Functional Safety Information

Design Guide for Functional Safety Compliant Systems Using mmWave Radar Sensors

Voona Deexith, Abhed Misra

ABSTRACT

Functional safety standards specifies the requirements of implementation of safety in a system and helps with outlining safety goals to be met by that system. System designs that include functional safety must not only have lower risk from improper operation, but detect faults and minimize their impact. With more autonomy in automotive and industrial systems, stringent functional safety requirements are mandated to minimize equipment failure and human injury resulting from systematic and random failures. Comprehensive Safety Standards like ISO 26262 and IEC 61508 outline and define the process, artifacts and compliances demanded by variety of applications across automotive and industrial domain, respectively.

Safety is an integral part of TI's mmWave Radar sensor products and they enable the customers to meet stringent and critical safety certifications for their applications; easily and comprehensively. For ex., with AWR2944 Single Chip mmWave sensor, TI offers high performance coupled with functional safety enablers to help customers design, certify and deliver safety compliant radar solutions to the automotive market.

This Design Guide will walk through various steps typically involved in developing a Functional Safety Compliant System design. Corner radar of a car and intelligent robot sensing system are used as examples of a system design. This document also talks about various functional safety artifacts essentially needed for the Functional Safety Compliant certification of Applications .

Table of Contents

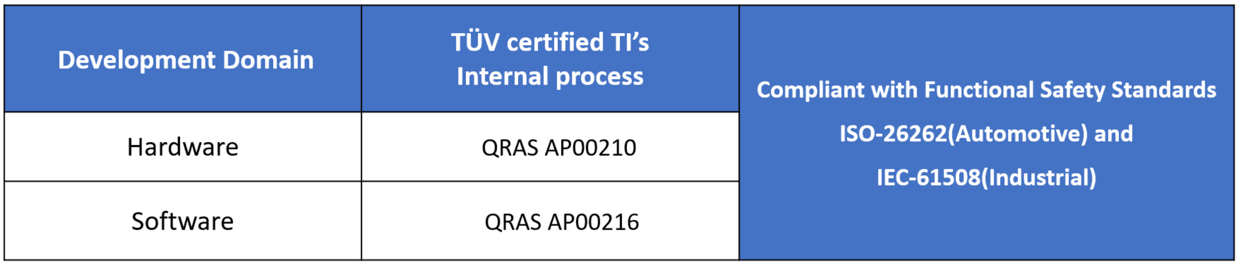
Trademarks

All trademarks are the property of their respective owners.

1 Introduction

Functional safety(FuSa) refers to the absence of unreasonable risk due to hazards caused by the malfunctioning behavior of electrical/electronic components in the systems (Ex: Anti-lock Braking systems, Elevators, Gesture Recognition, Intrusion Detection, Intelligent Robot sensing systems, Kick to open, Corner radar, Front Radar of Automotives, etc.). The objective of the functional safety in systems/subsystems is to minimize the risk associated with dangerous failures in causing physical injury to people or damage to the environment or property. TI addresses functional safety as an integral part of mmWave Radar Sensors.

For designing any FuSa compliant Radar sensor system, TI mmWave Radar sensors are a great choice because of their programmable versatility and the FuSa capabilities. TI mmWave Radar sensors assist vision sensing challenges in automotive and industrial applications which can withstand harsh environmental conditions. TI mmWave Radar sensor feature quick and reliable 3D presence detection and minimize possible collisions by lowering system/machine downtime. TI mmWave Radar sensors can be used for low power accurate motion detection to high-end imaging radar. As the automotive and industrial markets become more autonomous, they face an increasing need to meet stricter FuSa standards. TI mmWave Radar sensors are architected and designed using FuSa certified processes in compliance with the ISO 26262 and IEC 61508 safety standards for the Automotive and Industrial domain, respectively. To the world headed towards autonomy of systems, sensing the targets is vital for detection. Especially for FuSa compliant system, mmWave Radar sensor should detect only true positive targets where TI mmWave Radar sensors can play a crucial role in giving better and more reliable results to aid decisions on the range, velocity and angle of the target with good resolutions.

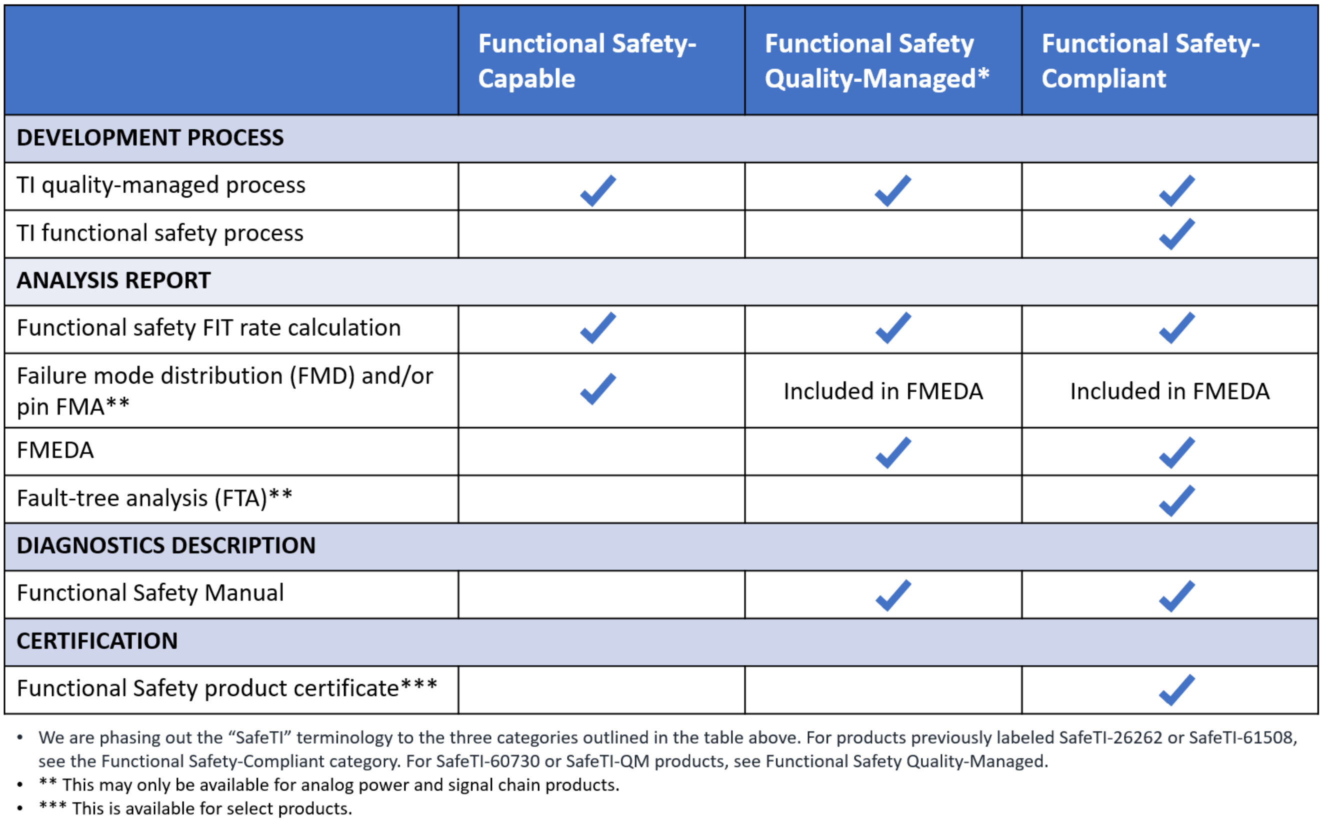


Development Domain	TÜV certified TI's Internal process	Compliant with Functional Safety Standards ISO-26262(Automotive) and IEC-61508(Industrial)
Hardware	QRAS AP00210	
Software	QRAS AP00216	

Figure 1-1. TI FuSa development processes

TI mmWave Radar sensors are developed using FuSa certified processes mentioned in the TI FuSa development processes as Safety Element out of Context(SEooC) with assumptions of application while deriving safety goals per IEC 61508 and ISO 26262 levels. TI mmWave Radar sensors are supported by FuSa compliance device certification from a third party certifier Technischer Überwachungsverein(TÜV). These certifications helps customers achieve safety goals of targeted applications quickly. TI mmWave Radar sensors can be used in applications where functional safety is critical such as in Automated Guided Vehicles, Industrial Robots, etc. All the TI automotive mmWave Radar sensor products are qualified for the AEC-Q100 standard that is accepted widely by the automotive industry for failure mechanism based stress test qualification in Integrated Circuits. Few TI mmWave Radar sensors have special features like low power mode operation; antenna on package; device security with edge intelligence.

