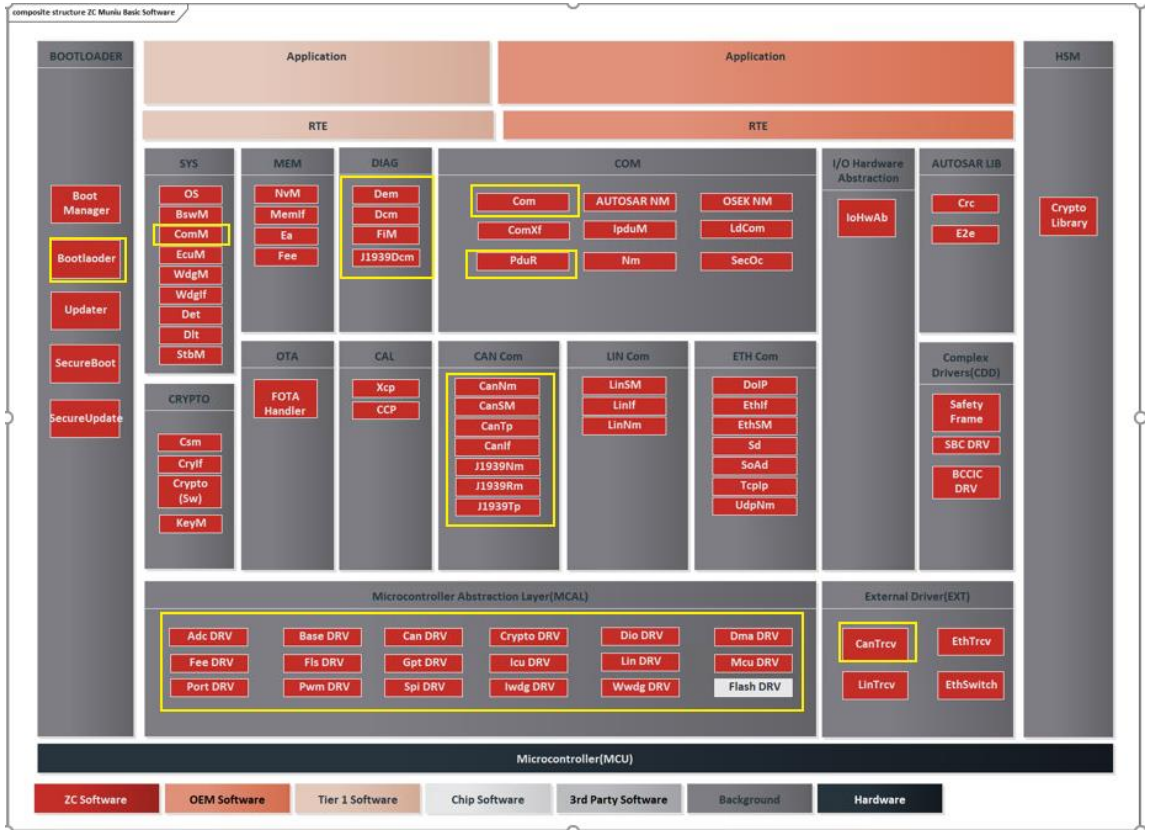
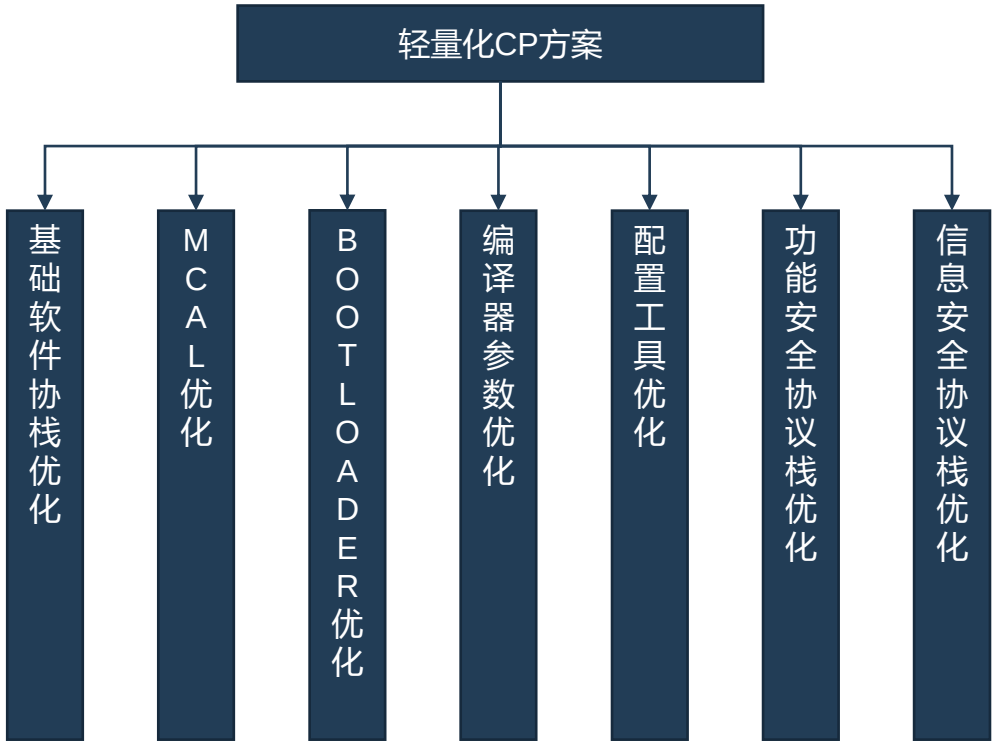


Figure 2.9: Methodology Overview: Workflow

- **标准化**
  模块标准化，接口标准化，思想统一，提高交流效率
- **移植性**
  架构分层，软件模块分开，提高软件可移植性
- **扩展性**
  支持可配置，配置和静态代码分离，降低用户使用成本
- **安全性**
  标准化接口，满足功能安全要求
- **方法论**
  提供控制器开发方法论，从系统、软件、实现全流程

