*Technical White Paper*

# *减轻安全认证系统开发的痛苦*

*Pekka Varis*

**摘要**

本白皮书以驾驶员监控系统 (DMS) 为例，介绍了在德州仪器 (TI) AM62A 器件和 Green Hills® Software 的 INTEGRITY® 实时操作系统 (RTOS) 的基础上构建安全认证系统所需的基本要素。

## 内容



## 插图清单



## 商标





English Document: SPRAD97

# 1 什么是 DMS？为什么它必须安全？

驾驶员监控系统 (DMS) 是车内感应系统的子集，车内感应系统可以使用多种传感器之一来收集有关车辆内部情况的信息。虽然大多数情况下会使用红外摄像头，但有些公司使用其他方法，例如雷达传感器或电阻器垫等更简单的技术（用于检测乘客座位上是否有乘员或行李）。DMS 于 2006 年左右首次推出，由欧盟（法规 2019/2144）定义，其中规定：驾驶员疲劳驾驶和注意力警告系统是指通过车辆系统分析评估驾驶员警觉性并在需要时向驾驶员发出警告的系统。

从那时起，在辅助驾驶和自动驾驶的行业趋势推动下，人们在 DMS 上投入了大量精力，使得 DMS 不仅可以检测和监控驾驶员分心（和/或疲劳驾驶），而且还可以涵盖眼睛注视、甚至驾驶员情绪等方面，以确保驾驶员准备好在必要时接管车辆控制。因此，特别是对于更高级别的自动驾驶（是指 SAE 3 级及更高级别），了解驾驶员所处的状态对于车辆的安全至关重要。

DMS 的供应商必须解决各种问题，以确保产品符合法规要求和市场期望：

- **光学**：光学系统必须能够在各种光照条件下工作，并具有高动态范围
- **硬件**：处理平台需要提供足够的计算能力，同时满足功能安全和功效等次要要求
- **软件**：软件栈需要通过高效地使用硬件资源来满足实时要求，并对硬件资源进行补充以实现功能安全措施。
- **经济性**：整个系统需要满足严格的汽车成本要求，同时必须具有高度的适应性和可扩展性，以覆盖各种车辆平台

由于这些领域之间存在明显的相互依赖关系，因此选择正确的硬件和软件平台可能颇具挑战性。

# 2 视觉计算硬件平台

AM62Ax 面向具有视觉和红外传感功能的独立 DMS，是 Sitara™ 新增的汽车和工业级嵌入式异构 Arm® 处理器产品系列，具有嵌入式深度学习 (DL)、视频和视觉处理加速、显示接口以及广泛的汽车外设和网络选项。AM62Ax 专为一系列成本敏感型汽车应用（包括驾驶员和车内监控系统与下一代电子后视镜系统）以及工厂自动化、楼宇自动化和其他市场中的广泛工业应用而构建。AM62Ax 成本经过优化，能够以业界卓越的功耗/性能比为传统和深度学习推理算法提供高性能计算，并具有很高的系统集成度，从而使支持独立电子控制单元 (ECU) 中多种传感器模式的高级汽车平台实现可扩展性和更低的成本。

A62Ax 的主处理器内核为多达四个运行频率为 1.4GHz 的 64 位 Arm® Cortex®-A53 内核、一个具有图像信号处理器 (ISP) 和多个视觉辅助加速器的视觉处理加速器 (VPAC)、多个深度学习 (DL) 和视频加速器、一个 Cortex®-R5F MCU 通道内核和一个 Cortex®-R5F 器件管理内核 (图 2-1)。Cortex-A53 内核提供了 Linux 应用所需的强大计算元件，以及驾驶员监控等基于视觉计算的传统算法的实现。TI 的第七代 ISP 以现有出色的 ISP 为基础，能够灵活地处理更广泛的传感器套件（包括 RGB-IR），支持更高的位深度，并且具有面向分析应用的特性。主加速器内核是 64 位 *C7x* DSP，具有标量和 256 位矢量功能，以及用于深度学习推理的专用矩阵乘法加速器 (MMA)，在典型的汽车最坏情况结温 125°C 下运行时，可在业界超低的功耗范围内实现高达 2TOPS 的性能。

