life.augmented

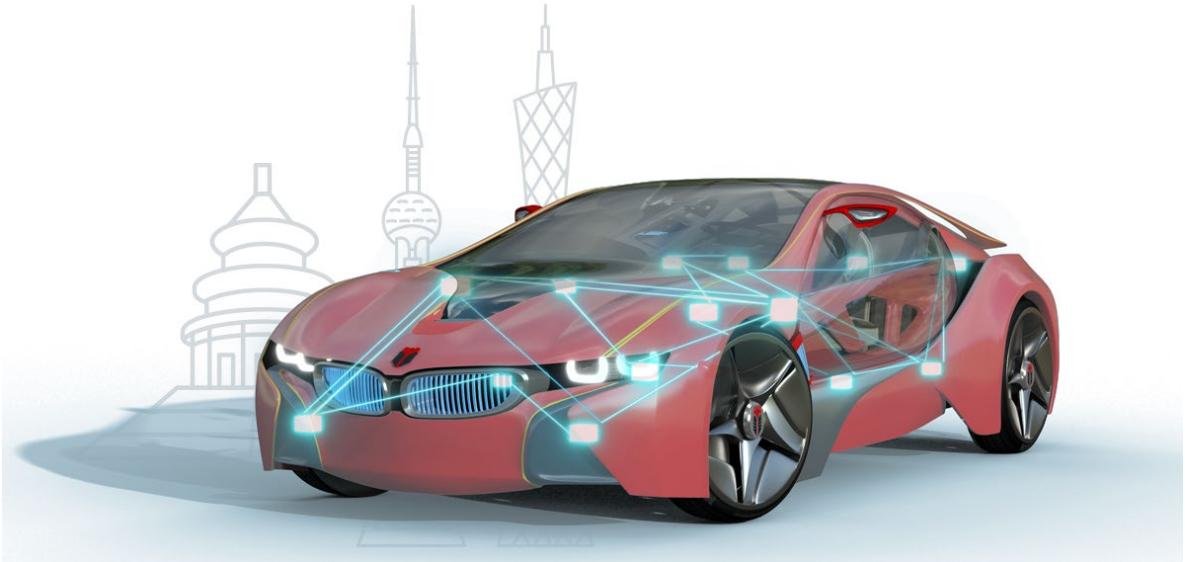
ZHI CONG KE JI 知从科技

知从青龙 BOOTLOADER ST SPC58NN GEELY GEEA2.0 产品手册

ZC.QINLONG BOOTLOADER PRODUCT MANUAL BASED ON ST SPC58NN FOR GEELY GEEA2.0

知从青龙 BootLoader

ZC.QingLong BootLoader



知从青龙 BOOTLOADER ST SPC58NN GEELY GEEA2.0 产品手册

ZC.QINLONG BOOTLOADER PRODUCT MANUAL BASED ON ST SPC58NN FOR GEELY GEEA2.0

知从青龙 BootLoader

ZC.QingLong BootLoader

1 功能概述 FUNCTION OVERVIEW

知从青龙 BootLoader 是由知从科技自主研发的程序刷新软件(BootLoader)。使用知从青龙 BootLoader 的控制器，可以通过 CAN、LIN、SPI、UART 等通信方式实现应用程序的更新功能。目前，知从青龙 BootLoader 已支持 NXP、Infineon、Renesas、ST 等多家芯片，并且支持多家整车厂程序刷新规范，可提供定制开发服务。

ZC.QingLong BOOTLOADER is a flash programming software (BOOTLOADER) independently developed by ZC Technology. Controllers using the ZC.QingLong BOOTLOADER can achieve the update function of applications through various communication methods such as CAN, LIN, SPI, UART, etc. Currently, ZC.QingLong BOOTLOADER has supported chips from multiple manufacturers including NXP, INFINEON, RENESAS, ST, etc., and complies with the program refreshing specifications of various vehicle manufacturers. It also offers customized development services.

此文档描述了知从青龙 BootLoader 基于 SPC58NN 平台，实现对 GEEA2.0 规范的支持。目前已实现支持 VBF 文件刷写、主从 BootLoader 刷写、压缩算法 LZSS、数字签名认证等功能需求，满足 GEEA2.0 规范中大部分的刷写需求。

This document describes the support for the GEEA2.0 specification based on the SPC58NN platform by the ZC.QingLong BootLoader. Currently, it has implemented support for VBF file flashing, master-slave BootLoader flashing, LZSS compression algorithm, digital signature authentication, and other functional requirements, meeting most of the flashing needs in the GEEA2.0 specification.

