知从木牛 SBC 英飞凌 TLF35584
产品手册

知从®木牛基础软件平台功能安全库

知从木牛 SBC 英飞凌 TLF35584

产品手册

知从®木牛基础软件平台功能安全库

1 功能概述

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。

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：

- SBC 与 MCU 通信 SPI 接口配置；
- 多路电源输出管理；
- SBC 状态机控制与 MCU 上下电管理；
- SBC 片内 ABIST/LBIST 自检等完整诊断策略；
- 看门狗管理与程序流监控 PFM（E-GAS L3 层）；
- ERR PIN 监控的 FSP 开发（结合知从 Safety library 系列产品）；
- SBC 片外安全关断路径及进入 Safe State 的外设驱动。

知从科技已适配开发的英飞凌 TLF35584 系列全部型号：

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

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：

- 智能驾驶控制器(ADAS)
- 智能网关控制器(Gateway)
- 智能刹车系统(iBooster)
- 车身稳定控制(ESC/Onebox)
- 电动助力转向(EPS)
- 电子驻车系统(EPB)
- 电池管理系统(BMS)
- 车身控制器(BCM)
- 发动机管理系统(EMS)
- 底盘域线控系统相关应用

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。

3 配置环境

配置环境	
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	
Tasking 编译选项	-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	-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="${PROJ}.mapxml":XML -Wl-mcrfiklsmnoduq -Wl--error-limit=42 -g
HighTec 编译选项	-I" D:\Git\xxx" -fno-common -Os -g3 -W -Wall -Wextra -Wdiv-by-zero -Warray-bounds -Wcast-align -Wignored-qualifiers -Wformat -Wformat-security -D_GNU_C_TRICORE_=1 -fshort-double -mcpu=tc27xx -mversion-info
HighTec 链接选项	-nocrt0 -T"..\Source\Application\src_mcal_pjt.ld" @iROM.objectlist -Wl,--gc-sections -mcpu=tc27xx -Wl,--mem-holes -Wl,--no-warn-flags -Wl,-Map="$(basename $(notdir $@)).map" -Wl,--cref -fshort-double " D:\Git\xxx \libSBST.a" -Wl,--extmap="a"

4 开发背景

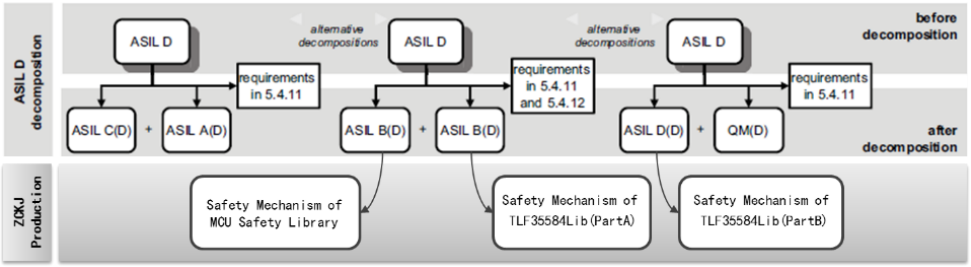
目前，汽车上的电子电气架构越来越复杂，对汽车电子的安全性要求也越来越高，为了满足汽车的安全性需求，汽车功能安全越来越受到重视。业界近年来，在功能安全标准上参考 ISO 26262；在软件架安全架构上参考 E-GAS 分层。英飞凌 TLF35584 适合所选应用，并符合此类应用标准，并在电子电气系统中，应用 SEooC(safety element out of context)进行设计开发。

