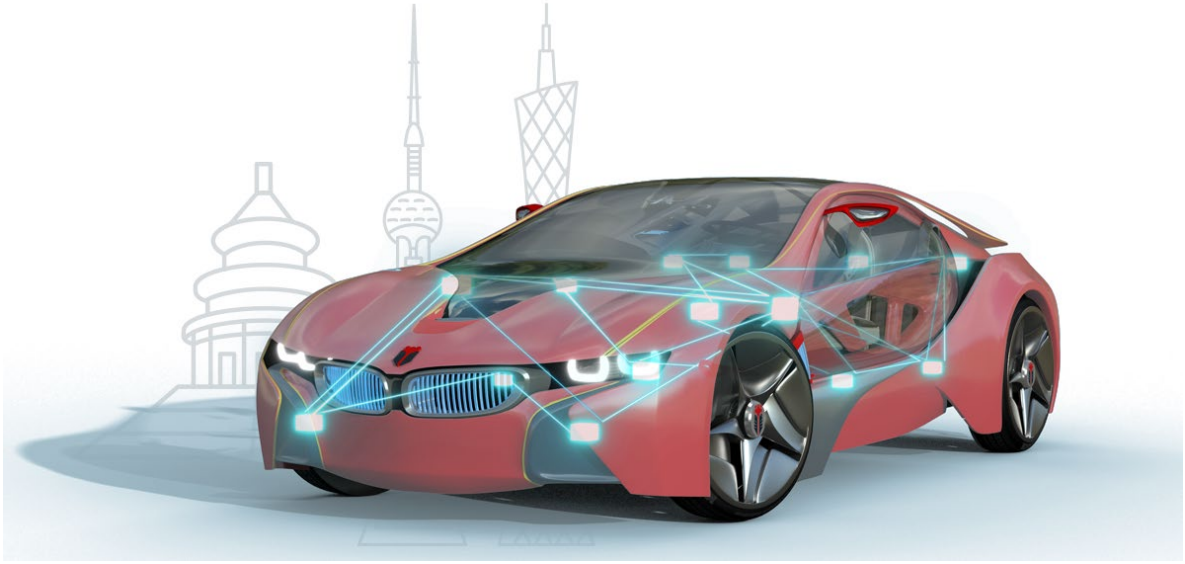
恩智浦 S32K3 芯片 FCCU 在功能安全中的应用

APPLICATION OF NXP S32K3 FCCU IN FUNCTIONAL SAFETY



恩智浦 S32K3 芯片 FCCU 在功能安全中的应用 APPLICATION OF NXP S32K3 FCCU IN FUNCTIONAL SAFETY

1 概述 OVERVIEW

在现代汽车电子系统中，功能安全是确保车辆可靠运行的核心要素。恩智浦 S32K3 系列 MCU 作为针对汽车应用的高性能车规级微控制器，最高支持 ASIL-D 等级的功能安全，广泛应用于电池管理系统（BMS）、底盘控制器、车身控制器等关键场景。其中，FCCU（Fault Collection and Control Unit）模块是实现功能安全的关键组件，负责统一管理和响应芯片运行时可能出现的各种硬件错误。

In modern automotive electronic systems, functional safety is a core element ensuring reliable vehicle operation. NXP's S32K3 series MCUs, as high-performance automotive-grade microcontrollers designed for automotive applications, support functional safety up to ASIL-D level. They are widely used in critical scenarios such as battery management systems (BMS), chassis controllers, and body controllers. Among these, the FCCU (Fault Collection and Control Unit) module serves as a key component for achieving functional safety, responsible for centrally managing and responding to various hardware errors that may occur during chip operation.

