Designing industrial controls for Industry 4.0 with Sitara™ AM6x processors

Texas Instruments

Mike Hannah
Embedded Processing

Texas Instruments

Introduction

In October 2012, a German working group brought initial recommendations to the German government regarding "Industrie 4.0," a term first coined in 2011 at the Hanover Fair. Industry 4.0 recommendations define what many expect will be a fourth era in modern factory automation, where cyber-physical systems (CPSs) integrate computation, networking and physical processes. They connect to each other and to the cloud; are easily configured; and incorporate sensors and analytics to make functionally safe, more autonomous systems.[1]

There are some basic design principles associated with the Industry 4.0 initiative:

- Interoperability: machines, devices, sensors and people connecting and communicating with each other through the Internet of Things (IoT).
- Information transparency: sensor data aggregated to higher levels to create models and provide information.
- Technical assistance:
  - Support humans by aggregating and helping to visualize information comprehensibly for decision-making and problem-solving.
  - Conduct a range of tasks that are unpleasant, too exhausting, or error-prone for humans to fulfill.
- Decentralized decisions: Perform tasks as autonomously as possible.[2]

Industry 4.0 is not the only initiative of its kind in the world:

- The U.S.-based Smart Manufacturing Leadership Coalition is an open smart manufacturing platform that enables manufacturers to easily access affordable and customizable modeling and analytical technologies without having to retrofit existing systems.
- In China, the Made in China 2025 initiative seeks to usher Chinese factories into the fourth generation, with machine-optimized efficiency driving lower costs and increased production.
- The Japanese Industrial Value Chain Initiative combines manufacturing and information technologies and seeks to reach some of the same goals as the other initiatives.

These initiatives have common objectives:

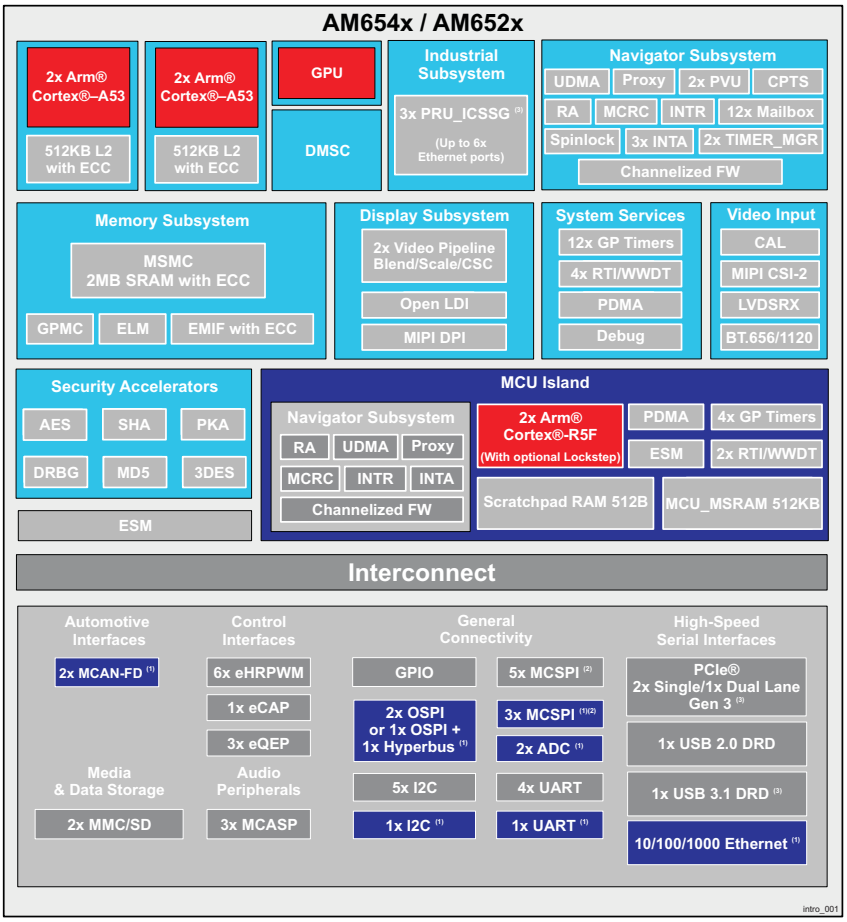
- Leverage global capabilities through the Internet and complex data management.
- Serve as a better link to enterprise and business-to-business systems.
- Improve resource and product traceability.
- Make smart processing and decision-making locally at the edge while keeping a full view in the cloud.
- Increase production-line flexibility and adaptability by reconfiguring quickly and addressing smaller lots.
- Increase production quality.
- Improve maintenance and reduce downtime.
- Improve functional safety and security.[3]

