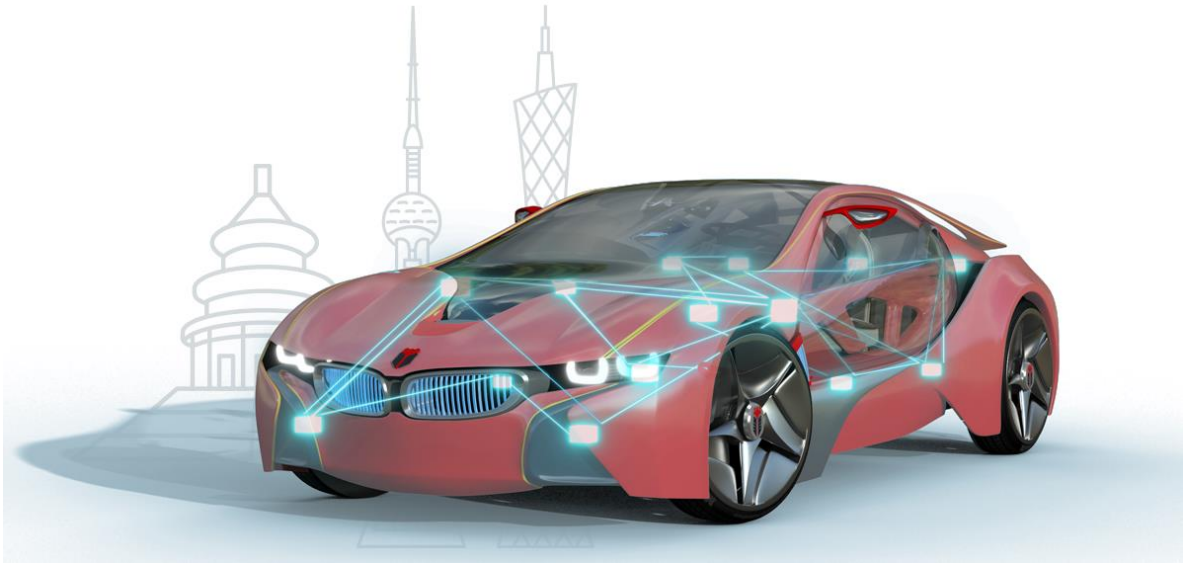
NXP FS85 电源芯片 FCCU 功能介绍

NXP FS85 POWER SUPPLY CHIP FCCU FUNCTION INTRODUCTION



NXP FS85 电源芯片 FCCU 功能介绍
NXP FS85 POWER SUPPLY CHIP FCCU FUNCTION INTRODUCTION

概述 Overview

FS85 是 NXP 推出的一款满足功能安全要求的车规级 SBC 芯片，FS85 系列 SBC 的功能安全等级达到最高的 ASIL-D，其主要应用在汽车雷达、ADAS 域控制器、车载娱乐信息系统等汽车应用中。本文将针对该芯片的 FCCU 功能进行简要介绍，具体内容包含 FCCU 的功能介绍、FCCU 支持的 FSP 协议、FCCU 的配置方法、FCCU 状态机以及 FCCU 的应用场景示例。

FS85 is a kind of automotive grade SBC chip introduced by NXP to meet the functional safety requirements. The FS85 series SBC has the highest functional safety level ASIL-D, and is mainly used in automotive applications such as automotive radar, ADAS domain controller, and in-vehicle entertainment information system. This paper will briefly introduce the FCCU function of the chip, including the function introduction of FCCU, the FSP protocol supported by FCCU, the configuration method of FCCU and the example of FCCU application scenario.

1 FCCU 功能介绍 THE FUNCTION INTRODUCTION OF FCCU

FCCU 提供了一个硬件接口，用于收集 MCU 的故障信息，并在检测到设备故障时将设备置于安全状态。在收集和控制操作过程中，无需 CPU 的干预。FCCU 提供了一种系统化的故障收集和控制方法。FS85 芯片支持两路故障信号输入 FCCU1 和 FCCU2 用于收集来自 MCU 的故障信息，支持单、双线 FCCU 故障监控。

The FCCU provides a hardware interface to collect fault information from the MCU and place the device in a safe state if a device fault is detected. No CPU intervention is required during the collection and control operations. FCCU provides a systematic approach to fault collection and control. The FS85 chip supports two fault signal inputs FCCU1 and FCCU2 for collecting fault information from MCU, and support single and double wire FCCU fault monitoring.