2 应用领域 APPLICATION FIELDS

知从青龙 BootLoader 可应用于使用 SPC58NN 系列芯片的控制器程序刷新功能。支持的控制器包括：

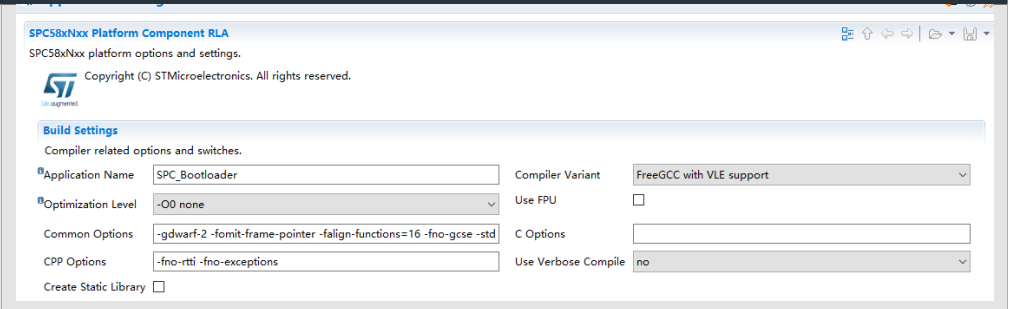
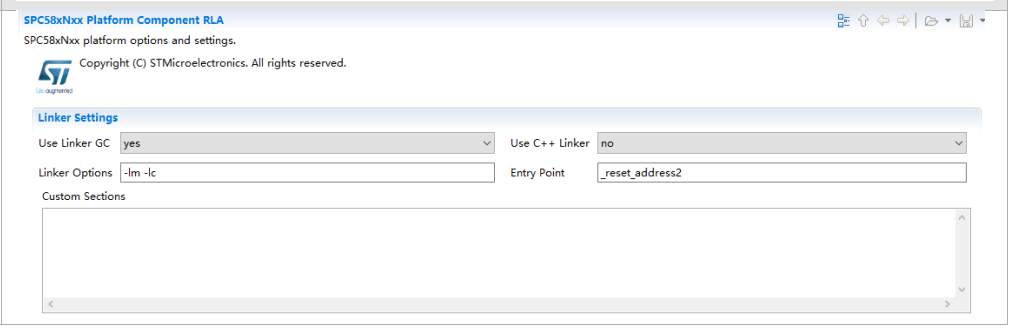
ZC.QingLong BootLoader can be applied to the program refreshing function of controllers using the SPC58NN series of chips. The supported controllers include:

- 车身控制器
  Body Control Module
- 网关控制器
  Gateway Controller
- 车载娱乐系统控制器
  In-vehicle Infotainment System Controller
- 电子驻车制动系统
  Electronic Parking Brake System
- 胎压监测系统
  Tire Pressure Monitoring System
- 电池管理系统
  Battery Management System
- 空调控制系统
  Air Conditioning Control System
- 车窗控制系统
  Window Control System
- 门控系统
  Door Control System

3 配置环境 CONFIGURE THE ENVIRONMENT

配置环境 Configuration Environment	
Hardware (Chip)	SPC58NN
Compilers Supported	HighTec 4.9.3.0 / SPC5 Studio 6.0.0
Debugger	Isystem (IC5700)

HighTec 编译器 HighTec Compiler	
编译选项 Compilation Options	@ccompilerincludelist.optfile -fno-common -O0 -g3 -W -Wall -Wextra -Wdiv-by-zero -Warray-bounds -Wcast-align -Wignored-qualifiers -Wformat -Wformat-security -pipe -DSTM_SPC58NN -DAUTOSAR_OS_NOT_USED -DCPU_SPC58NN84E7 -DUSE_CORE=2 -DUSE_IRQ -DUSE_EXCEPTIONS -fstrict-volatile-bitfields -fshort-double -mcpu=z4256n3 -mversion-info -std=gnu99 -mregnames
链接选项 Linker Options	-nocrt0 -nostartfiles -T"../ld/spc58nn-memory.x" -T"../ld/spc58nn-core2.ld" -Wl,--gc-sections -mcpu=z4256n3 -Wl,@objectlist.optfile -Wl,@libpathlist.optfile -lc55_gcc -Wl,-Map="$(basename $(notdir $@)).map" -Wl,--cref -fshort-double -Wl,-n -Wl,--extmap=a

SPC5 Studio 编译器 SPC5 Studio Compiler	
编译选项 Compilation Options	
链接选项 Linker Options	

4 开发背景 DEVELOPMENT BACKGROUND

目前，汽车上的电子电气架构越来越复杂，并伴随着汽车的电动化、智能化、网联化、共享化，软件的研发在汽车上占比越来越大。软件更新的频率越来越高。而且，在汽车的整个生命周期中，包括研发阶段、生产阶段、售后阶段，各个阶段都需要实现软件的更新功能。因此，客户对软件程序更新的需求越来越迫切。