Based on the safety standards ISO 26262 and IEC 61508, hardware element classes approximately map to TI's functional safety product categories as Functional Safety Capable, Functional Safety Quality Managed and Functional Safety Compliant. For more details on functional safety classifications after referring to the following Figure 1-2, visit this link.



	Functional Safety-Capable	Functional Safety Quality-Managed*	Functional Safety-Compliant
DEVELOPMENT PROCESS			
TI quality-managed process	✓	✓	✓
TI functional safety process			✓
ANALYSIS REPORT			
Functional safety FIT rate calculation	✓	✓	✓
Failure mode distribution (FMD) and/or pin FMA**	✓	Included in FMEDA	Included in FMEDA
FMEDA		✓	✓
Fault-tree analysis (FTA)**			✓
DIAGNOSTICS DESCRIPTION			
Functional Safety Manual		✓	✓
CERTIFICATION			
Functional Safety product certificate***			✓

- We are phasing out the "SafeTI" terminology to the three categories outlined in the table above. For products previously labeled SafeTI-26262 or SafeTI-61508, see the Functional Safety-Compliant category. For SafeTI-60730 or SafeTI-QM products, see Functional Safety Quality-Managed.
- ** This may only be available for analog power and signal chain products.
- *** This is available for select products.

Figure 1-2. TI Functional Safety Classification

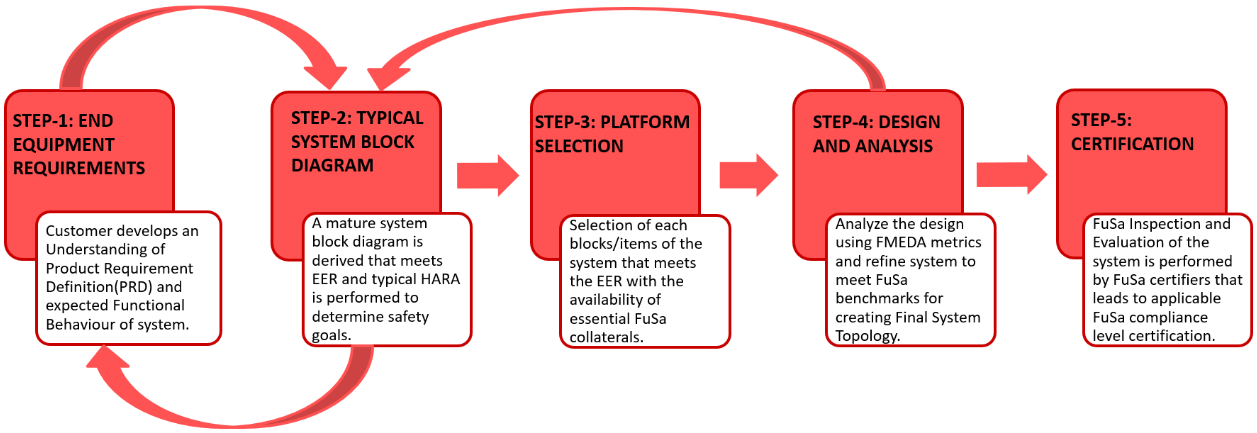
In this document, we will discuss developing a Radar sensor system design for FuSa certification using the TI mmWave Radar sensors. This document details a typical design life cycle of a functional safety compliant system that can help customers design a FuSa compliant Radar sensor system based on their targeted end system requirements. To develop any FuSa compliant system, the customer could follow the Verification and Validation(V&V) life cycle processes(as per IEEE Standard 1012-2016) in parallel to the proposed design life cycle. The V&V processes checks the system development process and ensures the integrated system accomplishes end equipment requirements by performing various tasks and activities(Requirement Evaluation, Hazard Analysis, Security Analysis, Risk Analysis, Criticality Analysis, etc.) on the system. For better understanding, we will be referring to examples like corner radar of a car based on TI's AWR2944 mmWave Radar sensor and intelligent robot sensing system for safer human presence detection based on IWRL6432 mmWave Radar sensor through out the proposed design life cycle to prepare the system design for FuSa certification as per applicable FuSa standards.

Note

- The safety integrity levels for Automotive applications are ASIL-A/B/C/D as per ISO 26262 standard with ASIL-D being the most stringent. Similarly, for Industrial applications as per IEC 61508 standard safety integrity levels are SIL-1/2/3/4 with SIL-4 being the most stringent.

2 Functional Safety Design Life Cycle

For designing any functional safety compliant system, it is recommended to follow the proposed Functional Safety design life cycle which would aid customers design their FuSa compliant systems safer, faster and more efficiently. The radar sensor systems are used in safety critical applications like anti-lock braking system in a vehicle, vacuum robots, etc making FuSa standard compliance particularly important. The proposed FuSa design life cycle is a typical FuSa system design flow, helps create a reliable FuSa compliant radar sensor system design that meets the targeted End Equipment Requirements (EER). The proposed design flow to create FuSa compliant system comprises of five steps that minimize the risk associated with failures that could cause physical injury or damage to an environment or property.



STEP-1: END EQUIPMENT REQUIREMENTS

Customer develops an Understanding of Product Requirement Definition(PRD) and expected Functional Behaviour of system.

STEP-2: TYPICAL SYSTEM BLOCK DIAGRAM

A mature system block diagram is derived that meets EER and typical HARA is performed to determine safety goals.

STEP-3: PLATFORM SELECTION

Selection of each blocks/items of the system that meets the EER with the availability of essential FuSa collaterals.

STEP-4: DESIGN AND ANALYSIS

Analyze the design using FMEDA metrics and refine system to meet FuSa benchmarks for creating Final System Topology.

STEP-5: CERTIFICATION

FuSa Inspection and Evaluation of the system is performed by FuSa certifiers that leads to applicable FuSa compliance level certification.

Figure 2-1. Typical Functional Safety System Design Life Cycle Flow

2.1 Step-1 : End Equipment Requirements

The development of any system starts with the customer understanding the targeted application and product requirements definition(PRD) also called as targeted End Equipment Requirements of the system. The targeted system application could be Kick to Open system(boot open), Child Presence Detection, Seat Belt Reminder, Corner Radar, Side Radar and Long Radar for Automotive Domain and Gesture Recognition system, Traffic Monitoring System, Security and Surveillance System, Occupancy Detection, Safer Human Presence Detection for Industrial Domain. The targeted End Equipment Requirements of the system would be consisting of :

- Safety and Security Requirements
  - FuSa Compliance Integrity Levels (ASIL- A/B/C/D, SIL- 1/2/3/4)
  - Essential FuSa Collaterals
  - Device Security (Cryptographic Hardware Accelarators, Secure authenticated and encrypted boot support)
- End Equipment/ Application Performance Requirements governed Radar Processing Algorithms needs to comply with Safety of the Intended Functionality(SOTIF) as per ISO 21448 standard that guarantees intended functionality in the absence of faults for Automotive applications.
- Technical and Logical Requirements (Functional Requirements)
  - Antennas
  - Power Block (Power supply)
  - Communication Interfaces
  - Flash Interfaces
  - Debugging and Development Interfaces

  - Power Management(PM) Components
  - Form Factor
  - Operational Frequency Range
  - Operational Junction Temperature Range
  - Maximum Range (LRR/MRR/SRR)
  - Range Resolution
  - Maximum Velocity
  - Velocity Resolution
  - Azimuthal Field of View(FOV)
  - Azimuthal Angle Resolution
  - Elevation Field of View(FOV)
  - Elevation Angle Resolution
  - Power Consumption (during Idle and Chirping time)
  - Cost
  - Response Time

The customer must be well aware of all the targeted end equipment requirements and the expected functional behavior of the system application. Understanding the functional behavior of system leads to awareness of Blocks/subsystems to be used in the system. Let's consider examples for designing a Corner Radar system for a Car and Industrial Robot sensor system for safer human presence detection around robot.