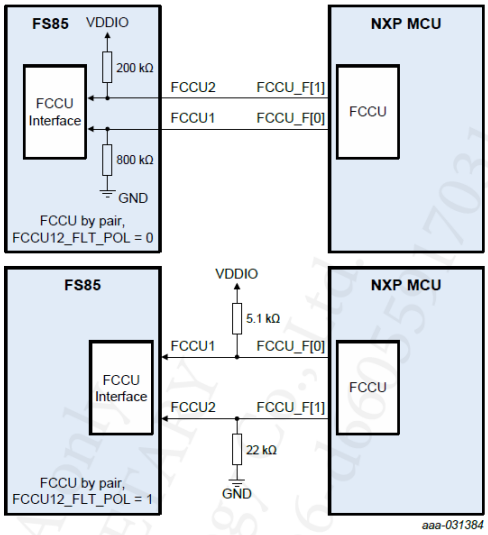


Figure 13. FCCU connection by pair

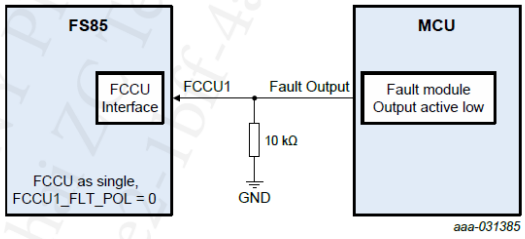


Figure 14. FCCU1 connection as single independent input with FCCU1_FTL_POL = 0

2 FCCU BI-STABLE 协议 FCCU BI-STABLE PROTOCOL

在 Bi-stable 协议下，通过配置 FCCU12 的故障极性还判断 FCCU 故障，其可以配置为 FCCU1 = 0 或 FCCU2 = 1 属于故障态，也可配置为 FCCU1 = 1 或 FCCU2 = 0 属于故障态。

Under the Bi-stable protocol, the FCCU fault can also be judged by configuring the fault polarity of FCCU12, which can be configured as FCCU1 = 0 or FCCU2 = 1 to belong to the fault state, or as FCCU1 = 1 or FCCU2 = 0 to belong to the fault state.

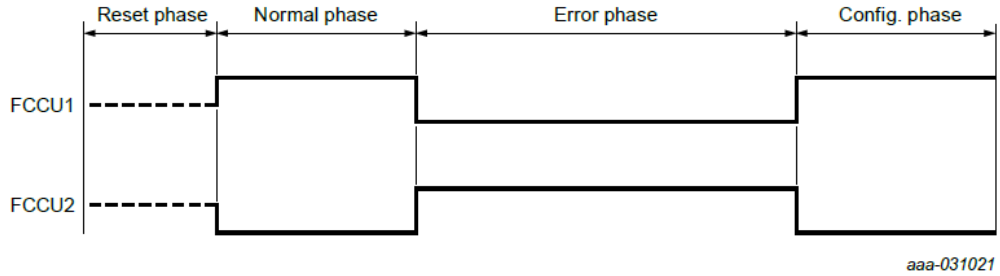


Figure 50. FCCU bi-stable protocol

Table 112. FCCU12 polarity configuration

FCCU12_FLT_POL	FCCU12 polarity
0 (default)	**FCCU1=0 or FCCU2=1 level is a fault**
1	FCCU1=1 or FCCU2=0 level is a fault
Reset condition	POR

3 FS85 FCCU 配置方法 FS85 FCCU CONFIGURATION METHOD

3.1 FCCU 功能使能(FCCU FUNCTION ENABLED)

必须通过 OTP 使用 FCCU_EN OTP 位来启用 FS85 的 FCCU 监控功能。如果将 FS85 与恩智浦 S32 系列芯片结合使用，并且启用了 FCCU 监控功能，那么可以通过 OTP 使用 FLT_RECOVERY_EN OTP 位来启用 FS85 故障恢复功能，从而使用微控制器的故障恢复策略。

The FCCU monitoring function of FS85 must be enabled by using the FCCU_EN OTP bit through the OTP. If FS85 is used in combination with NXP S32 series chips and FCCU monitoring is enabled, the FS85 fault recovery function can be enabled by OTP using the FLT_RECOVERY_EN OTP bit, thus using the fault recovery strategy of the microcontroller.

