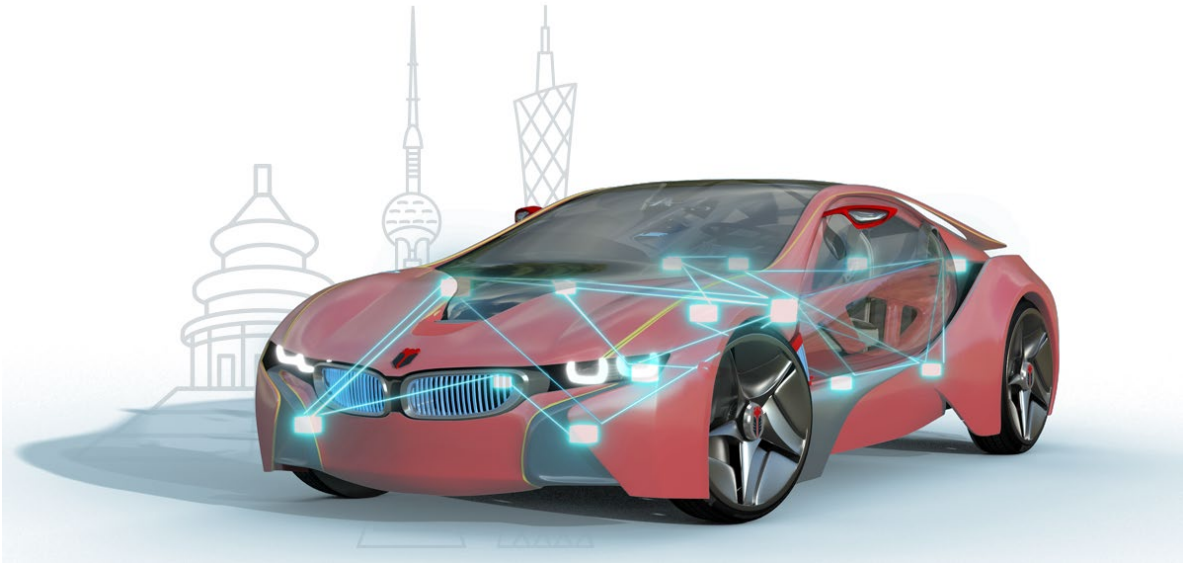
知从木牛 SBC 英飞凌 TLF35584 产品手册

ZC.MUNIU SBC PRODUCT MANUAL BASED ON INFINEON TLF35584

知从木牛基础软件平台功能安全库

ZC.MuNiu Basic Software Platform Safety Library



知从木牛 SBC 英飞凌 TLF35584 产品手册

ZC.MUNIU SBC PRODUCT MANUAL BASED ON INFINEON TLF35584

知从木牛基础软件平台功能安全库

ZC.MuNiu Basic Software Platform Safety Library

1 功能概述 FUNCTIONAL OVERVIEW

知从木牛功能安全 SBC 系列软件旨在打造知从科技自主研发的满足客户功能安全要求的 System Basis Chip（SBC）平台化软件产品。本手册说明了基于英飞凌 TLF35584 实现的功能安全应用方案、符合标准、软件架构、编程思路及配置工具等内容，推出可配置的 TLF35584Lib 软件库产品。

The ZC.MuNiu Functional Safety SBC series software aims to develop a platform-based System Basis Chip (SBC) software product that meets customer functional safety requirements, independently developed by ZC. This manual describes the functional safety application solutions based on Infineon TLF35584, including compliance with standards, software architecture, programming concepts, and configuration tools, and introduces the configurable TLF35584Lib software library product.

本产品实现了 SBC 端芯片 TLF35584（MCU 端芯片以 AURIX TC275 为例）的功能包含：

The product implements the functions of the SBC end chip TLF35584 (with AURIX TC275 as an example of the MCU end chip), including:

- SBC 与 MCU 通信 SPI 接口配置；
  Configuration of the SPI interface for communication between the SBC and MCU;
- 多路电源输出管理；
  Management of multiple power supply outputs;
- SBC 状态机控制与 MCU 上下电管理；
  Control of the SBC state machine and power management for MCU power on/off;
- SBC 片内 ABIST/LBIST 自检等完整诊断策略；
  Complete diagnostic strategies such as on-chip ABIST/LBIST self - test of the SBC;
- 看门狗管理与程序流监控 PFM（E-GAS L3 层）；
  Watchdog management and program flow monitoring PFM (E - GAS L3 layer);

- ERR PIN 监控的 FSP 开发（结合知从 Safety library 系列产品）；
  FSP development for ERR PIN monitoring (in combination with ZC Safety library series products);
- SBC 片外安全关断路径及进入 Safe State 的外设驱动。
  External safety shutdown path and peripheral driver for entering Safe State of the SBC.

知从科技已适配开发的英飞凌 TLF35584 系列全部型号：
ZC has developed and adapted all models of the Infineon TLF35584 series.