Currently, the electronic and electrical architecture in vehicles is becoming increasingly complex, alongside the electrification, intelligence, connectivity, and sharing of automobiles, the development of software is taking up a larger proportion in vehicles. The frequency of software updates is also rising. Moreover, throughout the entire life cycle of a vehicle, including the research and development phase, production phase, and after-sales service phase, the ability to update software is required at each stage. As a result, the demand from customers for software program updates is becoming more urgent.。

对于整车厂或供应商，BootLoader 是控制器开发必备的功能。并且，不同的整车厂有不同的程序更新规范，同时 BootLoader 驱动又依赖于不同的芯片。因此，为了满足不同的整车厂程序更新规范，又适配不同的芯片，知从科技提供了完整的 BootLoader 解决方案—知从青龙 BootLoader。知从青龙 BootLoader 既适用于不同的整车厂程序更新规范，又适用于不同芯片厂商的芯片，让客户更专注与自己的控制器产品研发。

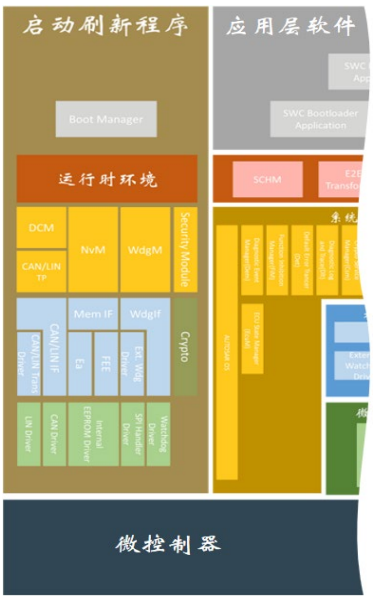
For vehicle manufacturers or suppliers, a BootLoader is an essential feature for controller development. Moreover, different vehicle manufacturers have their own specifications for program updates, and the BootLoader drivers are dependent on different chips. Therefore, to meet the varying program update specifications of vehicle manufacturers and to be compatible with different chips, ZC Technology has provided a comprehensive BootLoader solution—ZC.QingLong BootLoader. The ZC.QingLong BootLoader is suitable for the program update specifications of various vehicle manufacturers as well as for chips from different chip manufacturers, allowing customers to focus more on the development of their own controller products.

GEEA2.0 电子电气架构在 BootLoader 中，通过实现 PBL-SBL BootLoader 架构、Secure Boot、VBF 加密签名验证等功能，降低了在 MCU 更新过程中的安全风险，大幅提升了 BootLoader 的安全性以及可靠性。

In the GEEA2.0 electronic and electrical architecture, the implementation of features such as the PBL-SBL BootLoader architecture, Secure Boot, and VBF encryption signature verification within the BootLoader significantly reduces the security risks associated with MCU updates, greatly enhancing the security and reliability of the BootLoader.

知从.青龙

ZC.QingLong



5 功能描述 FUNCTION DESCRIPTION

5.1 产品特点 Product Features

- 适用于 GEEA2.0 平台规范

  Suitable for GEEA2.0 Platform Specifications

- 支持 PBL-SBL 的 BootLoader 架构

  Supports PBL-SBL BootLoader Architecture

- 支持应用程序和数据的更新功能

  Supports update functions for applications and data

- 支持 CAN/UART 等通信

  Supports communication via CAN/UART, etc.

- 支持主从节点间的 UART 通信刷写

  Supports UART communication between master and slave nodes for flashing

- 适配知从玄武程序更新工具，提供完整的程序更新解决方案

  Adapts to ZC.XuanWu program update tool, providing a complete program update solution

- 支持对称加密 SHA256 和 AES128 算法

  Supports symmetric encryption algorithms SHA256 and AES128

- 支持非对称加密 ECC 和 RSA2048 算法

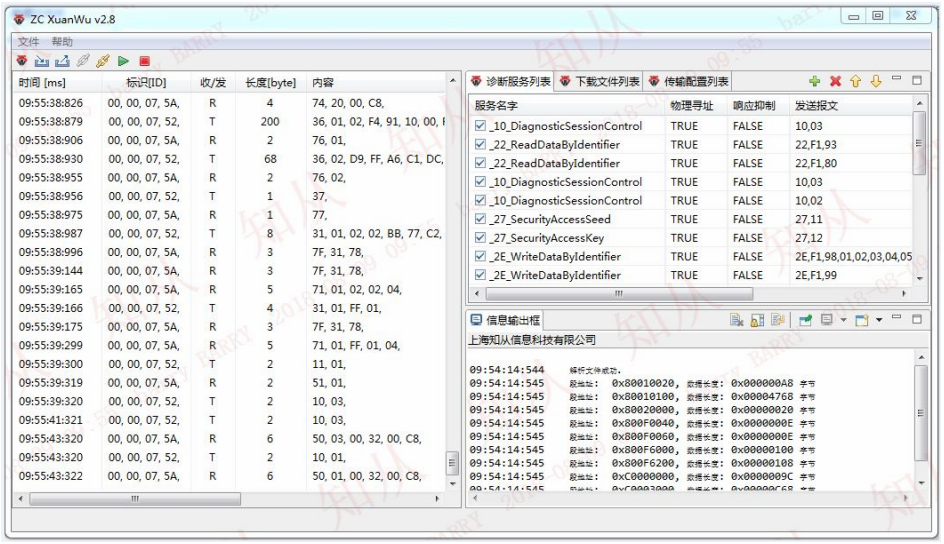
  Supports asymmetric encryption algorithms ECC and RSA2048