3.2 FCCU 硬件配置 (Hardware configuration of FCCU)

3.2.1 按对进行硬件配置(HARDWARE CONFIGURATION BY PAIR)

使能 FCCU（bi-stable 模式）需要将 FS_I_SAFE_INPUTS 寄存器的 FCCU_CFG 位设置为 01。

To enable FCCU (bi-stable mode), the FCCU_CFG bit of the FS_I_SAFE_INPUTS register is set to 01.

Table 111. FCCU pins configuration

FCCU_CFG[1:0]	FCCU pins configuration
00	No monitoring
01 (default)	**FCCU1 and FCCU2 monitoring by pair (bi-stable protocol)**
10	FCCU1 or FCCU2 input monitoring
11	FCCU1 input monitoring only
Reset condition	POR

3.2.2 硬件配置为单一独立输入模式(HARDWARE CONFIGURATION AS SINGLE INDEPENDENT INPUT)

使能 FCCU 的单一输入需要将 FS_I_SAFE_INPUTS 寄存器的 FCCU_CFG 位设置为 10/11。

Enabling a single input to the FCCU requires setting the FCCU_CFG bit of the FS_I_SAFE_INPUTS register to 10/11.

Table 111. FCCU pins configuration

FCCU_CFG[1:0]	FCCU pins configuration
00	No monitoring
01 (default)	**FCCU1 and FCCU2 monitoring by pair (bi-stable protocol)**
10	FCCU1 or FCCU2 input monitoring
11	FCCU1 input monitoring only
Reset condition	POR

3.2.3 故障极性配置（FAULT POLARITY CONFIGURATION）

当输入配置为引脚对输入模式时，错误信号的极性可以通过 FCCU12_FLT_POL 位进行配置。

When the input is configured in the pin-pair input mode, the polarity of the error signal can be configured via the FCCU12_FLT_POL bit.

Table 112. FCCU12 polarity configuration

FCCU12_FLT_POL	FCCU12 polarity
0 (default)	**FCCU1=0 or FCCU2=1 level is a fault**
1	FCCU1=1 or FCCU2=0 level is a fault
Reset condition	POR

当配置为单独输入模式时，FCCU 可以检测 2 路错误信号，每路错误信号的极性可以通过 FCCU1_FLT_POL 和 FCCU2_FLT_POL 单独配置。

When configured in separate input mode, the FCCU can detect 2-channel error signals, and the polarity of each channel error signal can be configured separately by FCCU1_FLT_POL and FCCU2_FLT_POL.

Table 114. FCCUx polarity configuration

FCCU1_FLT_POL	FCCU1 polarity
0 (default)	**FCCU1 low level is a fault**
1	FCCU1 high level is a fault
Reset condition	POR

FCCU2_FLT_POL	FCCU2 polarity
0 (default)	**FCCU2 low level is a fault**
1	FCCU2 high level is a fault
Reset condition	POR

3.2.4 FCCU12 错误影响配置（FCCU12 ERROR IMPACT CONFIGURATION）

当输入配置为引脚对输入模式时，FCCU 的错误响应通过 FCCU12_FS_IMPACT 进行配置。

The error response of the FCCU is configured through FCCU12_FS_IMPACT when the input is configured in the pin-pair input mode.

Table 113. FCCU12 error impact configuration

FCCU12_FS_IMPACT	FCCU12 impact on RSTB/FS0B
0	FS0B only is asserted
1 (default)	**FS0B and RSTB are asserted**
Reset condition	POR

当配置为单独输入模式时，FCCU 的错误响应通过 FCCU1/2_FS_IMPACT 进行单独配置。

When configured in separate input mode, the error response of the FCCU is individually configured via FCCU1/2_FS_IMPACT.