轻量化CP解决方案

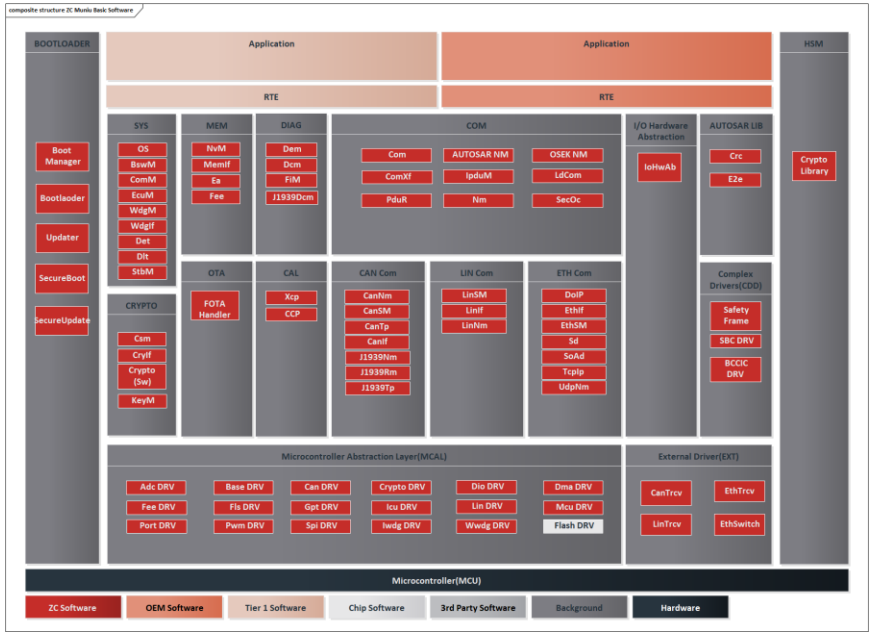

composite structure ZC Muniu Basic Software
BOOTLOADER
Application
Application
HSM
RTE
RTE
Boot Manager
Bootloader
Updater
SecureBoot
SecureUpdate
SYS
OS
BswM
ComM
EcuM
WdgM
WdgIf
Det
Dlt
StbM
MEM
NvM
MemIf
Ea
Fee
DIAG
Dem
Dcm
FiM
J1939Dcm
COM
Com
ComXf
PduR
AUTOSAR NM
IpduM
Nm
OSEK NM
LdCom
SecOc
I/O Hardware Abstraction
IoHwAb
AUTOSAR LIB
Crc
E2e
Crypto Library
CRYPTO
Csm
CryIf
Crypto (Sw)
KeyM
OTA
FOTA Handler
CAL
Xcp
CCP
CAN Com
CanNm
CanSM
CanTp
CanIf
J1939Nm
J1939Rm
J1939Tp
LIN Com
LinSM
LinIf
LinNm
ETH Com
DoIP
EthIf
EthSM
Sd
SoAd
TcpIp
UdpNm
Complex Drivers(CDD)
Safety Frame
SBC DRV
BCCIC DRV
Microcontroller Abstraction Layer(MCAL)
Adc DRV
Fee DRV
Port DRV
Base DRV
Fls DRV
Pwm DRV
Can DRV
Gpt DRV
Spi DRV
Crypto DRV
Icu DRV
Iwdg DRV
Dio DRV
Lin DRV
Wwdg DRV
Dma DRV
Mcu DRV
Flash DRV
External Driver(EXT)
CanTrcv
LinTrcv
EthTrcv
EthSwitch
Microcontroller(MCU)
ZC Software
OEM Software
Tier 1 Software
Chip Software
3rd Party Software
Background
Hardware


轻量化CP方案
基础软件协栈优化
MCAL优化
BOOTLOADER优化
编译器参数优化
配置工具优化
功能安全协议栈优化
信息安全协议栈优化

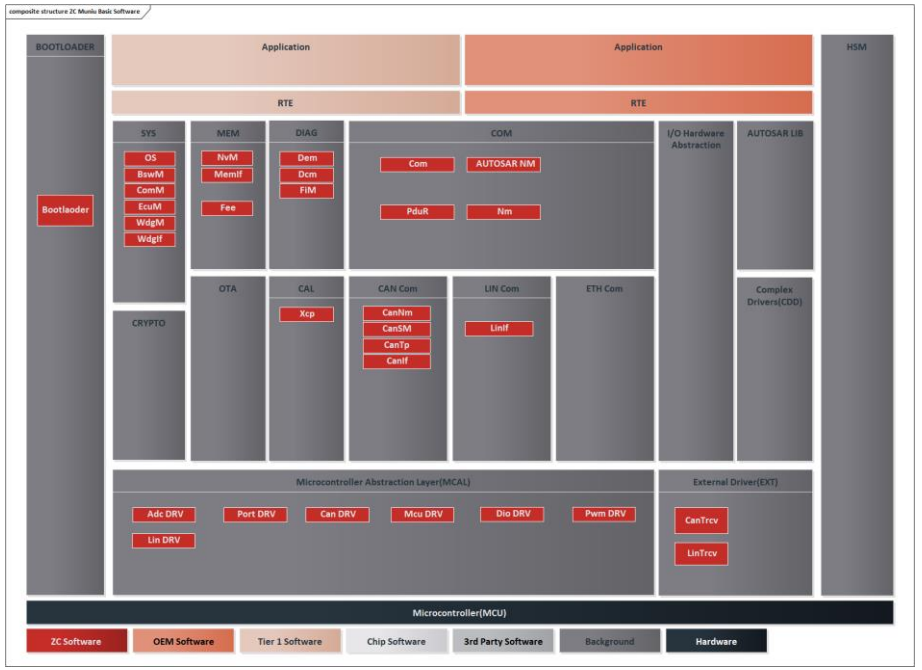
轻量化CP的特点

- 满足AUTOSAR规范，具有兼容性和可扩展性
- 功能精简，资源占用少
- 去掉复杂的交互逻辑，具有高实时性
- 保留核心功能，保证安全性

轻量化CP方案-基础软件协议栈优化



裁剪后



- 保留必要的协议栈　　CAN CANTP CANIF PDUR等
- 优化可选协议栈 满足最小功能Feature　COM UDS ComM等
- 完全裁剪多余的协议栈　OS XCP Fee BswM EcuM等