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。

	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 %

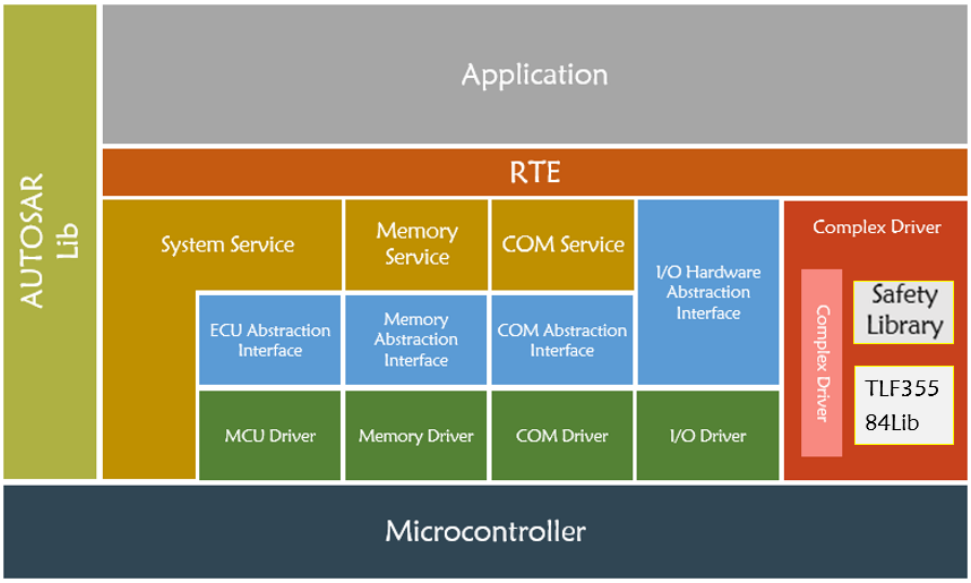
因此，在客户应用项目中若需符合 ASIL-D 安全等级，当前知从科技推荐方案分解到硬件和软件模块中：



- ✧ **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(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。

5 功能描述

5.1 产品特点



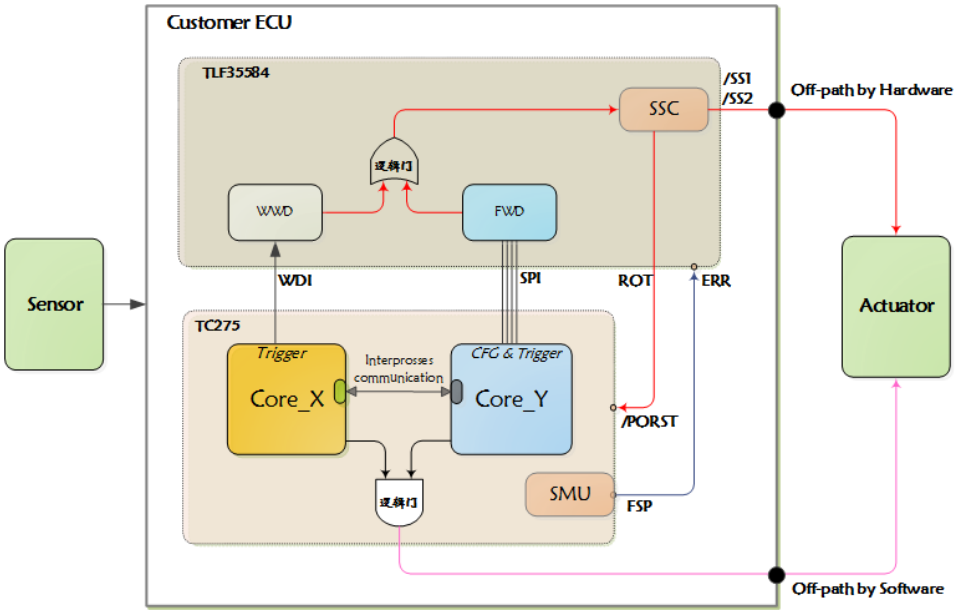
- 可作为复杂驱动集成到 AUTOSAR 中
- 可集成到非 AUTOSAR 软件架构中，灵活适配
- 高扩展性：各模块可配置满足不同客户的应用需求
- 高安全性：支持多核自检测试，搭配知从科技 Safety Library 可实现高达 ASIL-D 需求

5.1.1 看门狗机制

知从科技 TLF35584Lib 提供两种看门狗配置机制：

- **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.
- **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.