When creating Sitara™ AM6x processors, TI's design team analyzed Industry 4.0 goals and defined an architecture with these initiative

objectives in mind. The architecture had to meet next-generation communications for networking the factory. It also had to reach more stringent reliability and functional safety goals to provide increased operational longevity and reach safety targets that are typically difficult to reach with a single SoC. AM6x processors had to provide a more secure processing environment, with the latest in authentication and encryption technology, to protect tomorrow's factory systems from outside threats.

Sitara AM6x architecture highlights

Figure 1 offers a high-level overview of the AM6x SoC architecture. The AM6x is available in pin-compatible quad- and dual-core Arm® Cortex®-A53 configurations reaching frequencies of 1.1 GHz. Each dual-core cluster has 512 KB of L2 cache memory to provide independence between cluster processing and power scalability. There is single-error correct dual-error detect (SECDED) error-correcting code (ECC) protection on the L1 and L2 caches and parity or ECC on nearly all of the internal memories of the Arm cores for increased reliability. The processing cores have access to a 2 MB on-chip random access memory (OCRAM) that can be partitioned in 512-KB regions as static RAM (SRAM) or L3 cache. The large OCRAM is essential for minimizing worst-case latency for time-critical communication buffering instead of having to use double data rate (DDR) memory.



(1) This interface is located on the MCU Island but is available for the full system to access.
(2) One port is internally connected only; not connected to any pins.
(3) SGMII, USB3.1 and PCIe share a total of two SerDes lanes.

Figure 1: *Overview of AM6x SoC architecture.*

The multicore shared memory controller (MSMC) provides bandwidth-controlled, low-latency access to both the OCRAM and a 32-bit DDR external memory interface (EMIF). The DDR EMIF interfaces with DDR3L, DDR4 and low-power DDR4 (LPDDR4) and includes support for ECC.

A microcontroller subsystem (MCUSS) integrated into the AM6x enables additional low-power processing resources for the SoC. The MCUSS comprises an Arm dual-core R5F running up to 400 MHz, with 64 KB of tightly-coupled memory per core and 512 KB of OCRAM shared between the cores. The MCUSS has its own set of memory-mapped peripherals which can be used exclusively by the MCUSS or opened up to the A53 cores depending on the system need. It also has access to DDR if necessary.

Enhanced connectivity is central to the AM6x design. There are three next-generation industrial communication systems (ICSSs), each containing four programmable real-time units (PRUs) running at up to 250 MHz. PRUs are reduced instruction-set computer (RISC) cores with no cache and no pipeline to enable deterministic, single-cycle processing. Each PRU_ICSSG has two Reduced Gigabit Media Independent Interface (RGMII)-based Ethernet ports to support industrial switch implementations such as Time Sensitive Networking (TSN) up to gigabit speeds, as well as other industrial Ethernet protocols such as PROFINET®, EtherCAT®, EtherNet/IP™ and many others. There is also an additional Ethernet media access controller (MAC) supporting RGMII. In total, a single AM6x can enable seven concurrent Ethernet ports.