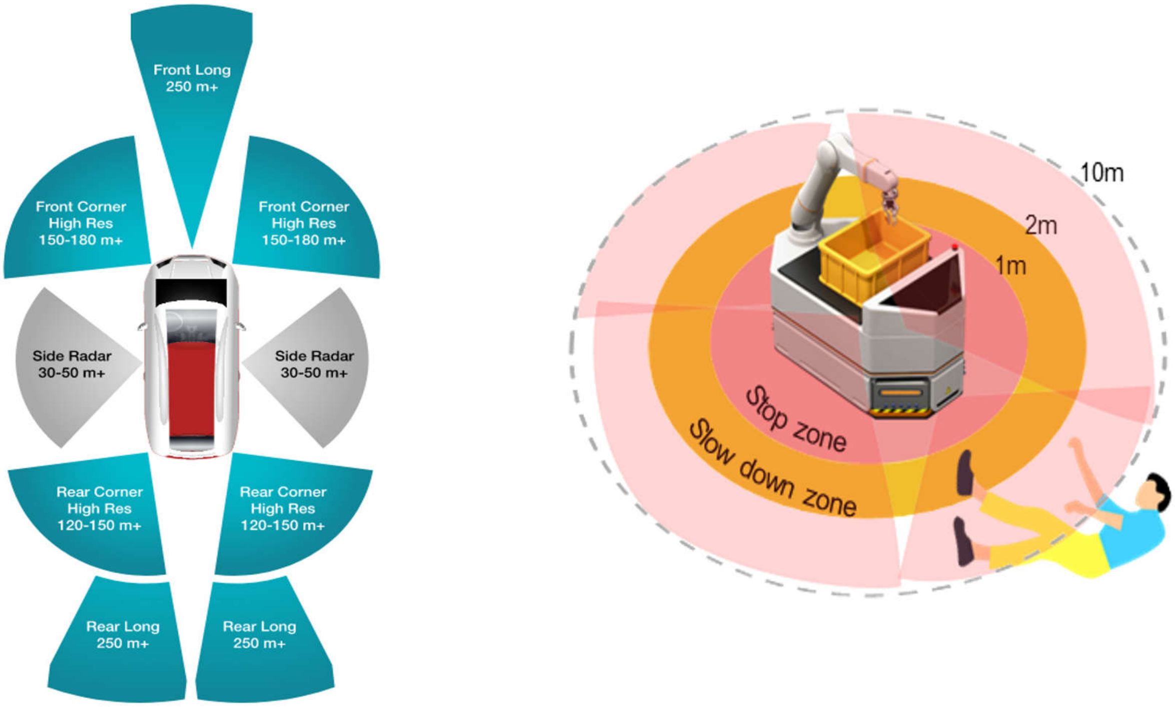


Figure 2-2. Automotive Radar(Car) and Industrial Robot(Safer Human Presence Detection)

Some of the targeted EER for these applications could be :

- Corner Radar System
  - Medium Range Radar(MRR)
  - ASIL-B FuSa Compliance as per ISO 26262
  - Operating Junction Temperature range of -40^{0}c to 125^{0}c
  - AEC-Q100 qualification
  - Small form factor
- Industrial Robot Sensor System
  - Short Range Radar(SRR)
  - SIL-2 FuSa Compliance as per IEC 61508

  - Low power consumption
  - Small form factor

Note

- The targeted EER includes Application Performance Requirements, Functional Requirements, Safety and Security requirements.

Key deliverables from this "**Step-1: End equipment requirements**" is the customer develops an understanding of End equipment requirements constituting PRD and expected functional behavior of the system application. This step paves the way to the next step for developing the block diagram of the system with awareness of blocks/subsystems to be used in system application.

2.2 Step-2 : Typical System Block Diagram

In this second step of the functional safety design life cycle with the understanding of PRD and blocks/ subsystems, the customer will refer to a typical system block diagram based on the end application. For reference block diagram of FuSa compliant Radar sensor system, the customer can refer to the TI mmWave Radar EVM's and TI Reference Designs. This step includes the hazard and risk analysis, a crucial and necessary part for determining safety integrity levels(ASIL-A/B/C/D, SIL-1/2/3/4) that sets the tone for system FuSa journey.

The hazard and risk analysis is performed on the reference block diagram. The safety requirements for automotive system application are formulated from Hazard Analysis and Risk Assessment(HARA) as per ISO 26262 standard requirement using metrics Exposure(E), Controllability(C) and Severity(S). For deriving safety goals in industrial domain system applications, there is no specific process/assessment to be followed as per IEC 61508 standard. So, typical HARA flow can be followed for determining the safety goals using metrics E,C and S.

Please note that compliance of AEC-Q100 standard is also important to electronic systems being developed for usage in Automotive applications. The typical HARA flow is shown in the following Figure 2-3.

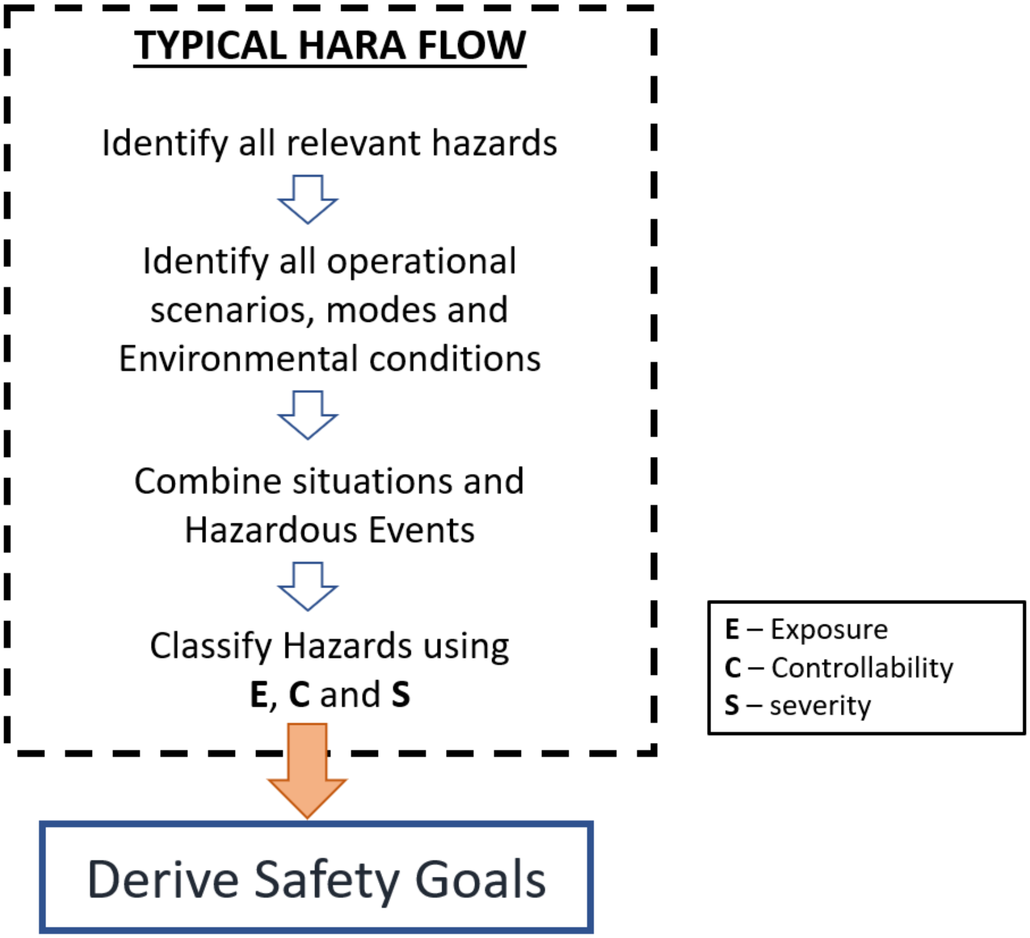

TYPICAL HARA FLOW
Identify all relevant hazards
Identify all operational scenarios, modes and Environmental conditions
Combine situations and Hazardous Events
Classify Hazards using E, C and S
E – Exposure
C – Controllability
S – severity
Derive Safety Goals

Figure 2-3. Typical HARA flow

The typical system block diagram of any FuSa compliant sensor system would consists of

- mmWave Radar Sensor
- RF Block
  - Antennas
  - External Crystal Oscillator
- Power Supply - PMIC / Discrete DC based power level converters
- Communication Interfaces
- Debugging and Development Interfaces
- Flash Interface
- PM Components

The mmWave Radar sensor system should support different interfaces like communication interfaces for data transfer, debugging and development interfaces for debugging and flash interfaces for externally flashing the device. RF antennas are used for the transmission and receiving of chirp signals for detection. Oscillator in the RF block is used to generate clock frequency. Power is supplied using power supply blocks like PMIC or discrete DC based power level converters for different power rails.

For ex., to design a high-performance corner radar system, AWR2944 mmWave Radar sensor, PMIC and CAN interface could be used. The customer can refer to AWR2944 EVM designed by TI for typical system block diagram, also mentioned in Figure 2-4.