Type	Package	Marking
TLF35584QVVS1 (5.0 V Variant)	PG-VQFN-48	TLF35584 / VS1
TLF35584QVVS2 (3.3 V Variant)	PG-VQFN-48	TLF35584 / VS2
TLF35584QKVS1 (5.0 V Variant)	PG-LQFP-64	TLF35584 / QK VS1
TLF35584QKVS2 (3.3 V Variant)	PG-LQFP-64	TLF35584 / QK VS2

2 应用领域 APPLICATION FIELD

知从木牛功能安全 SBC 英飞凌 TLF35584 产品可应用于有各功能安全等级需求的汽车控制器。例如：

The ZC.MuNiu Functional Safety SBC Infineon TLF35584 product can be applied to automotive controllers with various functional safety requirements. Examples include:

- 智能驾驶控制器 Advanced Driver Assistance Systems (ADAS)
- 智能网关控制器 Intelligent Gateway Controller (Gateway)
- 智能刹车系统 Intelligent Brake System (iBooster)
- 车身稳定控制 Electronic Stability Control (ESC/Onebox)
- 电动助力转向 Electric Power Steering (EPS)
- 电子驻车系统 Electronic Parking Brake (EPB)
- 电池管理系统 Battery Management System (BMS)
- 车身控制器 Body Control Module (BCM)
- 发动机管理系统 Engine Management System (EMS)
- 底盘域线控系统相关应用 Applications related to chassis-by-wire systems

本安全手册是为有经验的硬件、软件和功能安全工程师编写的，根据 ISO 26262 设计，并参考安全相关系统的 E-GAS 三层架构理论，考虑将 TLF35584 集成到客户应用产品的(子)系统中。我们的软件集成工程师可支持和确保 TLF35584Lib 适合所选择的应用程序的集成服务，并符合适当的应用程序标准，协助实现达到 ISO26262 ASIL-D 的等级要求。

This safety manual is written for experienced hardware, software, and functional safety engineers. It is designed in accordance with ISO 26262 and references the E-GAS three-layer architecture theory for safety-related systems, considering the integration of TLF35584 into the (sub)systems of customer application products. Our software integration engineers can provide support and ensure that the TLF35584Lib is suitable for integration services for the selected applications, meeting the appropriate application standards and assisting in achieving the ISO 26262 ASIL-D level requirements.

3 配置环境 CONFIGURATION ENVIRONMENT

配置环境 Configuration Environment	
Hardware (Chip)	INFINEON SAK-TC275TP_64F200W CA
Compilers Supported	Tasking 4.2r2 or HighTec 4.6.6.1
Evaluation Hardware	TriBoard TC2X5+TLF35584Demo
Debugger	Lauterbach (Trace32 R.2018.02) or Isystem (IC5700)
Configuration Tools	Muniu_v5.1.3
Configuration Environment	Win7 64bit

编译器选项 Compiler Options	
Tasking 编译选项 Compiler Options	-Ctc27x --lsl-core=vtc --iso=99 --language=-gcc,-volatile,+strings --switch=auto --align=4 --no-clear --default-near-size=0 --default-a0-size=0 --default-a1-size=0 -O2 --tradeoff=4 --compact-max-size=200 -g --source
Tasking 链接选项 Linker Options	-Ctc27x --lsl-core=vtc -I"D:\Git\xxx" -Wl-o"${PROJ}.hex":IHEX:4 -Wl-o"${PROJ}.sre":SREC:4 --hex-format=s -Wl-DMCU_SMALL_ENDIAN=1 "../xxx_SW.lsl" -Wl-OtxyCL -Wl--map-file="${PROJ}.mapxml":XML -Wl-mcrfiklsmnoduq -Wl--error-limit=42 -g
HighTec 编译选项 Compiler Options	-I" D:\Git\xxx" -fno-common -Os -g3 -W -Wall -Wextra -Wdiv-by-zero -Warray-bounds -Wcast-align -Wignored-qualifiers -Wformat -Wformat-security -D_GNU_C_TRICORE_=1 -fshort-double -mcpu=tc27xx -mversion-info
HighTec 链接选项 Linker Options	-nocrt0 -T"..\Source\Application\src_mcal_pjt.ld" @iROM.objectlist -Wl,--gc-sections -mcpu=tc27xx -Wl,--mem-holes -Wl,--no-warn-flags -Wl,-Map="$(basename $(notdir $@)).map" -Wl,--cref -fshort-double " D:\Git\xxx \libSBST.a" -Wl,--extmap="a"

4 开发背景 DEVELOPMENT BACKGROUND

目前，汽车上的电子电气架构越来越复杂，对汽车电子的安全性要求也越来越高，为了满足汽车的安全性需求，汽车功能安全越来越受到重视。业界近年来，在功能安全标准上参考 ISO 26262；在软件架安全架构上参考 E-GAS 分层。英飞凌 TLF35584 适合所选应用，并符合此类应用标准，并在电子电气系统中，应用 SEooC(safety element out of context)进行设计开发。

Currently, the electronic and electrical architecture in vehicles is becoming increasingly complex, and the requirements for the safety of automotive electronics are also rising. To meet these safety requirements, automotive functional safety is gaining more and more attention. In recent years, the industry has referred to ISO 26262 for functional safety standards and to the E-GAS layering for software safety architecture. The Infineon TLF35584 is suitable for the selected applications, complies with the standards for such applications, and is designed and developed using SEooC (Safety Element out of Context) in the electronic and electrical systems.