Table 115. FCCUx error impact configuration

FCCU1_FS_IMPACT	FCCU1 impact on RSTB/FS0B
0	FS0B only is asserted
1 (default)	**FS0B and RSTB are asserted**
Reset condition	POR

FCCU2_FS_IMPACT	FCCU2 impact on RSTB/FS0B
0	FS0B only is asserted
1 (default)	**FS0B and RSTB are asserted**
Reset condition	POR

3.2.5 微控制单元故障恢复策略（MCU FAULT RECOVERY STRATEGY）

故障恢复策略功能由 OTP_FLT_RECOVY_EN 位来启用。此功能会扩展看门狗窗口，以便微控制器能够执行故障恢复策略。其目的是在发生故障事件后，让微控制器在尝试恢复应用程序时不会进行复位操作。当微控制器通过其 FCCU 引脚触发故障时，设备会将 FSOB 引脚置高，此时看门狗窗口的持续时间会自动变为开放窗口（不再有占空比）。这种开放窗口的持续时间可在 INIT_FS 阶段通过 WDW_RECOVERY [3:0] 位进行配置。

The fault recovery strategy feature is enabled by OTP_FLT_RECOvERY_EN bit. This function extends the watchdog window to allow the MCU to perform a fault recovery strategy. The goal is to not reset the MCU while it is trying to recover the application after a failure event. When a fault is triggered by the MCU via its FCCU pins, the FSOB pin is asserted by the device and the watchdog window duration becomes automatically an open window (no more duty cycle). This open window duration is configurable with the WDW_RECOVERY [3:0] bits during the INIT_FS phase.

Table 110. Watchdog window in fault recovery configuration

WDW_RECOVERY [3:0]	Watchdog window duration when the device is in fault recovery strategy
0000	DISABLE
0001	1.0 ms
0010	2.0 ms
0011	3.0 ms
0100	4.0 ms
0101	6.0 ms
0110	8.0 ms
0111	12 ms
1000	16 ms
1001	24 ms
1010	32 ms
1011(default)	**64 ms**
1100	128 ms
1101	256 ms
1110	512 ms
1111	1024 ms
Reset condition	POR

4 FCCU 状态机（FCCU STATE MACHINE）

当 FCCU 引脚显示有错误且 FSOB 被激活时，就会从 WDW_PERIOD 状态转换到 WDW_RECOVERY 状态。如果在 WDW_RECOVERY 期间结束前，微控制器发送了有效的看门狗刷新信号，那么设备会切换回 WDW_PERIOD 状态及其对应的占空比，前提是 FCCU 引脚不再显示错误。否则，将开始一个新的 WDW_RECOVERY 期间。如果在 WDW_RECOVERY 期间结束前微控制器没有发送有效的看门狗刷新信号，那么会生成一个复位脉冲，并且故障安全状态机会返回到 INIT_FS 状态。

The transition from WDW_PERIOD to WDW_RECOVERY happens when the FCCU pin indicates an error and FSOB is asserted. If the MCU send a good watchdog refresh before the end of the WDW_RECOVERY duration, the device switches back to the WDW_PERIOD duration and associated duty cycle if the FCCU pins does not indicate an error anymore. Otherwise, a new WDW_RECOVERY period is started. If the MCU does not send a good watchdog refresh before the end of the WDW_RECOVERY duration, then a reset pulse is generated, and the fail-safe state machine moves back to INIT_FS.

