Product Overview

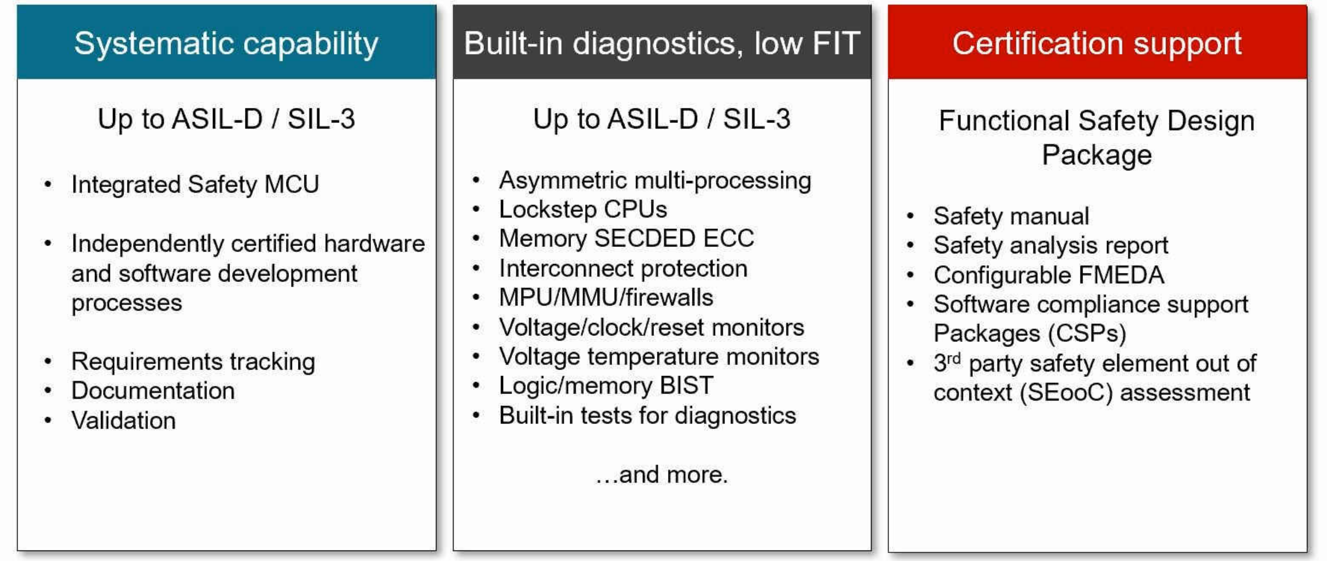
Jacinto™ 7 Safety Product Overview

Yining Yang

ABSTRACT

In this document, we will introduce Jacinto 7 safety fundamentals and the collateral TI provides for customers' functional safety implementation.

Jacinto SoCs are developed as a functional Safety Element Out of Context (SEooC) via ISO26262/IEC61508 processes to achieve ASIL-D/SIL-3 systematic fault integrity and includes hardware diagnostics to achieve up ASIL-D/SIL-3 random fault integrity. The device has gone through safety assessment by a certified third party (TUV-SUD) and a certificate will be provided.



Systematic capability

Up to ASIL-D / SIL-3

- Integrated Safety MCU
- Independently certified hardware and software development processes
- Requirements tracking
- Documentation
- Validation

Built-in diagnostics, low FIT

Up to ASIL-D / SIL-3

- Asymmetric multi-processing
- Lockstep CPUs
- Memory SECDED ECC
- Interconnect protection
- MPU/MMU/firewalls
- Voltage/clock/reset monitors
- Voltage temperature monitors
- Logic/memory BIST
- Built-in tests for diagnostics

…and more.

Certification support

Functional Safety Design Package

- Safety manual
- Safety analysis report
- Configurable FMEDA
- Software compliance support Packages (CSPs)
- 3rd party safety element out of context (SEooC) assessment

Table of Contents

Trademarks

All trademarks are the property of their respective owners.

Copyright © 2022 Texas Instruments Incorporated

1 Jacinto™ 7 Safety Architecture Concepts

For a full architectural overview of the Jacinto devices please review the device technical reference manual of the respective SoC. Jacinto 7 SoCs target mixed criticality with a heterogenous architecture and are scalable in terms performance, peripheral, and functional safety requirements. Each device within the Jacinto family will have a slightly different partitioning of safety components as well as safety targets, this is summarized within Table 1.