由于SBC做为特定ASIL-x等级MCU的供电系统、时序监控系统，按照ISO 26262-5(2011) Clause 8 中介绍了 2 个度量：Single-point fault metric(单点故障度量)和 Latent-fault metric(潜伏故障度量)，不同的 ASIL 等级要求和故障失效分析方法均要求其达到单点故障度量和潜伏故障度量需要达到相应同等 ASIL-x 等级。

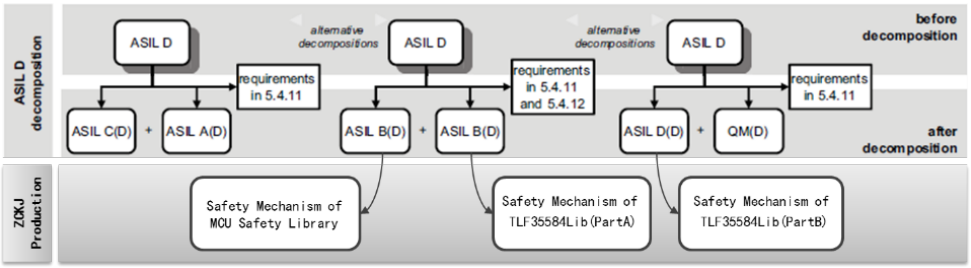
Since the SBC serves as the power supply system and timing monitoring system for specific ASIL-x grade MCUs, according to Clause 8 of ISO 26262-5 (2011), two metrics are introduced: the Single-point fault metric (single-point fault metric) and the Latent-fault metric (latent fault metric). Different ASIL grades and failure analysis methods require that these metrics achieve the corresponding ASIL-x grade for single-point and latent faults.

	ASIL B	ASIL C	ASIL D
Single-point fault metric	≥90 %	≥97 %	≥99 %

	ASIL B	ASIL C	ASIL D
Latent-fault metric	≥60 %	≥80 %	≥90 %

因此，在客户应用项目中若需符合 ASIL-D 安全等级，当前知从科技推荐方案分解到硬件和软件模块中：

Therefore, in customer application projects that need to comply with the ASIL-D safety grade, ZC currently recommends the following decomposition of the solution into hardware and software modules:



- **TLF35584Lib(PartA)**实现 MCU 端的 Safety Library 安全库 ASIL B(D)和 SBC 端的 TLF35584 ASIL B(D)两侧分解实施，需根据客户项目应用做配置。如，看门狗 FWD/WWD 监控、片外安全关断路径 SS1/SS2 等；

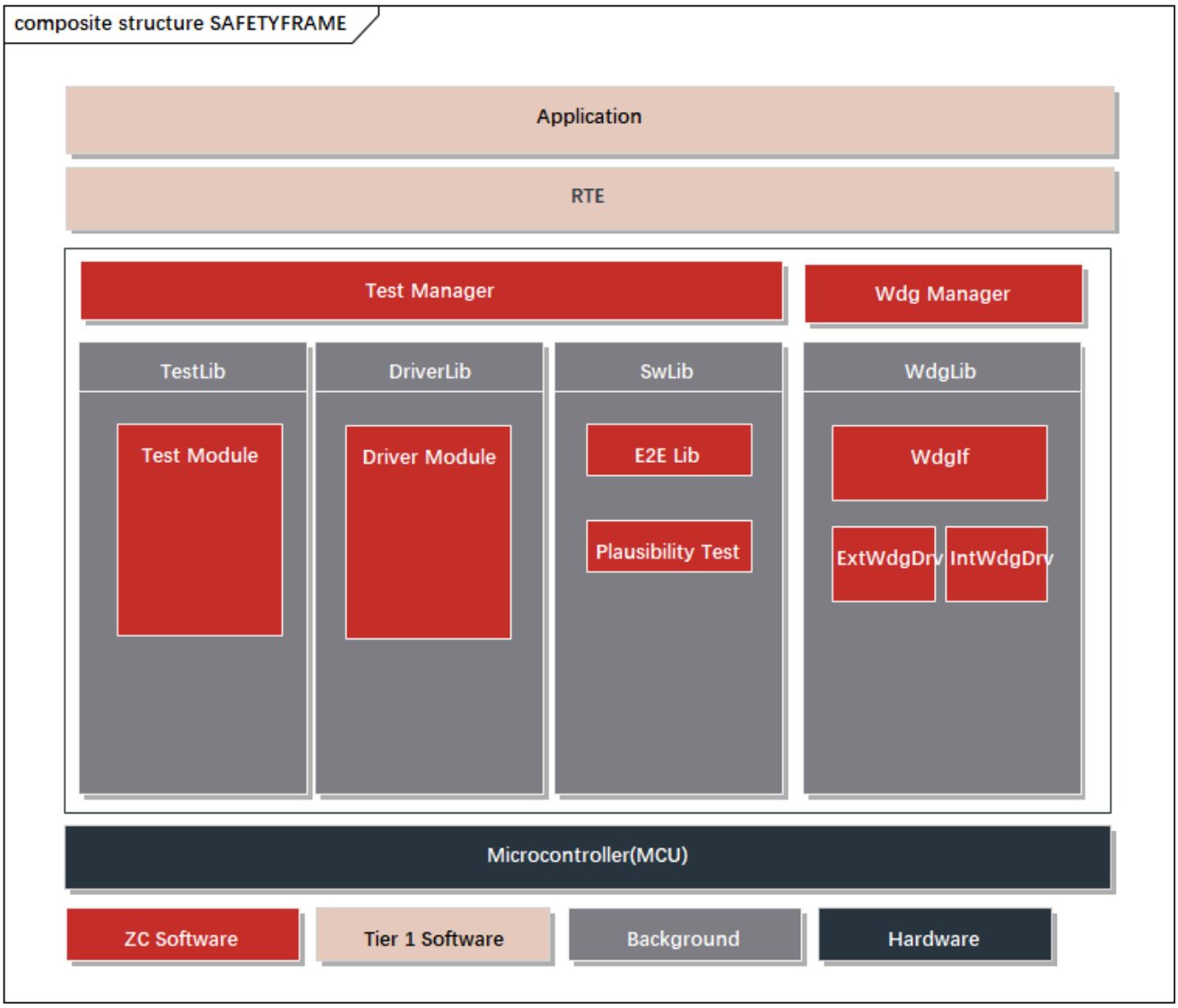
  TLF35584Lib (Part A) implements the Safety Library for the MCU side at ASIL B(D) and the TLF35584 for the SBC side at ASIL B(D). This requires configuration according to the customer's project requirements. For example, watchdog FWD/WWD monitoring and external safety shutdown paths SS1/SS2, etc.

