Technical White Paper Easing the Pain of Safety Certified System Development



Pekka Varis

ABSTRACT

This white paper uses the example of a driver monitoring system (DMS) to explain the fundamental elements required to build a safety certifiable system based on Texas Instruments AM62A device and Green Hills[®] Software's INTEGRITY[®] real-time operating system (RTOS).

Table of Contents

1 What is a DMS and Why Does it Have to be Safe?	2
2 Hardware Platform for Vision Computing	2
3 Targeting Safety-Critical Applications	
4 Safety OS as a Foundation for Safe Software	
5 Freedom from Interference	6
6 Enabling Safe Symmetric Multi-Processing (SMP)	6
7 Safety BSP – Bridging the Gap Between Hardware and Software	
8 Summary	
9 Reference	

List of Figures

Figure 2-1. Functional Block Diagram of the Texas Instruments AM62Ax	3
Figure 4-1. INTEGRITY RTOS from Green Hills Software	5

Trademarks

Sitara[™] is a trademark of Texas Instruments.

Green Hills® and INTEGRITY® are registered trademarks of Green Hills Software.

 $\mbox{Arm}^{\mbox{$\mathbb{R}$}}$ and $\mbox{Cortex}^{\mbox{$\mathbb{R}$}}$ are registered trademarks of Arm Limited.

All trademarks are the property of their respective owners.

1



1 What is a DMS and Why Does it Have to be Safe?

Driver Monitoring Systems (DMS) are subset of so-called interior sensing systems which can use one of several sensor types to gather information about what is going on inside a vehicle. While in most cases infrared cameras are used, there are companies using other methods, for example, radar sensors or even simpler technologies like resistor-mats (to detect whether the passenger seat is occupied by a person or a bag). DMS were first introduced around 2006 and are defined by the European Union (regulation 2019/2144) which states: Driver drowsiness and attention warning means a system that assesses the driver's alertness through vehicle systems analysis and warns the driver if needed.

Since then, predominantly driven by the industry trend of driver assisted and autonomous driving, a lot of effort has been put into DMS to not only detect and monitor driver distraction (and or drowsiness), but also cover aspects like eye-gaze and even driver emotions to make sure the driver is ready to take over vehicle controls when necessary. Therefore, specifically for higher levels of automated driving – referring to SAE Level 3 and higher – knowing the state the driver is in, is vital for the safety of the vehicle.

Suppliers of DMS have to tackle various problems to make sure the product meets both regulations and market expectations:

- Optics: the optical system has to work under various lighting conditions, with high dynamic range
- **Hardware**: the processing platform needs to provide sufficient compute power while at the same time fulfilling secondary requirements like functional safety and power efficiency
- **Software**: the software stack needs to fulfill real-time requirements by efficiently using the hardware resources and complement them for functional safety measures.
- **Economics**: the overall system needs to meet stringent automotive cost requirements and at the same time must be highly adaptable and scalable to cover various vehicle platforms

With the obvious interdependencies between these areas choosing the correct hardware and software platform can be a challenging task.

2 Hardware Platform for Vision Computing

AM62Ax, which is targeted towards stand-alone DMS with vision and IR based sensing, is an extension of the Sitara[™] automotive- and industrial grade family of embedded heterogeneous Arm® processors with embedded Deep Learning (DL), Video and Vision Processing acceleration, display interface and extensive automotive peripheral and networking options. AM62Ax is built for a set of cost-sensitive automotive applications including driver and in-cabin monitoring systems, next generation of eMirror system, as well as a broad set of industrial applications in Factory Automation, Building Automation, and other markets. The cost optimized AM62Ax provides high-performance compute for both traditional and deep learning inference-based algorithms at industry leading power/performance ratios with a high level of system integration to enable scalability and lower costs for advanced automotive platforms supporting multiple sensor modalities in stand-alone Electronic Control Units (ECUs).

Main processor cores of the A62Ax are up to four 64-bit Arm[®] Cortex[®]-A53 cores running at 1.4GHz, a Vision Processing Accelerator (VPAC) with Image Signal Processor (ISP) and multiple vision assist accelerators, Deep Learning (DL) and video accelerators, a Cortex®-R5F MCU Channel core and a Cortex®-R5F Device Management core (Figure 2-1). The Cortex- A53s provide the powerful computing elements necessary for Linux applications as well as the implementation of traditional vision computing based-algorithms such as driver monitoring. Building on the existing world-class ISP, TI's seventh generation ISP includes flexibility to process a broader sensor suite including RGB-InfraRed (RGB-IR), support for higher bit depth, and features targeting analytic applications. Main accelerator core is 64-bit *C7x* DSP with scalar and 256-bit vector capability, dedicated matrix multiply accelerator (MMA) for deep learning inference enabling performance up to 2 TOPS within the lowest power envelope in the industry when operating at the typical automotive worst case junction temperature of 125°C.

