助力采用 MCU 的自主系统实现自主安全性

Microchip Technology Inc.
资深技术顾问
Bob Martin

人工智能（AI）和机器学习（ML）技术在自主性日益增强的系统中的应用越来越普遍，这将提高各行各业对更智能的安全系统的要求。关注重点已经从节约成本转向给用户带来便利性和安全性。这需要一个完整的功能安全（FuSa）层，其中包括安全协处理器与可信的输入/输出控制器，两者协同工作来保护系统。单片机（MCU）为实现这些安全协处理器提供了低成本的解决方案，是当今新一代自主系统的核心。

自主安全功能和规范

安全协处理器可以执行部署的 ML 模型，这种模型用于接收视频、音频、环境和操作员数据等外部数据流，而在某些情况下，也可以同时接收所有这些数据流。这些数据流必须具有固有的可信度。

同样重要的是，安全协处理器必须信任它们为电机、继电器、指示器和其他执行器产生的输出状态的真实再现。如果发生故障，主处理器也应该能够依靠这些输入/输出（边带）控制器快速做出明智的决策。

使用 MCU 作为安全协处理器

在全面的开发生态系统的支持下，8 位和 32 位 MCU 主要用于四大功能安全领域，业内为此制定了下列工业标准规范：

- ISO 26262：汽车安全完整性等级（ASIL），适用于汽车应用
- IEC 61508：安全完整性等级（SIL），适用于工业应用
- IEC 60730：家用电器功能安全标准
- IEC 60730：医疗设备功能安全标准

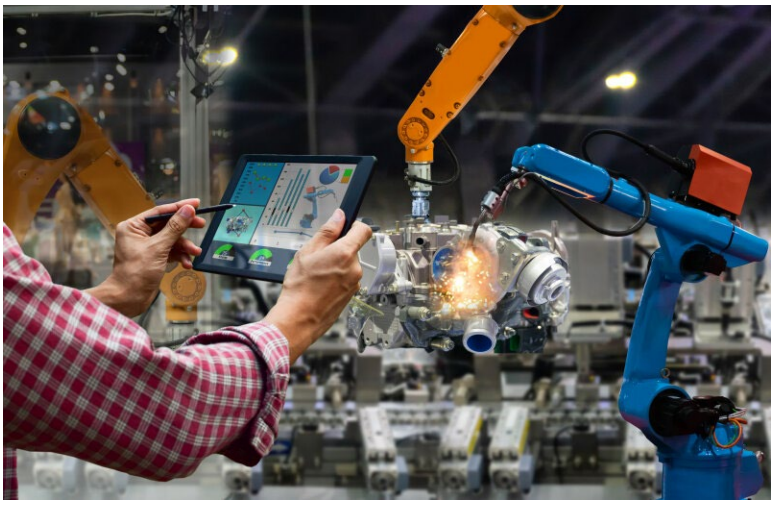

图 1. 工业机器人正在焊接大型重物

开发工具生态系统有两个重要的后端要求。第一个要求是在开发过程中以及在编译成机器码过程中采用稳健的编码。使用功能安全编译器可满足此要求，这些编译器通过 TÜV SÜD（一家国际认可的测试机构）等组织获得 ISO 或 IEC 功能安全标准认证。第二个后端功能是详细分析在一个典型的测试周期中，哪些代码被执行，哪些代码被遗漏。这需要一个代码覆盖率分析插件。