Several other connectivity options are available on the AM6x. A Peripheral Component Interconnect Express (PCIe) Generation 3 controller supporting speeds up to 8 GT/s per serializer-deserializer (SerDes) lane can be configured as root complex or end point, with unique quality-of-service configuration ports on the AM6x to facilitate low-latency access to OCRAM for specific virtual channel data. There are two PCIe controllers with two SerDes lanes to enable 2-by-1 or 1-by-2 controller/SerDes configurations. A general-purpose memory controller (GPMC) interface with 23 address lines and 16 data lines can interface with field-programmable gate arrays, bus adapters or backplanes. The GPMC supports multiplexed and non-multiplexed address/data modes with synchronous and asynchronous operation. There are two updated octal Serial Peripheral Interfaces (Octal SPIs) that support Flash speeds up to 133-MHz DDR and quad-, dual- and single-SPI flashes as well. Multiple instances of popular industrial serial interfaces are also provided, including Controller Area Network with Flexible Data Rate (CAN-FD), multi-channel SPI, universal asynchronous receiver transmitter (UART) and Inter-Integrated Circuit (I^2C).

A central processing resource new to the AM6x architecture called the device management security controller (DMSC) delivers secure device services to the SoC. The DMSC controls device power and reset. It also controls all isolation via on-chip firewalls, fulfilling access requests and managing secure authentication requests. Other security features of the AM6x processor include secure boot with programmable keys and runtime security.

Some unique investments made in the AM6x processor design were to enhance reliability and to provide the ability to reach higher levels functional safety. The AM6x provides at least 10 years of operation at maximum junction temperature with extended longevity estimates for customers interested in longer lifetimes for their systems. To allow functionally-safe systems to be implemented, the AM6x processor has integrated the dual-core R5F-based MCU technology from the Hercules™ product family. TI's Hercules MCUs have been assessed and certified to meet the IEC 61508 safety

integrity level of SIL 3. For functional safety-enabled AM6x devices, the R5F can be configured to run in lock-step mode instead of dual-core mode. The MCUSS can be isolated by internal SPI interfaces to create a chip-within-a-chip architecture for freedom from interference just as if the safety MCU was external to the SoC.

Real-time industrial communications via PRU_ICSSG

Industrial Ethernet technology is replacing serial field buses in systems such as factories and grid infrastructures. However, standard Ethernet is also non-deterministic and not suitable for real-time applications, whereas modern factory automation requires deterministic operation and time synchronization. This non-determinism and lack of time synchronization led to the development of a variety of industrial communication standards such as EtherNet/IP, PROFINET and EtherCAT to accommodate these features. In parallel to these efforts, the automotive industry started Ethernet Audio-Video Bridging efforts in 2005 for some of the same reasons to enable real-time transmission audio and video data within the car. This brought about the 802.1 AVB standardization efforts which were later renamed to Time Sensitive Networking (TSN). Many of the TSN features have been included in the IEEE 802.1Q-2018 standard Ethernet specification.

TSN grew into the collection of 802.1 standards shown in **Table 1** and has become important to communications for industrial applications. With several of the 802.1 standards that make up TSN still in development, it was apparent that a flexible communication solution was required for the industrial market.

TI's innovation for time-sensitive industrial communications is the PRU-ICSS, which has been integrated into Sitara devices such as the AM335x, AM437x and AM57x processors. The PRU-ICSS provides versatile, programmable industrial Ethernet and serial field-bus communications to accommodate protocols such as PROFIBUS®,

802.1 TSN Standards

Standard*	Alias	Description
IEEE P802.1AS/Rev 1588v2	Timing & synchronization	Provides layer 2 time synchronization
IEEE 802.1Qbv	Time-aware shaper	Runs the 8 port output queues of a bridge on a rotating schedule. Blocks all ports except one based on a time schedule in order to prevent delays during scheduled transmission
IEEE 802.3Qbr	Interspersed express traffic	Interrupts transmission of an ordinary frame to transmit an "express" frame, then resumes the ordinary
IEEE 802.1Qbu	Frame preemption	This basically just adds 802.3Qbr to 802.1Qbv. It allows for the interruption of non-time-critical frames to allow time-critical frames through
IEEE 802.1Qca	Path control & reservation	Discovers the network by collecting topology information from nodes in order to find redundant paths through the network and to ensure redundancy in the future
IEEE 802.1CB	Redundancy	Messages are copied and communicated in parallel over disjoint paths and then redundant duplicates are removed at the receiver end
IEEE P802.1Qcc	Enhancements and improvements for stream reservation	Improves existing reservation protocols by supporting more streams, configurable stream reservation classes and streams, support for layer 3 streaming, improved description of stream characteristics
IEEE 802.1Qch	Cyclic queuing & forwarding	Collects packets according to their traffic class and forwards them in one cycle. Provides a simple way to use TSN if controlled timing is desired, but reducing latency isn't important
IEEE 802.1Qci	Per-stream filtering and policing	Filters frames on ingress ports based on arrival times, rates and bandwidth to protect against excess bandwidth usage, burst sizes as well as against faulty or malicious endpoints
IEEE 802.1CM	Time-sensitive network for fronthaul	Enables the transport of time-sensitive fronthaul streams in Ethernet-bridged networks – new standalone TSN base standard