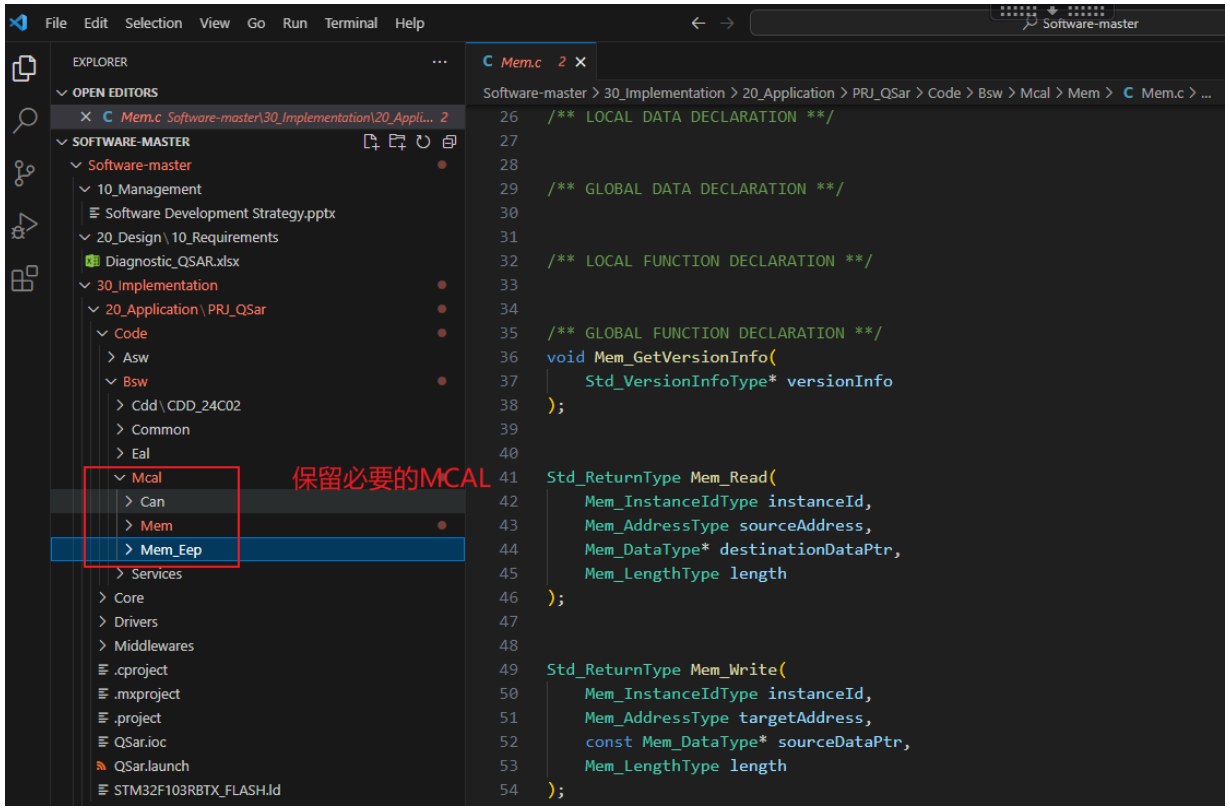
轻量化CP方案--MCAL优化

- 保留必要的模块

CanDrv、FlsDrv、DioDrv、AdcDrv、GptDrv等

- 完全裁剪多余的协议栈

CryptoDrv、FeeDrv等



轻量化CP方案-Bootloader优化

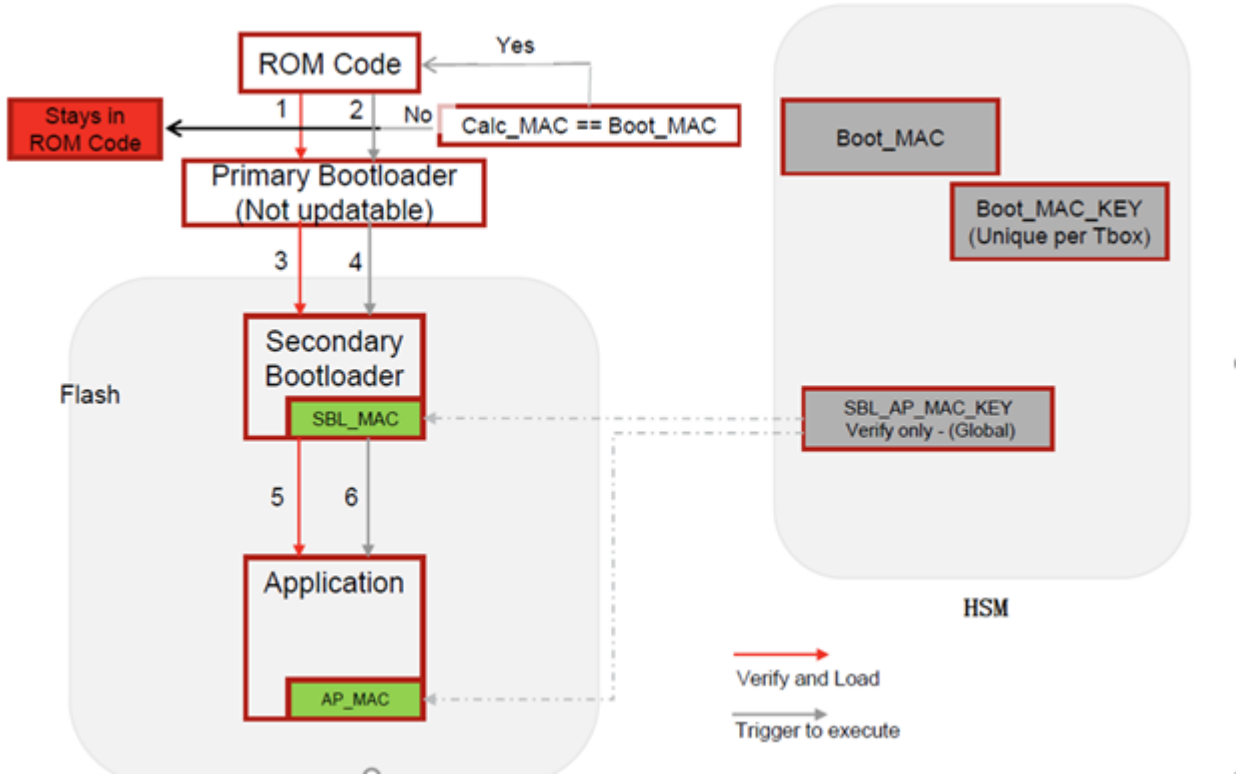
- 支持基本刷写功能的服务

  10,11,22,27,31,34,36,37 SID

- 简化存储策略

