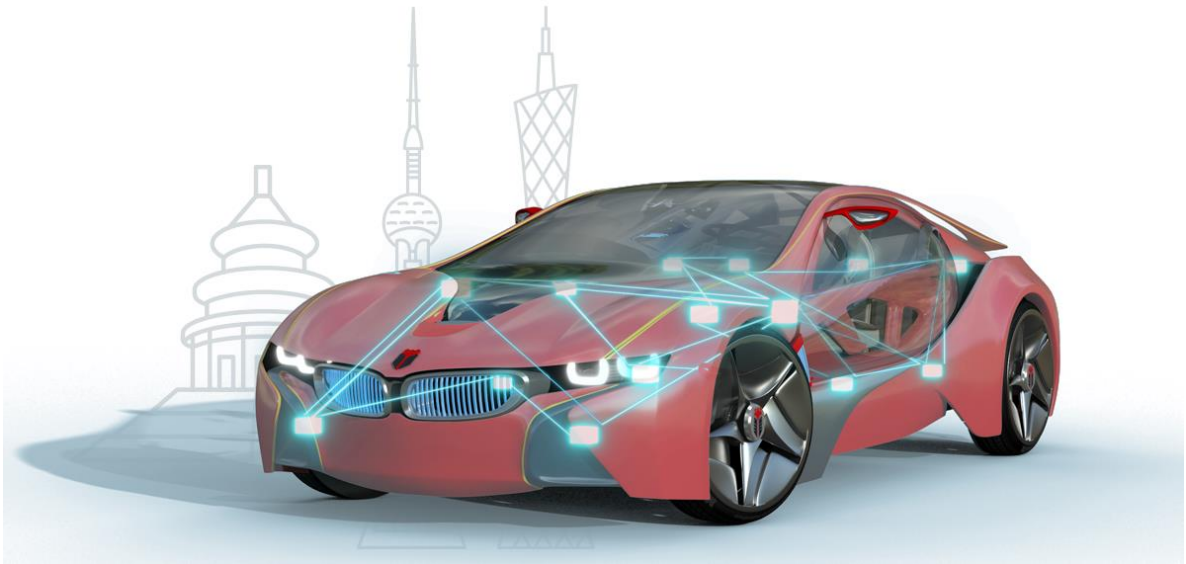
知从基于恩智浦 S32K3 系列芯片
功能安全包可提供的服务手册

知从®工程服务



知从基于恩智浦 S32K3 系列芯片功能安全包可提供的服务手册

知从®工程服务

1 功能概述

S32K3 safety software 是由 NXP 官方提供的软件包，用于帮助客户实现基于 S32K3 芯片的汽车电子控制器产品的功能安全要求。S32K3 safety software 满足 S32K3xx Safety Manual 的要求的大部分芯片层级的功能安全需求，其中包括了 SAF (safety software framework) / SPD (safety peripheral driver) / SCST (core self-test code) / RTD (Real-Time Drivers)内容。

知从针对恩智浦 S32K3 系列 MCU 的 S32K3 safety software 可以提供相应的集成测试服务。

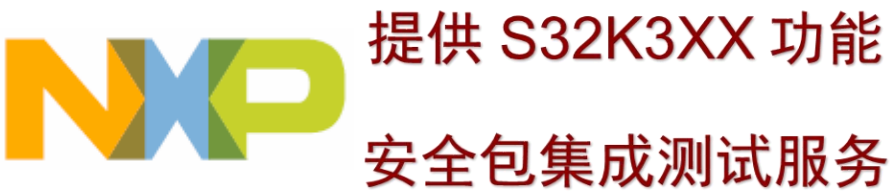
针对 S32K3 Safety software 需要根据客户安全需求进行动态配置才能完全覆盖客户的应用需求的特点，我们可以根据不同的客户项目要求进行配置，最终满足客户功能安全部分的工程需求。

S32K3 safety software 用于实现芯片 MCU 的安全机制 ，包括 MCU 内部模块的测试和硬件安全机制的驱动。

目前，我们服务支持过如下芯片：

© 2017-2023 上海知从科技有限公司

编号	产品名称	芯片企业	芯片型号	编译器	调试器
No.1	S32K3 safety software	恩智浦	S32K322	Green Hills Compiler 2021.1	lauterbach(Trace32 R.2022.02) iSystem(IC5700,5000)
No.2	S32K3 safety software	恩智浦	S32K324	S32DS Version: 3.4	lauterbach(Trace32 R.2022.02) iSystem(IC5700,5000)
No.3	S32K3 safety software	恩智浦	S32K322	Green Hills Compiler 2021.1	lauterbach(Trace32 R.2022.02) iSystem(IC5700,5000)
No.4	S32K3 safety software	恩智浦	S32K342	Green Hills Compiler 2021.1	lauterbach(Trace32 R.2022.02) iSystem(IC5700,5000)
No.5	S32K3 safety software	恩智浦	S32K344	Green Hills Compiler 2021.1	lauterbach(Trace32 R.2022.02) iSystem(IC5700,5000)