1.1 FCCU 模块的核心特性与工作机制 Feature and Operating Mechanism of the FCCU Module

特性列表 Feature List:

FCCU 模块作为 S32K3 芯片中的错误收集和控制中心，具有以下核心特性：

The FCCU module, serving as the error collection and control center within the S32K3 chip, possesses the following core features:

- **全面错误管理：**管理非关键故障，处理硬件和软件的故障恢复

Comprehensive Error Management: Managing non-critical failures and handling hardware and software fault recovery

- **安全相关监控：**对芯片上安全相关的模块进行系统化错误收集

Security-related monitoring: Systematic error collection for security-related modules on the chip

- **可配置响应机制：**可针对每个非关键故障配置不同的芯片内部响应（包括功能性复位、NMI 中断、IRQ 或不采取行动）

Configurable response mechanism: Different on-chip responses can be configured for each non-critical fault (including functional reset, NMI interrupt, IRQ, or no action).

- **错误注入功能：**支持错误注入测试，便于验证系统安全机制

Error Injection Functionality: Supports error injection testing to facilitate verification of system security mechanisms.

- **安全锁定机制：**配置完成后可进行锁定，防止意外修改

Security Locking Mechanism: Once configured, it can be locked to prevent accidental modifications.

1.2 FCCU 状态机介绍 Introduction to the FCCU State Machine

FCCU 的功能通过有限状态机状态图进行描述，见下图：

The functionality of the FCCU is described using a finite state machine state diagram, as shown below:

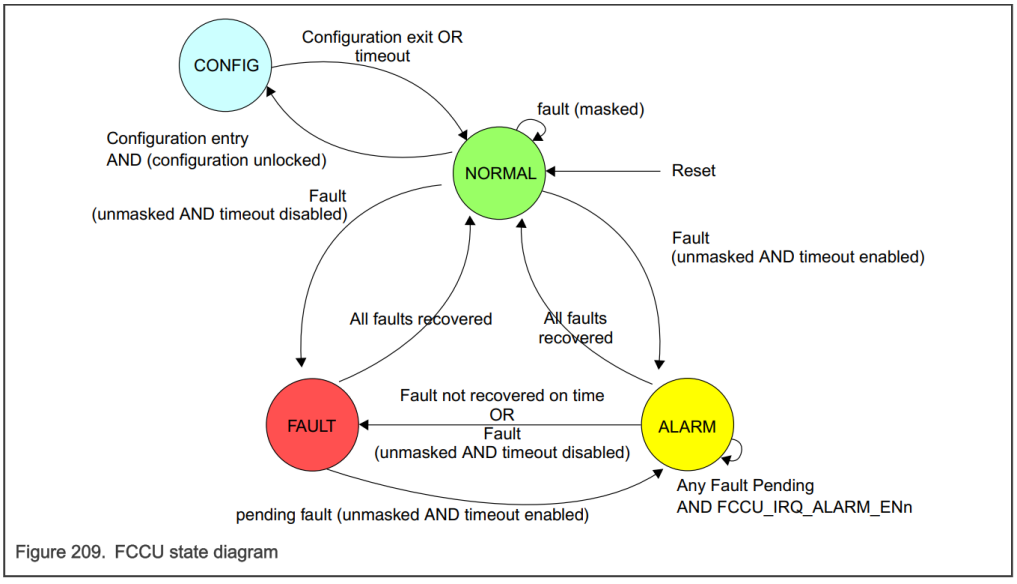


图 1. FCCU 状态机（摘录自芯片手册）
Figure 1. FCCU State Machine (Excerpt from Chip Manual)

FCCU 模块通过精细的状态机实现错误处理，包含四种主要工作状态：

The FCCU module implements error handling through a sophisticated state machine, encompassing four primary operational states:

1. **CONFIG 状态**：S32K3 启动后的默认状态，在此状态下可对 FCCU 寄存器进行配置，完成后手动切换到 NORMAL 模式。

   CONFIG State: The default state after S32K3 startup. In this state, the FCCU registers can be configured. After configuration, manually switch to NORMAL mode.