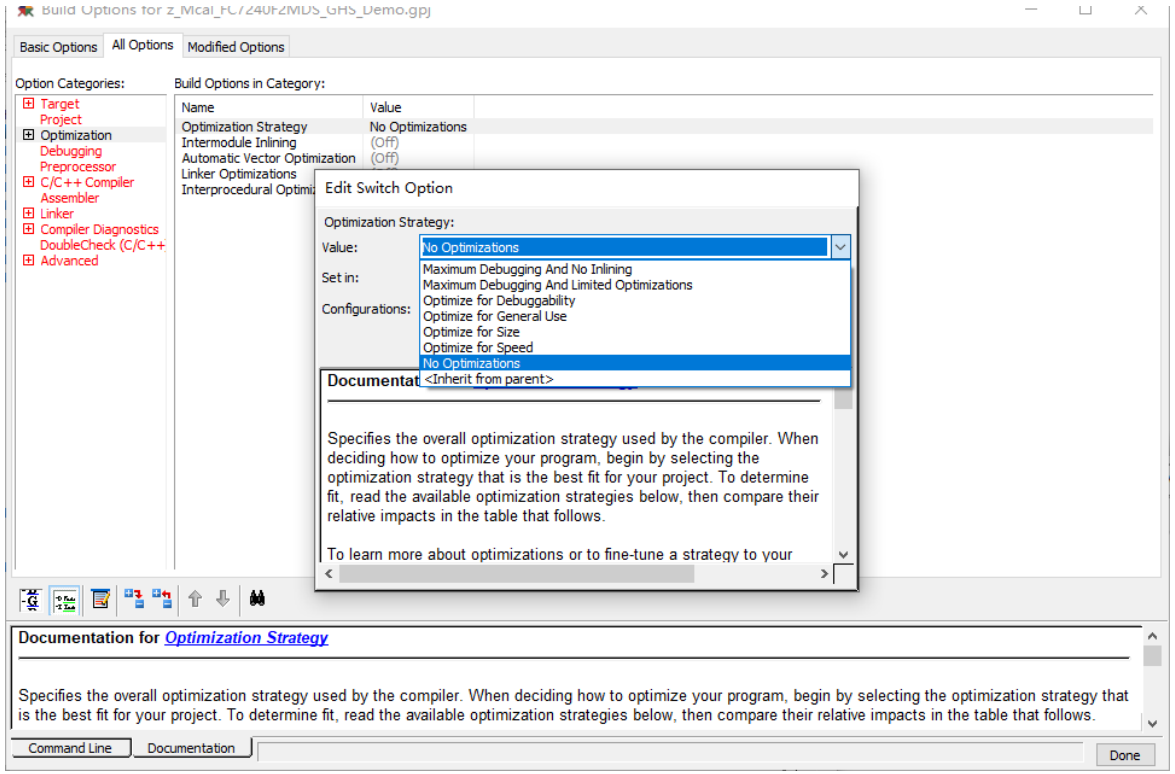
  支持基本的存储Fls，Fee

- 优化Bootloader启动时间



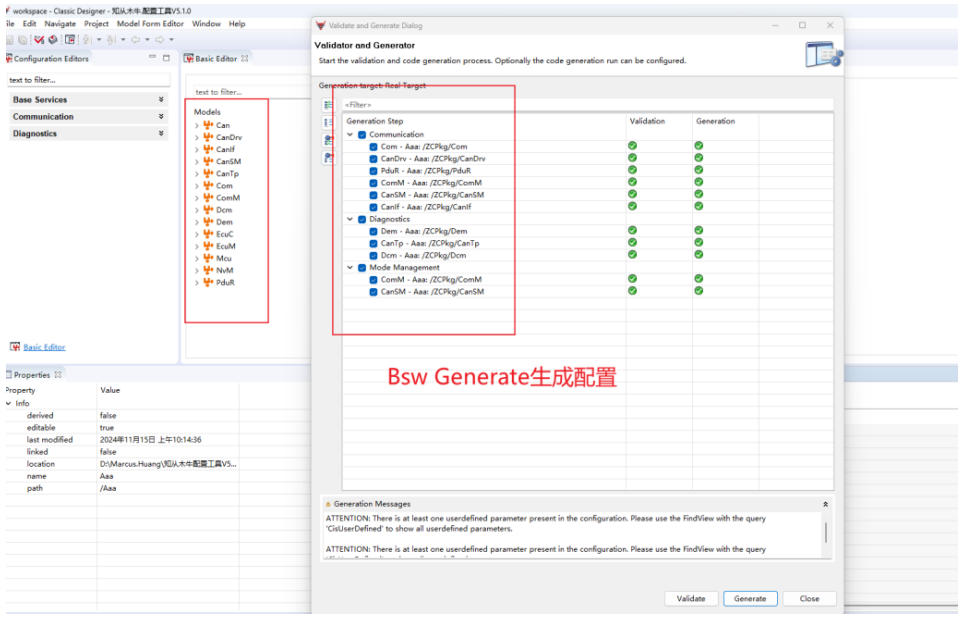
轻量化CP方案-编译器参数优化

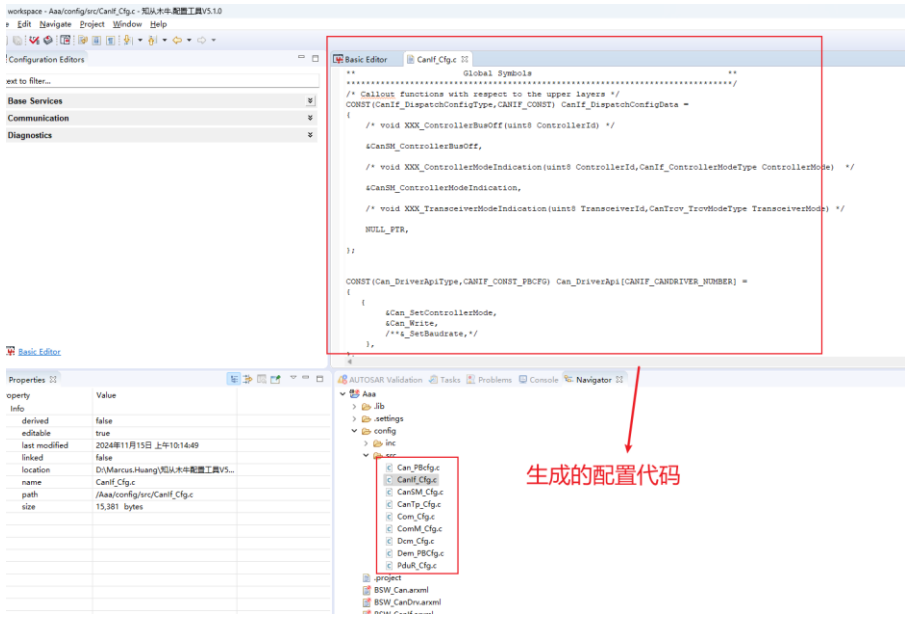
- 基础优化等级设置-balance –size 等
- 针对文件级进行优化
- 单个函数的优化



轻量化CP方案-配置工具优化