2 应用领域

S32K3 safety software 可应用于有功能安全等级需求的控制器。例如：

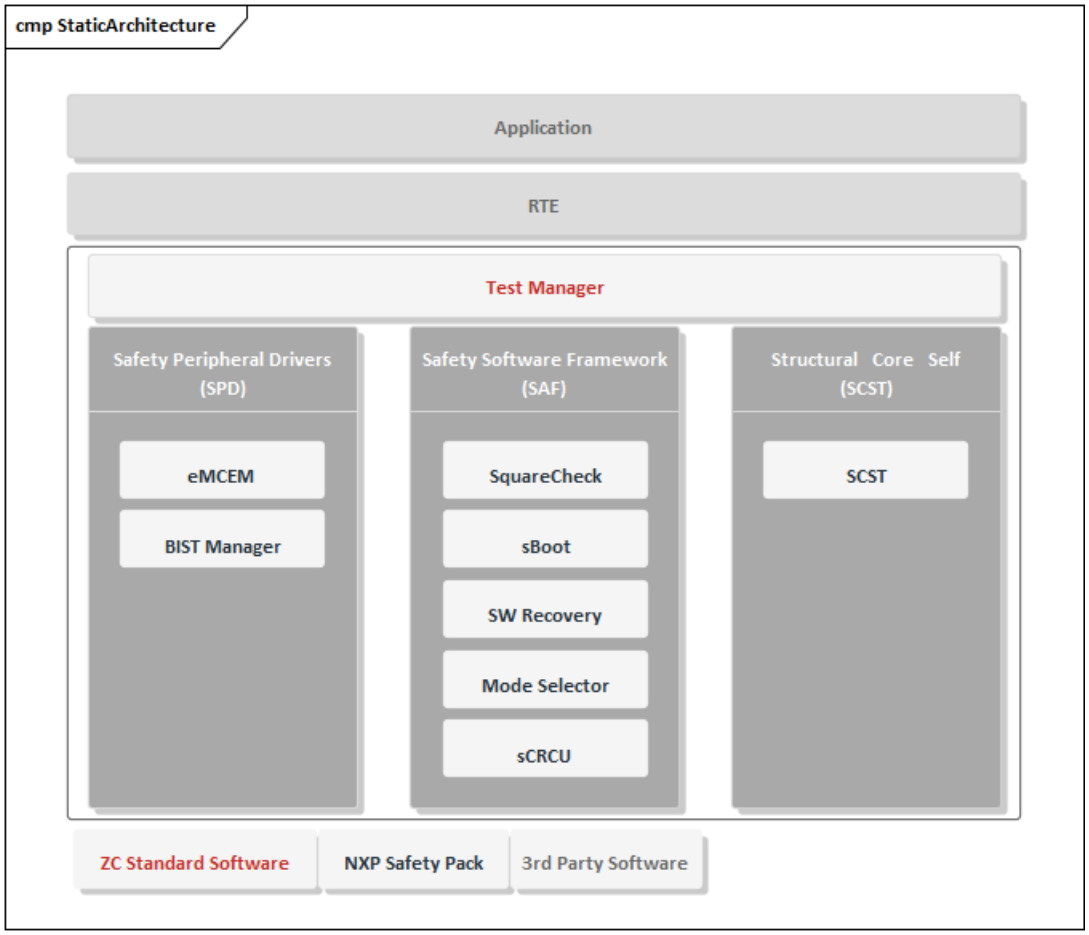
- 娱乐中控 IO 控制器
- 汽车区域控制器
- 电子换挡器
- 电池管理系统(BMS)
- 电泵
- 皮带驱动起动发电机（BSG）
- 车身控制器(BCM)