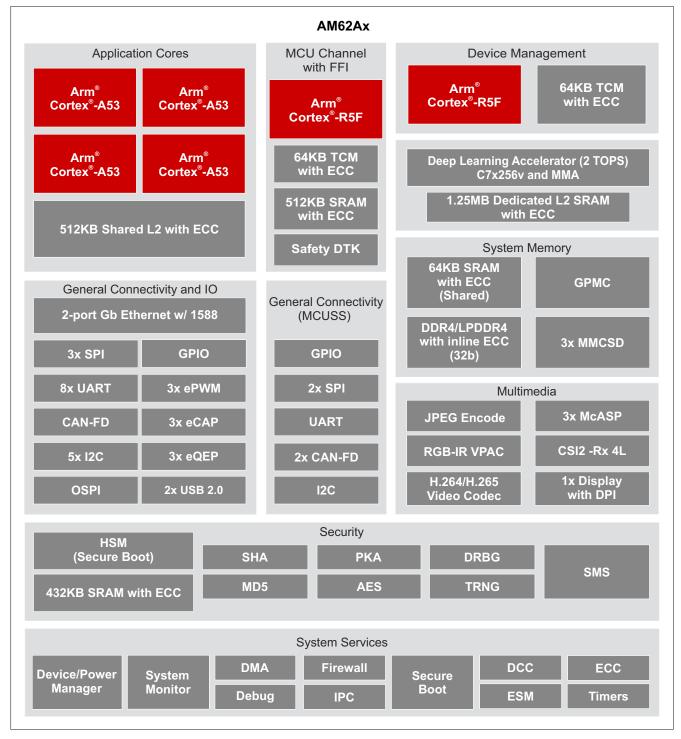


Figure 2-1. Functional Block Diagram of the Texas Instruments AM62Ax



3 Targeting Safety-Critical Applications

AM62Ax is ASIL-B/SIL-2 (Automotive Safety Integrity Level B/Safety Integrity Level 2) functional safety compliant device and supports several functional safety features such as a dedicated safety domain called the MCU domain which integrates the Cortex-R5F MCU. Freedom from interference and isolation features are provided to isolate the MCU domain from the main domain. The AM62Ax component is targeted at general-purpose functional safety applications. Development is done as Safety Element out of Context (SEooC) according to the automotive specification ISO 26262-10:2018, for example, the designer of the safety device can refer to the assessment report of the purchased component and must adhere to safety assumptions of use (AoU) and guidelines provided in the safety manual of the SEooC. This method is also used to meet the related requirements of the industrial specification IEC 61508 at the semiconductor level.

AM62Ax achieves systematic integrity of ASIL-D/SIL-3 and includes sufficient functional safety mechanisms for random fault integrity requirements of ASIL-B/SIL-2 for the entire device. The Cortex R5 MCU channel can be used to provide a CPU core and associated peripherals to monitor the primary function such as driver monitoring systems and transition the system to the safe state in the case a fault is detected. AM62Ax devices target a Safe Failure Fraction (SFF) of 90% - 99% (SIL-2) and a Single Point Fault Metric (SPFM) of 90-99% (ASIL-B) in the entire device. The MCU domain includes dedicated peripherals such as I2C, SPI, UART, and GPIOs that are supplied by an independent voltage domain within the MCU domain. The device contains an Error Signaling module (ESM) that collects error flags from the different device domains. When a fault is reported through the ESM, this is considered to be a fault detected state. If the system is in a fault detected state, software may attempt to recover from the fault before a safety goal is violated.



4 Safety OS as a Foundation for Safe Software

In general, an RTOS (real time operating system), like the Green Hills Software INTEGRITY RTOS, is in charge of scheduling tasks, providing synchronization and communication mechanisms, as well as objects to configure periodic events (timers) and other resource allocations. As such, the RTOS is the foundation for the whole application of the embedded system. Furthermore, the RTOS needs to follow the respective safety standards when used in a safety-critical application. What does that mean?

Functional safety is built on two pillars: fault avoidance and fault control. Fault avoidance deals with systematic failures, caused by faults originating before system installation. These are addressed in the standards by specifying a development process, off target. The corresponding certificate is the assurance that the safety element is suitable for use and free of systematic errors.

Figure 4-1 was specifically built for usage in a safety-critical applications, therefore it was developed according to the safety standards to address fault avoidance – it is certified according to ISO26262 ASIL D [1], IEC61508 SIL 3 [2] and EN50128 SW SIL 4 [3]. With these safety standards, it is possible to certify/assess a single component, such as an RTOS, treating it as a Safety Element out of Context.

Beyond this, fault control must deal with potential run-time errors for example, radiation-induced soft-errors. These errors are caused by faults originating after system installation and need to be addressed not only by the hardware but also by the software on the target. The standards describe diagnostics and techniques that shall be applied, including the corresponding diagnostic coverage: Low (60%), Medium (90%) or High (>=99%). The higher the required Safety Integrity Level (SIL, ASIL for ISO26262) the more rigid development process (fault avoidance) and diagnostic coverage (fault control) shall be applied. For ASIL C and D a high diagnostic coverage is required.

