Leverage Jacinto™ 7 processors functional safety features for automotive designs

Yashwant Dutt
Engineering Manager
Jacinto™ Processors

Sam Visalli
Functional Safety Manager
Jacinto Processors

Mahmut Cifti
Systems Architect
Jacinto Processors

Dave Maples
General Manager Automotive Gateway and Infotainment
Jacinto Processors

Krishna Gopalakrishnan
Quality Manager
Embedded Processing

Texas Instruments

Introduction

The onset of autonomous driving, connected cars and electric vehicles/hybrid electric vehicles is changing paradigms in the automotive industry. Functional safety, which is central to these technologies, is no longer limited to traditional microcontrollers (MCUs) but needs to be supported in application processors as well. Engine control unit (ECU) compute requirements are increasing, which drives the need for more capable processors, hardware accelerators and digital signal processors (DSPs) to realize application needs. When you consider these parameters, it becomes more challenging for existing cores to process safety-related data and host mixed-criticality functions. Mixed-criticality systems run tasks with different criticality levels on a shared platform. In mixed-criticality systems, the timing of safety-critical tasks must be strictly guaranteed.

TI Jacinto™ 7 system-on-chip (SoC) family for automotive not only integrates an isolated ASIL-D safety MCU, but also provides higher levels of ASIL functional safety for all processing cores. In this white paper, we will review the safety diagnostics built into the Jacinto 7 SoC family, which includes TDA4x and DRA8x devices, the various isolation mechanisms available to support a mixed-criticality system, the software architecture, software product offerings, and how to construct a complete solution.

What is functional safety?

Functional safety is a system's ability to respond to malfunctioning behavior, whether that's a random failure, hardware failure or environmental stress, in a way that minimizes harm. As per ISO 26262, this simply means freedom from unacceptable risk. Although the concept of functional safety has been around in the automotive industry for quite some time, its adoption in application processors has been nascent. Keeping ASIL-D-compliant applications in mind, Jacinto 7 processors introduce safety concepts that were once limited to MCU-class devices to application processors.

These processors use hardware-assisted isolation techniques that enable mixed-criticality systems. The ability to seamlessly host both safety-critical and non-safety-critical tasks on one device helps reduce system cost.

The Jacinto 7 processor family provides a comprehensive safety solution involving both hardware and software. It is designed systematically for ASIL-D capability using a hardware development process that is certified by an independent functional safety assessor, like TÜV SÜD. It has diagnostics circuitry capable of detecting random faults and can be categorized into three broad categories:

- Fundamental diagnostics, which cover test circuitry for memory, clocks, power, core and interconnect.
- Hardware isolation capabilities like separate voltage/power/reset, firewalls, memory management units (MMUs) and microprocessors (MPUs), which simplify Freedom From Interference (FFI) in systems that support mixed-criticality operations (Ex: ASIL-B and ASIL-D).

- Application-specific hardware diagnostics such as freeze-frame detection.

The Jacinto 7 processor family will also be externally certified as a system element out of context to the ASIL level required by the targeted end equipment. Like the hardware development process, the software development process is also certified by an independent functional safety assessor, like TÜV SÜD. Jacinto 7 software components that have safety requirements are designed to support up to ASIL-D functional safety requirements. Software components are not externally certified. A certification support package gives you the ability to certify your final software/system. Software diagnostics libraries are delivered with examples of on-chip diagnostics usage. TI offers functional safety certificates for compatible hardware and software.

One of the key safety architecture differentiations of Jacinto 7 processors is the integration of MCU functionality, which simplify the system design, reduce the number of components on the board and reduce space. The application processor is divided into two independent domains: the main domain and the MCU domain. The main domain provides high-performance compute cores such as an MPU and a graphics processing unit (GPU), multimedia, and vision hardware accelerators including DSPs, as well as the necessary peripherals. The MCU domain is an independent domain for safety functions with high FFI.

The Jacinto 7 processors are safety-compliant devices that come with functional safety documentation that includes:

- A safety manual, which provides information to help you create a safety-critical system using a supported Jacinto 7 processor family. This document contains details about the development process, functional safety architecture and implemented functional safety mechanisms.
- A safety analysis report, which contains information regarding the device's ability to achieve the stated functional safety goals.
- A quantitative functional safety analysis (also known as failure mode, effects and diagnostic analysis [FMEDA]) is also a part of the safety analysis report, but it is a separate document. It contains details about the different parts of the component, suitable to enable calculations based on a customized application of diagnostics functional safety mechanisms and contains information about FIT, diagnostic coverage, SPFM/LFM, and failure modes.