- **TLF35584Lib(PartB)**对于单点失效 ASIL D 要求的部分安全机制则按照英飞凌提供的 Safety Manual 手册诊断覆盖开发，是根据 Safety Manual 开发的标准库。如，SBC 片内 ABIST/LBIST 自检功能、各路电源输出的对电源（或对 GND）短接自检功能等。

  TLF35584Lib (Part B) develops the standard library based on the Safety Manual provided by Infineon for the safety mechanisms required to meet the single-point failure ASIL D requirements. This includes functions such as the on-chip ABIST/LBIST self - test of the SBC and the short - circuit self - test function of each power supply output to the power supply (or to GND).

5 功能描述 FUNCTIONAL DESCRIPTION

5.1 产品特点 Product Features



- 可作为复杂驱动集成到 AUTOSAR 中

  Can be integrated as a complex driver into AUTOSAR .

- 可集成到非 AUTOSAR 软件架构中，灵活适配

  Can be integrated into non-AUTOSAR software architectures.

- 支持多核测试及应用

  Support multi-core testing and applications.

- Safety Library 具有内部程序流监控

  Safety Frame has internal program flow monitoring.

- 高安全性：支持多核自检测试，搭配知从科技 TLF35584Lib 可实现高达 ASIL-D 需求

High security: Supports multi-core self-testing, and can achieve up to ASIL-D requirements when paired with ZC 's TLF35584Lib.

- 高扩展性：各模块可配置满足不同客户的应用需求

  High scalability: Each module can be configured to meet the application requirements of different customers.

5.1.1 看门狗机制/ WATCHDOG MECHANISM

知从科技 TLF35584Lib 提供两种看门狗配置机制：

ZC's TLF35584Lib provides two watchdog configuration mechanisms:

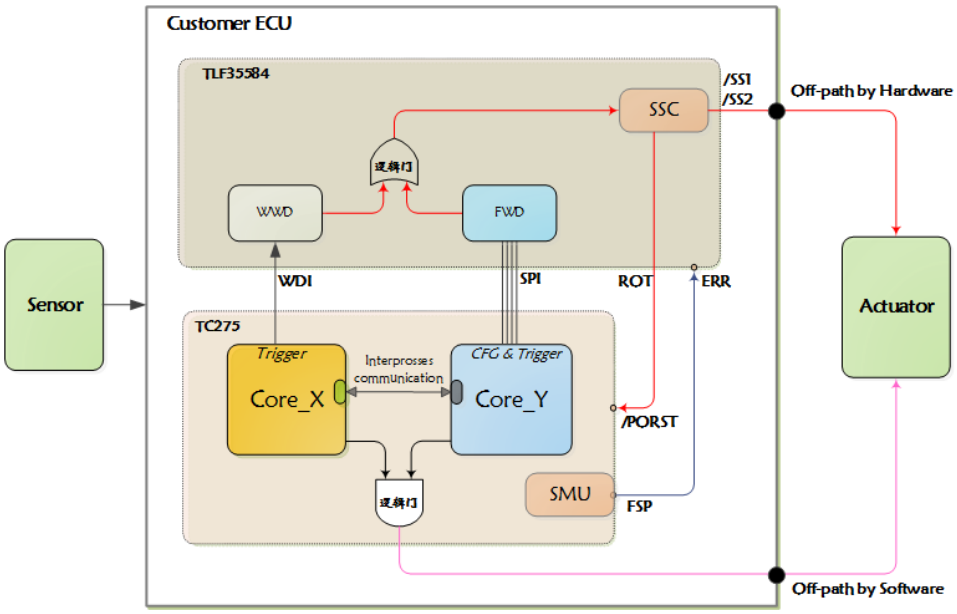
- **外部问答狗**：由 TLF35584 Functional-Watchdog 做为 External Watchdog 执行监控 MCU 主控芯片程序运行的 Logic Supervision 和 Temporal Supervision.

  External Functional Watchdog: The TLF35584 Functional-Watchdog acts as an External Watchdog to perform Logic Supervision and Temporal Supervision of the main MCU's program execution.

- **内部安全狗搭配外部窗口狗**：由 MCU 主控芯片的 Internal Safety WDTs 执行程序运行的 Logic Supervision，同时由 External TLF35584 Window-Watchdog 覆盖程序运行的 Temporal Supervision.

  Internal Safety Watchdog with External Window Watchdog: The main MCU's Internal Safety WDTs perform Logic Supervision of the program execution, while the External TLF35584 Window-Watchdog covers Temporal Supervision of the program execution.