Table 1. Safety Scalability Table

	Main Domain	MCU Domain	Extended MCU Island	Total ASIL-D/SIL-3 DMIPs
DRA829/TDA4VM	ASIL-B/SIL-2	ASIL-D/SIL-3	N/A	Up to 2K
DRA821	ASIL-B/SIL-2	ASIL-D/SIL-3	ASIL-D/SIL-3	Up to 4K

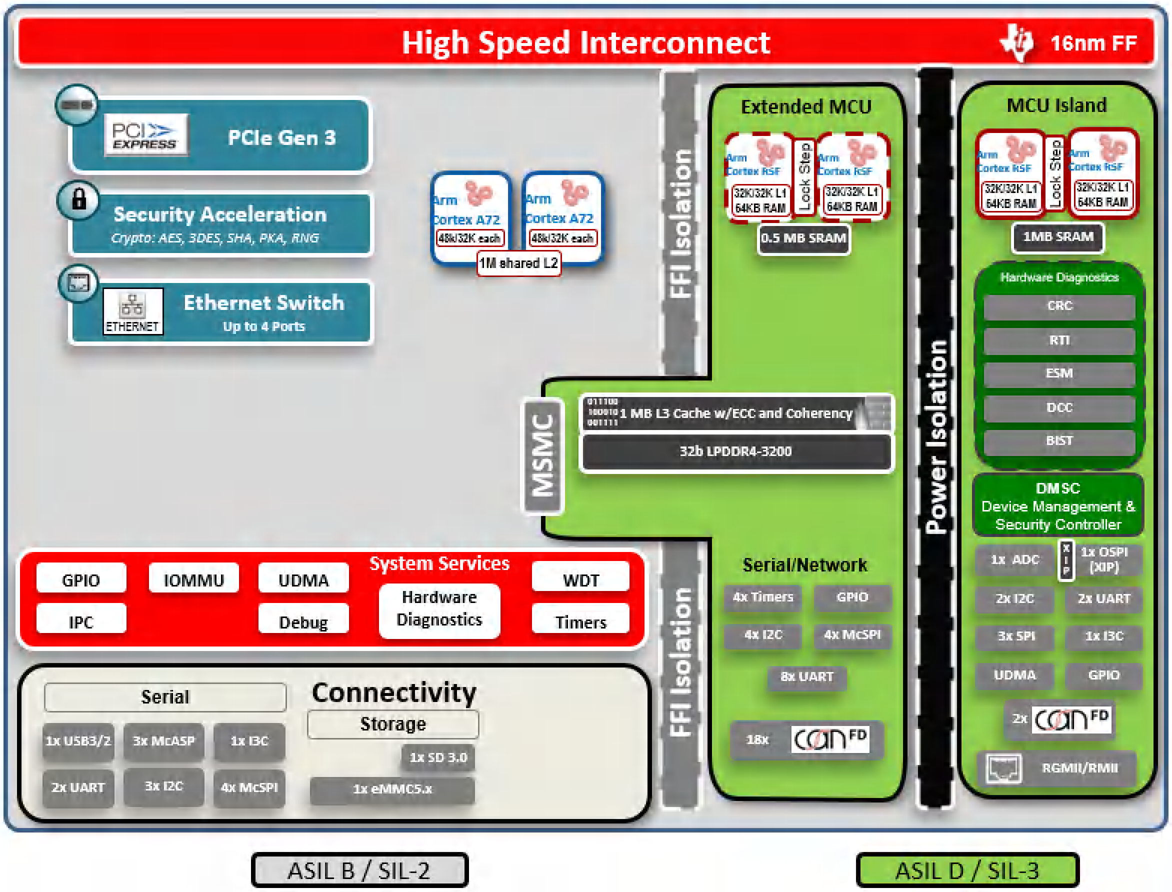


Figure 1. DRA821 Device

1.1 Safety Architectural Overview: MCU Island and Extended MCU Island

The entire chip achieves systematic fault integrity of ASIL-D/SIL-3. The random fault metric integrity of each respective domain assumes that sufficient hardware diagnostics are used in conjunction with recommended software/system diagnostics and assumptions of use (AoU) are implemented.

MCU Island: Jacinto 7 family of products integrates a safety MCU inside the SoC to perform monitoring of safety critical functions and signals. This is referred to as the MCU island and is shown in the block diagram above in green. The MCU island provides a safety partition with sufficient hardware diagnostics in place to achieve random fault integrity of ASIL-D/SIL-3. It is comprised of a pair of R5F cores which can be operated in lockstep, safe interconnects for intra-domain communication, as well as a diverse set of peripherals.

Extended MCU Island: On some devices within the Jacinto 7 family (please see Table 1: Safety Scalability Table) an extended MCU island is present. This partition is shown in green in the block diagram above and

Copyright © 2022 Texas Instruments Incorporated

increases ASIL-D/SIL-3 performance with additional R5F core(s) for increased ASIL-D/SIL-3 DMIPS as well as additional instances of peripherals that can achieve random fault integrity of ASIL-D/SIL-3. The extended MCU also enables up to ASIL-D/SIL-3 access to DDR, which is beneficial if safe data access is required and on-chip memory within the safety island or extended safety island is not sufficient.