5.1.2 OFF-PATH 安全机制



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。

5.1.3 参考 E-GAS 架构开发

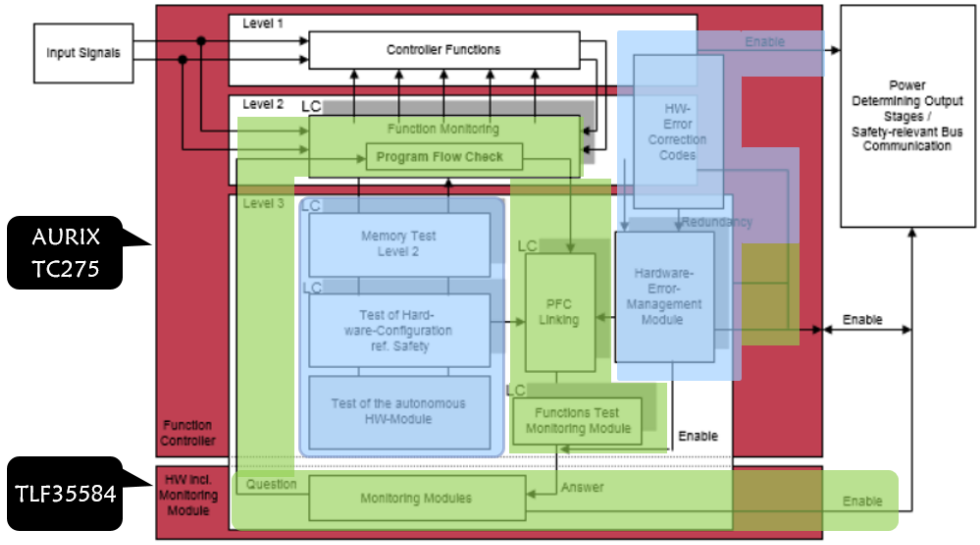
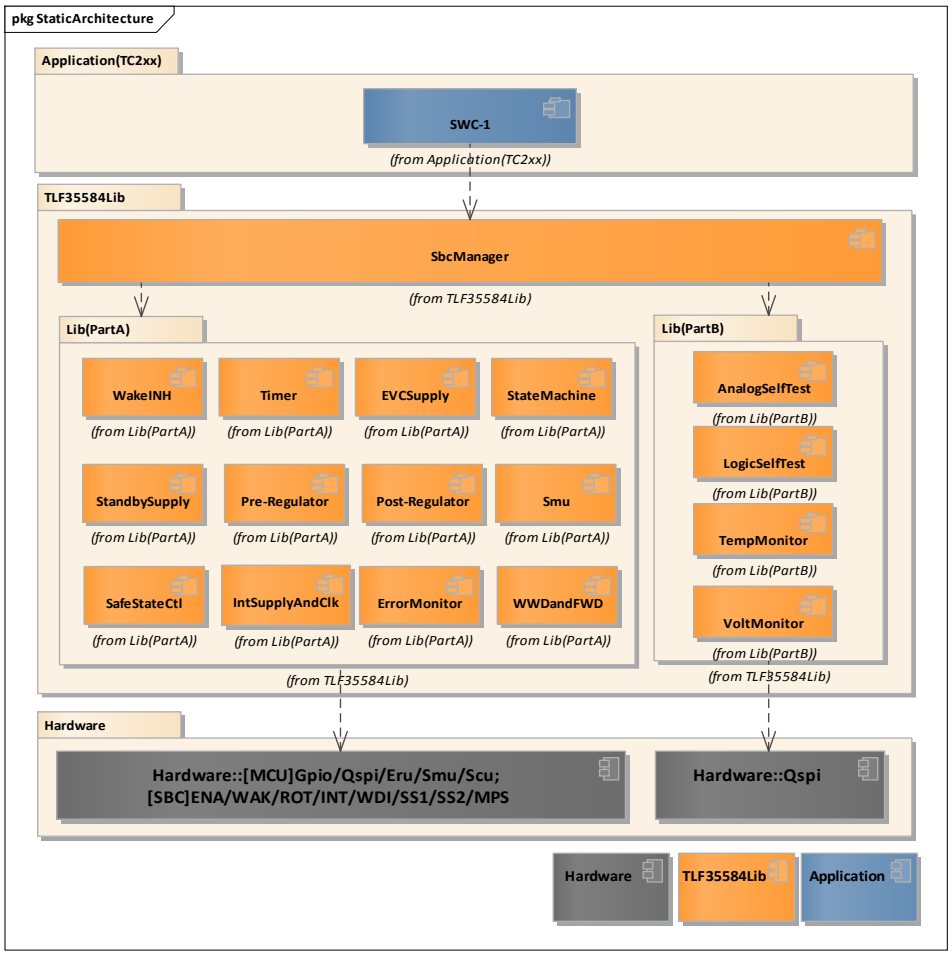