自主安全功能的工作原理

与外界的主要交互是通过硬件层实现的，首先需要支持 FuSa 的 MCU（位于边缘）提供的直接传感器和执行器接口。请参见下面的图 2。

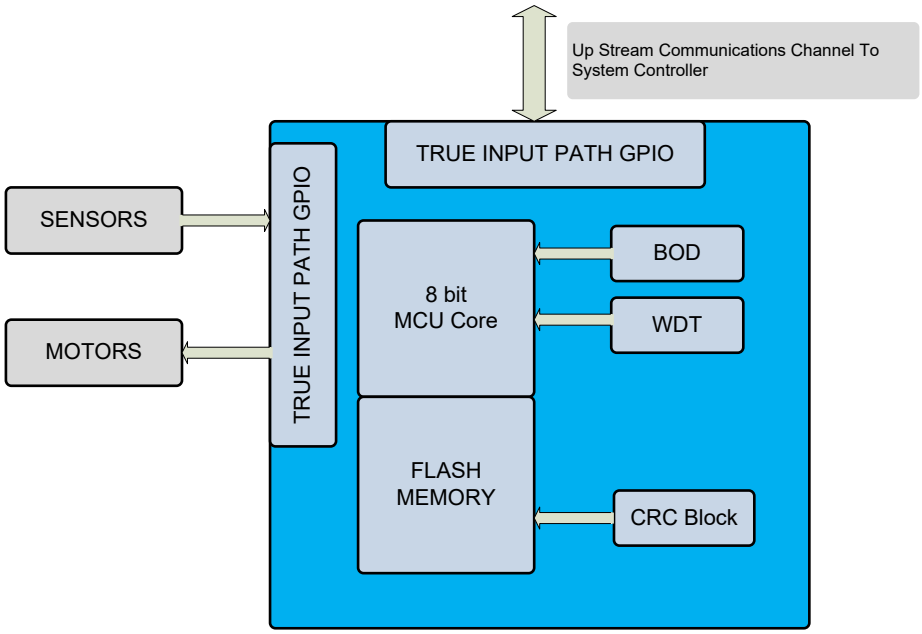

图 2. 8 位单片机的自主安全功能

主要功能包括：

欠压检测（BOD）

拥有理想电源的工作环境十分少见。微波炉和激光打印机会导致灯光闪烁，大型电动工具会触发断路器。自主系统必须提前预知其电源要发生故障，从而可以启用备用电源，或者设置关键数据和输出状态以确保干净的掉电。

这些 MCU 中的 BOD 电路可以持续监视电源电压，并以两种特定方式对下降的电压作出反应。首先，当电压超过某个可选阈值时，电压监视（VLM）功能将触发中断，从而在超过实际 BOD 电压阈值之前立即执行紧急关断任务。超过 BOD 电压后，设备将保持在复位状态，直到消除此条件。同时，也可以确定复位事件的原因，以确保采取适当的恢复策略，这可能与第一次的上电周期不同。

窗口化看门狗定时器

现代 MCU 使用看门狗定时器作为故障恢复机制，旨在终止无限循环（又称“自旋锁”）条件，这种条件除了采取严厉的措施外没有任何解决方法。早期版本设置了以秒或毫秒为单位的超时阈值，然后需要在达到此阈值之前对运行代码进行某种类型的“刺激”。确认后，超时阈值重置，倒计时重新开始。懒惰的程序员使用周期性中断服务程序来更新定时器，但是即使系统的其他部分卡在某个无限循环中，这些程序仍会自行继续执行，不会通过系统复位来解决这种情况。

窗口看门狗定时器通过允许指定看门狗服务窗口解决了部分问题。这样一来，看门狗定时器的服务速度不能太慢，也不能太快。这使得依赖已知执行时间短于最大阈值的代码变得更加困难。

循环冗余校验（CRC）代码扫描

CRC 代码扫描外设可确保已编程代码映像的完整性。它比单纯的校验和更加强大，因为校验和很容易被数学操作欺骗。可将特定的 MCU 硬件模块配置为在程序存储器的自举程序部分、应用程序部分或整个闪存阵列上运行扫描。然后，外设会将其 CRC 结果与附加在指定代码空间末尾的正确校验和进行比较。如果这两个 16 位数字匹配，则证明代码空间未遭到修改。可将匹配失败配置为产生不可屏蔽中断，以进一步处理该问题。

实际输入路径通用输入/输出（GPIO）外设

在早期的 MCU 中，如果将 GPIO 引脚配置为输出，验证引脚电压（即 5V）与控制位值（即 1）相匹配的惟一方法是使用配置为输入的单独 GPIO 引脚来读取电压。配置为输出的 GPIO 引脚不能回读实际电压，而只能回读写入的值；因此，“输入”值始终保持一致。

实际输入路径 GPIO 单元可以提供到离散的内部输入寄存器的独立电气路径，从而反映引脚上设置的实际电平。虽然该电平只能以逻辑 1 或逻辑 0 的方式读取，但它仍可提供足够的反馈来验证写入输出控制寄存器的内容。这两个值应始终保持一致。如果两者之间存在差异，则表明该特定 GPIO 引脚上存在短路或开路情况，需要适当的处理。

具有这些功能的 MCU 可为完整的 FuSa 层奠定基础。随着基于 AI/ML 的自动化将关注重点从系统生产和维护成本节约转向用户体验的安全性和便利性，FuSa 层的重要性将不断提高。

###