*https://1.ieee802.org/tsn/

Table 1. *List of TSN standards.*

PROFINET, EtherCAT, EtherNet/IP, SERCOS® III and POWERLINK™. The current generation of PRU-ICSS enables 100 Mbps of real-time Ethernet data throughput while achieving industrial protocol cycle times as low as 31.25 microseconds.

For the industrial network evolution to TSN, TI created a more powerful, scalable processing solution, the PRU_ICSSG, by upgrading the existing ICSS architecture with added PRUs and accelerators. The design of the PRU_ICSSG does not force a software rework of industrial Ethernet protocols already implemented on current PRU-ICSS devices. The next generation of PRU_ICSSG is integrated into AM6x processors and achieves 1-Gbps throughput and delivers the same real-time industrial Ethernet protocol cycle times. With a total of 1 GHz of real-time, deterministic PRU processing capability, hardware accelerators for common Ethernet processing tasks and increased high-bandwidth memory, the PRU_ICSSG can meet Industry 4.0 communication challenges.

Figure 2 is a block diagram of the PRU_ICSSG. All three instances of the PRU_ICSSG in AM6x devices have RGMII; one instance also has two Serial Gigabit Media Independent Interfaces (SGMIIs) enabled through the AM6x SerDes.

Security advancements

As noted previously, the DMSC centralizes control of the security of the AM6x processor. The DMSC is an integral part of the multi-core AM6x SoC device family and acts as a central authority for device management, boot sequence, power management and security, as shown in **Figure 3** on the following page. All critical assets (keys, configuration data) are secured in the DMSC, which reduces the opportunity for attacks. The DMSC ensures that all secure resources are working in harmony and