通过将 S32K3 safety software 集成到汽车电子控制器产品中，最高可满足 ISO26262 ASIL-D 的功能安全等级要求。

© 2017-2023 上海知从科技有限公司

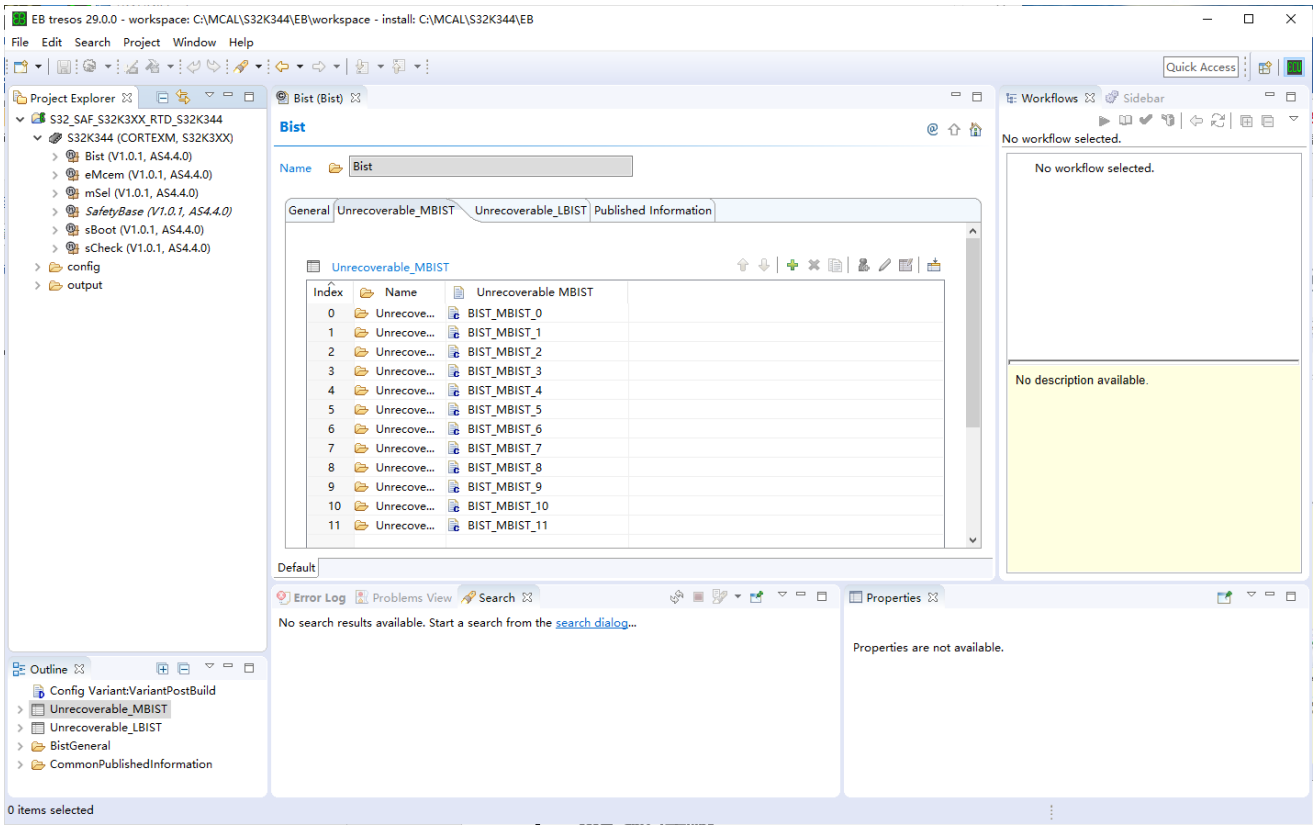
3 技术服务

3.1 功能介绍



Safety Pack 软件架构图

© 2017-2023 上海知从科技有限公司



Safety Pack 配置界面图

3.1.1 SAF 介绍

S32K3 安全软件框架（Safety Software Framework）提供硬件故障的检测和故障响应机制（单点故障和潜伏故障）。其功能涵盖了如下内容：

- BIST - 控制 MCU 的 STCU2 模块执行 MBIST 和 LBIST 自测试
- eMcem - 基于 MCU 的 FCCU 模块执行故障收集和处理
- sCheck – 通过注入故障并检测故障，实现对 MCU 内部各种硬件安全机制的诊断
- mSel – 基于 BIST, eMcem 和 sCheck 的检测和诊断结果，选择 MCU 的软件工作模式
- sBoot – 对某些与安全有关的寄存器执行静态检查，确保这些寄存器的设定值符合要求
- sReco – 执行软件故障恢复

