



## Semper™ Flash：功能安全使能 针对汽车和工业系统

Sandeep Krishnegowda和Pritesh Mandaliya

### 简介

汽车和工业市场中的应用，越来越依赖电子系统来解决实时、复杂的问题，因此对各种关键应用的安全性的关注度明显提高。这些关键任务系统失效绝非想要的选择，因此要不惜一切代价避免失效的发生。在汽车行业中，ISO 26262安全标准对汽车安全系统的设计给出了要求，而IEC 61508安全标准则制定了工业控制系统的要求。本白皮书概述了赛普拉斯Semper NOR Flash解决方案中所集成的各种安全特性，通过这些特性可以简化系统级功能安全设计，从而使设计符合ISO 26262和IEC 61508标准。

### 什么是功能安全？

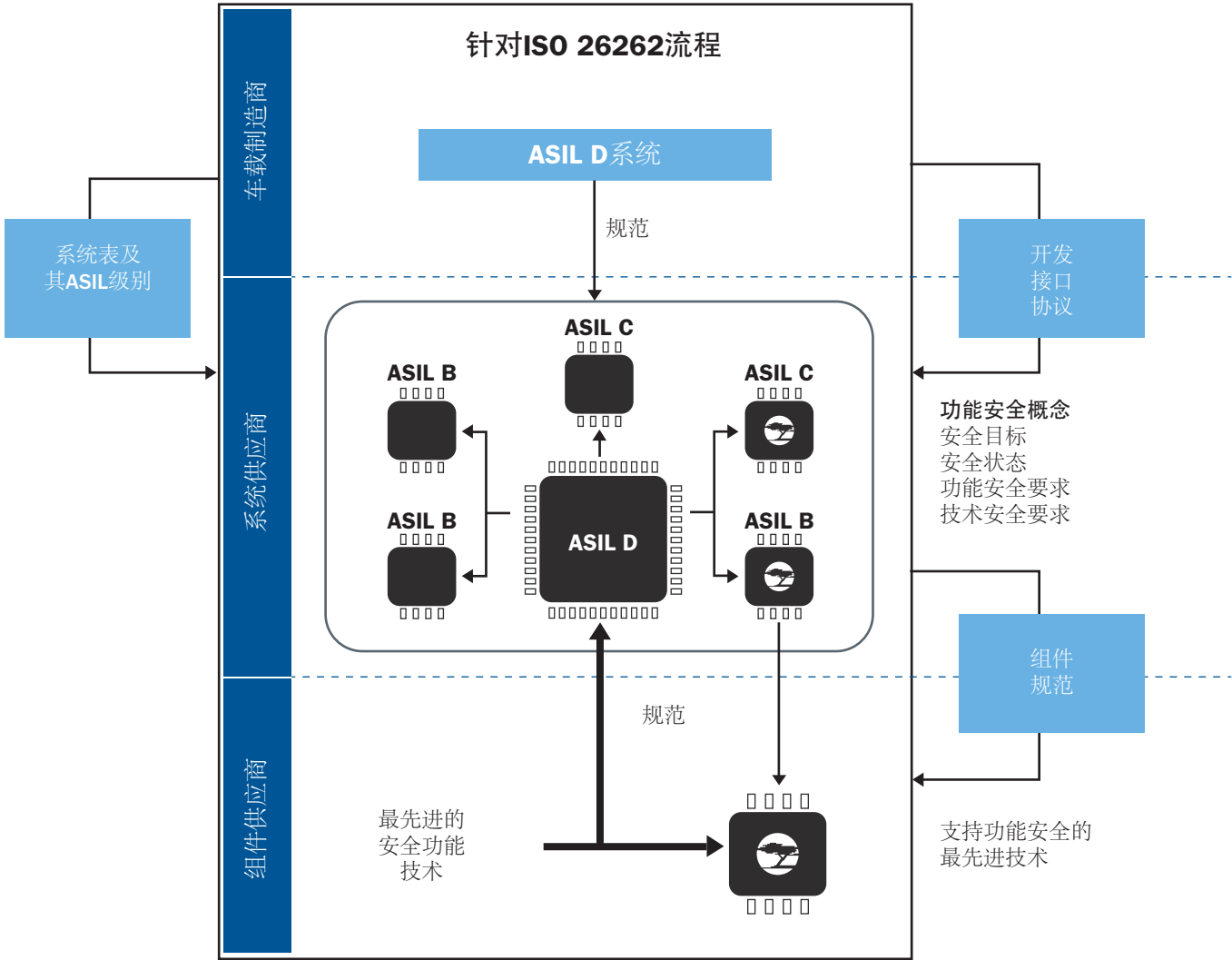
根据ISO 26262标准，功能安全被定义为：“不存在由电子电气系统的功能异常表现引起的危害导致的不合理风险”。在电子系统中，导致系统异常表现的故障原因可能是设计中存在的系统故障，或由软性错误引起的随机故障，或随时间推移的概率可靠性故障导致的随机故障。功能安全ISO 26262和IEC 61508标准对安全完整性等级进行了定义（如汽车系统的ASIL A ~ ASIL D，工业系统的SIL 1 ~ SIL 4），每个等级表示更高的安全等级和更少的失败可能性，如表1所示。同时，图1中的示例介绍了当前汽车系统中如何实现安全性，以及车辆制造商、系统供应商和组件供应商如何遵循安全性流程。