The rest of the SOC (main domain as show in the grey areas of Figure 1) achieves random fault integrity requirements of up to ASIL-B/SIL-2.

1.2 Implementing Mixed Criticality - Freedom from Interference (FFI)

When mixed ASIL components co-exist in a system, ISO26262 mandates freedom from interference. This prevents cascading faults from lower criticality elements from affecting higher criticality elements. The Jacinto family of products implement several architectural features to facilitate FFI.

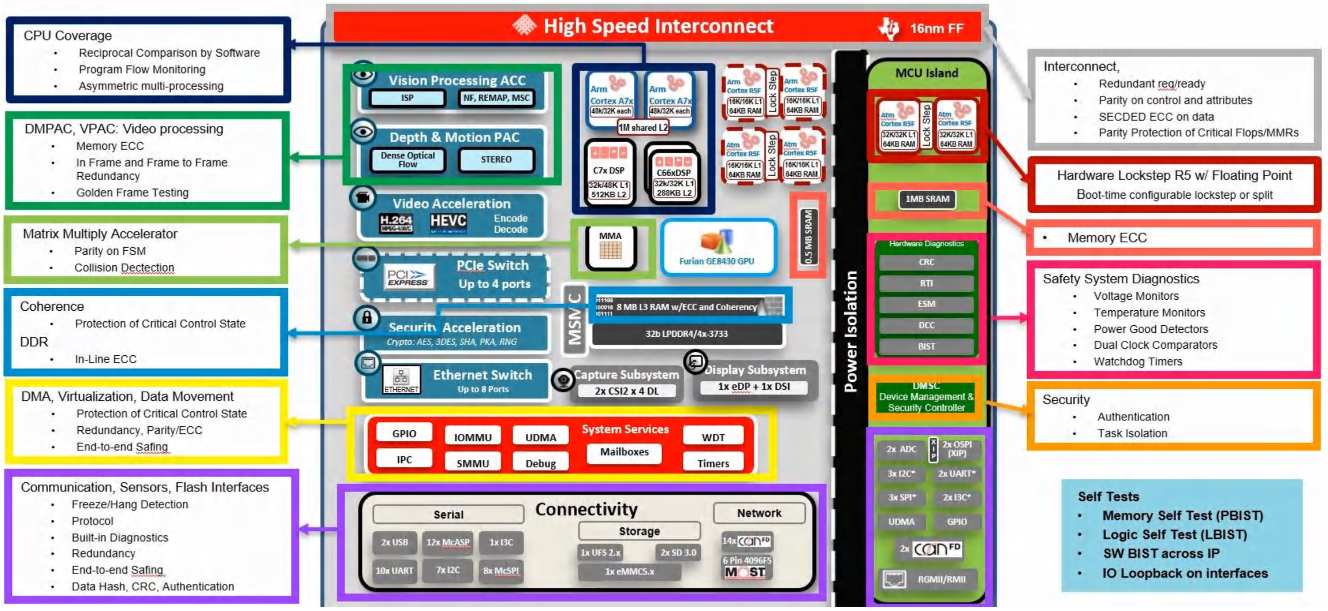
- **HW Isolation**: The MCU Safety Island is an independent domain with a high degree of FFI from the rest of the SoC. This is accomplished via separate voltage, clock, and reset domains as well as its own dedicated set of peripherals and resources. The MCU domain can still continue to operate on safety critical functions if the main domain crashes, hangs, or needs to be reset.
- **Firewalls**: A Firewall is a module that restricts access of incoming bus transactions based on configuration settings. Firewalls can be configured for certain policies to ensure that non-safe or less safe components will not be able to access or manipulate safety critical cores, peripherals, or memory. Policies can be set to monitor an incoming transaction’s address and attributes (Read, Write, Secure, etc.) to either block or allow access.
- **Isolation Gaskets**: The MCU island and extended MCU island have isolation gaskets in place which serve as fault tolerant connections to less safety critical resources that are shared throughout the SoC.
- **PVU/MMU**: In addition to enabling features like virtualization, MMUs help separate memory paths via memory mapping to allow mixed criticality use cases. The module can be configured to ensure that less safety critical cores can only access its own address space and peripherals.