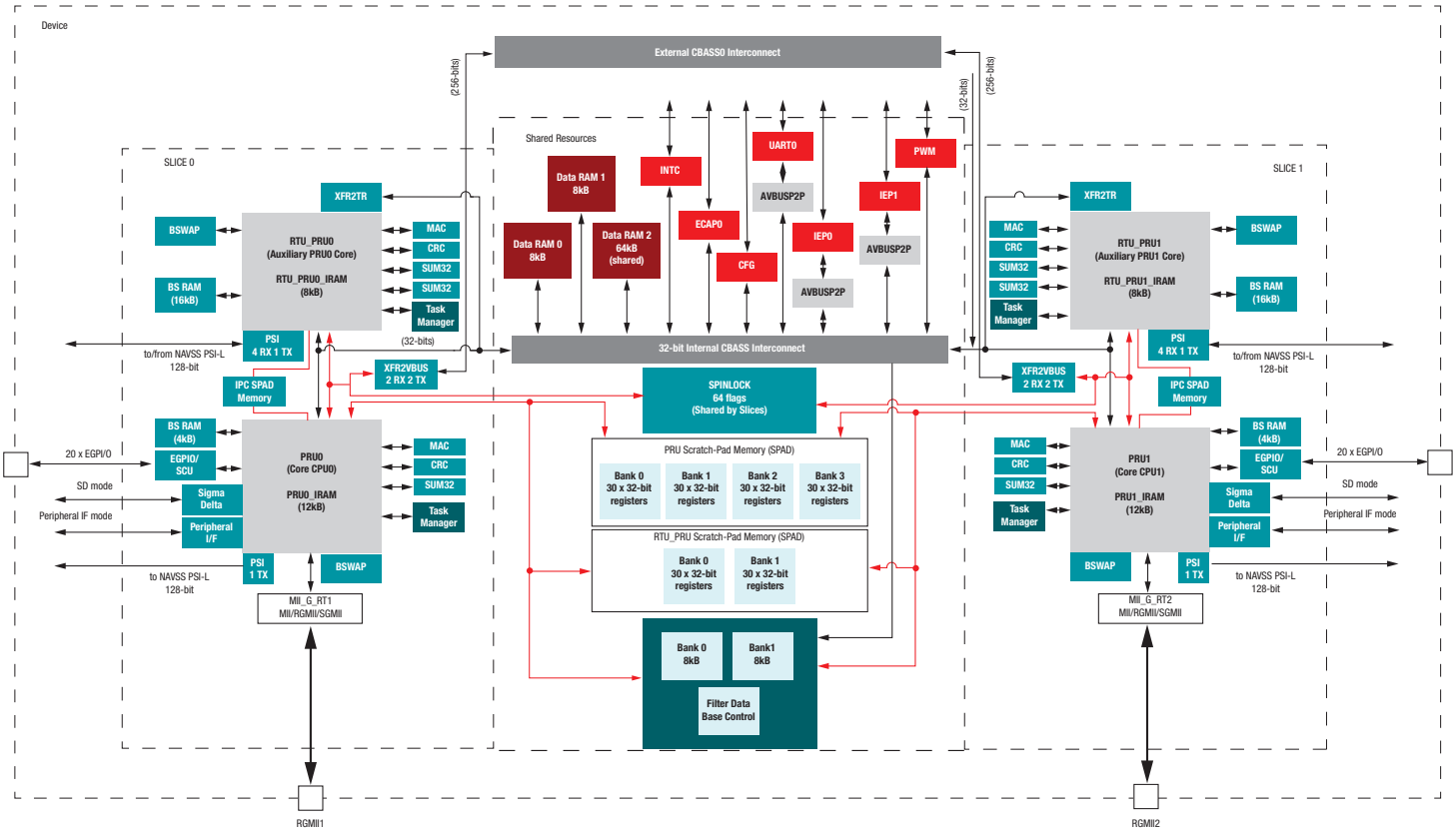


Figure 2: *Block diagram of the PRU_ICSSG on AM6x processors.*

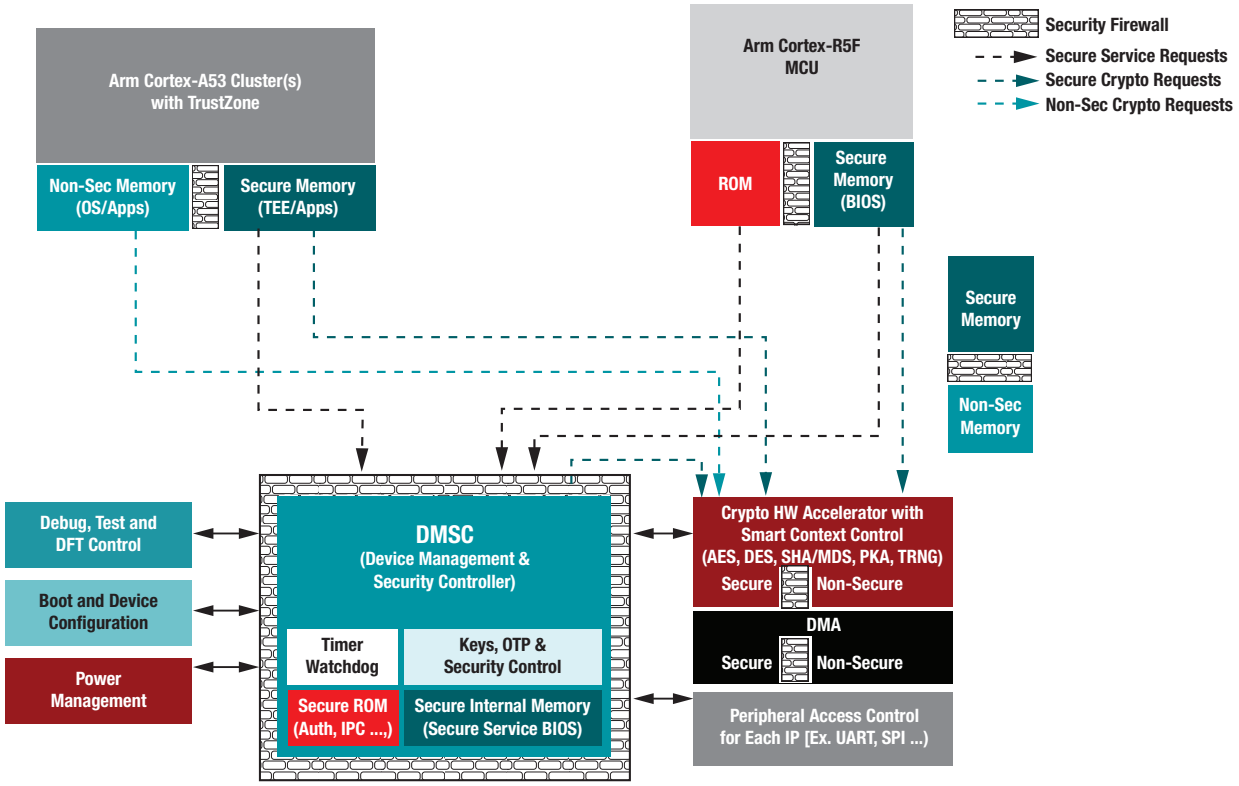


Figure 3: *DMSC features integrated on AM6x processors.*

that a security hack in one part of the device does not lead to the collapse of the entire SoC. TI owns the secure part of the DMSC firmware and makes it available only in binary. The AM6x architecture design supports an enhanced firewall architecture that permits dynamic access control to all SoC resources (memories, peripherals, cores, etc.). The DMSC provides the ability to promote or demote firewall access to resources. DMSC resources are accessible through defined application programming interfaces.

The cryptographic subsystem of the AM6x device was also upgraded to meet the latest in cryptographic requirements. The National Institute of Standards and Technology's Elliptic Curve Digital Signature Algorithm (ECDSA) and the deterministic random bit generator (DRBG) are supported in hardware, in addition to the Advanced Encryption Standard (AES), Triple Data Encryption Algorithm (3DES), Secure Hash Algorithm-1 and -2 (SHA-1,-2) and Message Digest 5 (MD5).

AM6x device enhanced control allows security-aware debugging. For example, the SoC provides the ability to lock the secure world while debugging in the public world. The DMSC-controlled challenge-response protocol opens debugging capabilities.

Enhanced features for functional safety and enhanced reliability