5.1.2 OFF-PATH 安全机制/ OFF-PATH SAFETY MECHANISM



对于国内客户采用的 AUTOSAR OS 未符合 SC3/SC4 要求的操作系统应用，或者前后台多核独立运行的中断系统，知从科技提供可利用 TLF35584Lib 软件库调用和驱动安全状态控制模块(Safe State Control)覆盖从“多核时序监控”到外设执行器的两种方式的“关闭路径驱动”的技术方案，大大增强了控制器系统的安全性。

For domestic customers using AUTOSAR OS that does not meet SC3/SC4 requirements or applications with interrupt systems running independently on multiple cores in a foreground-background manner, ZC provides a technical solution that utilizes the TLF35584Lib software library to call and drive the Safe State Control module. This solution covers the "shutdown path drive" from "multi-core timing monitoring" to peripheral actuators in two ways, significantly enhancing the safety of the controller system.

5.1.3 参考 E-GAS 架构开发/ DEVELOPMENT BASED ON E-GAS ARCHITECTURE

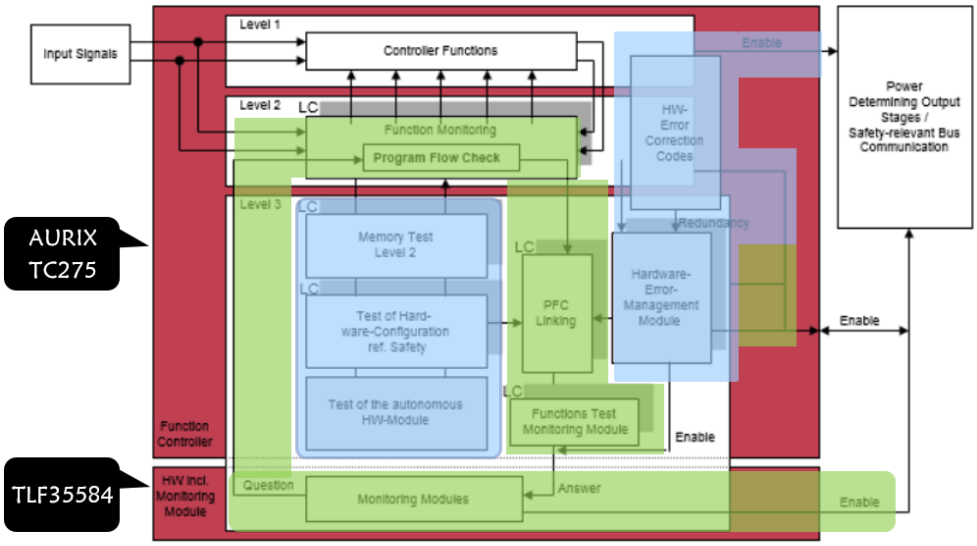


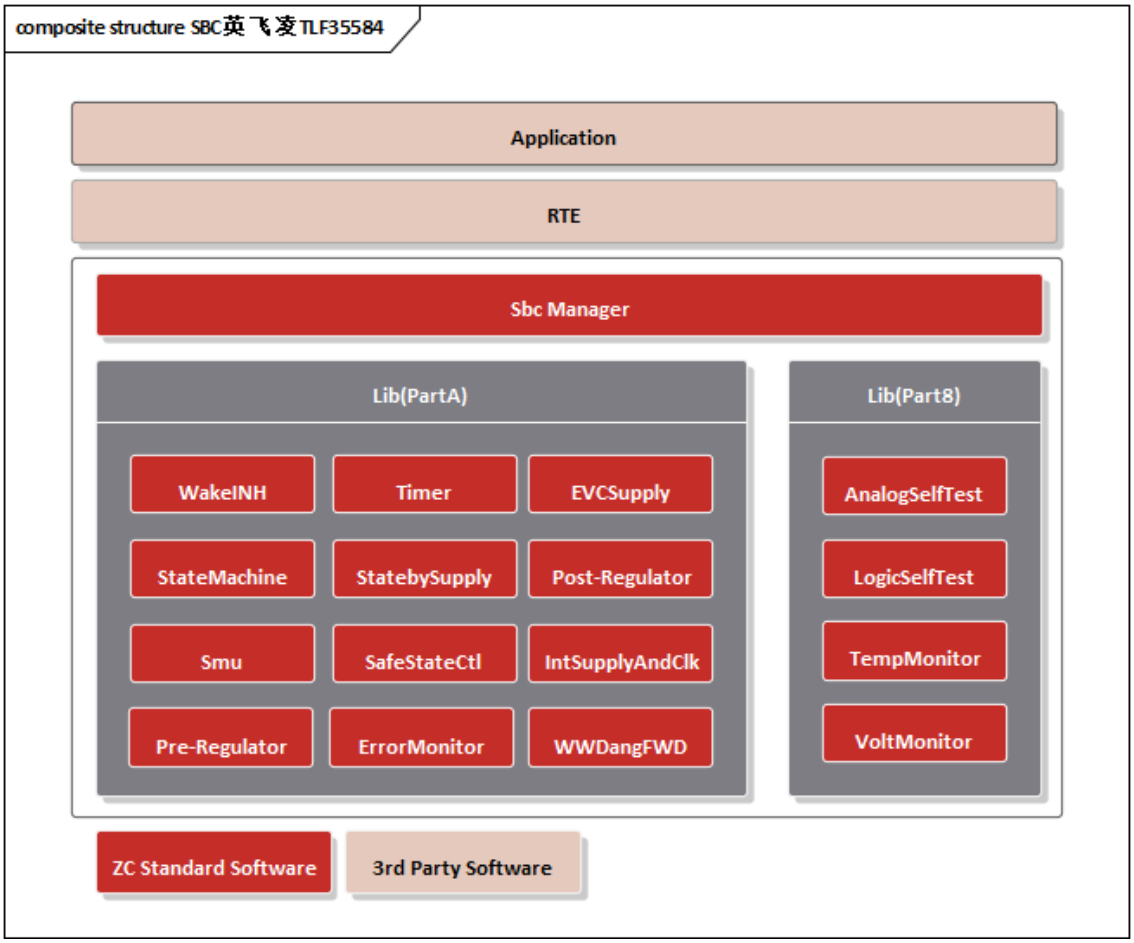
Fig 4 System overview; 3 level concept of the engine controller with lockstep-core (LC)