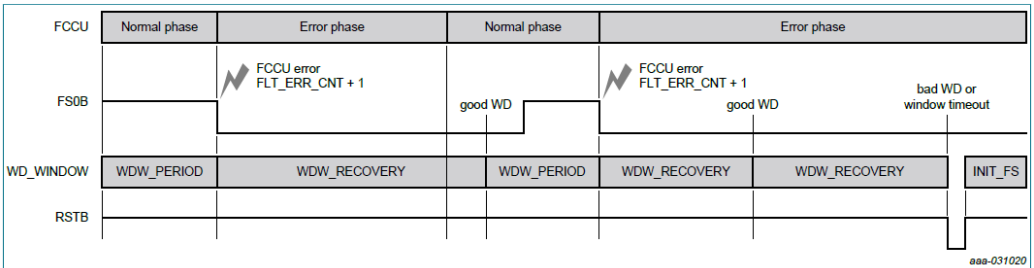


Figure 49. Fault recovery strategy principle

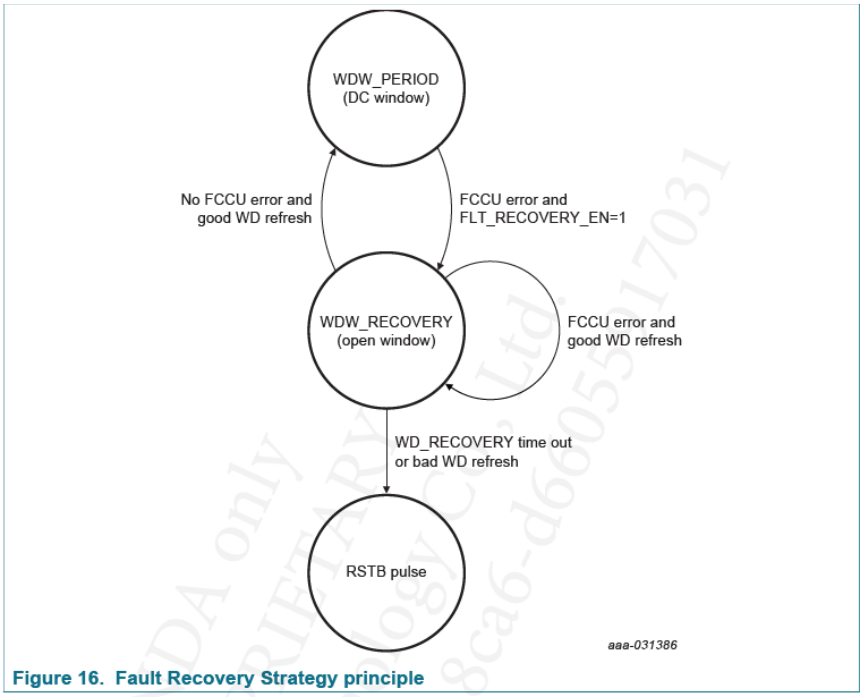


Figure 16. Fault Recovery Strategy principle

5 FCCU 的应用场景示例(EXAMPLE OF APPLICATION SCENARIO OF FCCU)

应用场景（Application Scenarios）：TC397_SMU + FS8530_FCCU

FCCU 配置（FCCU configuration）：

FS_I_SAFE_INPUTS. FCCU_CFG = 01（Bi-statble）、

FS_I_SAFE_INPUTS. FCCU12_FLT_POL = 0 （FCCU1 = 0 or FCCU2 = 1 level is a fault）

FS_I_SAFE_INPUTS. FCCU12_FS_IMPACT = 0（FS0B only is asserted）

FS_WD_WINDOW. WDW_RECOVERY = 0x7（12ms）

测试结果（Test Result）：

6 ZC TC3XX SAFETYFRAME 产品介绍（ZC TC3XX SAFETYFRAME PRODUCT INTRODUCTION）

汽车电控系统的电气化、智能化发展日趋复杂，对于电子电气架构的安全性要求也越来越高。通过对道路车辆应用场景的HARA分析，为了使安全目标被降级分解、保持危害发生可能性低于风险的受限值，汽车功能安全越来越受到重视。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。在电子电气系统中，对于通用的 Element 通常采用 SEooC(safety element out of context)方法进行设计开发。

The electrification and intelligent development of automobile electronic control system is becoming more and more complex, and the safety requirements of electronic and electrical architecture are becoming higher and higher. Through HARA analysis of road vehicle application scenarios, more and more attention is paid to vehicle functional safety in order to degrade and decompose safety objectives and keep the possibility of hazard occurrence lower than the risk limit. In recent years, reference has been made to ISO 26262 for functional safety standards; Refer to E-GAS layering for the software shelf security architecture. In electronic and electrical systems, For the common Element, the SEooC (safety element out of context) approach is usually adopted for its design and development.

知从科技推出 SAFETY FRAME 为各车载控制器客户提供 ASIL 等级分解咨询、FMEDA 分析过程支持、芯片级自检安全机制开发、SafetyFrame 配置与软件集成等全流程功能安全服务。

ZC launched SAFETY FRAME to provide customers with ASIL level decomposition consultation, FMEDA analysis process support, chip-level self-check safety mechanism development, SafetyFrame configuration and software integration and other full-process functional safety services.