表1: 建议的安全完整性级别

工业标准 (IEC 61508)	
完整性级别	随机失效率
SIL 4	$\geq 10^{-9}$ 至 $< 10^{-8}$
SIL 3	$\geq 10^{-8}$ 至 $< 10^{-7}$
SIL 2	$\geq 10^{-7}$ 至 $< 10^{-6}$
SIL 1	$\geq 10^{-6}$ 至 $< 10^{-5}$

汽车标准 (ISO 26262)	
完整性级别	随机失效率
ASIL D	$< 10^{-8}$
ASIL C	$< 10^{-7}$
ASIL B	$< 10^{-7}$

图1：汽车系统中的安全实施



Semper NOR Flash ISO 26262 ASIL B功能安全合规性

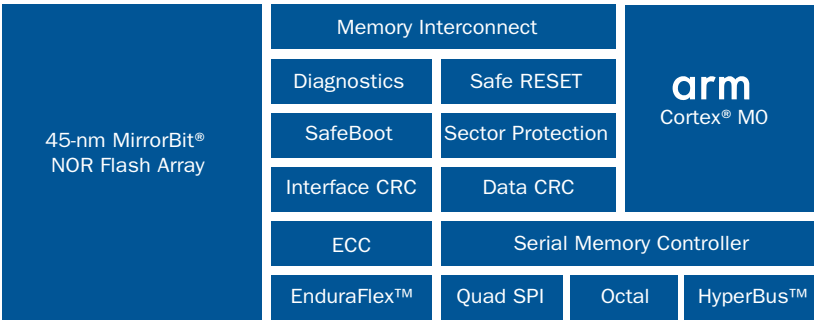
在安全关键应用（如ADAS）中，汽车应用使用了外部NOR Flash，用于存储系统上电或运行期间必须读取的关键代码、数据和图形映射。这些外部闪存解决方案的安全要求取决于安全关键应用中不同的使用。

下面是四个不同的外部闪存使用示例：

- 1. 存储和下载（SnD）：闪存内容在启动期间被复制到本地RAM中并被执行，而不需要访问闪存。
- 2. EPROM模拟：Flash用于存储安全关键数据
- 3. 运行期间连续读取：主机在安全关键操作期间从闪存中读取数据。
- 4. 代码执行：安全关键应用在运行期间直接从外部闪存执行。

Semper NOR Flash系列架构和设计可满足汽车行业用于构建故障保护嵌入式系统的ISO 26262功能安全标准（见图2）。该系列产品符合AEC-Q100汽车标准以及ASIL B功能安全标准，可在汽车和工业应用的极限温度（-40°C至+ 125°C）下提供卓越的耐久性（100万次存储周期）和25年的数据保持时间。

图2：Semper NOR Flash的架构框图



## Semper Flash的主要功能安全特性

### 1. 纠错码（ECC）

在存储器中可能会出现软错误或硬错误。一旦出现硬错误，便是永久性的。它们这些错误是由芯片缺陷、被干扰位或由于老化、振动或环境压力导致封装金属化而引起的。而软错误则是由带电粒子、辐射或宇宙射线引起的。当闪存存储器单元受此类错误影响时，读取数据将被破坏，并可能会影响应用的功能。Semper NOR Flash器件通过在存储器阵列编程期间生成嵌入式ECC来支持单错误纠正和双错误检测（SECCDED），另外，该ECC将用于读取操作期间发生的错误检测和纠正。

### 2. 数据CRC

Semper Flash器件中的数据CRC在用户定义的地址范围内执行循环冗余校验（CRC）计算。CRC流程将计算从起始地址到结束地址中所包含的数据的校验值，从而检测系统启动期间或每个用户命令中存在的任何错误。

### 3. 接口CRC

Semper NOR Flash器件是高频存储器，支持高达200 MHz的双倍数据速率。由于发送器、接收器或两者一起引起的噪声通道或错误，原始数据可能被破坏。因此，为了保持系统安全运行，主机和从机之间通信的最关键因素之一便是确保传输信息的完整性。Semper NOR Flash x8接口器件具有接口CRC，这是一种用于器件的错误检测码，可检测主机和存储器间在数据传输过程中所发生的意外故障。

### 4. SafeBoot（安全启动）— 启动失败恢复

大多数汽车和工业应用中使用了NOR Flash器件来存储启动期间所使用的代码。如果NOR Flash器件本身无法正确启动，则相应的应用也可能无法正确被初始化，或者一旦启动失败，Semper NOR Flash器件将保持忙碌状态，或通过状态寄存器报告启动失败。

### 5. 配置数据损坏

更新非易失性配置寄存器期间发生电源掉电或硬件复位，指的是用于配置器件非易失性的配置数据可能发生错误。Semper NOR Flash器件可以检测到被损配置并进入可以被访问的默认模式。