通过以上安全机制的实施, 提升客户控制器安全等级, 减少失效影响。

3.1.2 SPD 介绍

S32K3 安全外设驱动模块（Safety Peripheral Driver）是 SAF 的子集，包含上述的 BIST 和 eMcem 模块。

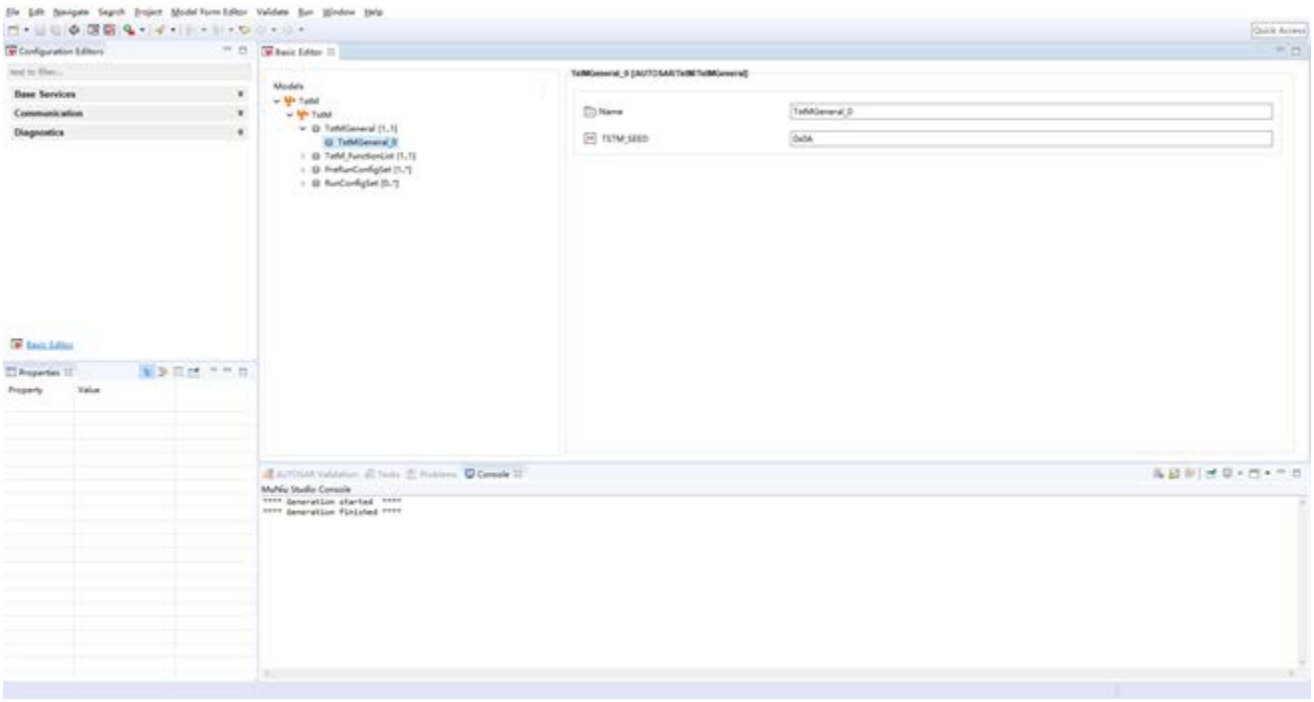
© 2017-2023 上海知从科技有限公司

3.1.3 SCST 介绍

S32K3 安全软件（Structural Core Self Test）组件用于检测内核逻辑中的永久性硬件故障，可以在运行时定期执行实现单点故障检测，其集成与编译器无关，检测代码使用汇编代码编写，无需昂贵的故障模拟工具，即可覆盖诊断所需的检测项。其可达到的安全等级为 ASIL B。

3.2 知从 Test Manager 模块介绍

Test Manager 模块是由知从在集成 Safety Pack 到实际工程中时添加的核心管理调度模块，用于管理 Safety Pack 的测试流程以及管理与应用层的接口。



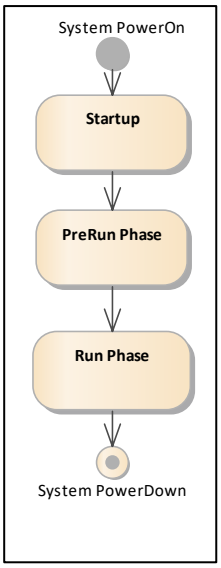
木牛配置工具界面

功能包括：

- Safety Pack 中测试的调度（SAF，SPD 以及 SCST）
- Safety Pack 初始化
- PreRun 阶段测试（启动阶段）
- Run 阶段测试
- PostRun 阶段测试