The AM6x architecture was built with integrated features enabling functional safety. **Figure 4** on the following page shows the IEC 61508 functional safety standard levels that can be targeted for systems using the AM6x processor. For industrial control applications, designers can use the AM6x device to design systems for levels up to SIL 3. TI provides a SafeTI™ design package to assist designers in meeting functional safety requirements

IEC 61508
(General safety for industrial)
PFH (Probability of Failure per Hour)

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

SFF (Safe Failure Fraction)
Table 3 — Maximum allowable safety integrity level for safety function carried out by a type B safety-related element or subsystem

Safety failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60%	Not allowed	SIL 1	SIL 2
60% – <90%	SIL 1	SIL 2	SIL 3
90% – <99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

Figure 4: *Functional safety standards.*

for systems integrating the AM6x processor. **Figure 5** offers an overview of SafeTI design packages.

As specified by the IEC 61508 standard, TI follows independently certified hardware and software development processes with requirements tracking, documentation and validation. A TI-provided software compliance package and compiler qualification kit help manage systematic failures. For random failures, TI provides a configurable AM6x failure mode effects and diagnostics analysis (FMEDA) tool to detail failure modes and metrics from the device design as well as diagnostic coverage. The AM6x device Safety Manual details the hardware, software and combined hardware/software diagnostics available with the AM6x processor. Finally, the SafeTI package offers a safety analysis report, which is a certification summary from the third-party assessment of the AM6x device as a safety element out of context (SEooC).