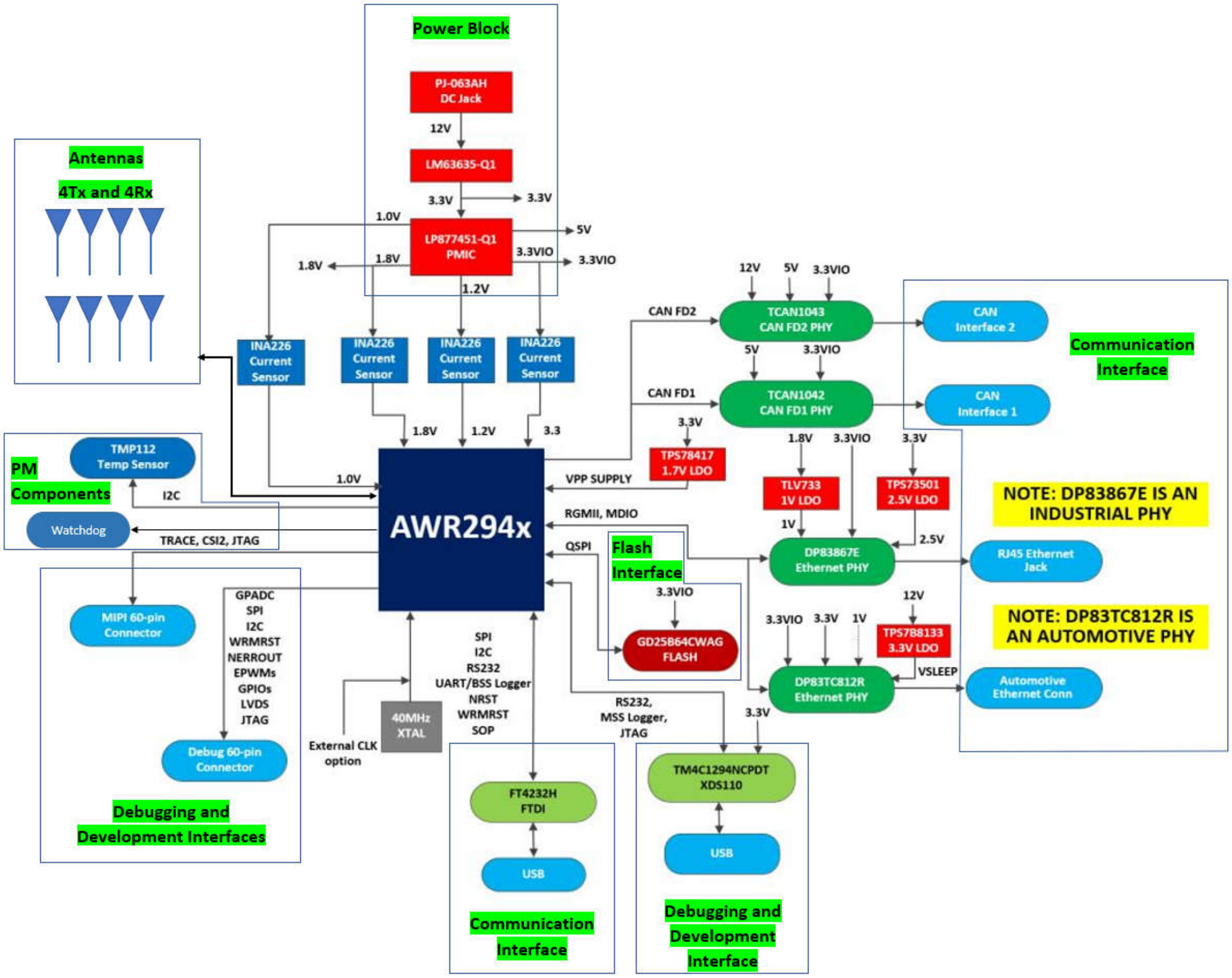


Figure 2-4. AWR2944 EVM

Similarly, to create an intelligent robot sensing system for safer human presence detection, IWRL6432 mmWave Radar sensors can be used by considering IWRL6432 EVM as a reference to the typical system block diagram, also mentioned in Figure 2-5. In this example, we are considering coverage of single sensor. For 360^0 safer human presence detection, multiple IWRL6432 mmWave Radar sensors could be used for covering the total perimeter of industrial robot.

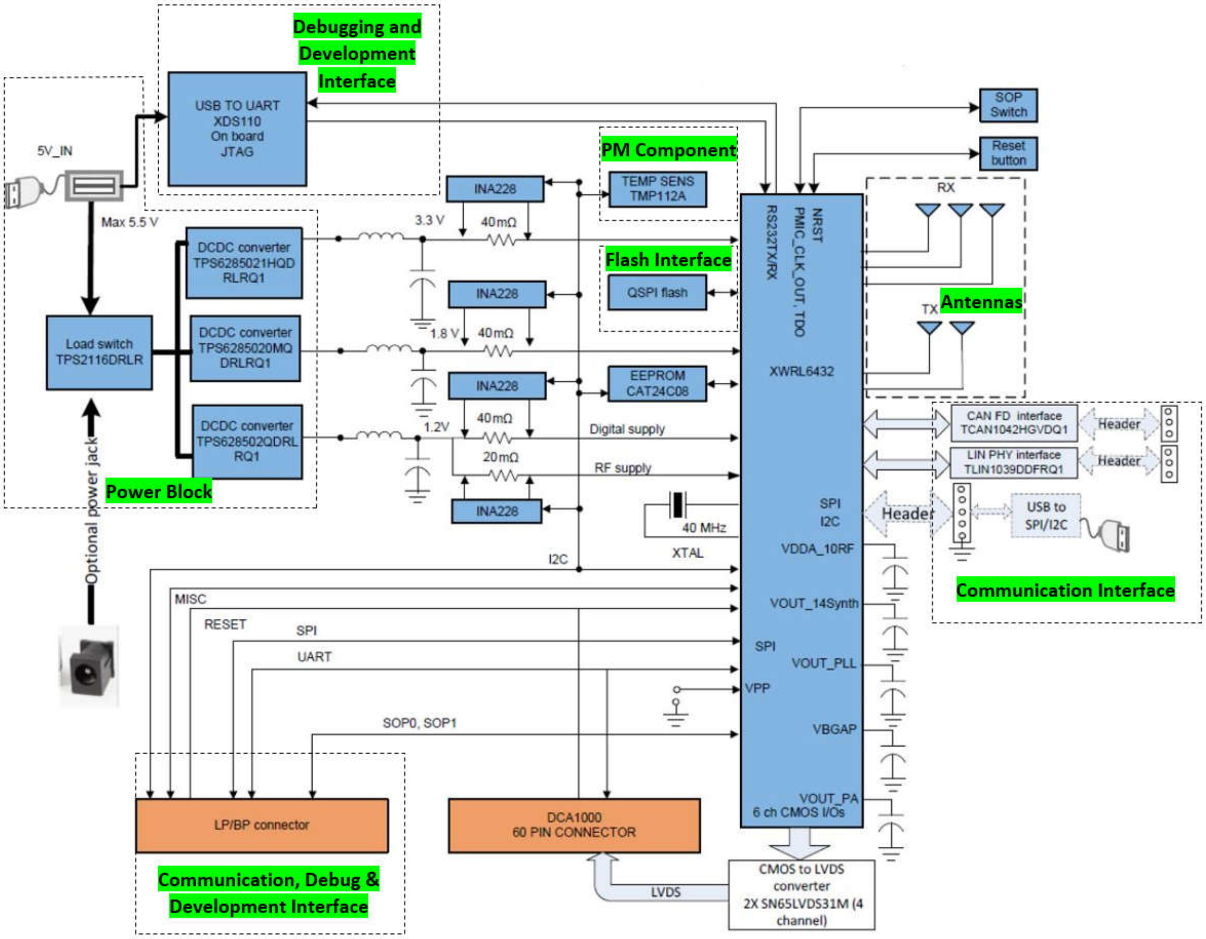


Figure 2-5. IWRL6432 EVM

Safety goals are determined by assessing the system block diagram. Some additional hardware safety mechanisms might be added in its design to meet targeted safety goals. If the safety goals are still not meeting the targeted safety requirements after modifying block diagram then the customer has to look up for refining the safety end equipment requirements.