Software functional safety overview

Software is an important element in reaching the overall safety goal of a product. Safety for Jacinto 7 software consists of the following two facets:

- Systematic capabilities of software components used in the safety path.
- Comprehensive software support for the hardware diagnostics and reference example code.

For systematic capability, TI follows a well-defined, common software development process and tools used across its various teams. An independent software quality organization is responsible for approving all software products. TI's overall functional safety deliverables include:

- **Process compliance:** Functional safety software development process is certified by TÜV SÜD for ISO 26262 for ASIL-D and IEC 61508.
- **Project compliance:** Project compliance is ensured via internal audit and is conducted

against the ISO 26262 or IEC 61508 processes. Any noncompliance is corrected with an improvement plan and actions.

- **Enabling customer certification:** All software that is developed following the using safety process is provided with a Compliance Support Package (CSP). The CSP includes:
  - A TI internal audit report.
  - Requirements, a test plan and reports.
  - A traceability report.
  - A dynamic code coverage analysis report.
  - A static code analysis/Motor Industry Software Reliability Association-C report.
  - A functional safety diagnostics library and manual.
  - A compiler qualification kit.
  - A software failure mode and effects analysis report.

The unified Jacinto 7 software development kit (SDK) also provides software support that enables you to build your safety solution. Components that are supposed to be used in a system "as is" and that are part of a safety loop are developed according to TI's functional safety software development process. The process includes a software diagnostic library for all key safety IPs and functional software like microcontroller abstraction level drivers, IPC and DMA.

TI also provides various reference examples that help you understand how to use these safety features in your applications. Since safety features can vary from application to application, reference software is not developed using the safety process and instead follows the TI baseline process.

Table 1 shows various examples of what is provided in the diagnostics software, functional software and reference software that is included in the SDK.

Safety application mapping

Typical SoC architectures built for data center and mobile applications lack the safety features necessary for automotive applications and in turn require additional computing performance to add software-based safety diagnostics. The various hardware and software safety features of the Jacinto 7 processor family, when used in an end application, help reduce the need for computing performance.

Figure 1 on the following page illustrates a typical vision-based system. The input camera data is captured via Camera Serial Interface and is then sent to a vision processing hardware engine for conversion from raw to YUV. Various analytics and

Software diagnostics	Functional software	Reference software
Software Diagnostic Library (SDL)—Software functions and response handlers for various safety features • LBIST / PBIST for various modules • Peripheral viz CAN, SPI • Safety IP: CRC, ECC, RTI, DCC, ESM • Ability to inject error • Software with systematic capability	**Components in safety path**—SDK component built with systematic capability • AUTOSAR MCAL (CAN, DIO, SPI, ETH, IPC, ADC, PWM, WDG, GPT) • CSL-FLs for Safety IPs like ECC, CRC, DCC, ESM, BIST, VTM, PGD, POK, ADC • SCI client, DMA • SYSFW firmware • TI-RTOS • CSL-FLs for all IPs in safety path • MMA, TIDL Library • LLDs for CSI2, VHWA, IPC • Compiler Qualification Kit	• Example code for FFI, Main / MCU island isolation and other safety features • Reference software demonstrating Safety IP usage in use case context • Reference software demonstrating diagnostics listed in safety manual
Functional Safety software development process	**Software Compliance Support Package (CSP)**	Standard software development process

***Table 1**. Software functional safety offerings.*

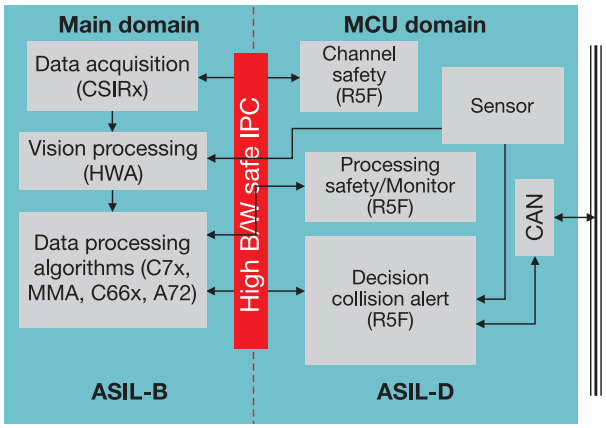

***Figure 1**. Typical vision processing.*

deep learning algorithms like object classification and free space detection are run on the processor's on-chip C7x DSP, MMA and Arm® Cortex®-A72 cores. The MCU domain acts like a checker for each step and periodically validates and monitors the data being processed. The MCU domain also takes final decisions of the safety functions based on other sensor inputs, which are then communicated to other automotive ECUs via a communication protocol like Controller Area Network (CAN).