The AM6x SoC was architected for mixed-criticality functional safety applications. TI designed the MCUSS to natively target SIL 3, while the main SoC domain was designed to natively target SIL 2 so that functional safety system designers could target a SIL 3 level for their end systems. The MCUSS leveraged TI's experience with Hercules functional safety MCUs to create a "safe island" within the SoC, just as if the MCU was external to the SoC, as depicted in **Figure 6** on the following page.

The MCUSS is heavily protected by hardware diagnostic measures focused on power, clocks, central processing units, memories and interconnect. Once the correct operation of the MCUSS safe island is established, the logic in this region can provide diagnostic coverage in other regions of the SoC. The MCUSS stays alive even if the main SoC domain crashes and can reboot it. This partitioning and separation provides a basis for effective functional safety metrics while providing benefits to minimize the overall bill of materials.

Features such as white-list firewalls on all internal bus slaves provide freedom from interference (FFI). The firewalls can be based on

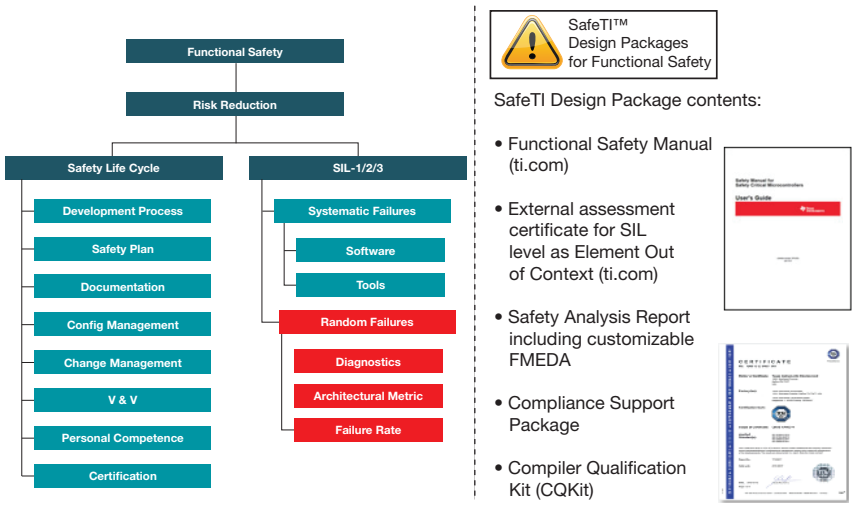


Figure 5: *Overview of SafeTI design packages.*

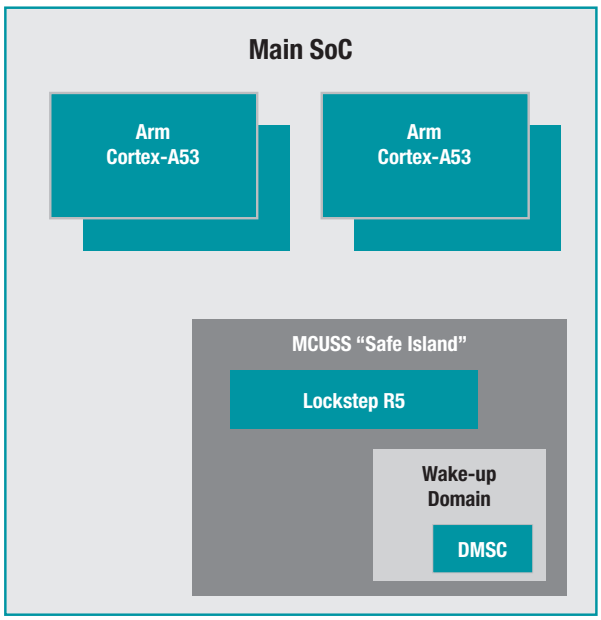


Figure 6: *MCUSS in the AM6x processor.*

privilege identity, level and access type. Although communication between the main SoC domain and MCUSS can occur through the traditional interconnect, the Cross-Bar Architecture Sub-System (CBASS), it can also be limited to internal SPI connections to further increase FFI for critical functional safety applications.