安全机制覆盖： 知从科技Safety library软件库 知从科技TLF35584Lib软件库

知从科技的 TLF35584Lib 开发流程中，充分参考业界普遍参考的 E-GAS(v6.0)三层架构的需求，支持客户目标项目应用层开发对基础软件库的软件分层与安全等级的模块化分区等要求。

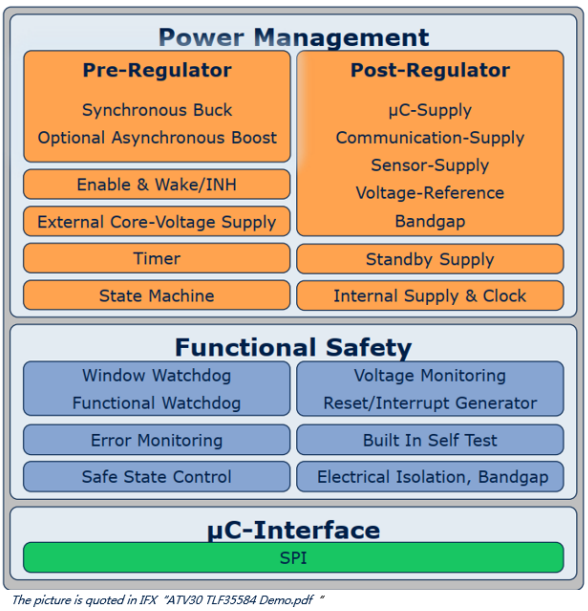
In the development process of ZC's TLF35584Lib, the requirements of the widely referenced E-GAS (v6.0) three-layer architecture in the industry have been fully considered. It supports the customer's target project application layer development requirements for software layering of the basic software library and modular zoning of safety levels.

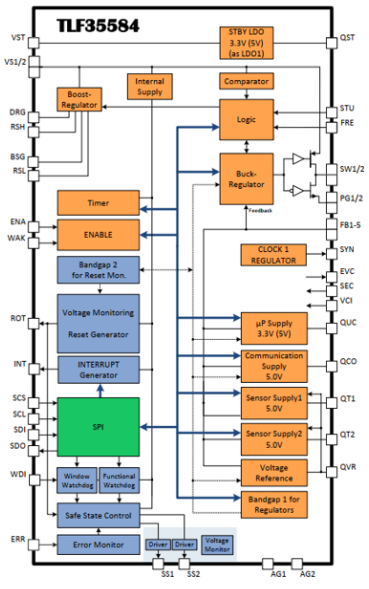
5.2 软件架构 Software Architecture



知从科技遵守英飞凌手册各模块要求全覆盖 TLF35584Lib 开发。

ZC complies with the requirements of all modules in the Infineon manual to achieve full coverage in the development of TLF35584Lib.





The picture is quoted in IFX "ATV30 TLF35584 Demo.pdf "

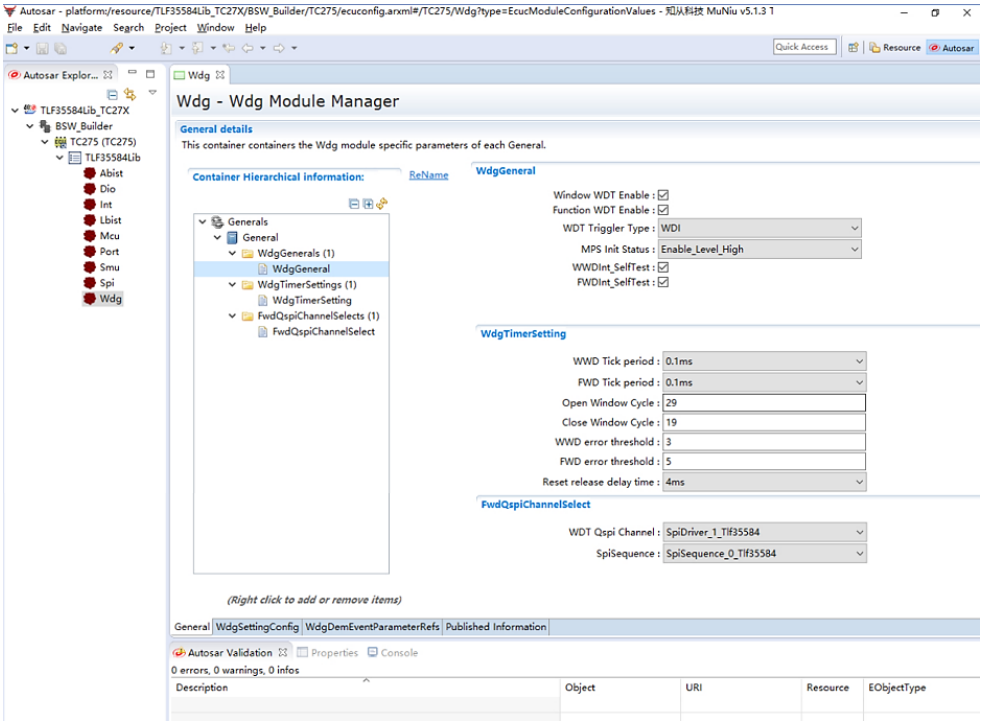
模块 Module	子模块 Submodule	描述 Description
TLF35584 Lib(PartA) 软件库	Wake/INH	实现Enable&Wake/INH的功能配置，根据边沿或电平方式唤醒。 Implementation of the Enable & Wake/INH function configuration, enabling wake-up based on edge or level triggering.
	Timer	实现SBC内部的定时计数、响应处理的延时等时间基准功能。 Implementation of internal timing and counting within the SBC, as well as delay functions for response handling and other time - based functionalities.
	EVCSupply	实现External Core-Voltage Supply选配输出外部核供电功能。 Implementation of the optional External Core - Voltage Supply output function for external core power supply.
	StateMachine	实现SBC工作状态机控制，根据Qspi帧命令的功耗管理与电源输出功能。 Implementation of SBC state machine control for power management and power output functions based on Qspi frame commands.
	StandbySupply	实现稳压器LDO_STBY为待机电源提供精确的3.3 V（或5.0V） VLDO_µC输出电压（可选配）功能。 Implementation of the regulator LDO_STBY to provide an accurate 3.3 V (or 5.0 V) VLDO_µC output voltage for standby power (optional).
	Pre-Regulator	实现前置稳压器的配置与检测功能；如，同步降压Buck/可选异步升压Boost的灵活模式配置。 Implementation of configuration and detection functions for the front - end regulator, such as flexible mode configuration for synchronous buck