2. **NORMAL 状态**：正常工作状态，当检测到非关键故障（NCF）通道有错误时，会根据配置切换到 ALARM 或 FAULT 状态。

   NORMAL state: Normal operating state. When an error is detected on a non-critical fault (NCF) channel, the system will switch to ALARM or FAULT state based on configuration.

3. **ALARM 状态**：当使能了 ALARM 中断的 NCF 通道出现错误时，系统进入此状态并触发 ALARM 中断，开发者可在中断中进行错误处理。

   ALARM State: When an error occurs on an NCF channel with enabled ALARM interrupts, the system enters this state and triggers an ALARM interrupt. Developers can handle the error within the interrupt routine.

4. **FAULT 状态**：严重错误状态，可触发功能性复位或 NMI 中断，若错误持续存在，可能依次启动多次功能性复位甚至破坏性复位。

   FAULT state: A critical error condition that may trigger a functional reset or NMI interrupt. If the error persists, it may sequentially initiate multiple functional resets or even a destructive reset.

1.3 错误处理流程 Error Handling Process

FCCU 的错误处理流程体现了其多层容错机制。当非关键故障出现时，系统首先进入 ALARM 状态，为用户提供处理机会；若在预定时间内未能解决，则升级到 FAULT 状态，启动更严格的错误控制措施。这种渐进式响应策略避免了不必要的系统重启，同时确保了安全关键应用的可靠性。

The FCCU's error handling process embodies its multi-level fault tolerance mechanism. When non-critical faults occur, the system first enters the ALARM state, providing users an opportunity to address the issue. If the fault remains unresolved within the predetermined timeframe, the system escalates to the FAULT state, initiating more stringent error control measures. This progressive response strategy avoids unnecessary system reboots while ensuring the reliability of safety-critical applications.

2 FCCU 在功能安全应用中的关键作用 THE CRITICAL ROLE OF FCCU IN FUNCTIONAL SAFETY APPLICATIONS

2.1 满足 ASIL-D 安全要求 Meets ASIL-D safety requirements

S32K3 系列 MCU 通过 FCCU 与其他安全机制（如锁步核、硬件看门狗等）的协同工作，能够满足最高等级（ASIL-D） 的汽车功能安全要求。FCCU 的核心价值在于它提供了一种系统化的错误管理方法，而不是依赖分散的错误处理机制。

The S32K3 series MCUs meet the highest level (ASIL-D) of automotive functional safety requirements through the coordinated operation of the FCCU with other safety mechanisms, such as lockstep cores and hardware watchdogs. The core value of the FCCU lies in its provision of a systematic error management approach, rather than relying on decentralized error handling mechanisms.

2.2 在电池管理系统（BMS）中的应用 Applications in Battery Management Systems (BMS)

在电动汽车的 BMS 中，FCCU 模块确保了对电池状态监控的持续可靠性。当检测到电压、温度采集异常或通信故障时，FCCU 可根据错误严重程度启动相应处理流程，防止错误传播，保障电池系统的安全运行。

In the BMS of electric vehicles, the FCCU module ensures continuous and reliable monitoring of battery status. When abnormal voltage or temperature readings, or communication failures are detected, the FCCU initiates corresponding handling procedures based on the severity of the error. This prevents error propagation and safeguards the safe operation of the battery system.

2.3 在车身控制系统中的应用 Applications in Body Control Systems

对于车身控制器（如门控、座椅调整、照明管理），FCCU 提供的错误收集和处理机制确保即使发生非关键故障，系统也能通过预定义的安全策略维持基本功能或优雅降级，避免严重影响用户体验或安全。

For body controllers (such as door control, seat adjustment, and lighting management), the FCCU's error collection and handling mechanism ensures that even in the event of non-critical faults, the system can maintain basic functionality or gracefully degrade through predefined safety policies, thereby preventing severe impacts on user experience or safety.