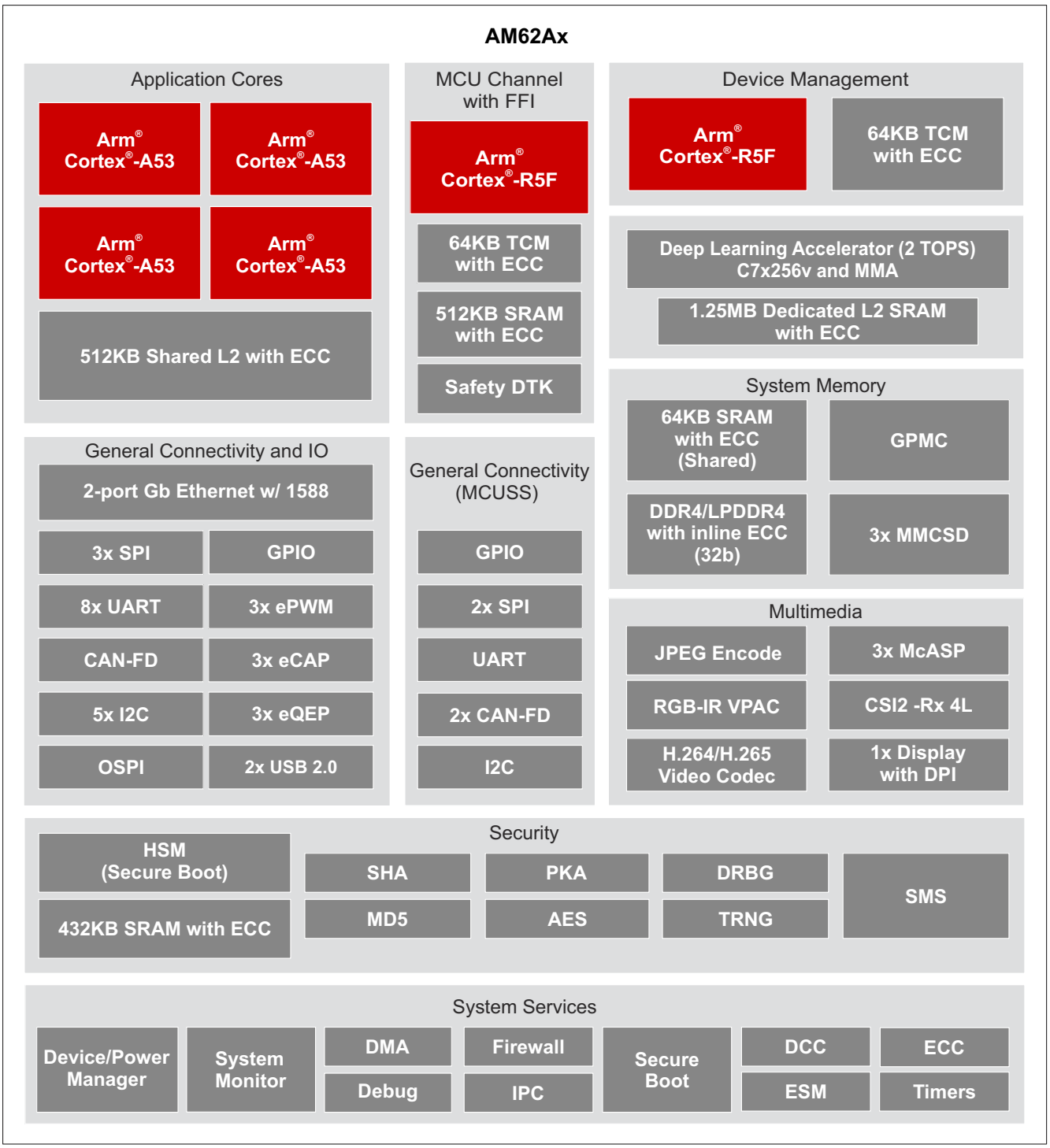


**图 2-1. 德州仪器 (TI) AM62Ax 的功能方框图**

# 3 面向安全关键型应用

AM62Ax 是符合 ASIL-B/SIL-2 ( 汽车安全完整性等级 B/安全完整性等级 2 ) 功能安全标准的器件，支持多种功能安全特性，例如集成 Cortex-R5F MCU 的专用安全域 ( 称为 MCU 域 ) 。该器件提供了防止干扰和隔离特性，以将 MCU 域与主域隔离开来。AM62Ax 元件面向通用功能安全应用。开发是根据汽车规范 ISO 26262-10:2018 等作为独立安全元素 (SEooC) 进行的，安全设备的设计人员可以参考所购组件的评估报告，并且必须遵守 SEooC 安全手册中提供的安全使用假设 (AoU) 和指南。该方法还用于满足工业规范 IEC 61508 在半导体级别的相关要求。