		and optional asynchronous boost.
	Post-Regulator	实现后置稳压器的配置功能；如，µC-Supply/Communication-Supply/Sensor-Supply/Voltage-Reference/Bandgap等输出控制。Implementation of configuration functions for the back - end regulator, such as output control for µC - Supply, Communication - Supply, Sensor - Supply, Voltage - Reference, and Bandgap.
	Smu	实现MCU端的Safety management unit (SMU).功能配置与安全机制的7个Alarm group相关的FSP功能配置（该功能也可在知从科技软件库Safety Library中实现）。Implementation of the Safety management unit (SMU) function configuration at the MCU end and FSP function configuration related to the 7 Alarm groups of the safety mechanism (this function can also be implemented in the ZC Safety Library).
	SafeStateCtl	实现SBC安全状态控制模块（SSC）的配置检测功能，可实现Off-Path实时关断外设SS1&SS2并触发ROT等。Implementation of configuration and detection functions for the SBC Safety State Control module (SSC), capable of real - time shutdown of peripherals SS1 & SS2 via Off - Path and triggering ROT, etc.
	IntSupplyAndClk	实现针对内部不同Bandgap之间的间隔超过预定义的警告级别的监控，设备异常时将生成INT信号作为适当的设备操作可能会受到威胁，并可能随后触发输出电压监控功能。Implementation of monitoring for intervals between different internal Bandgaps exceeding predefined warning levels, with the generation of an INT signal during device anomalies to indicate potential

		threats to proper device operation and subsequent triggering of output voltage monitoring functions.
TLF35584 Lib(PartB) 软件库	ErrMonitor	提供了通过ERR引脚监视微处理器安全管理单元（SMU）的功能，当MCU端外发频率或电平异常时，按初始化配置的既定安全机制进入安全状态。 Provision of the function to monitor the microprocessor Safety Management Unit (SMU) via the ERR pin, entering a safe state according to the predefined safety mechanism in the initial configuration when the frequency or level emitted from the MCU end is abnormal.
	WWDandFWD	实现 Window Watchdog Functional Watchdog 配置初始化、程序流监控等功能。 Implementation of Window Watchdog and Functional Watchdog for configuration initialization and program flow monitoring functions.
	AnalogSelfTest	实现检测项包括：第二安全关断路径的激活；测试中断事件产生；测试比较器逻辑部分、一致性逻辑，Qspi通讯诊断等。 Implementation of detection items including activation of the second safety shutdown path, generation of test interrupt events, testing of comparator logic sections, consistency logic, and Qspi communication diagnostics.
	LogicSelfTest	实现检测项包括：分别针对WWD和FWD的有效性初始检测，并由其触发的INT、ROT及SSC链路有效性测试等。 Implementation of detection items including initial validity tests for WWD and FWD, and validity tests for INT, ROT, and SSC link triggered thereby.
	TempMonitor	实现SBC过温监控的诊断功能。

		Implementation of diagnostic functions for SBC over - temperature monitoring.
	VoltMonitor	实现SBC各输入输出稳压模块的过欠压、对电源/GND短路、过流等异常工况的诊断覆盖检测。 Implementation of diagnostic coverage detection for abnormal conditions such as over - voltage, under - voltage, short - circuit to power/GND, and over - current in the input and output regulator modules of the SBC.