- 支持 VBF 文件解析

  Supports parsing of VBF files

- 支持 LZSS 压缩算法的压缩和解压

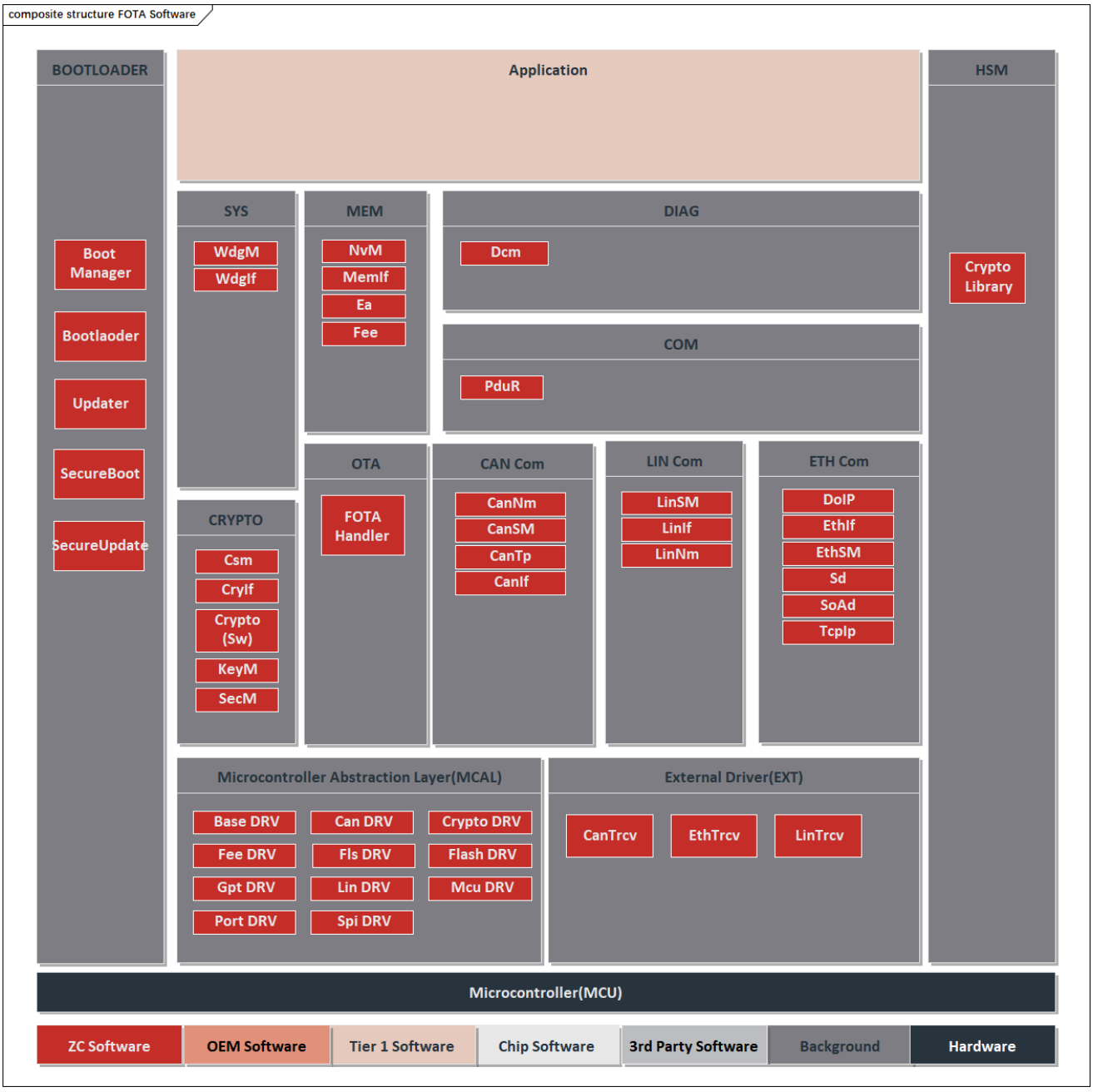
  Supports compression and decompression using the LZSS compression algorithm