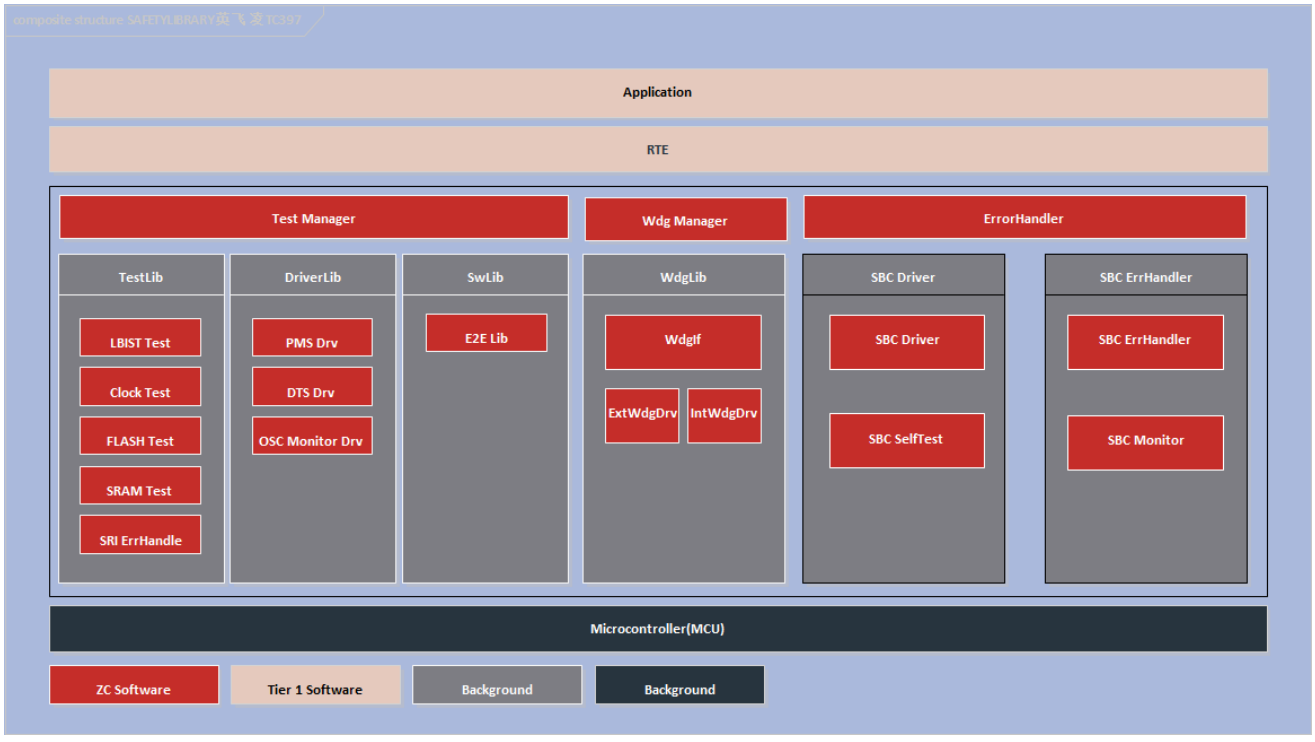
SAFETY FRAME 包括 3 个组件：MCU 内部模块自检测试组件（即 SF.MCU）、SBC 硬件安全机制的驱动组件(即 SF.SBC)、安全架构组件(即 SF.Architecture)。SF.Architecture 的核心模块为 Test Manager，用于 MCU&SBC 的 Safety Library 调度管理，包括 Safety WdgM、Safety SBC/ASIC 驱动模块调度、与应用层 PFC(Program Flow Check)接口等，SF.MCU 包含 3 大模块：

SAFETY FRAME consists of 3 components: the internal module self-checking test component of MCU (i.e. SF.MCU), the driver component of SBC's hardware security mechanism (i.e. SF.SBC), and the safety architecture component (i.e. SF.Architecture). The core module of SF.Architecture is Test Manager, which is used for the scheduling management of Safety Library for MCU and SBC, including Safety Wdgm, scheduling of Safety SBC/ASIC driver modules, and interfaces with application layer PFC (Program Flow Check), etc. SF.MCU contains 3 major modules:

- TestLib--实现 MCU 芯片模块的检测。
  TestLib-- Implementation of MCU chip module inspection.
- DriverLib--实现 MCU 芯片模块的驱动。
  DriverLib-- Implements the MCU chip module driver.
- SwLib--用户常用的数字签名库、端到端保护库等接口。
  SwLib-- Interfaces such as digital signature database and end-to-end protection database are commonly used by users.