Along with the safety requirements and goals identification, there are certain additional critical analysis (For ex., DFA and Coexistence Analysis) needed from a system level integration perspective. Dependent Failure Analysis(DFA) is performed on the system to identify Common Cause Failures(CCF) and Cascading Failures in the system. For the most cost-effective FuSa compliant system, the multiple safety mechanisms implemented in the system may have different applicable safety integrity levels(ASIL-A/B/C/D or SIL-1/2/3/4). Coexistence Analysis is performed on the system to detect or prevent the interference of high failure rate(Ex.: SIL-1, ASIL-A) subsystems driving low failure rate(Ex.: SIL-3, ASIL-C) subsystems, achieving Freedom From Interference(FFI). FFI is achieved through the prevention of cascading failures in a system, which is often accomplished via block partitioning the system to locate the failure origin and prevent its propagation to other system/subsystems. The first two steps of proposed FuSa design flow will be in a cyclic process starting with end equipment requirements and ends with a mature system block diagram that meets targeted end equipment requirements. The system block diagram is said to be mature only when the system block diagram meets end equipment requirements including safety requirements.

Key deliverables from the "**Step-2: Typical system block diagram**" of the proposed FuSa design life cycle is a mature system-level block diagram that meets the targeted end equipment requirements. Safety goals of the system are derived in this step by performing typical HARA on the block diagram. This step is one of the most crucial steps of designing functionally safe systems and sets a tone for the system FuSa journey by deriving the system application's safety goals.

2.3 Step-3 : Platform Selection

Platform Selection is one of the most crucial steps in the design life cycle. Once a mature system block diagram gets finalized from the second step, the important task is selection of the system blocks/subsystems based on performance requirements. TI's wide portfolio of mmWave Radar sensors can help achieve many performance requirements such as long-range or medium-range, angular resolution, range resolution, velocity resolution and so on.

For developing a FuSa compliant mmWave Radar sensor system, TI mmWave Radar sensors becomes the first choice to customers because of their versatile nature for vast applications and the availability of essential collaterals. TI mmWave Radar sensors uses FMCW for sensing the range, velocity and angle of multiple targets with better resolutions. TI mmWave Radar sensors mainly classify as Automotive and Industrial products based on the end application. TI mmWave Radar sensors are developed utilizing the Safety Element out of Context (SEooC) concept that allowed TI to develop systems independently with a view of assumed hazards, risks and FuSa standards suitable for vast safety critical applications. mmWave Radar sensors range from highly accurate front-end types to highly integrable complex SoC types with HWA for faster computations. mmWave Radar sensors certified with functional safety support the hardware integrity level up to ASIL-B or SIL-2. mmWave Radar sensors with non-functional safety variants are also available to the customers.

The versatility of the TI mmWave Radar sensor operation is programmable for detecting targets within the specified limits as per the customer's requirement that are good enough for typical automotive and industrial applications. TI mmWave Radar sensors supports operating radio frequency ranges of 76-81GHz and 57-64GHz for automotive and industrial domain applications complying with government regulations such as FCC, ETSI and TRAI. High-performance TI mmWave Radar sensors are incorporated with HWA in the design for faster computations improving the response time. TI mmWave Radar sensors support many communication interfaces with peripherals (some maybe only debug) like SPI, QSPI, I2C, CAN, LIN, RS232, GPIO, CSI2, PWM, GPADC, DMM, JTAG and so on specified in the datasheet of the mmWave Radar sensor.

TI mmWave Radar sensors also have variants with device security consisting of Hardware Security Module (HSM) supported by crypto hardware accelerators aiding secure authenticated and encrypted boot support and custom programmable root keys with key revocation capability. Thus, TI mmWave Radar sensors can be integrated into various highly integrated, distributed system applications such as automotive braking and steering systems, corner radar of car, industrial automation and drives, industrial robot sensor system for safer human presence detection and many others.

For ex., to design a corner radar of a car for safety applications, functional safety compliance of sensor system's hardware blocks/subsystems such as TI mmWave Radar sensor and Power supply block is crucial. The mmWave Radar sensor should possess some mandatory characteristics to be used in the FuSa compliant sensor system. The comparison table for few mandatory characteristics of the mmWave Radar sensor in FuSa compliant sensor system and TI's AWR2944 mmWave Radar sensor's best characteristics is mentioned below to check whether AWR2944 can be used in Corner Radar of a car.

All the characteristics of AWR2944 look compatible with the below mentioned mandatory requirements in Table 2-1, which makes AWR2944 suitable for this FuSa compliant Corner Radar sensor system.

Table 2-1. Comparison table of Corner Radar system requirements with AWR2944 mmWave Radar Sensor

	Corner Radar of a Car	**AWR2944**
AEC-Q100 Compliance	Yes	Yes
CAN-FD Interface	Yes	Yes (2 CAN-FD Interfaces available)
Device Security	Yes	Yes (Support through HSM and secure authenticated and encrypted boot)
Essential FuSa Collaterals[1]	Yes	Available
Ethernet Interface	Yes	Yes (High speed 100Mbps Fast Ethernet)
FuSa Compliance per ISO 26262	ASIL-B	ASIL-B targeted (supports Hardware Integrity up to)
Operating Frequency	77-81GHz	76-81GHz supported
Range	150m (Medium Range)	<=253m
Range Resolution	0.075m	>=0.0375m (Best resolution for 4GHZ Bandwidth)
Operating Junction Temperature Range	-40^{0}c to 125^{0}c	Yes (supports -40^{0}c to 125^{0}c)
Maximum Velocity	140kmph	<=143kmph
Power Consumption	3W(typical at 25^{0}c)	<3W(can support less than 3W at 25^{0}c)

Similarly, to design an Industrial Robot Sensor System for safer human presence detection, the system application requires safety related Hardware elements/blocks like TI mmWave Radar sensor to be FuSa compliant. Similar to the previous case, the mmWave Radar sensor must have some mandatory characteristics for its inclusion in the FuSa compliant sensor system. As an example, few mandatory requirements for the system are compared with the TI's IWRL6432 mmWave Radar sensor's best values for its inclusion in the system application. The comparison can be checked in the following table.

Table 2-2. Comparison table of Industrial robot sensor system requirements with IWRL6432 mmWave Radar Sensor

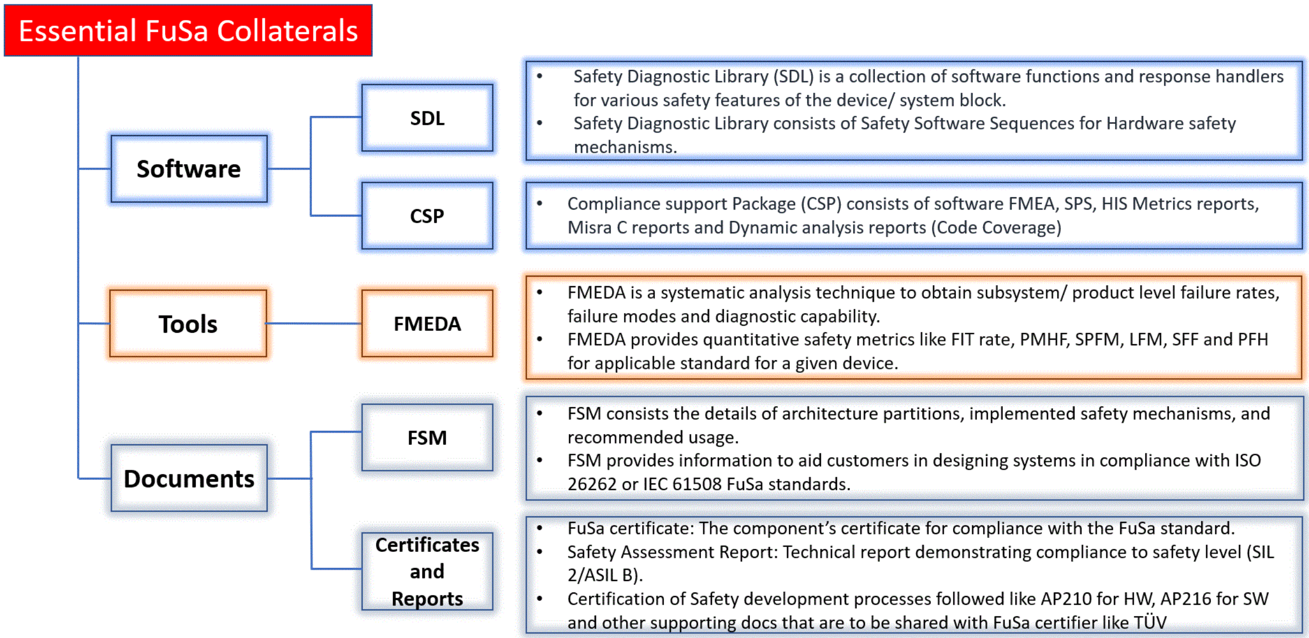
	Industrial Robot Sensor System	**IWRL6432**
CAN-FD Interface	Yes	Yes (CAN-FD Interface available)
FuSa Compliance per IEC 61508	SIL-2	SIL-2 targeted
High Speed Data Interface	Yes	Yes (supported by RDIF)
JTAG	Yes	Yes (supported for debug/development)
Maximum Range	5m	<=12m
Operating Frequency	57-64GHz	57-64GHz
SPI Interface	Yes	Yes (supported for control/communication)
Operating Junction Temperature Range	-40^{0}c to 105^{0}c	Yes (supports -40^{0}c to 105^{0}c)
UART Interface	Yes	Yes (2 UART's supported)