知从玄武—程序更新工具 ZC.XuanWu—Program Update Tool

ZC.XuanWu—Program Update Tool

5.2 软件架构 Software Architecture



FOTA 系统架构
FOTA SYSTEM ARCHITECTURE

知从青龙 FOTA 系统架构支持 CAN、LIN、SPI、Ethernet 通信场景下的 FOTA 功能，通过 Dcm 模块实现 UDS 报文解析和诊断刷写，并通过适配 Crypto Library 实现各 OEM 规范的信息安全需求。以下为各模块的功能描述：

- Bootloader

BootManager 模块提供 FOTA 启动管理功能，支持适配软硬件 SecureBoot 功能，通过烧录和刷写存储 Bootloader 和 Application 的期望 MAC 值，启动阶段 SecureBoot 通过计算比较 Bootloader 和 Application 的 MAC 执行软件完整性校验，保证软件安全需求。

- Can Com

  Can 模块支持 CAN、CANFD 通信功能。

- Spi Com

  Spi 模块支持主从刷写功能，通过适配 5、6、7 线硬件配置，可支持多种 SPI 通信刷写模式。

- Ethernet Com

  DoIP 模块基于 TCP/IP 协议实现 Ethernet 通信收发功能，满足 ISO 13400 标准定义。通过车辆识别、路由激活、诊断消息功能实现 UDS 刷写流程，实现 Ethernet OTA 功能。

- Dcm

  Dcm 模块基于通信模块支持实现诊断功能，满足 ISO 14229 以及 ISO 15765 标准定义。

- Crypto、HSM

  Ethernet OTA 支持适配木牛加密库功能，支持非对称加密算法和加密算法结合实现安全刷写功能，适配证书认证功能满足安全诊断功能，适配 HSM 提高信息安全功能的稳定性和校验速度。

The Qinglong Ethernet FOTA system architecture supports the FOTA function in communication scenarios such as CAN, LIN, SPI, and Ethernet. It realizes the parsing of UDS messages and diagnostic programming through the Dcm module, and meets the information security requirements of various OEM specifications by adapting to the Crypto Library. The following are the functional descriptions of each module:

- Bootloader

  The BootManager module provides FOTA startup management functions and supports the adaptation of hardware and software SecureBoot functions. It stores the expected MAC values of the Bootloader and Application through programming and flashing. During the startup phase, SecureBoot performs software integrity verification by calculating and comparing the MACs of the Bootloader and Application to ensure software security requirements.

- Can Com

  The Can module supports CAN and CANFD communication functions.

- Spi Com

  The Spi module supports the master-slave programming function. By adapting to the hardware configurations of 5, 6, and 7 wires, it can support multiple SPI communication programming modes.

- Ethernet Com

  The DoIP module realizes the Ethernet communication sending and receiving functions based on the TCP/IP protocol, meeting the definition of the ISO 13400 standard. It implements the UDS flashing process through vehicle identification, routing activation, and diagnostic message functions, thereby achieving the Ethernet OTA function.