AM62Ax 实现了 ASIL-D/SIL-3 的系统完整性，并包含足够的功能安全机制，以满足 ASIL-B/SIL-2 对整个设备的随机故障完整性要求。Cortex R5 MCU 通道可用于提供 CPU 内核和相关外设，以监控驾驶员监控系统等主要功能，并在检测到故障时将系统转换到安全状态。AM62Ax 器件的目标是在整个设备中实现 90%- 99% (SIL-2) 的安全失效分数 (SFF)和 90%- 99% (ASIL-B) 的单点故障指标 (SPFM)。MCU 域包括 I2C、SPI、UART 和 GPIO 等专用外设，这些外设由 MCU 域内的独立电压域供电。此器件包含一个错误信令模块 (ESM)，该模块从不同的器件域中收集错误标志。当器件通过 ESM 报告故障时，这将被视为一个故障检测状态。如果系统处于故障检测状态，软件可能会在违反安全目标之前尝试从故障中恢复。

## 4 安全操作系统是安全软件的基础

一般来说，Green Hills Software INTEGRITY RTOS 等 RTOS（实时操作系统）负责调度任务、提供同步和通信机制，以及用于配置周期性事件（计时器）和其他资源分配的对象。因此，RTOS 是整个嵌入式系统应用的基础。此外，在用于安全关键型应用时，RTOS 需要遵循相应的安全标准。这意味着什么？

功能安全基于两个核心要素：故障避免和故障控制。故障避免处理由系统安装前产生的故障引起的系统故障。这些在标准中通过指定目标外的开发流程来解决。相应的证书保证安全元件适合使用并且没有系统错误。

图 4-1 是专为在安全关键型应用中使用而构建的，因此它是根据安全标准开发来解决故障避免问题的。它通过了 ISO26262 ASIL D [1]、IEC61508 SIL 3 [2] 和 EN50128 SW SIL 4 [3] 认证。借助这些安全标准，可以对单个组件（如 RTOS）进行认证/评估，将其视为独立安全元素。

除此之外，故障控制还必须处理潜在的运行时错误，例如辐射引起的软错误。这些错误是由系统安装后产生的故障引起的，要加以解决，不仅涉及硬件，还需要考虑目标上的软件。这些标准描述了应采用的诊断和技术，包括相应的诊断覆盖范围：低 (60%)、中 (90%) 或高 (>=99%)。所需的安全完整性等级（对于 ISO26262，为 SIL、ASIL）越高，要采用的开发过程（故障避免）和诊断覆盖（故障控制）就越严格。对于 ASIL C 和 D，需要高诊断覆盖率。

如果经过认证的软件安全层实现了高诊断覆盖率技术，例如时间监视、期限监控、序列指向、安全存储、不变 RAM 保护、MMU 页表检查和安全进程间通信，可以为设备的安全设计人员增加很多价值。Green Hills Software 结合 INTEGRITY 分离内核提供了这些功能。