The requirements of a mmWave Radar sensor for safer human presence detection are fulfilled by the IWRL6432 Radar sensor with respect to the above requirements mentioned in Table 2-2. As industrial robots might work continuously for longer duration, TI's IWRL6432 being a low power consumption device becomes an added advantage for the system. Please note that the parameters like range, velocity , angle and their resolutions of mmWave radar sensor are also dependent on the system's antenna design. So far, we have been discussing about the mmWave Radar sensor platform selection in FuSa system. In a similar way, the remaining blocks of the system must be compared with the system requirements and the decision to select the platform should be done wisely. All the safety hardware blocks of the sensor system must comply with safety standards for the successful FuSa certification of the system. All the components should have essential collaterals that are mandatory for the system's safety certification process. Please note that currently AWR2944 and IWRL6432 are FuSa targeted and the author is confident that FuSa certification for the device will be available in a short time.

The following documents come under essential collaterals, which are available for FuSa complaint TI mmWave Radar sensors like

- FMEDA(Failure Mode, Effect and Diagnostic Analysis)
- Safety Analysis Report(SAR)
- Functional Safety Manual(FSM)
- Functional Safety Certificate
- Test reports of the Firmware block
- Compliance support package

For FuSa-compliant sensor system, all the hardware, software and firmware blocks of the system/subsystems have to comply with FuSa standards and essential FuSa collaterals have to be available. For ex., mmWave Radar sensor should be checked for FuSa compliance and the availability of essential FuSa collaterals. The essential collaterals of system blocks, required for the successful FuSa certification of the system are mentioned briefly in this Figure 2-6.



- Safety Diagnostic Library (SDL) is a collection of software functions and response handlers for various safety features of the device/ system block.
- Safety Diagnostic Library consists of Safety Software Sequences for Hardware safety mechanisms.

- Compliance support Package (CSP) consists of software FMEA, SPS, HIS Metrics reports, Misra C reports and Dynamic analysis reports (Code Coverage)

- FMEDA is a systematic analysis technique to obtain subsystem/ product level failure rates, failure modes and diagnostic capability.
- FMEDA provides quantitative safety metrics like FIT rate, PMHF, SPFM, LFM, SFF and PFH for applicable standard for a given device.

- FSM consists the details of architecture partitions, implemented safety mechanisms, and recommended usage.
- FSM provides information to aid customers in designing systems in compliance with ISO 26262 or IEC 61508 FuSa standards.

- FuSa certificate: The component's certificate for compliance with the FuSa standard.
- Safety Assessment Report: Technical report demonstrating compliance to safety level (SIL 2/ASIL B).
- Certification of Safety development processes followed like AP210 for HW, AP216 for SW and other supporting docs that are to be shared with FuSa certifier like TÜV

Figure 2-6. Essential Collaterals

Software-related safety enablers like Functional Safety Diagnostic Software Library, Safety Compiler Qualification Kit and Safety software sequence document are only disclosed to the customers on request through mySecureSoftware. With all the FuSa requirements fulfillment, TI's mmWave Radar sensors becomes a great choice for sensing targets in Radar sensor system applications. For TI mmWave Radar sensor functional safety enablers, visit here. All the essential collaterals of the TI mmWave Radar sensor are provided to the customer through the TI website on respective product page or through mySecureSoftware for confidential FuSa collaterals. Similarly for the various blocks of the system, TI's wide product portfolio could be a solution. For ex., TI PMIC(LP87745-Q1) is the better choice for power supply in the FuSa system because of the FuSa compliance and the availability of essential FuSa collaterals.

Key Deliverables from the "**Step-3: Platform Selection**" are the selection of each of the blocks or components of the FuSa compliant sensor system meeting the end equipment functional and behavioural requirements, compliance with applicable FuSa standards with the availability of essential FuSa collaterals that supports FuSa certification of system.

2.4 Step-4 : Design and Analysis

Once the platforms are selected for all the blocks of the system in the Platform Selection step, the design of the mmWave Radar sensor system has to be analyzed for FuSa compliance. This step is comprehensive, important and could be the time consuming part of the proposed FuSa design life cycle since the system design is analyzed here properly and refined by addressing faults to meet the benchmarks of FuSa certification levels. The reliability of FuSa in the sensor system design is checked in this step by following the Design and Analysis flow. The flow starts with performing Failure Modes, Effects and Diagnostic Analysis(FMEDA) on the system design and the resultant metrics are compared with applicable FuSa certification level benchmarks for finalizing the topology of sensor system design. The functional safety issues that could arise in the system are addressed in this step by updating/configuring the safety hooks/ mechanisms of the system.

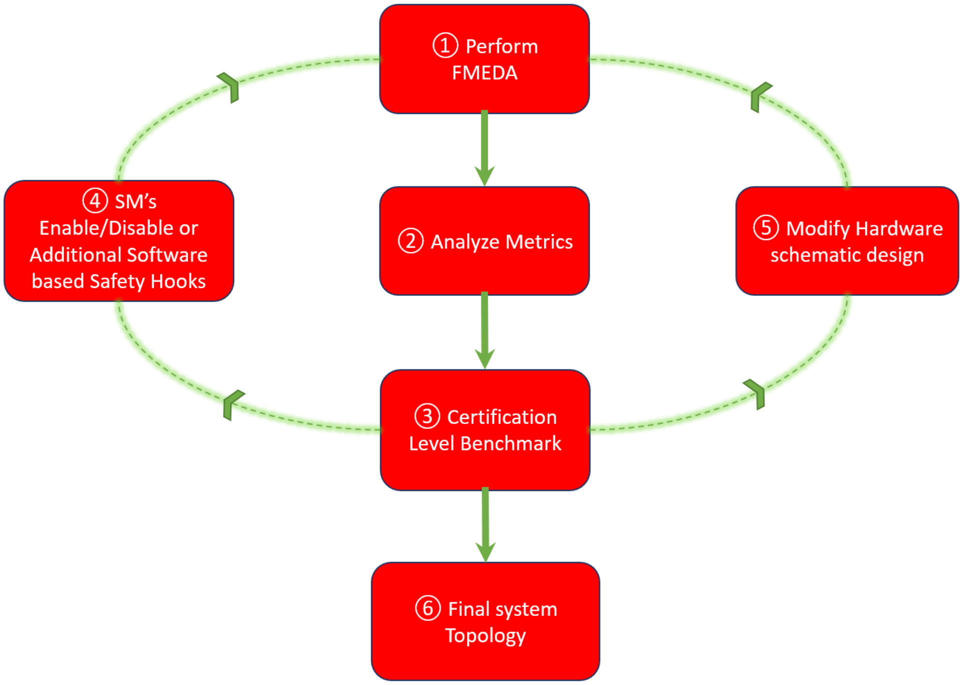

① Perform FMEDA
② Analyze Metrics
③ Certification Level Benchmark
④ SM's Enable/Disable or Additional Software based Safety Hooks
⑤ Modify Hardware schematic design
⑥ Final system Topology

Figure 2-7. Design and Analysis

1. **Perform FMEDA**: A FMEDA is a common functional safety analysis technique used to determine the effectiveness of a functional safety architecture. FMEDA provides insightful information regarding safety goals met by safety related parts in the system by providing quantitative safety metrics of the system to measure random hardware failure metrics of a design according to the applicable FuSa standards ISO 26262/IEC 61508. TI has created a FMEDA for the mmWave Radar device that allows the user to tailor the metrics to their specific use case based on which features or design blocks are being used as part of the safety function. This tool additionally allows the user to modify the environmental factors, device power consumption, and other factors that affect the raw (base) FIT rates. Using TI FMEDA tool, we can configure the sensor system through Mission profile tailoring, Pin level tailoring, Function and Diagnostic tailoring.
   - Mission profile tailoring : This sheet allows the users to control the following parameters to update the calculations accordingly: Package Type, Life Cycle for the device (in hours) up to a maximum of 20 years, safe vs non-safe control for each component type, ambient temperature, etc.
   - Pin level tailoring : This sheet takes the raw (base) package FIT rate and distributes it equally among each of the pins (or balls) of the device. The user should use the FMEDA and safety manual to determine which device pins are used in their application for a safety-related function. The unused device pins have to be removed from the FIT calculation.