Separation of power and clocks between the MCUSS and the main SoC domain is essential for FFI. Each domain has its own separate clock sources, separate PLLs and independent watchdogs. There are no shared power rails between the MCUSS and the main SoC domain. Each domain has its own voltage sources.

For AM6x devices with functional safety enabled, the dual R5F cores can be booted into a lock-step mode. All R5F memories and memories within the MCUSS are covered by SECDED ECC. Additionally, there are integrated ECC aggregators (one per core) with support for error injection to all R5F ECC memory blocks to test the ECC functionality for safety-critical applications. This error injection feature is unique to TI's R5F implementation.

In the main SoC domain, functional safety also guided the Cortex-A53's integration into the design. The main SoC domain itself (excluding the MCUSS) targets SIL 2 certification. There is ECC protection for the L1 data cache (data RAM), the L2 cache (data RAM and tag RAM) and L1 Snoop Control Unit (SCU) duplicate tags. There is parity protection for the L1 instruction cache (data RAM and tag RAM), L1 data cache (tag RAM and dirty bits) and translation lookaside buffers. TI also added error injection capability for all supported ECC memory blocks for each A53 core with ECC aggregators.

AM6x software, like all Sitara device software, is delivered via the Processor software development kit (SDK). For those interested in using the AM6x device for functional safety applications, a processor SDK add-on package is available through a controlled TI secure software portal. The AM6x SoC safety package is a compliance support package with quality records to support customer certification efforts.

For industrial applications that do not have functional safety requirements but require low Mean Time Between Failure (MTBF), the AM6x architecture with extensive ECC coverage on memories across the SoC and the design strategy to limit failures in time (FIT) in the logic together drive a total soft error rate (SER) FIT of less than 250 FIT at maximum junction temperature and New York City sea level. The AM6x device has an industrial temperature rating, with junction temperatures ranging from –40°C to 105°C. At a maximum junction temperature of 105°C, the AM6x SoC has an estimated operation life of 100,000 power-on hours (POH), with all A53s operating at 1.0 GHz and the rest of the device operating at maximum frequencies. With a minor reduction in junction temperature to 95°C, the AM6x SoC can be extended to an estimated lifetime up to 200,000 POH.

Beyond connectivity, security and safety

While there was significant design focus in the areas of connectivity, security and functional safety in the development of Sitara AM6x processors, there are other important requirements for industrial applications that the AM6x SoC is built to address. With 0.8-mm pitch routing rules, a 23-mm-by-23-mm package and much of the power supply and sequencing solution integrated into the SoC, the AM6x device can fit into small-form-factor, fan-less enclosures without complex printed circuit board design. The active power envelope was restricted to less than 5 W for most use cases, enabling passively cooled end-equipment designs.

For applications that require a graphical user interface or display, the low-voltage differential signaling (LVDS) interface was integrated along with a 24-pin Mobile Industry Processor Interface (MIPI) Display Pixel Interface (DPI) to facilitate the connection of a human machine interface. With the dual-core Arm Cortex-A53 AM652x processor and the quad-core AM654x processor, the AM65x device family can address the performance, power and cost targets of many industrial applications.

The AM6x family of devices was designed with Industry 4.0 requirements as a foundation. That foundation drove the creation of AM6x SoC performance and features that will meet the needs for industrial control solutions for tomorrow's factories and other industrial end equipment markets.

Related websites:

- Learn more about the **AM6x processor** family

References:

[1] NIST Cyber Physical Systems Public Working Group **https://pages.nist.gov/cpspwg/**

[2] Marr, B. (2016, June 20) *What everyone must know about Industry 4.0*. Retrieved from **https://www.forbes.com/sites/bernardmarr/2016/06/20/what-everyone-must-know-about-industry-4-0/#6605d71e795f**

[3] Forschungsunion, acatech (2013, April 8) *Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Final report of the Industrie 4.0 Working Group*. Retrieved from **https://www.acatech.de/Publikation/recommendations-for-implementing-the-strategic-initiative-industrie-4-0-final-report-of-the-industrie-4-0-working-group/**

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