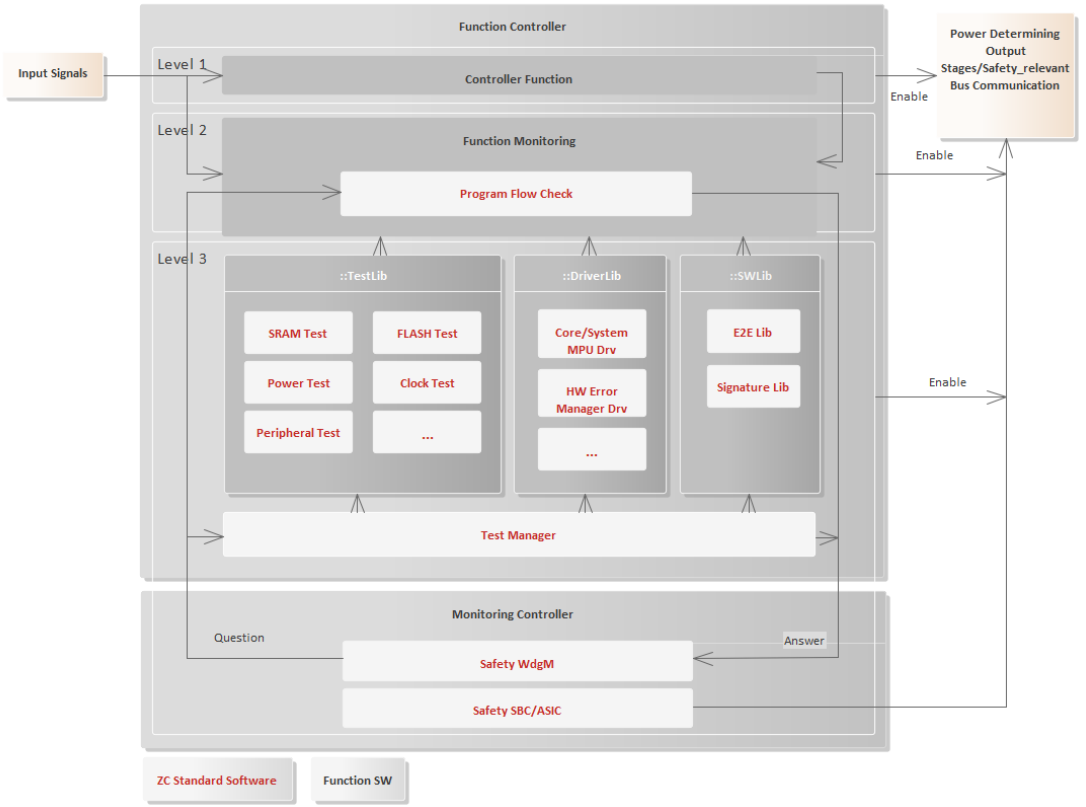
- 只保留各模块基本Feature的轻量化配置工具
- 将轻量化的MCAL和BSW配置放在同一个工具
- 适配整套轻量化CP协议栈的配置工具





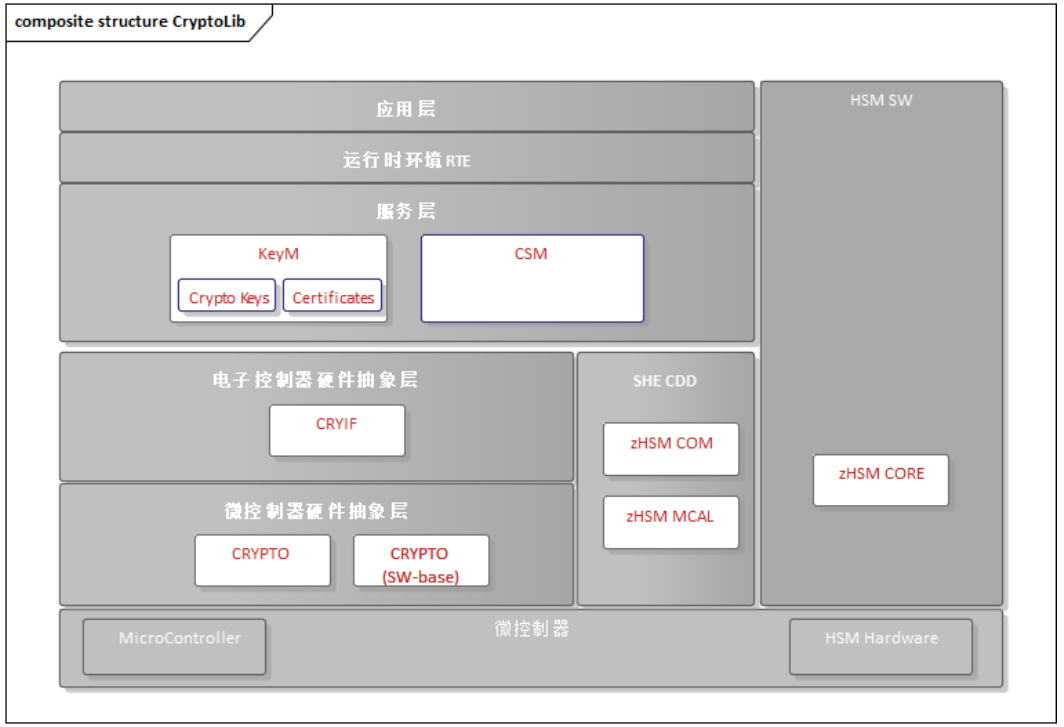
轻量化CP方案-功能安全库优化

- 参考EGAS三层架构设计，包含：
  - MCU内部模块自检测试（即SF.MCU）
  - SBC硬件安全机制的驱动（即SF.SBC)
- 保留必要的功能安全机制