- Function and Diagnostic tailoring : This sheet captures raw FIT rate for permanent, transient and latent fault and distributes them among each of the design blocks (sometimes referred to hardware elements or IP blocks) of the device. Each row represents the lowest part of this analysis and each row gets a percentage of the FIT based on its transistor count or memory size. The user should refer to the Safety Manual in combination with this FMEDA to determine which design blocks are used in their application for a safety-related function. The unused design blocks have to be removed from the FIT calculation.

2. **Analyze Metrics**: FMEDA is mainly used to know Diagnostic Coverage (DC) and Failure in time (FIT) of the system. For Industrial applications, as per IEC 61508, FMEDA reports safety metrics Safe Failure Fraction(SFF) and Probability of Failure on Demand per Hour(PFH). Similarly for Automotive applications, as per ISO 26262, FMEDA reports safety metrics Probabilistic Metrics for Hardware Failures(PMFH), Single Point Fault Metric(SPFM) and Latent Fault Metric(LFM). The Pin Failure Modes and Effects Analysis is performed on the system/device pins to check the pin damages that could result in malfunction of the system/device.
3. **Certification Level Benchmark**: The metrics of the sensor system from the FMEDA tool are compared with the safety integrity level benchmarks as per FuSa standards ISO26262/IEC61508 to check the safety capabilities of the design. If the metrics meets the targeted safety level benchmarks then the system design can become the final system topology. Else, customer could move to step 4 and step 5 for improving the system safety. The certification level benchmarks according to ISO 26262 and IEC 61508 are mentioned in Table 2-3 and Table 2-4 respectively.

Table 2-3. Certification Level Benchmarks According to ISO 26262-5

ASIL Level	SPFM	LFM	PMHF (in FIT; Failures in Time)
ASIL-B	≥90%	≥60%	≤100 FIT
ASIL-C	≥97%	≥80%	≤100 FIT
ASIL-D	≥99%	≥90%	≤10 FIT

Table 2-4. Certification Level Benchmarks According to IEC 61508

SIL Level	SFF	PFH (in FIT; Failures in Time)
SIL-2	≥90%	≥100 FIT to <1000 FIT
SIL-3	≥99%	≥10 FIT to <100 FIT

4. **SM's Enable/Disable or Additional Software based Safety Hooks**: If certification level benchmarks are not met, the customer can configure the available safety mechanisms(enabling/disabling) to bring down the failures of the system. The customer must repeat the step 1, 2 and 3 of this flow after configuration changes. In order to further improve the diagnostic coverage of faults and reduce the faults of the system, the customer may add some additional software safety mechanisms. However, the steps 1, 2 and 3 have to be repeated again.
5. **Modify Hardware schematic design**: To improve the system's safety, the customer can also modify system hardware design starting with minor changes in parallel to the software safety hooks step. In order to further improve the safety and reduce the faults, the customer might have to replace that hardware part by performing the platform selection or sometimes even change the system block diagram. After updating these changes, the system design metrics are expected to meet the FuSa certification level benchmarks.
6. **Final system Topology**: Once the FMEDA metrics meet the targeted FuSa certification level benchmarks(SIL-1/2/3/4 or ASIL-A/B/C/D), the system block diagram can be called as final sensor system topology. This final sensor system topology will now be ready for FuSa Cerification step.

Note

- Faults can either be Random or Systematic. Both IEC 61508 and ISO 26262 exclude systematic faults while calculating random hardware metrics. The faults leading from human error in hardware development, software development and the tools used in designing the system are systematic faults, and can be avoided by following the best design practices.
- FMEDA tool for the respective TI mmWave Radar sensor can be shared with the customers under NDA with TI.
- Estimations of failure rate are often defined in terms of Failures In Time (FIT - failures for 10^9 hours of operation).
- Base Failure Rates (BFR) of the system are based on IEC 62380 standard that quantifies the intrinsic reliability of the semiconductor components while operating under normal environmental conditions.
- While developing any system, designing and refining of the system block diagram should be done in parallel to avoid architectural changes which might occur later. Refinement can be in Hardware design or Software design or both.

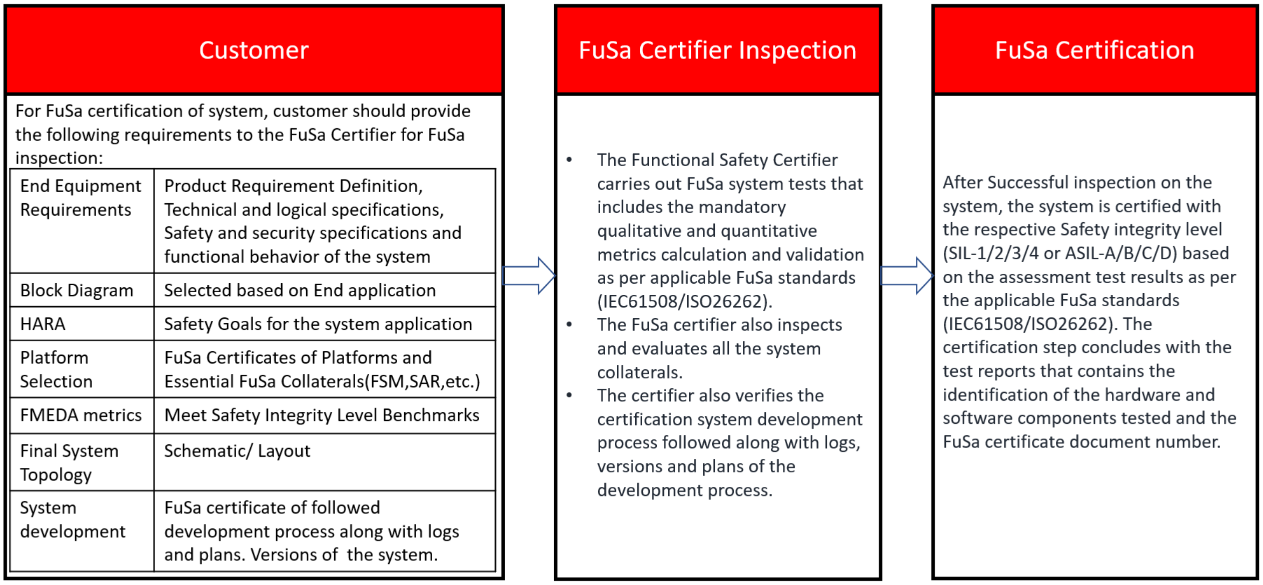
From the corner radar example, after all the blocks of sensor system are selected from the Platform selection step, the system design has to be analyzed for its reliable usage in safety applications. The corner radar system is checked for Diagnostic coverage and FIT rate by performing the FMEDA on the system design. Let us consider that the customer infers from good engineering judgment and FMEDA metrics that most faults caused by the power supply rails in the system are not letting the system meet the certification level benchmarks. To improve the safety, the customer can choose to add software safety hook like resetting the entire system if the power supply to a certain block is found below the minimal operational range. Or, the customer can add hardware power management component like VMON for asserting the reset signal on detecting these faults. As mentioned, the updated design have to go through 1,2 and 3 steps of Design and Analysis flow again. The FMEDA results after updating the design might meet the Certification level benchmarks and then design can be referred as Final system Topology for that system application.

Key Deliverables from the "**Step-4: Design and Analysis**" is preparing the final sensor system topology, ready for FuSa certification. This could be the most critical and probably the most time taking step of the FuSa design life cycle. The refinement of the system design through analysis is done either by software changes or hardware changes or both to meet the applicable FuSa standards benchmarks. This step validates the Final sensor system design for reliability with FuSa compliance level benchmarks.

2.5 Step-5: Certification

The FuSa certification is the final step of proposed FuSa design life cycle. The final system topology along with all the essential safety collaterals of the blocks is now ready for the FuSa certification process. A qualified Functional Safety Expert (FSE) plays a vital role in building the FuSa compliant sensor system by following the FuSa certified system development process.