Each of the blocks in **Figure 1** are modules on the Jacinto 7 processor and include hardware diagnostics to meet the overall safety goal without using CPU resources. **Table 2** maps the same vision application referred to earlier and shows the functional safety differentiation between the Jacinto 7 processor family compared to a typical SoC.

Jacinto Processor-compatible power management solutions

In parallel to the Jacinto processor family, TI developed two high-accuracy, flexible Power Management Integrated Circuits (PMICs) that are suitable for automotive applications requiring functional safety and come with functional safety documentation. These PMICs, TPS6594-Q1 and LP8764-Q1 PMICs, provide a scalable power management solution for both the main domain and the MCU domain and support functional safety up to ASIL-D.

Safety domain	Feature	Typical automotive system	Jacinto 7 processor family advantage
• Architecture	• Integrating MCU island • Heterogeneous safety cores	• Uses an external MCU • Uses hypervisor and an external MCU; requires an extra CPU load for hypervisor	• System cost optimization • Scalable safety performance • Fail-safe and recovery without hypervisor
• Fundamental safety • Transient and permanent faults	• Built-in self-test for cores, memories and hardware accelerators • Error-correcting code for memories • Lockstep DMIPS • CRC, watchdog, clock comparator • Safety on interconnect	• Typically not available in application processors • Additional load on all cores for software diagnostics	• Available all in hardware • Negligible additional CPU load
• Isolation • FFI	• MMU, MPU, firewalls, timeout gaskets	• Hypervisor – software-based method – loads processing cores • Additional load on all cores for software diagnostics	• Hardware isolation between safety and non-safety tasks • Negligible additional CPU load
• Application safety features	• Black frame • Freeze frame • Camera blockage • Deep learning network parameter safety	• Software-based method – loads processing cores • Additional load on all cores for software diagnostics	• Freeze-frame monitor: hardware-assisted freeze-frame detect. No CPU load • Hardware CRC-based Deep learning network safety. No additional CPU load

***Table 2**. Safety mapping to applications.*

A properly architected system supports functional safety requirements, including:

- The SoC checks sensor data
- The MCU checks the SoC
- The MCU controls the actuators
- The MCU checks whether the actuators react on the control in the expected way
- PMIC monitors MCU hardware and software execution
- PMIC monitors application processor hardware operation

If the PMIC detects an erroneous operation, it will put the system in safe state by forcing the ENDRV output pin low. Examples of errors include:

- Failures in supply voltages to the MCU or the SoC
- Failure in input supply voltage to PMICs
- MCU software or hardware error
- SoC hardware error reported by the ESM for SoC

The TPS6594-Q1 and the LP8764-Q1 devices can be used as standalone PMICs, but in systems where multiple PMICS are utilized together for scalability with a processor or MCU, the PMICs communicate with each other over a two-wire interface covered with CRC protocol. The interface allows synchronizing power states and error handling between the PMICs. Periodic polling of the bus checks the health status of all the PMICs on the communication bus. This implementation ensures rapid response to system fault conditions and therefore enables the solution to target higher functional safety goals of the end system. **Figure 2** illustrates one example connection between the two PMICs and a Jacinto 7 processor system use case. Most applications will utilize one TPS6594-Q1, but the use of an additional LP8764-Q1 will support additional system features and higher performance