轻量化CP方案-信息安全库优化

- 基于硬件加密模块（HSM）的信息安全库
- 带有加密算法硬件加速器实现硬件驱动
- 保留必要的信息安全机制
- 纯软件实现信息安全算法

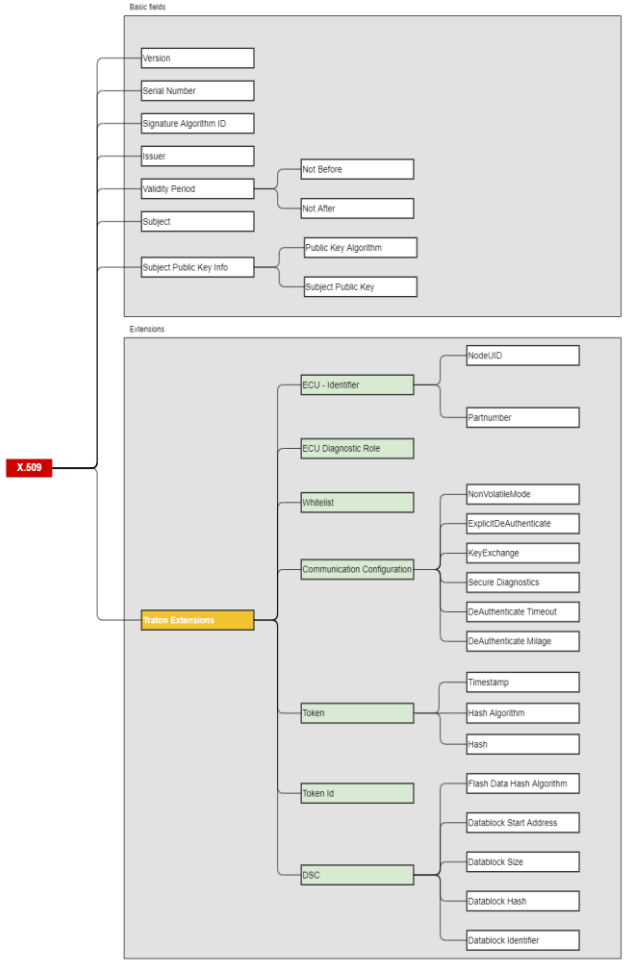


算法支持

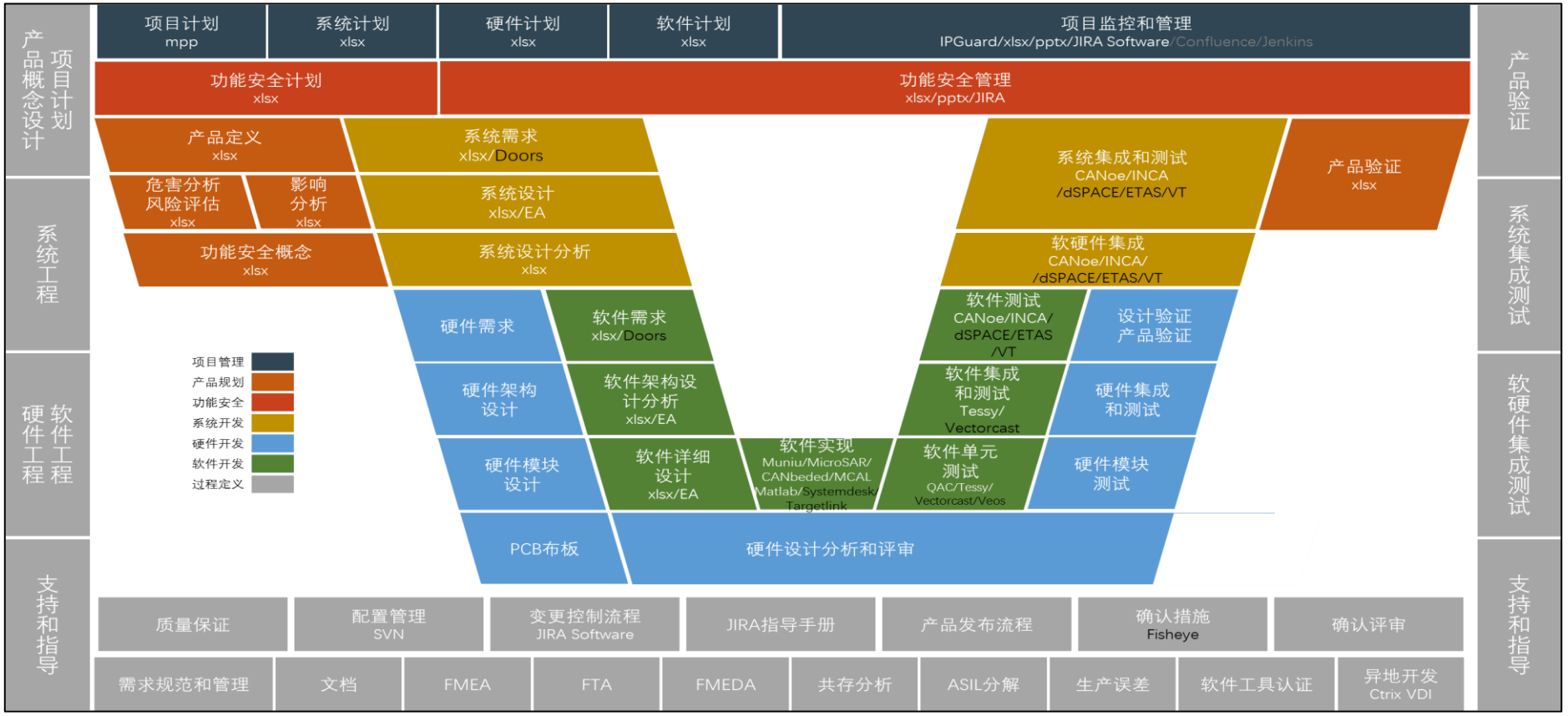
轻量化CP信息安全库精简加解密算法

- AES
- HASH
- CMAC
- ECC
- RSA
- 国密SM2\3\4
- ED25519
- X25519密钥交换
- X.509证书解析
- ……