SAFETY FRAME 在软件模块化分层原则上，将 Function Controller 和 Monitoring Controller 分别由 SF.MCU 和 SF.SBC 实现，并部署在 EGAS Level2 和 Level3 层级，充分考虑了程序流监控和关断路径设计的应用需求。

In the principle of software modular layering, Function Controller and Monitoring Controller are implemented by SF.MCU and SF.SBC, respectively. It is also deployed at EGAS Level2 and Level3 levels, taking into account the application requirements of program flow monitoring and shutdown path design.



软件架构 / Software Architecture

知从 SafetyFrame 产品实现的功能安全模块包括：Test Manager 模块、LBIST Test 模块、MBIST Test 模块、PFlash Test 模块、MCU Firmware Test 模块、Register Test 模块、DMA Test 模块、SRI Error Handling 模块、MONBIST Test 模块、Mcu Register Monitor 模块、Register Monitor Test 模块、Evadc Test 模块、Interrupt monitor Test 模块、Clock Plausibility Test 模块、DAM Test 模块、Convctrl Test 模块、CPU Internal BUS Test 模块、STM Test 模块、GTM TIM

Clock Test 模块、Gtm IOM Alarm Test 模块、Gtm Tom Tim Test 模块、Port Test 模块、GptTst 模块、PMS configuration 模块、DTS Configuration 模块、OSC Clock Monitor 模块、SMU Error Handler 模块、SMU Software Alarm Drv 模块、IR FFI Control 模块、GTM IOM Configuration 模块、ERU Configuration 模块、TLF35584 Driver 模块、TLF35584 Error Handler 模块、E2E 保护模块、Safe Watchdog Manager 模块、Safe Watchdog Interface 模块、Safe Internal Watchdog 模块、Safe SBC Watchdog 模块。

The functional safety modules implemented by ZC SafetyFrame products include: Test Manager module, LBIST Test module, MBIST Test module, PFlash Test module, MCU Firmware Test module, Register Test module, DMA Test module, SRI Error Handling module, MONBIST Test module, Mcu Register Monitor module, Register Monitor Test module, Evadc Test module, Interrupt monitor Test module, Clock Plausibility Test module, DAM Test module, Convctrl Test module, CPU Internal BUS Test module, STM Test module, GTM TIM Clock Test module, Gtm IOM Alarm Test module, Gtm Tom Tim Test module, Port Test module, GptTst module, PMS configuration module, DTS Configuration module, OSC Clock Monitor module, SMU Error Handler module, SMU Software Alarm Drv module, IR FFI Control module, GTM IOM Configuration module, ERU Configuration module, TLF35584 Driver module, TLF35584 Error Handler module, E2E protection module, Safe Watchdog Manager module, Safe Watchdog Interface module, Safe Internal Watchdog module, Safe SBC Watchdog module.

知从 SafetyFrame 产品针对本文中提及的 FS85 芯片实现了看门狗监控 WDGM 模块，以及配合 TC3XX SMU 模块应用 FCCU 功能实现了 SMUErrHdl 模块，模块实现了以下安全机制。

ZC's SafetyFrame product implements the watchdog monitoring WDGM module for the FS85 chip mentioned in this paper, and implements the SMUErrHdl module with the FCCU function in the TC3XX SMU module. The module implements the following security mechanisms.

安全机制(Safety Mechanism)
ESM[SW]:SYS:SW_SUPERVISION
ESM[SW]:CPU:SOFTERR_MONITOR
ESM[SW]:SMU:APPLICATION_SW_ALARM
SM[HW]:SMU:FSP_MONITOR