2.4 支持功能安全认证 Supports functional safety certification

对于需要 ISO 26262 功能安全认证的应用，FCCU 模块提供的系统化错误管理框架大大简化了认证材料的准备。恩智浦提供的安全文档、安全软件库及 MCU+SBC 的系统安全方案，可帮助客户快速完成功能安全开发。

For applications requiring ISO 26262 functional safety certification, the FCCU module's systematic error management framework significantly simplifies the preparation of certification documentation. NXP's safety documentation, safety software libraries, and MCU+SBC system safety solutions enable customers to rapidly complete functional safety development.

3 开发支持与实践 DEVELOPMENT SUPPORT AND PRACTICES

3.1 与安全软件框架（SAF）的协同 Synergy with the Security Architecture Framework (SAF)

恩智浦提供的安全软件框架（SAF） 与 FCCU 硬件机制协同工作，为开发者提供了完整的故障检测和响应解决方案。这一组合显著减少了功能安全实现的开发工作量。

NXP's Safety Software Framework (SAF) works in tandem with the FCCU hardware mechanism to provide developers with a complete fault detection and response solution. This combination significantly reduces the development effort required for functional safety implementation.

3.2 与 SBC 的协同 Synergy with SBC

3.2.1 信号传递 SIGNAL TRANSMISSION

联动的起点是 S32K3 内部发生的各种硬件错误。FCCU 模块通过其 DCM（诊断控制模块） 收集来自芯片内部多达 86 个以上的错误通道（如锁步核差异、存储器 ECC 错误、时钟监控单元错误等），并将其归纳为 8 个 NCF（非关键故障） 通道组。

The trigger for the chain reaction is various hardware errors occurring within the S32K3. The FCCU module collects data from over 86 internal error channels (such as lockstep core discrepancies, memory ECC errors, clock monitoring unit errors, etc.) via its DCM (Diagnostic Control Module) and categorizes them into 8 NCF (Non-Critical Failure) channel groups.

当错误被确认后，FCCU 会根据预先的配置，通过 EOUT0 和 EOUT1 两个互补的引脚信号将错误状态传递给外部的 FS26。这两个引脚是 MCU 与 SBC 之间关键的安全通信链路。根据官方文档，EOUT[1:0]的电平信号是互补相反的，这种设计增强了信号传输的可靠性。

Upon error confirmation, the FCCU transmits the error status to the external FS26 via two complementary pin signals, EOUT0 and EOUT1, according to predefined configurations. These pins form the critical safety communication link between the MCU and SBC. As per official documentation, the EOUT[1:0] signals are complementary and oppositely phased, a design that enhances signal transmission reliability.

3.2.2 FS26 的安全执行机制 FS26 SECURITY EXECUTION MECHANISM

FS26 在收到 FCCU 发出的错误信号后，会启动相应的硬件保护动作，主要包括以下几个方面：

Upon receiving an error signal from the FCCU, FS26 will initiate corresponding hardware protection actions, primarily encompassing the following aspects:

强制硬件复位：FS26 会通过拉低 RSTB 引脚，对 S32K3 MCU 进行硬件复位。这是最常见的错误恢复手段。

Forced hardware reset: FS26 performs a hardware reset on the S32K3 MCU by pulling the RSTB pin low. This is the most common error recovery method.

关断安全输出：在更严重的安全故障下（例如需要立即停止电机转动），FS26 会通过拉低 FS0B 和 FS1B 这两个故障安全输出引脚，来直接关闭外部的驱动芯片或功率器件，从而切断危险源，实现“故障静默”。

Shutdown Safety Output : In the event of more severe safety faults (such as those requiring immediate motor shutdown), the FS26 directly deactivates external driver chips or power devices by pulling down the FS0B and FS1B fail-safe output pins. This action isolates the hazard source, achieving “fail-safe silencing.”