软件算法实现			
分类	使用算法	扩展&模式	备注
单向加密	SHA1	NA	输出长度20Bytes
	SHA224	NA	输出长度28Bytes
	SHA256	NA	输出长度32Bytes
	SHA512	NA	输出长度64Bytes
	CMAC	NA	CBC-MAC
	MAC	GCM	GCM模式
		GMAC	GMAC模式
	HMAC	HMAC_SHA1	
		HMAC_SHA256	
		HMAC_RIPEMD-160	
	MD5	NA	
	RIPEMD-160	NA	一种HASH算法
对称加密	RC2	NA	
	AES128	NA	输出长度128位
	AES192	NA	输出长度192位
	AES256	NA	输出长度256位
	DES	NA	
	TDES	NA	三重DES
非对称加密	ECC	NA	椭圆曲线加密，根据参数不同有不同的模式
	RSA	RSA-OAEP_SHA1	OAEP填充方式
		RSA-OAEP_SHA256	
		RSA-PSS_SHA1	PSS填充方式
		RSA-PSS_SHA256	
		RSA-PSS_RIPEMD-160	

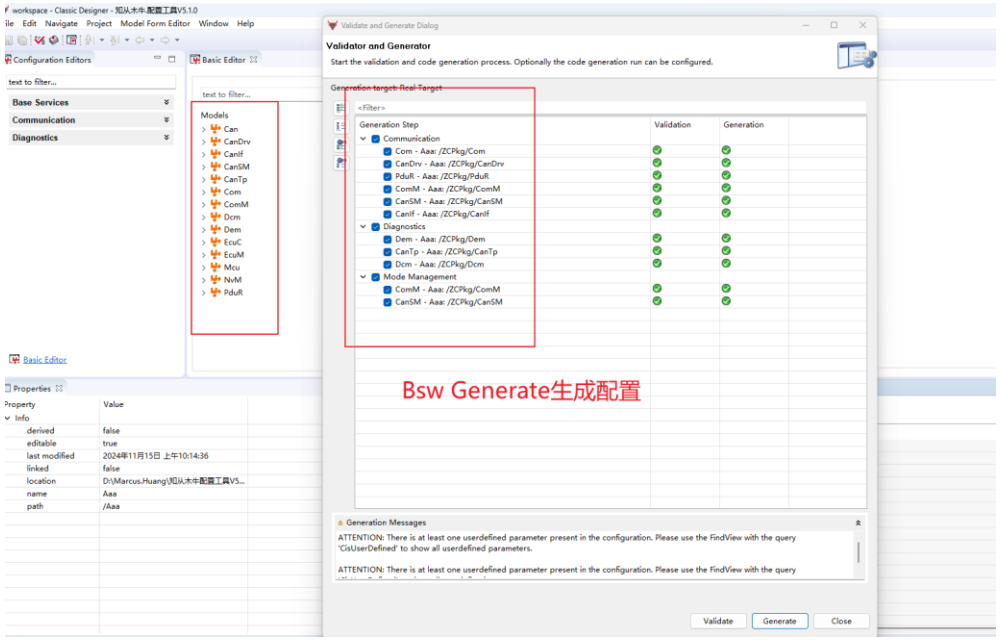


开发流程


产品概念设计
项目计划
系统工程
软件工程
硬件工程
支持和指导
项目计划 mpp
系统计划 xlsx
硬件计划 xlsx
软件计划 xlsx
项目监控和管理 IPGuard/xlsx/pptx/JIRA Software/Confluence/Jenkins
功能安全计划 xlsx
功能安全管理 xlsx/pptx/JIRA
产品定义 xlsx
危害分析 风险评估 xlsx
影响分析 xlsx
功能安全概念 xlsx
系统需求 xlsx/Doors
系统设计 xlsx/EA
系统设计分析 xlsx
硬件需求
软件需求 xlsx/Doors
硬件架构设计
软件架构设计分析 xlsx/EA
硬件模块设计
软件详细设计 xlsx/EA
软件实现 Muniu/MicroSAR/ CANbeded/MCAL Matlab/Systemdesk/ Targetlink
PCB布板
硬件设计分析和评审
软件单元测试 QAC/Tessy/ Vectorcast/Veos
软件集成和测试 Tessy/ Vectorcast
软件测试 CANoe/INCA/ dSPACE/ETAS /VT
硬件模块测试
硬件集成和测试
设计验证 产品验证
软硬件集成 CANoe/INCA/ /dSPACE/ETAS/VT
系统集成和测试 CANoe/INCA /dSPACE/ETAS/VT
产品验证 xlsx
项目管理
产品规划
功能安全
系统开发
硬件开发
软件开发
过程定义
产品验证
系统集成测试
软硬件集成测试
支持和指导
质量保证
配置管理 SVN
变更控制流程 JIRA Software
JIRA指导手册
产品发布流程
确认措施 Fisheye
确认评审
需求规范和管理
文档
FMEA
FTA
FMEDA
共存分析
ASIL分解
生产误差
软件工具认证
异地开发 Ctrix VDI