### 6. EnduraFlex™架构

所有闪存存储器都会受到物理降解的影响，甚至会引起器件故障。一些汽车应用需要Flash器件具有高耐久性和长期保存特性，较低的数据保留或耐久性可能会影响系统功能。赛普拉斯的EnduraFlex™架构通过将Semper Flash器件划分为多个分区来优化系统设计，可独立配置这些分区，从而实现高耐久性和长期保存特性。对于频繁进行数据写入操作，512 Mb容量的分区部件提供高达128万次编程擦除周期，1 Gb容量的部件则提供256万次周期。对于代码和配置存储，可以将分区的数据保持时间配置为25年。

### 7. 高级扇区保护（ASP）

如果主机在编程/擦除操作中所发送的位由于噪声信道或随机故障而发生改变，则闪存器件可能对不正确的扇区执行操作，从而导致系统操作失败。Semper NOR Flash器件提供高级扇区保护（ASP）功能，可避免对任何扇区执行意外的编程和擦除操作。

### 8. 扇区擦除掉电检测

在通用的Flash器件中，如果在系统执行扇区擦除操作时发生电源故障，系统不知道相应扇区擦除操作时的当前状态。Semper NOR Flash器件为每个扇区执行一个擦除掉电指示，以标识在扇区擦除期间发生断电事件。

### 9. 安全复位

在Flash器件停止响应主机/系统的情况下，赛普拉斯Semper Flash器件中的安全复位功能通过使用现有的SPI信号，包括芯片选择（CS#）、串行时钟（CK）和串行输入（SI / DQ0）来启动SPI Flash硬件复位，而不依赖于器件的操作状态。此功能为所有封装类型（包括8 pin封装）提供了硬件复位机制。

## 10. 诊断功能

Semper NOR Flash支持以下诊断功能，可为系统提供关键的嵌入式操作状态。

- 编程错误状态标志报告编程操作失败
- 编程操作挂起状态标志用于指示编程操作是否被挂起
- 擦除错误状态标志报告擦除操作失败。它表明最后一次擦除操作发生了错误。
- 扇区擦除成功/失败状态标志指示扇区上的擦除操作是否成功完成
- 擦除操作挂起状态标志用于指示擦除操作是否被挂起
- 存储器阵列数据crc挂起状态标志用于确定器件何时处于存储器阵列数据crc挂起模式
- 存储器阵列数据crc中止状态标志表示存储器阵列数据crc操作已被中止
- 器件就绪/繁忙状态表示器件正在执行嵌入式操作、发生某个故障情况还是处于待机模式以准备接收新的数据操作

## 赛普拉斯汽车功能安全保证程序

赛普拉斯有15年以上的参与汽车功能安全领域的经验，并且是业界领先的功能安全汽车产品（MCU，模拟PMIC，存储器和软件）供应商之一。在功能安全方面，赛普拉斯是关键零部件供应商。该行业中各供应商之间的关系通过开发接口协议（DIA）进行管理，该协议可确保从开发伊始就集成了安全标准。赛普拉斯的专家队伍将从项目的开始到结束整个过程均负责定义和维护这些标准。这批专家可确保我们的产品符合ISO 26262安全标准。他们审查并分析产品功能和客户反馈，从而确保产品符合安全标准和所需等级水平，同时还确保了赛普拉斯能够凭借其技术始终处于领先地位。

赛普拉斯的业务流程还得到了专门独立功能安全审查委员会的支持，该委员会确认了在设计过程中所开发的可交付产品的执行情况。赛普拉斯的软件质量保证部门可确保在软件开发过程中所有可交付产品都符合标准。汽车软件开发过程已通过TÜV SÜD认证，从而确保符合ISO 26262标准。

## 功能安全文档

赛普拉斯会根据要求向符合条件的客户提供符合ISO 26262标准的功能安全文档。联系您当地的赛普拉斯销售代表或创建支持案例，以获取以下Semper NOR Flash器件功能安全文档：

- 器件安全手册
  - 产品安全架构和假定使用情况
- 安全分析报告概述
  - FIT率和FMEDA结果总结
- 详细的安全分析报告
  - 完整的解析到块级别的安全分析，安全机制和诊断范围等内容

## 总结

- 由于对电子元件依赖性的增加以及为了确保驾驶员的安全，汽车应用需要具备功能安全。
- 汽车行业广泛采用了ISO 26262合规性。
- 凭借安全设计部分提到的功能安全机制和附加功能，使赛普拉斯的Semper NOR Flash器件在目前汽车和工业系统中运行稳健可靠。
- 赛普拉斯了解其产品的功能安全要求，并致力于设计符合ISO 26262和其他主要行业标准的下一代汽车NOR Flash器件。

可访问以下链接了解更多有关Semper NOR Flash系列功能安全特性的信息：

<http://www.cypress.com/semper>.

赛普拉斯半导体公司

198 Champion Court, San Jose CA 95134

电话 +1 408.943.2600 传真 +1 408.943.6848

免费电话 +1 800.858.1810（仅限美国）按“1”与您当地的销售代表联系

© 赛普拉斯半导体公司。保留所有权利。所有其他商标均归其各自所有者所有。

002-25065 \*\*