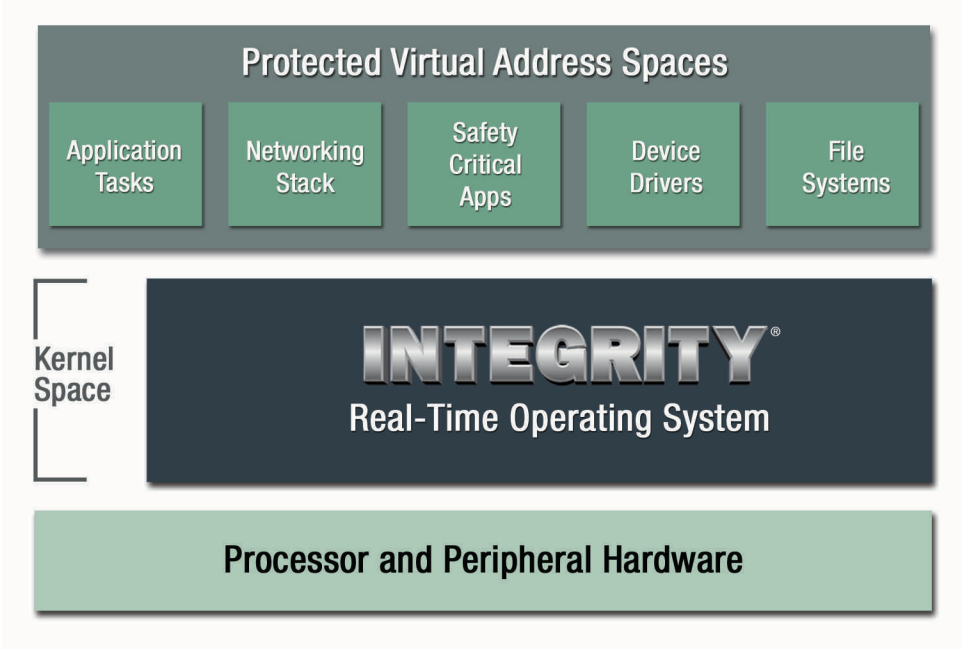


**图 4-1. Green Hills Software 的 INTEGRITY RTOS**

## 5 防止干扰

IEC 61508 明确规定了不干扰是指单个计算机系统上托管的软件元素之间可以*独立执行*。*独立执行*一词意味着元素不会对彼此的执行行为产生不利影响，从而可能出现危险的故障。独立执行应当在空间和时间两个领域上实现并得到证明。所有这些都可以通过使用经过认证的分离内核来实现，例如 Green Hills Software 的 INTEGRITY RTOS。INTEGRITY 分离内核可以严格分离内存、CPU 时间和其他资源。这种分离能力已根据上述安全标准获得了认证。

这种分离有很多好处：您可以在同一系统上并排运行质量管控应用分区和安全关键软件分区。这意味着在更新质量管控应用分区时，无需对设备进行重新认证。此外，以太网、TCP/IP 或 CAN 堆栈等未经认证的标准通信可以从非关键分区运行，安全关键型应用通过“黑色通道”将数据传递到关键分区中的安全应用。黑色通道通信原则是一种常见的分层方法，其中安全功能不依赖于通信介质来实现指定的内容交付。安全协议负责执行所有必要的安全检查，以实现对从传感器到计算的通信进行端到端保护。最终结果是要认证的软件以及认证频率都有所减少，这显著节省了开发成本，并且甚至允许频繁更新质量管控应用，而不会影响所需的安全级别。

## 6 启用安全对称多处理 (SMP)

RTOS（调度）也将常规同质多核 CPU 视为多核，例如在不同内核上同时运行多个任务。在考虑防止关键和非关键软件分区之间产生干扰时，必须考虑一个新的方面：内核。内核共享交叉开关、高速缓存和内存等资源，因此可能会相互干扰。经过认证的 INTEGRITY RTOS 软件包（分离内核、安全层）可以防止内核干扰，同时可以利用软件锁步功能检测软错误并提供高诊断覆盖率。对于软件锁步，使用不同算法执行相同计算的安全关键任务由操作系统在不同内核上并行调度。然后，安全层使得可以定义同步点来检查（中间）结果的一致性，从而检测安全相关故障。

## 7 安全 BSP – 在硬件和软件之间架起桥梁

板级支持包 (BSP) 提供应用程序与实际硬件和设备之间的接口。因此，BSP 充当硬件抽象层。如果在安全系统中使用 BSP，则需要根据安全标准设计 BSP，以满足故障避免需求，与上述针对 RTOS 的情况类似。但是，BSP 通常不会设计为独立使用，因为 BSP 是针对特定硬件和特定用例而设计的，所以 BSP 必须在上下文中进行认证。这意味着，BSP 附带上下文证书和安全手册。此外，BSP 必须解决故障控制问题，因为 BSP 驱动程序需要有适当的措施来缓解系统和随机硬件及软件错误。如上所述，BSP 需要充分利用有助于降低风险的硬件功能，这与 AM62Ax 提供的功能类似。

## 8 总结

在开发复杂系统时，必须考虑许多方面：性能、质量、（长期）供货情况、可维护性、功能和成本等。具体而言，当系统发生的故障可能危及人类的福祉、健康或生命时，安全必须是第一要务。为了解决这一问题，Green Hills Software 和德州仪器 (TI) 为客户提供集成设计，从而帮助客户缩短开发时间、降低成本、减少工作量并缩短产品上市时间。此外，使用与 TI 的 Sitara AM62Ax 和 Green Hills Software 的 INTEGRITY RTOS 类似的已知良好构建块不仅可以省去获得系统认证的麻烦，而且该设计还可以拯救生命。

## 9 参考


- ISO 标准，*ISO 26262:2018，道路车辆 – 功能安全，第 1-10 部分*。
- IEC，*IEC 61508:2010，电气/电子/可编程电子安全相关系统的功能安全，第 1-7 部分*。
- 欧洲标准，*EN 50128:2011，铁路应用 - 通信、信号和处理系统 - 铁路控制和保护系统软件*。

# 重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265