轻量化CP效果

- 轻量化CP全部内存占用64KB以内
- 功能安全达到ASIL B



进一步优化机制

- 代码深度优化

  利用更加先进的编译技术和压缩算法，减少代码体积

- 硬件适配精细化

  针对不同MCU进行更加精细化的硬件适配优化，定制开发适配方案

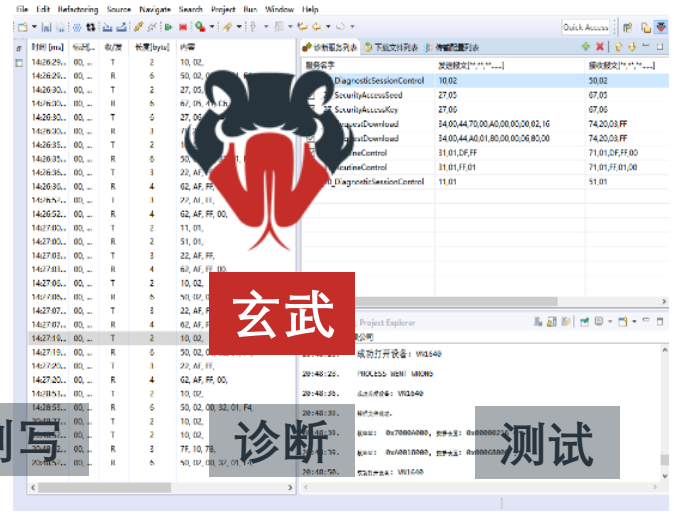
- 增强任务调度算法

  开发更加智能的任务调度算法，根据系统的实时负载和任务优先级，动态调整任务的执行顺利和时间分配

- 中断处理优化

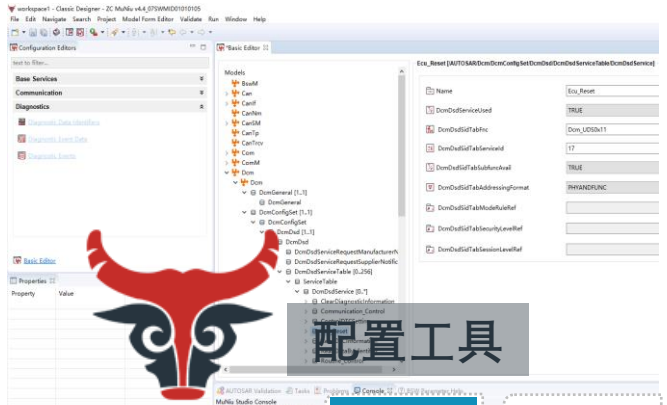
  优化中断处理机制，减少中断响应时间和处理延迟

知从科技--全球领先完整AUTOSAR软件产品方案

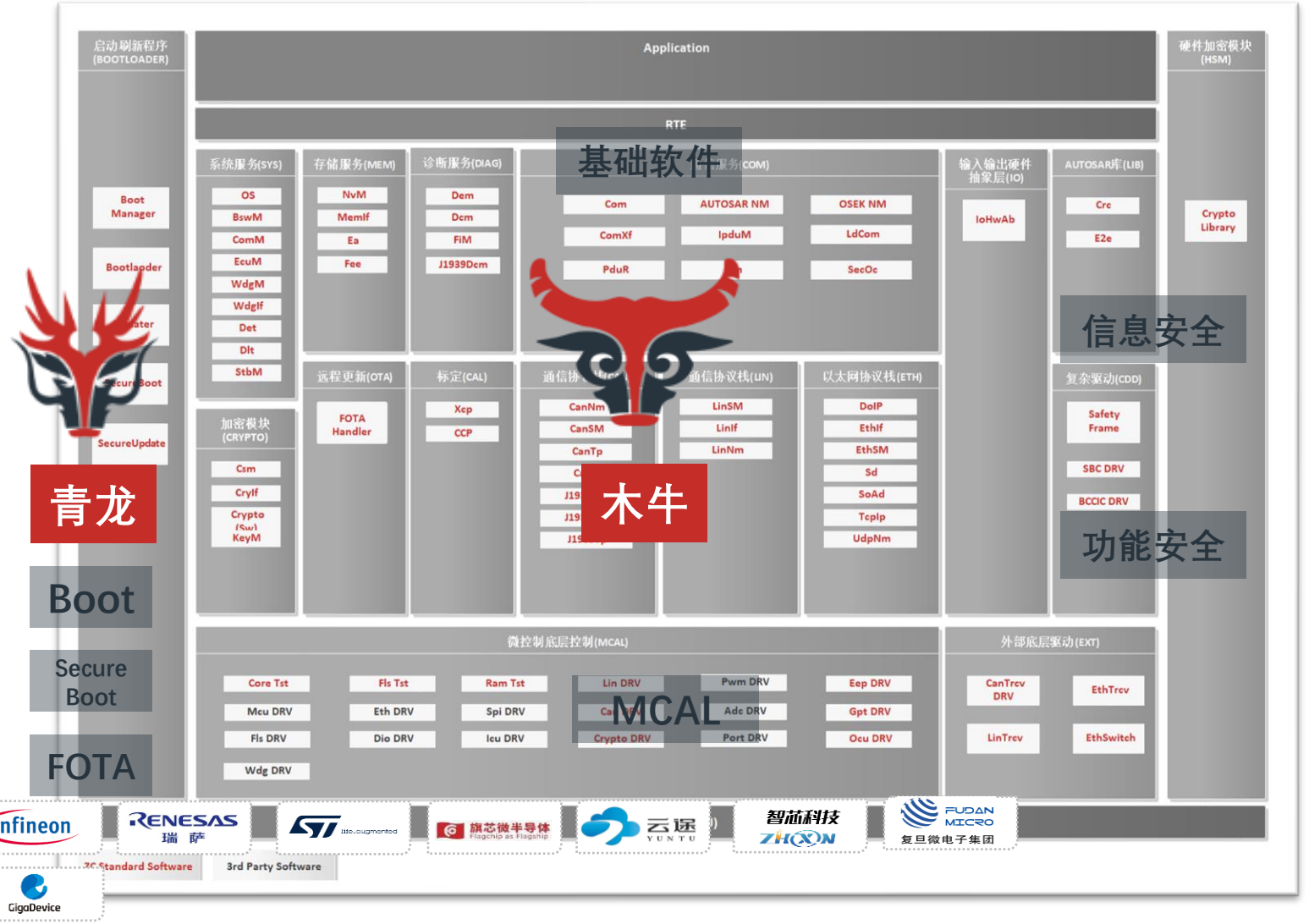


玄武

刷写 诊断 测试



配置工具



BMW · Honda · BOSCH · Continental · Ford · gm · Mercedes-Benz · STELLANTIS · TOYOTA · VOLKSWAGEN GROUP