Copyright © 2022 Texas Instruments Incorporated

2 Overview of Safety Mechanisms

For system level safety, robust hardware diagnostics for basic operations are layered with system and software diagnostic to meet random fault integrity metrics on the SoC. There are three basic categories of diagnostic coverage:

- *Hardware safety mechanisms*: Once enabled, these mechanisms operate continuously.
  - Examples of this include but are not limited to: SECDED ECC and Parity for memories and interconnect, PLL slip and loss of lock detection, over/under-voltage detection.
- *Hardware + Software safety mechanisms*: These mechanisms depend on hardware but require periodic software interaction to initiate or maintain the operation.
  - Examples of this include but are not limited to: watchdog timers, CRC hardware support for checks of memory and registers, dual clock comparators.
- *Software safety mechanisms*: These mechanisms are based on software performing some test and checking the results.
  - Examples of this include but are not limited to: Information redundancy techniques, transmission redundancy, software test of basic functionality. Implementation of these mechanisms are usually dependent on customer application and use case.



CPU Coverage
- Reciprocal Comparison by Software
- Program Flow Monitoring
- Asymmetric multi-processing

DMPAC, VPAC: Video processing
- Memory ECC
- In Frame and Frame to Frame Redundancy
- Golden Frame Testing

Matrix Multiply Accelerator
- Parity on FSM
- Collision Dectection

Coherence
- Protection of Critical Control State

DDR
- In-Line ECC

DMA, Virtualization, Data Movement
- Protection of Critical Control State
- Redundancy, Parity/ECC
- End-to-end Safing

Communication, Sensors, Flash Interfaces
- Freeze/Hang Detection
- Protocol
- Built-in Diagnostics
- Redundancy
- End-to-end Safing
- Data Hash, CRC, Authentication

Interconnect,
- Redundant req/ready
- Parity on control and attributes
- SECDED ECC on data
- Parity Protection of Critical Flops/MMRs

Hardware Lockstep R5 w/ Floating Point
Boot-time configurable lockstep or split

- Memory ECC

Safety System Diagnostics
- Voltage Monitors
- Temperature Monitors
- Power Good Detectors
- Dual Clock Comparators
- Watchdog Timers

Security
- Authentication
- Task Isolation

Self Tests
- **Memory Self Test (PBIST)**
- **Logic Self Test (LBIST)**
- **SW BIST across IP**
- **IO Loopback on interfaces**

Figure 2. Select Diagnostics on TDA4VM

Figure 2 demonstrates some safety mechanisms that can be implemented in the SoC (based of TDA4VM). This diagram is for informational purposes only and is not all inclusive. Please refer to SoC specific Safety Reference Manual for in depth descriptions of the diagnostics as well as for SOC specific modules and peripherals.

Copyright © 2022 Texas Instruments Incorporated

3 Implementation of Safety in Your System

3.1 Hardware Collateral

TI provides comprehensive collateral and deliverables to enable safety support and certification of the SoC as a Safety Element out of Context (SEooC) in a system.

- **Device Safety Manual**: Details product safety architecture and recommended usage Used during the system design process
- **Safety Analysis Report**: Summary of FIT rates and diagnostic coverage at the device level according to IEC 61508 and/or ISO 26262.
- **FMEDA (Failure Mode, Effects, Diagnostics Analysis)**: The FMEDA is a fully customizable document that is used to ensure a safety use case meets target metrics and safety goals as defined by the customer during their safety analysis. Used during the end of the system design process
- **Assessment Certificate**: Summary of compliance to IEC 61508 and/or ISO 26262 Used as a part of system safety case

A customer must have a valid Safety NDA in place to access aforementioned safety documents. The documentation is available via mysecuresw and access can be requested here.

3.2 Software Support

To enable customers on their safety journey, TI provides a ASIL-D/SIL-3 safety assessed Software Diagnostic Library (SDL) that covers system level diagnostics and safety features. The SDL is a collection of initialization/configuration, self-test, runtime, and response handler APIs that support various safety mechanisms. It is a fully self-contained library with no dependency on external software and provides an OS Abstraction Layer (OSAL) supporting implementation in both OS and non-OS (baremetal) environments. A compliance support package (CSP) is also provided alongside the SDL to support customers in re-qualification efforts on their system.

Both the SDL and CSP can be accessed via mysecuresw and access can be requested here.

Table 2. Summary of SDL and CSP Product Deliverables

SDL Supported Functions	CSP Deliverables
Diagnostics: Memory BIST, Logic BIST, ECC and Parity, ECC Aggregator, Error Signaling Module, R5F Lockstep (CCM) **Safety Features:** Clock Monitor, Voltage Monitors, Temperature Sensors, Timeout/Isolation Gaskets, Watchdog Timers, R5F MPU, PMU, VIM, and RAT Support	• Requirements, test plan and reports • Traceability report • Dynamic code coverage analysis report • Static code analysis/MISRA-C report • User guide with safety manual • Software FMEA report

Copyright © 2022 Texas Instruments Incorporated

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 © 2022, Texas Instruments Incorporated