© 2017-2023 上海知从科技有限公司

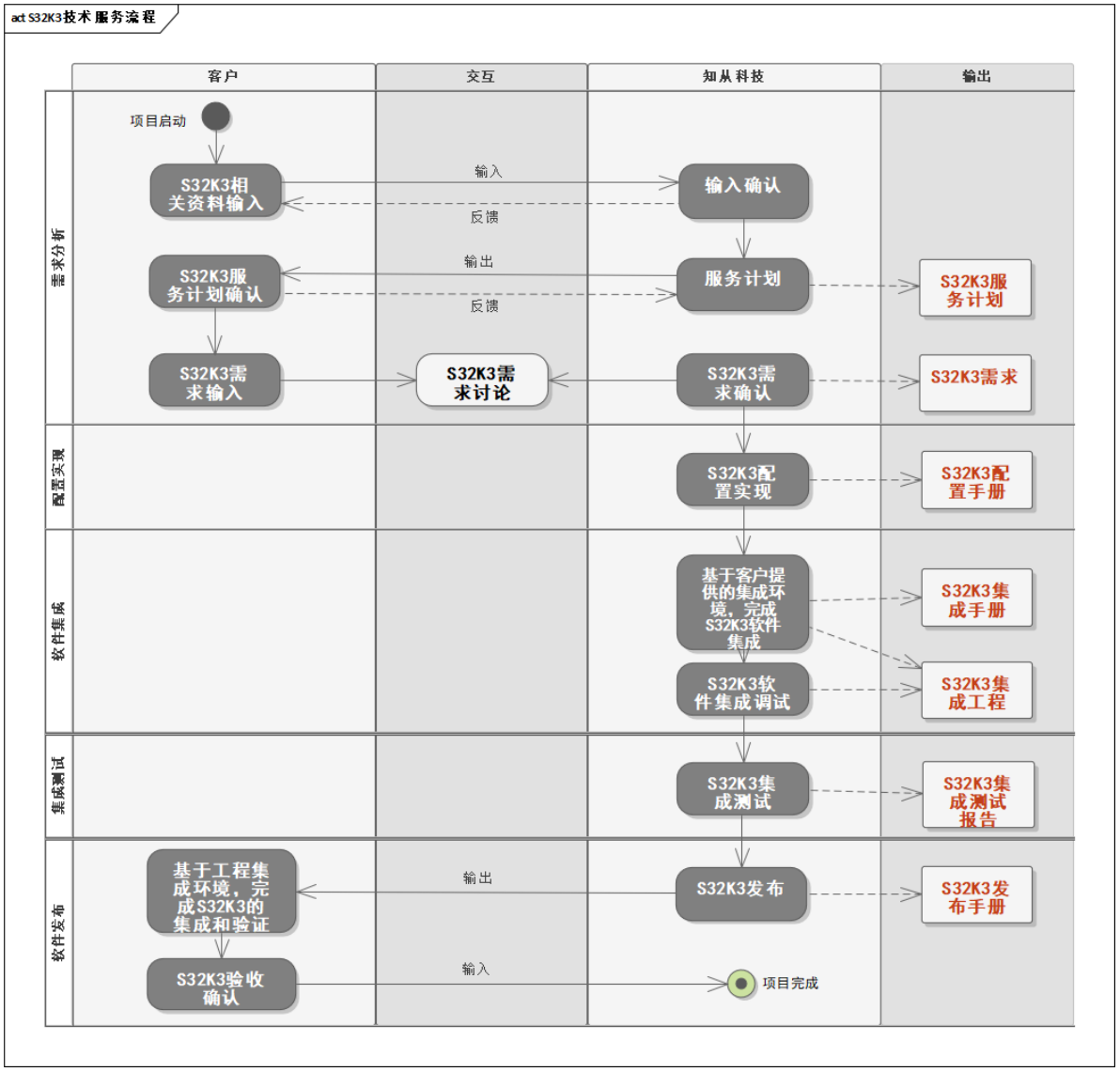
➢ 将 Safety Pack 的检测结果反馈给应用层



3.3 项目实施

知从科技可以配合客户项目进行项目实施，主要包含需求分析、配置实现、软件集成、集成测试、软件发布工作。详细过程如下图，单个项目实施周期在 8 到 12 个工作周。

© 2017-2023 上海知从科技有限公司



项目实施输出物：

编号	S32K3安全包服务输出物
No.1	配置集成计划
No.2	配置需求
No.3	配置手册
No.4	配置工程
No.5	安全包集成工程
No.6	集成手册
No.7	集成测试报告
No.8	发布文档

通过我们的产品和服务,提高汽车电子控制器开发的质量和速度,降低客户成本,增强产品的可维护性。
Our products and services will improve the quality and speed of ECU development, reduce customer costs, and enhance the maintainability of their product.

© 2017-2023 上海知从科技有限公司