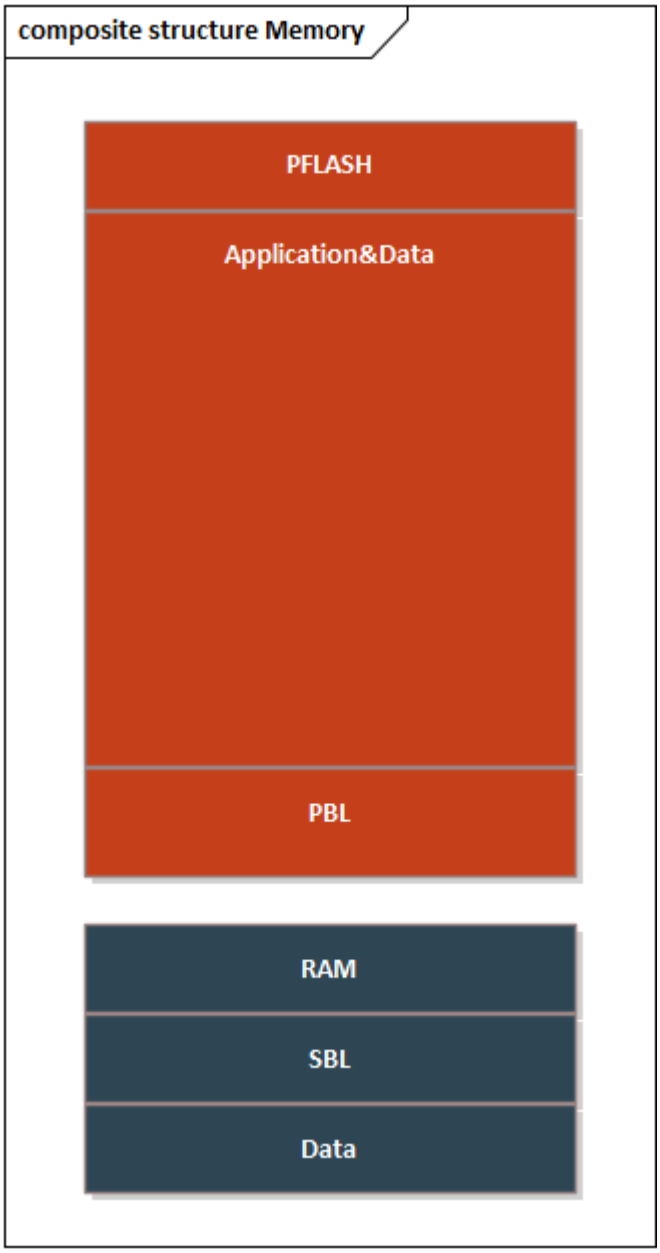
- Dcm

  The Dcm module realizes the diagnostic function based on the support of the communication module, meeting the definitions of ISO 14229 and ISO 15765 standards.

- Crypto, HSM

  The Ethernet OTA supports the adaptation of the Muniu Crypto Library functions. It combines asymmetric encryption algorithms with other encryption algorithms to achieve the secure flashing function. It adapts to the certificate authentication function to meet the security diagnostic requirements and adapts to the HSM to improve the stability and verification speed of the Cybersecurity function.

5.3 内存结构 Memory Structure



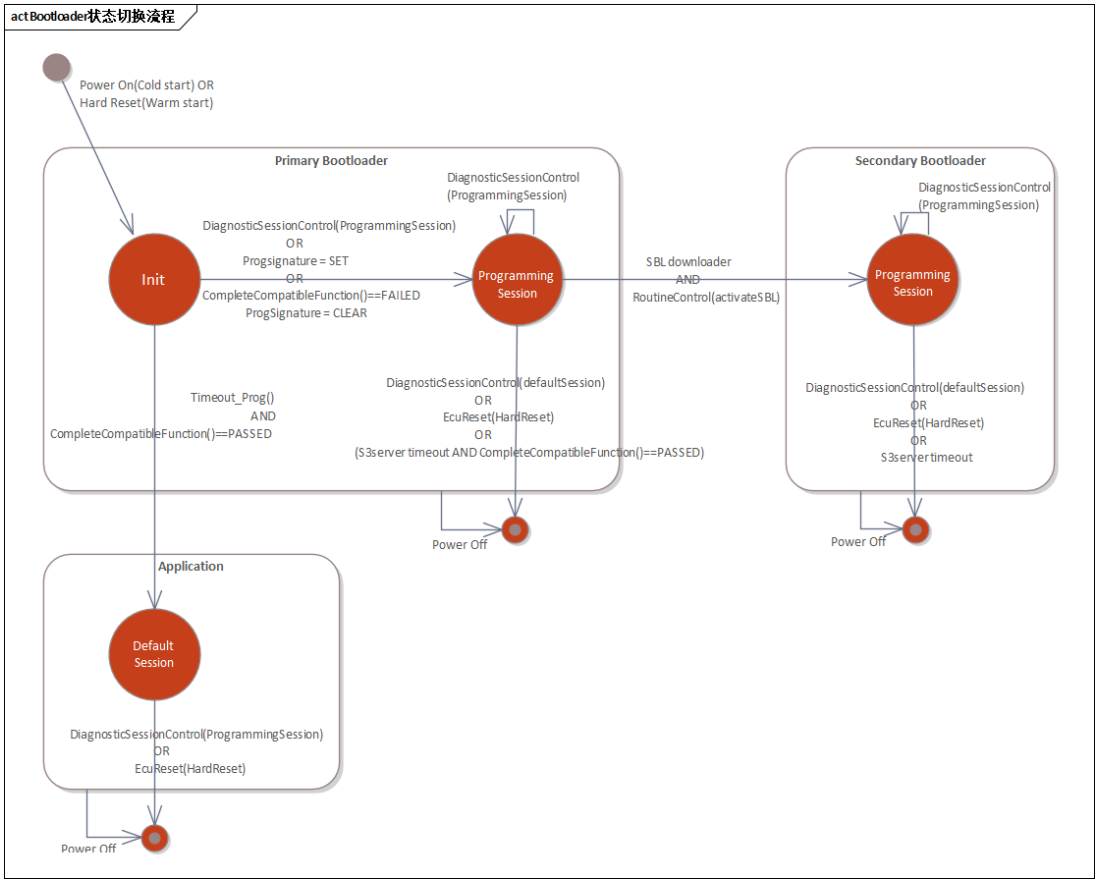
ECU 的内存分为 PFLASH 和 RAM，PFLASH 区分为 Application&Data 和 BootLoader 区，RAM 区分为 SBL 和 Data。