看门狗协同：FS26 自身也集成了看门狗功能。FS26 的看门狗分为简单喂狗和复杂喂狗，复杂喂狗适配 ASIL D 等级，需要使用随机密钥。正确的喂狗操作必须在看门狗周期内的“OPEN”窗口阶段进行，并且需要在没有 FCCU 错误的情况下才有效。如果 S32K3 因程序跑飞而无法正常喂狗，或者存在 FCCU 错误，FS26 的看门狗超时也会触发系统复位或安全动作。

Watchdog Collaboration: The FS26 also integrates a built-in watchdog function. The FS26 watchdog features both simple and complex feeding modes. Complex feeding is designed for ASIL D compliance and requires the use of a random key. Valid feeding operations must occur during the “OPEN” window phase within the watchdog cycle and are only effective when no FCCU errors are present. If the S32K3 cannot perform proper watchdog feeding due to program runaway or if FCCU errors exist, FS26's watchdog timeout will trigger a system reset or safety action.

总而言之，S32K3 的 FCCU 与 FS26 的联动，将一个复杂的片上安全管理系统扩展为了一个强大的片内外协同安全堡垒。这种深度集成的硬件安全架构，是开发满足 ASIL D 等级的车规级产品的重要基石。

In summary, the interplay between the S32K3's FCCU and the FS26 expands a complex on-chip security management system into a robust on-chip/off-chip collaborative security fortress. This deeply integrated hardware security architecture serves as a crucial foundation for developing automotive-grade products that meet ASIL D requirements.

3.3 错误注入测试 Error Injection Testing

利用 FCCU 的错误注入功能，开发者可以在开发阶段主动模拟各种错误条件，验证系统错误响应机制的有效性，这是功能安全开发中的重要实践。例如，S32K3 提供的 EIM（错误注入模块） 是验证这套联动机制是否有效的关键工具。开发者可以主动在 SRAM 等部件中注入

ECC 错误，模拟硬件故障，从而观察从 FCCU 报警到 FS26 执行复位的完整链条是否按设计运行。这为功能安全认证提供了重要的实验数据。

By leveraging the error injection capability of the FCCU, developers can proactively simulate various error conditions during the development phase to validate the effectiveness of the system's error response mechanisms. This constitutes a critical practice in functional safety development. For example, the EIM (Error Injection Module) provided by the S32K3 serves as a key tool for validating the effectiveness of this interlock mechanism. Developers can proactively inject ECC errors into components like SRAM to simulate hardware failures, thereby observing whether the entire chain—from FCCU alarm to FS26 reset execution—operates as designed. This provides critical experimental data for functional safety certification.

4 结语 CONCLUSION

恩智浦 S32K3 中的 FCCU 模块代表了汽车微控制器功能安全的先进水平，其精妙的状态机设计和可配置的错误响应机制为汽车电子系统提供了坚实的可靠性基础。随着汽车电子电气架构向域控制和区域控制演进，FCCU 支持的功能安全特性将在确保新一代智能网联汽车安全方面发挥更加关键的作用。

The FCCU module in NXP's S32K3 represents the cutting edge of functional safety in automotive microcontrollers. Its sophisticated state machine design and configurable error response mechanisms provide a robust reliability foundation for automotive electronic systems. As automotive electronic architectures evolve toward domain and zone control, the functional safety features supported by the FCCU will play an increasingly critical role in ensuring the safety of next-generation intelligent connected vehicles.

对于开发者而言，深入理解 FCCU 模块的工作原理并合理配置其参数，是构建符合 ISO 26262 标准的安全关键系统的重要前提。恩智浦提供的完整开发生态进一步降低了这一过程的技术门槛，加速了安全关键应用的上市时间。

For developers, gaining a thorough understanding of how the FCCU module operates and properly configuring its parameters is a critical prerequisite for building safety-critical systems compliant with the ISO 26262 standard. NXP's comprehensive development ecosystem further lowers the technical barriers in this process, accelerating time-to-market for safety-critical applications.