



简化安全关键型应用开发的单片机

Microchip Technology Inc.

单片机业务部业务拓展经理

Maria Teresa Jacob

道路车辆的电气化、自动驾驶能力的进步以及工业自动化的普及，加大了对高可靠性系统的需求。由于这些应用涉及可能影响人类生命和财产的安全关键型功能，严格遵守国际功能安全标准至关重要。安全关键型任务的示例包括：监测电池是否过热、在气体泄漏时关闭阀门、展开安全气囊以及在机器人活动的工业区域检测人员。以下是工程师们面临的三个常见挑战及应对技巧。

纷繁的选项选择往往使得挑选合适的器件成为一项艰巨的任务。选择那些按照国际功能安全标准设计的组件是一个良好的开端。这确保了器件的设计实现了在安全需求、设计实现以及验证与确认过程之间的高度可追溯性。您通常可以获得与安全相关的文档，其中包含安全案例、各种故障分析报告以及关于功能安全推荐使用的手册。避免过度设计或选择现有最先进的器件，这可能会增加开发时间和成本，而应选择最简单的选项以保持复杂度可控。

设计安全的系统通常需要在硬件或软件中加入诊断机制，以便在故障最早出现时进行检测。然而，这可能是一项复杂的任务。例如，开发用于检测单片机（MCU）的 CPU 故障或内存损坏的诊断程序，需要对器件的架构和运行有深入的理解。认识到这一挑战后，许多制造商提供具备内置硬件特性的 MCU，例如以锁步方式运行的双 CPU、CRC（循环冗余校验）扫描模块以及适用于存储器的 ECC（纠错码）机制。在设计软件诊断程序以测试硬件模块是否按预期工作时，能够向内置安全特性注入故障的能力也非常有益。Microchip 的 AVR® SD MCU 就是这样一款器件，它在硬件中提供多种错误注入机制，可通过设置寄存器中的特定位来启用。

工程师面临的第三个挑战是更新现有系统以达到特定的功能安全标准。这需要在从头开始设计系统与尝试将安全措施改造到原始设计之间做出抉择。选择可能高度依赖于具体应用，但推荐的安全实践是重新设计。这确保了项目开发以安全为首要考虑，使工程师免于在设计过程后期遭遇棘手的意外情况。另一种替代方案是通过将安全关键型功能卸载到另一个器件上来简化设计。例如，如果系统中的主处理器正在执行多项功能，那么部分或全部安全关键型任务可以转移到一台复杂性较低的 MCU 上。

配合专用的安全软件框架，Microchip 的 AVR SD MCU 是首款入门级同类产品——价格低廉——专为符合 ISO 26262（ASIL C）和 IEC 61508（SIL 2）标准而设计。借助 AVR SD 系列，设计人员可以显著缩短开发时间，并最大程度地降低系统和认证成本。

选择那些按照功能安全标准制造、提供多种内置诊断机制和错误注入能力的组件，将帮助设计人员开发安全关键型系统时更为从容。