The adherence to safety goals as per applicable FuSa standards by the system will be assessed by the third-party certification bodies like Technischer Überwachungsverein (TÜV) for the FuSa compliance level certification. The essential collaterals, logs, versions, FuSa certificate of followed System development process(Hardware and Software) and safety plans of the system design ought to be shared with the FuSa certification body with evidences which are taken care by the system integrator's FSE. The FSE takes feedback from the certifier during the inspection for improving the safety of system until the targeted FuSa certification benchmarks are met. The certification body reviews the system documentation collaterals, verifies the system development process and evaluates the system design by performing FuSa system tests. After successful inspection by FuSa certifier, based on the assessment results, the system will be certified with respective safety integrity level as per FuSa standards and concludes with the report on certificate. Once the system is FuSa compliance certified, the sensor system is now ready to be used in Safety applications like Automotive and Industrial applications as per the FuSa certification safety integrity level. The following Figure 2-8 describes the flow of the certification step.



Customer

For FuSa certification of system, customer should provide the following requirements to the FuSa Certifier for FuSa inspection:

End Equipment Requirements	Product Requirement Definition, Technical and logical specifications, Safety and security specifications and functional behavior of the system
Block Diagram	Selected based on End application
HARA	Safety Goals for the system application
Platform Selection	FuSa Certificates of Platforms and Essential FuSa Collaterals(FSM,SAR,etc.)
FMEDA metrics	Meet Safety Integrity Level Benchmarks
Final System Topology	Schematic/ Layout
System development	FuSa certificate of followed development process along with logs and plans. Versions of the system.

FuSa Certifier Inspection

- The Functional Safety Certifier carries out FuSa system tests that includes the mandatory qualitative and quantitative metrics calculation and validation as per applicable FuSa standards (IEC61508/ISO26262).
- The FuSa certifier also inspects and evaluates all the system collaterals.
- The certifier also verifies the certification system development process followed along with logs, versions and plans of the development process.

FuSa Certification

After Successful inspection on the system, the system is certified with the respective Safety integrity level (SIL-1/2/3/4 or ASIL-A/B/C/D) based on the assessment test results as per the applicable FuSa standards (IEC61508/ISO26262). The certification step concludes with the test reports that contains the identification of the hardware and software components tested and the FuSa certificate document number.

Figure 2-8. FuSa Certification step flow

For ex., the FuSa certification of the corner radar system developed by the customer as per automotive FuSa standard ISO 26262 has to be certified by the Third party certifiers like TÜV. The essential collaterals of the system, versions, logs, followed system development process and safety plans of system must be readily available to share with certifier for FuSa compliance level certification. Similarly, for the FuSa certification of the Intelligent Robot sensing system of safer human presence detection as per industrial FuSa standard IEC 61508, the customer must provide the essential collaterals, versions, logs of system design, safety plans and the followed system development process to the certification body for assessing the system and certify safety integrity level(SIL-1/2/3/4) to the system.

Note

- The role of TI or other companies whose component has also been used is in the system for safety is only to share the essential collaterals of that component which might support the customer. The customer possess the whole responsibility of the system design and its usage in safety applications.
- Sometimes as a feedback from the FuSa certifier, customer might be asked to add safety hooks to the system which might lead to hardware changes, not only software. After every update to the design at this stage, Design and Analysis flow must be repeated again.

Key Deliverables from the "**Step-5: Certification**" is the safety integrity level(ASIL-A/B/C/D or SIL-1/2/3/4) certification of the system's design from the FuSa certification body as per applicable FuSa standards. In this FuSa certification step, the FuSa certification body assesses the system by performing tests, evaluates all the collaterals and verifies system development process(logs, versions and plans). The FSE plays a crucial role by managing the system design process for FuSa certification of system. Once, the customer's system design is certified with safety integrity level compliance according to applicable FuSa standards, the FuSa certificate acts as license for system design usage in appropriate safety critical applications.

3 References

- IEC 61508: Second edition 2010-04: Functional safety of electrical/electronic/programmable electronic safety – related systems.
- ISO 26262: Second Edition 2018-12: Road Vehicles – Functional Safety, ISO 26262, International Organization for Standardization (2018)
- IEEE Standard 1012-2016: IEEE Standard for System, Software, and Hardware Verification and Validation
- ISO Standard 21448-2022: Road vehicles – Safety of the intended functionality
- QRAS AP00210 : FuSa Certificate of Hardware Development Process
- QRAS AP00216 : FuSa Certificate of Software Development Process
- AWR2944 : Device Datasheet of AWR2944
- AWRL6432 : Device Datasheet of AWRL6432
- IWRL6432 : Device Datasheet of IWRL6432
- AWRL1432 : Device Datasheet of AWRL1432
- AWR2944 TRM : Technical Reference Manual(TRM) of AWR2944
- IWRL6432 TRM : Technical Reference Manual(TRM) of IWRL6432
- AWR2944 EVM : Evaluation Module(EVM) of AWR2944
- IWRL6432 BOOST : Evaluation Module(EVM) of IWRL6432
- **Functional Safety Manual(FSM)** of **AWR2944** will be available to customers under NDA with TI.
- **Functional Safety Manual(FSM)** of **xWRLx432** for IWRL6432 will be available to customers under NDA with TI.

4 Acronyms

AEC	Automotive Electronics Council
ASIL	Automotive Safety Integrity Level
BFR	Base Failure Rate
BIST	Built-in self-test
BP	BoosterPack
BSS	BIST Subsystem
CAN-FD	Controllable Area Network - Flexible Data
CCF	Common Cause Failures
CMOS	Complementary Metal Oxide Semiconductor
CSI2	Camera Serial Interface
CSL	Chip Support Library
CSP	Compliance Support Package
DC	Diagnostic Coverage
DCA	Data Capture Adapter
DFA	Dependent Failure Analysis
DMM	Data Modification Module
DSP	Digital Signal Processor
ECC	Error Correction Code
EEPROM	Electrically Erasable Programmable Read-Only Memory
EER	End Equipment Requirements
ETSI	European Telecommunications Standards Institute
EVM	Evaluation Module
FCC	Federal Communications Commission
FFI	Freedom From Interference
FIT	Failure In Time
FMA	Failure Mode Analysis
FMCW	Frequency Modulated Continuous Wave
FMD	Failure Mode Distribution
FMEA	Failure Mode and Effect Analysis
FMEDA	Failure Mode, Effect and Diagnostic Analysis
FOV	Field of View
FSE	Functional Safety Expert
FSM	Functional Safety Manual
FTA	Fault-Tree Analysis
FuSa	Functional Safety
GPADC	General Purpose Analog Digital Converter
GPIO	General Purpose Input Output
HARA	Hazard Analysis and Risk Assessment
HIS	Hersteller Initiative Software
HSM	Hardware Security Module
HW	Hardware
HWA	Hardware Accelerator
I2C	Inter Integrated Circuits
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INA	Instrumentation Amplifier
IP	Intellectual Property

ISO	International Organization for Standardization
JTAG	Joint Test Action Group
LFM	Latent Fault Metric
LIN	Local Interconnect Network
LP	LaunchPad
LRR	Long Range Radar
LVDS	Low-Voltage Differential Signaling
MCU	Microcontroller unit
MIPI	Mobile Industry Processor Interface
MISRA	Motor Industry Software Reliability Association
mmWave	Millimeter Wave
MRR	Medium Range Radar
MTTF	Mean Time To Failure
NDA	Non Disclosure Agreement
PFH	Probability of Failure on Demand per Hour
PM	Power Management
PMHF	Probabilistic Metrics for Hardware Failures
PMIC	Power Management Integrated Circuit
PRD	Product Requirements Definition
PWM	Pulse Width Modulation
QM	Quality-Managed
QRAS	Quantitative Risk Assessment System
QSPI	Quad Serial Peripheral Interface
RF	Radio Frequency
RS232	Recommended Standard 232
SAR	Safety Analysis Report
SDL	Safety Diagnostic Library
SEooC	Safety Element out of Context
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SM	Safety Mechanisms
SoC	System on Chip
SOP	Sense On Power
SOTIF	Safety of the Intended Functionality
SPFM	Single Point Fault Metric
SPI	Serial Peripheral Interface
SPS	Software Product Specification
SRR	Short Range Radar
SW	Software
TI	Texas Instruments
TRAI	Telecom Regulatory Authority of India
TÜV	Technischer Überwachungsverein
UART	Universal Asynchronous Receiver-Transmitter
USB	Universal Serial Bus
V&V	Verification and Validation

5 Revision History

NOTE: Page numbers for previous revisions may differ from page numbers in the current version.

Changes from June 15, 2022 to April 4, 2024 (from Revision * (June 2022) to Revision A (April 2024))	Page
• Updated Table 2-4 with correct PFH(in FIT) values	13
• Updated Notes section	13

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