5.3 配置工具 Configuration Tool



知从科技平台化基础软件配置工具 Muniu_v5.1.3 版本可支持 TLF35584Lib 软件库的配置，以满足不同客户的产品应用需求，并且可与知从科技 Safety Library 软件库的各个模块良好兼容性，自动生成 C 语言代码进行软件集成，增强客户对软件的灵活变更需要。

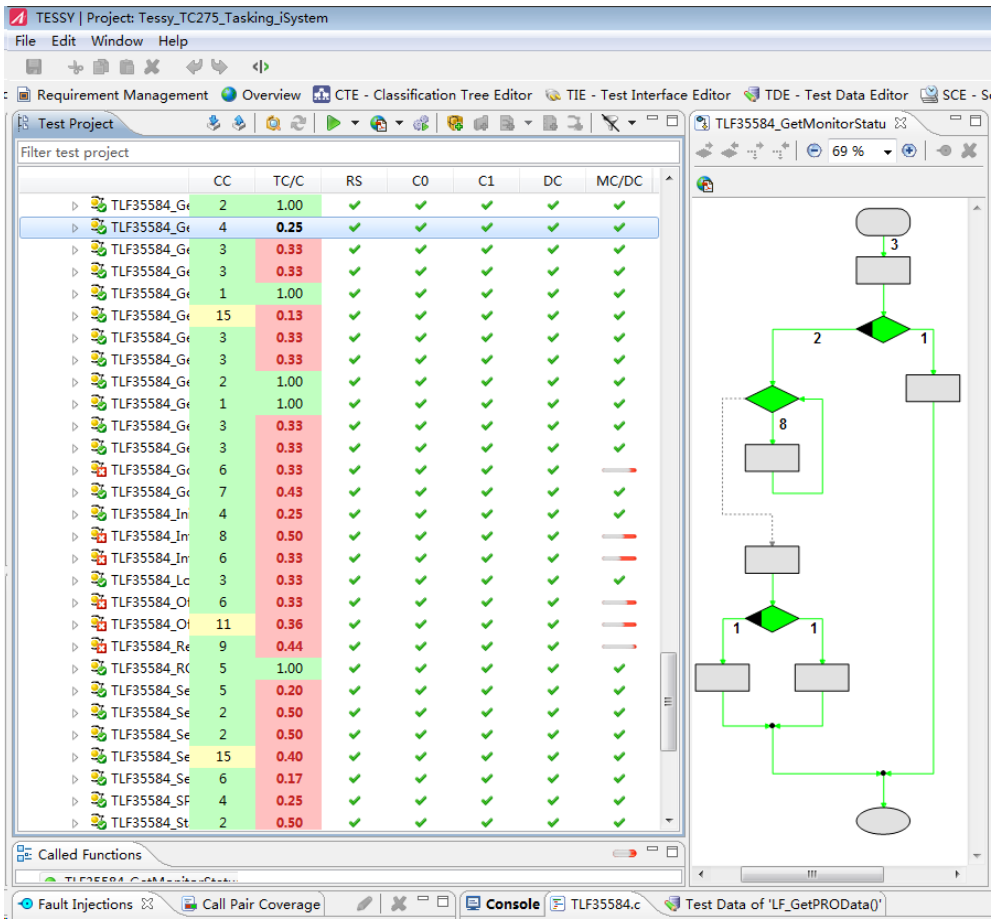
The ZC platform-based basic software configuration tool Muniu_v5.1.3 supports the configuration of the TLF35584Lib software library to meet the application requirements of different customer products. It is also fully compatible with various modules of the ZC Safety Library software library. The tool can automatically generate C language code for software integration, enhancing the flexibility for customers to modify the software.

因此，客户平台 ECU 产品的衍生车型项目开发时，不但可实现开发周期缩减，而且可以仅做极少的验证测试而获得最佳的高可靠性软件。

Therefore, when customers develop derivative vehicle projects for their ECU products, they can not only shorten the development cycle but also achieve highly reliable software with minimal validation and testing.

5.4 软件测试 Software Testing

测试环境 Testing Environment	
静态代码 QAC **Static Code QAC**	7.2 R MISRA-C：2004
动态 Tessy **Dynamic Tessy**	4.2.8
Evaluation Hardware	TriBoard TC2x5 V2.0 with Evaluation Board TLF35584
Configuration Environment	Win7 64bit



开发流程 Development Process	文档描述 Documentation Description
需求收集 Requirement Collection	客户需求文档 Customer Requirement Document
软件需求分析 Software Requirement Analysis	需求分析 Requirement Analysis
	需求分析规格书 Requirement Analysis Specification
	软件需求追踪表 Software Requirement Traceability Table
	客户问题沟通表 Customer Issue Communication Form
软件架构设计 Software Architecture Design	软件架构说明书 Software Architecture Description
	软件架构的追踪表 Software Architecture Traceability Table
软件详细设计和单元设计 Software Detailed Design and Unit Design	TLF35584Lib 详细设计说明书 TLF35584Lib Detailed Design Description
	MuNiu 配置工具设计 MuNiu Configuration Tool Design
	软件详细设计追踪表 Software Detailed Design Traceability Table
	TLF35584Lib 详细设计评审 TLF35584Lib Detailed Design Review
软件单元测试 Software Unit Testing	QAC 分析报告 QAC Analysis Report
	Tessy 测试报告 Tessy Test Report
	软件单元验证策略 Software Unit Verification Strategy
软件集成和集成测试	集成策略 Integration Strategy

开发流程 Development Process	文档描述 Documentation Description
Software Integration and Integration Testing	集成手册 Integration Manual
	集成测试策略 Integration Testing Strategy
	集成测试报告 Integration Testing Report
	资源分析报告 Resource Analysis Report
软件认可测试 **Software Acceptance Testing**	TLF35584Lib 软件测试报告 TLF35584Lib Software Test Report
	TLF35584Lib 软件测试报告评审 TLF35584Lib Software Test Report Review
发布 **Release**	发布文档 Release Documentation

7 功能安全 FUNCTIONAL SAFETY

7.1 功能安全评估报告 Functional Safety Assessment Report

7.2 功能安全证书 Functional Safety Certificate

To be continued.