Fig 4 System overview; 3 level concept of the engine controller with lockstep-core (LC)

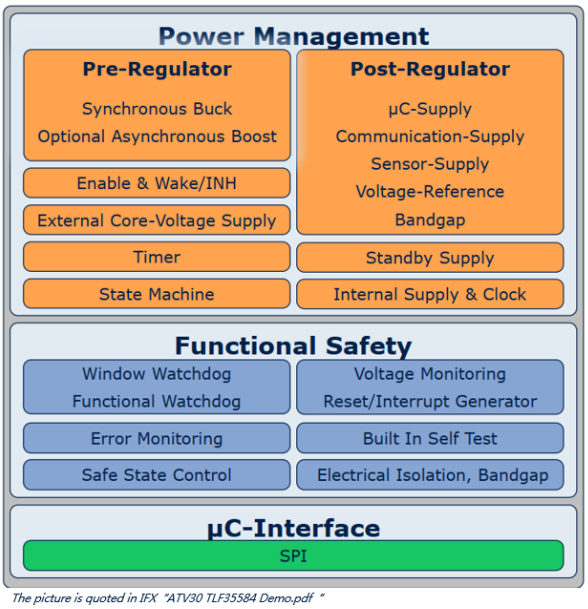
安全机制覆盖：知从科技Safety library软件库　知从科技TLF35584Lib软件库

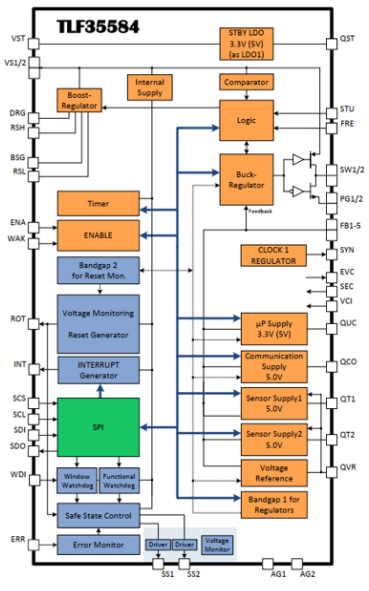
知从科技的 TLF35584Lib 开发流程中，充分参考业界普遍参考的 E-GAS(v6.0)三层架构的需求，支持客户目标项目应用层开发对基础软件库的软件分层与安全等级的模块化分区等要求。