A certified software safety layer implementing high diagnostic coverage techniques such as time supervision, deadline monitoring, sequence pointing, safe storage, invariable RAM protection, MMU-page table checking, and safe inter process communication adds a lot of value to the safety designer of the device. Green Hills Software provides these capabilities in combination with the INTEGRITY Separation Kernel.

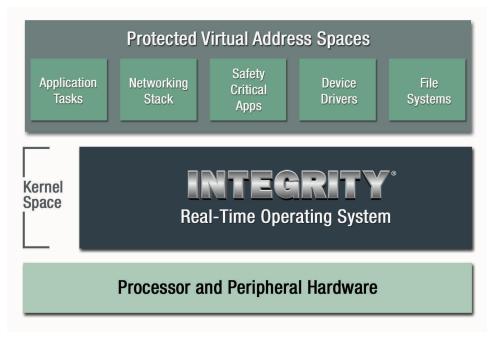


Figure 4-1. INTEGRITY RTOS from Green Hills Software

5



5 Freedom from Interference

IEC 61508 clearly expresses non-interference in terms of *independence of execution* between software elements, which are hosted on a single computer system. The term *independence of execution* means that elements do not adversely interfere with each others execution behavior such that a dangerous failure can occur. Independence of execution shall be achieved and demonstrated both in the spatial and temporal domains. All of this can be achieved by using a certified separation kernel, such as the INTEGRITY RTOS from Green Hills Software. INTEGRITY is a Separation Kernel that provides strict separation of memory, CPU time and other resources. This separation capability is certified according to the above-mentioned safety standard.

The benefits of this separation are numerous: you can run quality managed applications and safety critical software partitions side-by-side on the same system. This means that there is no need to re-certify the device when the quality managed application partitions are updated. Additionally standard non-certified communication such as Ethernet, TCP/IP, or CAN stacks can run from non-critical partitions with the safety critical application passing data over a "black channel" to a safety application in a critical partition. Black channel communication principle is common layered approach where the safety function does not rely on the communication medium for specified delivery of content. The safety protocol performs all the required safety checks for end-to-end protection of communication from sensor to compute. The net result is less software to certify less frequently, which is a significant development cost saving, even while allowing frequent updates to the quality managed application without compromising the required safety level.

6 Enabling Safe Symmetric Multi-Processing (SMP)

Regular homogenous multicore CPUs are also treated as multicore by the RTOS (scheduling), for example, running multiple tasks at the same time on different cores. When looking at freedom of interference between critical and non-critical software partitions a new dimension has to be considered: the cores. Cores share resources such as crossbars, cache and memory, and therefore can interfere with each other. The certified INTEGRITY RTOS package (separation kernel, safety layer) provides interference freedom of the cores and yet detects soft errors with high diagnostic coverage utilizing software lock-step. For the software lock-step, safety-critical tasks, performing identical calculations with differing algorithms, are scheduled in parallel on different cores by the OS. Then, the safety layer provides the possibility to define synchronization points to check for consistency of the (intermediate) results to detect safety-relevant faults.

7 Safety BSP – Bridging the Gap Between Hardware and Software

The Board Support Package (BSP) provides the interface between the application and the actual hardware and devices. As such BSP acts as a hardware abstraction layer. If the BSP is used in a safety system, BSP needs to be designed according to the safety standards to address fault avoidance, similar as mentioned above for the RTOS. But the BSP is usually not designed to be used out of context, as the BSP is designed for a certain hardware and a certain use-case, so BSP must be certified in-context. That means, a BSP comes with an in-context certificate and safety manual. Also, the BSP has to address fault control, in that the BSP drivers need to have appropriate measures to mitigate systematic and random hardware and software errors. The BSP needs to make good use of the hardware features that help mitigate risks, similar to the ones provided by the AM62Ax, as mentioned previously.

8 Summary

When developing a complex system many aspects must be taken into account: performance, quality, (long-term) availability, maintainability, features and cost for example. Specifically, when malfunctioning of a system can endanger well being, health or life of a human being, safety has to be the number one priority. To address this, Green Hills Software and Texas Instruments are providing an integrated design to their customers, reducing development time, cost, effort, and shortening the time to market. Also, using known-good building blocks similar to TI's Sitara AM62Ax and Green Hills Software's INTEGRITY RTOS does not only ease the pain of achieving system certification, but the design can also save lives.

9 Reference

- ISO Standards, ISO 26262:2018, Road Vehicles Functional Safety, Part 1-10.
- IEC, IEC 61508:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems, Parts 1-7.
- European Standards, EN 50128:2011, Railway Applications Communications, Signaling and Processing Systems Software for Railway Control and Protection Systems.

7

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES "AS IS" AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI's products are provided subject to TI's Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI's provision of these resources does not expand or otherwise alter TI's applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265 Copyright © 2023, Texas Instruments Incorporated