The memory of the Electronic Control Unit (ECU) is divided into PFLASH and RAM. The PFLASH is segmented into the Application & Data area and the BootLoader area, while the RAM is segmented into the SBL (Secondary BootLoader) and Data area.。

5.4 支持 GEEA2.0 规范 Supports GEEA2.0 Specification

知从青龙 BootLoader 支持 GEEA2.0 规范的 BootLoader 状态切换流程，下图为 BootLoader 在不同状态切换的简化示例图:

ZC.QingLong BootLoader supports the BootLoader state transition process as specified in the GEEA2.0 standard. Below is a simplified illustration of the BootLoader state transitions:



当 Application 执行上电启动或执行复位启动时，PBL 应开始执行初始化状态，其中 PBL 决定是否应启动 Application。

When the Application performs a power-on start or executes a reset start, the Primary BootLoader (PBL) should begin executing in the initialization state, where the PBL determines whether the Application should be launched.

如果 ECU 认为其存在有效 Application，PBL 将启动 Application。

If the ECU deems that it has a valid Application, the PBL will launch the Application.

如果 Application 接收到诊断请求 DiagnosticSessionControl，将通过执行 Reset 跳转 PBL。

If the Application receives a diagnostic request DiagnosticSessionControl, it will transition back to the PBL by executing a Reset.。

如果 Reset 是由应用程序中的诊断请求 DiagnosticSessionControl（programmingSession）Warm start 启动的，或者如果没有出现有效 Application，则进入 programmingSession 状态。

If a Reset is initiated by the diagnostic request DiagnosticSessionControl (programmingSession) Warm start from within the Application, or if no valid Application is present, the system enters the programmingSession state.。

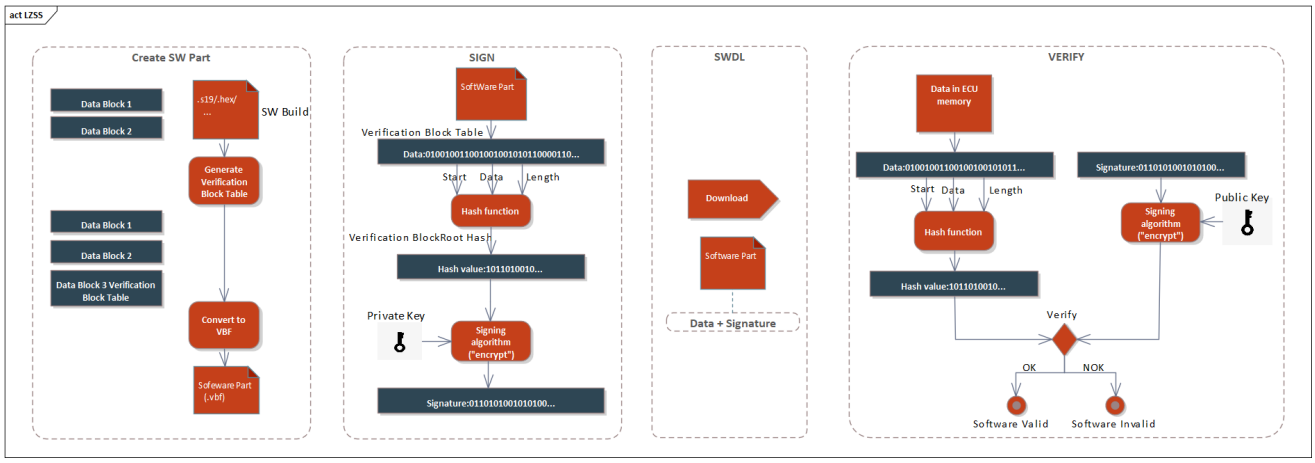
如果启动类型是 Cold start 且存在有效 Application，则 Application 启动.

If the startup type is Cold start and a valid Application exists, then the Application will launch.