5.2 软件架构



知从科技遵守英飞凌手册各模块要求全覆盖 TLF35584Lib 开发。

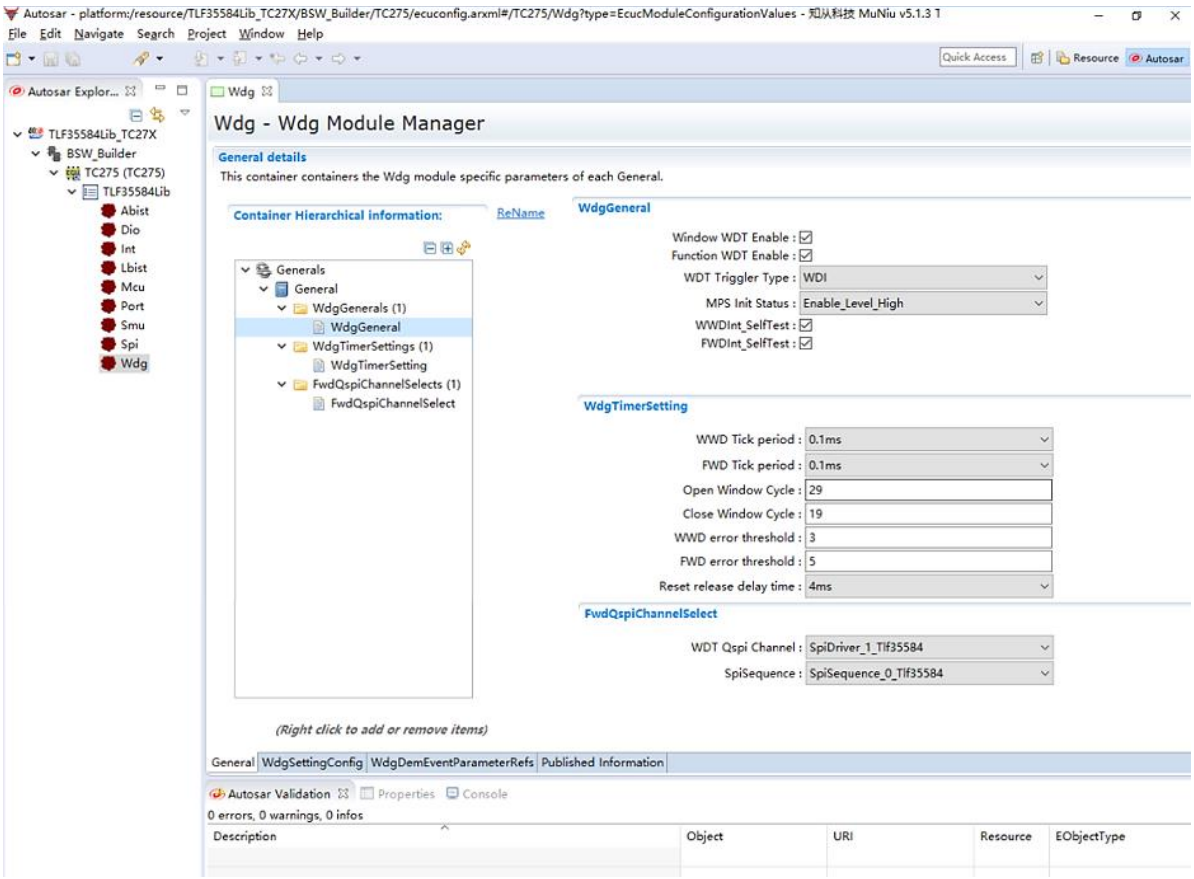




The picture is quoted in IFX "ATV30 TLF35584 Demo.pdf "

模块	子模块	描述
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。
	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。
	EVCSupply	实现External Core-Voltage Supply选配输出外部核供电功能。
	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。
	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。
	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。
	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。
	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）。
	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。
	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。
	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。
	WWDandFWD	实现 Window Watchdog Functional Watchdog 配置初始化、程序流监控等功能。
TLF35584 Lib(PartB) 软件库	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。
	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。
	TempMonitor	实现SBC过温监控的诊断功能。
	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。