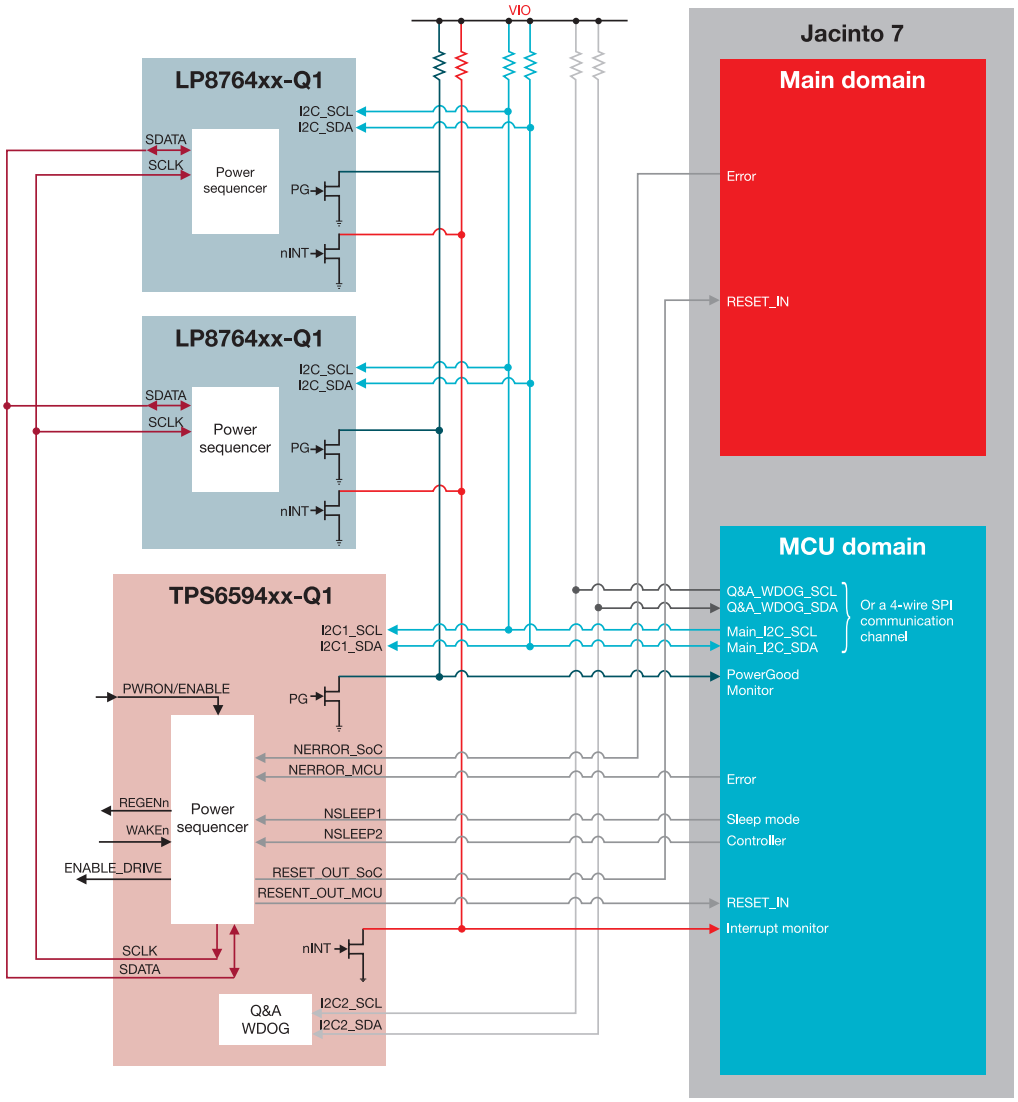

***Figure 2**. TPS6594-Q1 + LP8764-Q1 + LP8764-Q1 communication as "virtual" PMIC*

will support additional system features and higher performance. This ability to use one or more PMICs to power the SoC by a "virtual" PMIC allows optimization of system cost in use cases requiring lower power while enabling the highest performance systems as well.

Conclusion

TI's new Jacinto 7 processor family with integrated functional safety features on chip enables customers to better reach their safety certification and goals of their end product. The extensive safety features help reduce system BOM and can save performance overhead across various cores. In addition, TI's software SDK provides safety-related drivers and diagnostics libraries to help customers achieve their safety software development goals. A simplified safety architecture and software offering can help customers save significant engineering development effort.

Additional resources

- Kumar, VC. "The state of functional safety in Industry 4.0." Texas Instruments white paper SPRY329, 2018.
- Thomas, Jay, and Siddharth Deshpande. "Foundational Software for Functional Safety." Texas Instruments white paper SPNY007, 2015.
- Functional safety hardware certificate.
- Functional safety software certificate.
- Chitnis, Kedar, et al. "Enabling Functional Safety ASIL Compliance for Autonomous Driving Software Systems." *Electronic Imaging, Autonomous Vehicles and Machines* 2017, Society for Imaging Science and Technology (Jan. 29, 2017), pp. 35–40.
- Haworth, David, Tobias Jordan and Alexander Much. "Freedom from Interference from AUTOSAR-Based ECUs: A Partitioned AUTOSAR Stack." *Automotive – Safety & Security*, LNI 210 (2012), pp. 85–98.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), 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, 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 (www.ti.com/legal/termsofsale.html) 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.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265