知从青龙 BootLoader 支持 GEEA2.0 规范的 BootLoader 刷写需求，以下为部分已实现的 GEEA2.0 规范的需求功能：

ZC.Qinglong BootLoader supports the bootloader flashing requirements of the GEEA 2.0 specification, and the following are some of the implemented GEEA 2.0 specification requirements:

- 安全刷写 Secure Flashing：



知从青龙 BootLoader 根据存储在非易失性存储器的 Root Public Key，通过非对称加密算法 RSA，对数据的真实性校验。若校验成功则通过对称加密算法 SHA256 和非对称算法 RSA2048 对数据完整性进行校验，保证安全刷写流程。

ZC.QingLong BootLoader performs authenticity verification of data using the Root Public Key stored in non-volatile memory, through the asymmetric encryption algorithm RSA. If the verification is successful, it then uses the symmetric encryption algorithm SHA256 and the asymmetric algorithm RSA2048 to verify the integrity of the data, ensuring a secure flashing process.。

- 压缩算法 Compression Algorithm：

知从青龙 BootLoader 支持解析 LZSS 压缩算法对数据的压缩及对应数据结构的封装数据，同时支持非压缩数据的刷写。

ZC.QingLong BootLoader supports parsing data compressed with the LZSS compression algorithm and encapsulating the corresponding data structures. It also supports the flashing of uncompressed data.

- 主从 BootLoader Master-Slav Bootloader ：

知从青龙 BootLoader 支持主从刷写功能。BootLoader 在主节点上通过 UART 将上位机传输的 Application 数据转发给从节点上的 BootLoader，并通过从 BootLoader 完成从节点上 Application 的更新。

ZC.QingLong BootLoader supports master-slave flashing functionality. The BootLoader on the master node forwards the Application data transmitted by the host computer to the BootLoader on the slave node via UART, and the update of the Application on the slave node is completed through the slave BootLoader.

- 支持 VBF 文件下载 Supports VBF File Download：

通过搭配知从玄武程序更新工具，知从青龙 BootLoader 可以解析 VBF 文件数据，将数据下载到 ECU 中，并按照 GEEA2.0 规范使用 VBF 中携带的 Verification Block 和 Signature 数据对完整性和可靠性进行校验。

By integrating with the ZC.XuanWu program update tool, ZC.QingLong BootLoader can parse the data within VBF files, download the data into the ECU, and verify the integrity and reliability using the Verification Block and Signature data carried within the VBF, in accordance with the GEEA2.0 specification. This ensures that the update process is secure and the data has not been tampered with or corrupted during transmission.

6 过程文档 PROCESS DOCUMENTATION

开发流程 Development Process	文档描述 Document Description
需求收集 Requirement Collection	顾客的需求文档 Customer Requirements Document
软件需求分析 Software Requirement Analysis	需求分析 Requirement Analysis
	需求分析规格书 Requirements Analysis Specification Document
	软件需求追踪表 Software Requirements Traceability Matrix
	客户的问题沟通表 Customer Issue Communication Form
软件架构设计 Software Architecture Design	软件架构说明书 Software Architecture Specification Document
	软件架构的追踪表 Software Architecture Traceability Matrix
软件详细设计和单元设计 Software Detailed Design and Unit Design	BootLoader 详细设计说明书 BootLoaderDetailed Design Specification Document
	配置工具设计 Configuration Tool Design
	软件详细设计追踪表 Software Detailed Design Traceability Matrix
	BootLoader 详细设计评审 BootLoaderDetailed Design Review
软件单元测试 Software Unit Testing	QAC 分析报告 QACAnalysis Report
	Tessy 测试报告 TessyTest Report
	软件单元验证策略 Software Unit Verification Strategy
	集成策略

开发流程 Development Process	文档描述 Document Description
软件集成和集成测试 **Software Integration and Integration Testing**	Integration Strategy
	集成手册 Integration Manual
	集成测试策略 Integration Testing Strategy
	集成测试报告 Integration Test Report
	资源分析报告 Resource Analysis Report
软件认可测试 **Software Acceptance Testing**	BootLoader 软件测试报告 BootLoader Software Test Report
	BootLoader 软件测试报告评审 BootLoaderSoftware Test Report Review
发布 **Release**	发布文档 Release Documentation

7 证书 CERTIFICATES

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3073051号

软件名称：知从青龙bootloader软件
[简称：青龙]
V1.0

著作权人：上海知从科技有限公司

开发完成日期：2018年01月04日

首次发表日期：2018年01月10日

权利取得方式：原始取得

权利范围：全部权利

登记号：2018SR743956

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
2018年09月13日

No. 02965607

青龙软件著作权登记证书
QINGLONG SOFTWARE COPYRIGHT REGISTRATION CERTIFICATE

中国软件产品评估 CSPE CSIA CHINA SOFTWARE PRODUCTS EVALUATION

软件产品证书

经评估，知从青龙bootloader软件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《软件产品评估标准》（T/SIA003 2017）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：沪RC-2019-3315
证书编号：嵌入式应用软件
有 效 期：五年

评估机构：上海市软件行业协会
日期：二〇一九 年 九 月 廿五 日

上海市软件行业协会 软件产品评估证书专用章

青龙软件产品登记证书
QINGLONG SOFTWARE COPYRIGHT REGISTRATION CERTIFICATE