5.3 配置工具

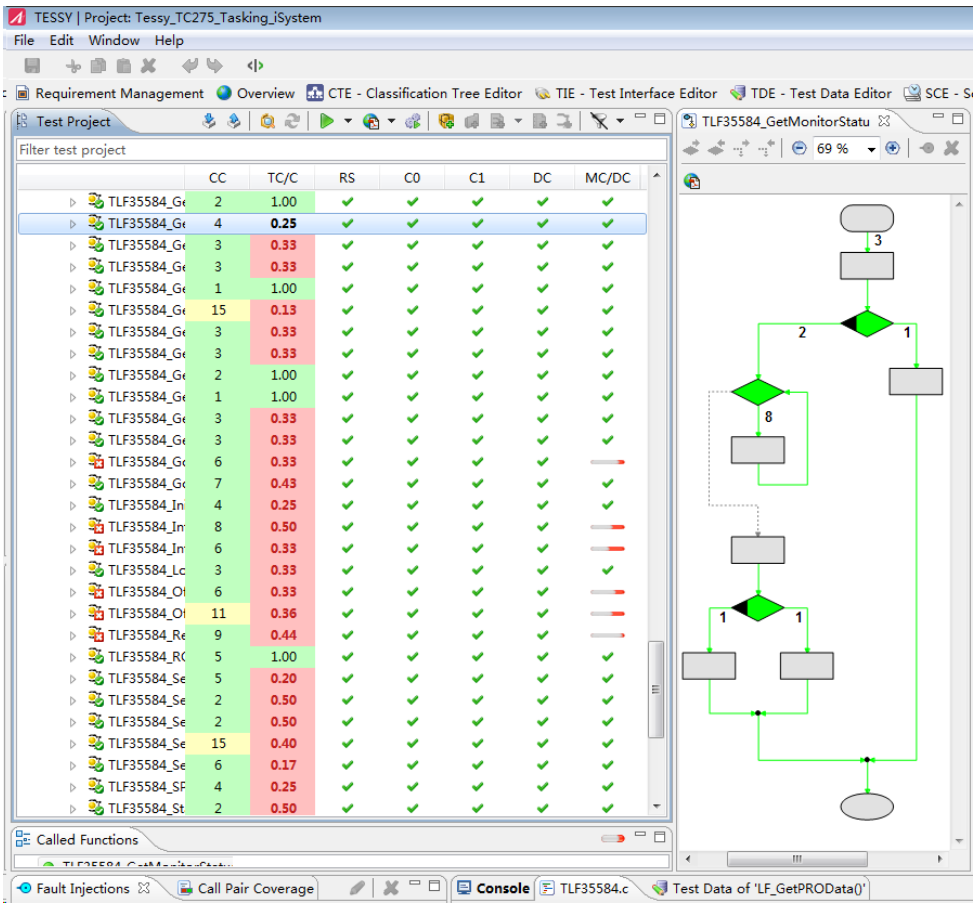


知从科技平台化基础软件配置工具 Muniu_v5.1.3 版本可支持 TLF35584Lib 软件库的配置，以满足不同客户的产品应用需求，并且可与知从科技 Safety Library 软件库的各个模块良好兼容性，自动生成 C 语言代码进行软件集成，增强客户对软件的灵活变更需要。

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。

5.4 软件测试

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



6 过程文档

开发流程	文档描述
需求收集	客户需求文档
软件需求分析	需求分析
	需求分析规格书
	软件需求追踪表
	客户问题沟通表
软件架构设计	软件架构说明书
	软件架构的追踪表
软件详细设计和单元设计	TLF35584Lib 详细设计说明书
	Muni 配置工具设计
	软件详细设计追踪表
	TLF35584Lib 详细设计评审
软件单元测试	QAC 分析报告
	Tessy 测试报告
	软件单元验证策略
软件集成和集成测试	集成策略
	集成手册
	集成测试策略
	集成测试报告
	资源分析报告
软件认可测试	TLF35584Lib 软件测试报告
	TLF35584Lib 软件测试报告评审
发布	发布文档

7 功能安全

7.1 功能安全评估报告

申请评估中。

7.2 功能安全证书

申请认证中。