오토모티브 설계 시 Jacinto™ 7 프로세서의 기능적 안전성 활용하기

Yashwant Dutt
엔지니어링 관리자
Jacinto™ 프로세서

Sam Visalli
기능 안전 관리자
Jacinto 프로세서

Mahmut Cifti
시스템 설계자
Jacinto 프로세서

Dave Maples
이사, 오토모티브 게이트웨이
및 인포테인먼트
Jacinto 프로세서

Krishna Gopalakrishnan
품질 관리자
임베디드 프로세싱

텍사스 인스트루먼트

개요

자율주행, 커넥티드 카 및 하이브리드 전기 자동차/ 전기 자동차(HEV/EV)의 출현은 자동차 산업의 패러다임을 변화시키고 있습니다. 이러한 기술의 핵심인 기능적 안전성은 더 이상 기존의 마이크로 컨트롤러(MCU)에만 국한되지 않고 애플리케이션 프로세서에서도 지원되어야 합니다. ECU(엔진 제어 장치) 컴퓨팅 요구 사항이 증가함에 따라 애플리케이션 요구를 실현하기 위해 더 많은 기능을 갖춘 프로세서, 하드웨어 가속기 및 DSP(디지털 신호 프로세서)가 필요합니다. 이러한 매개 변수를 고려해보면, 기존 코어로는 안전과 관련된 데이터를 처리하거나 다중 중요도 기능을 수행하기가 더욱 어려워졌습니다. 공유된 플랫폼의 다중 중요도 시스템에서는 중요도 수준에 따라 업무가 수행됩니다. 다중 중요도 시스템에서는 필수 안전 작업의 타이밍이 엄격하게 보장되어야 합니다.

TI의 차량용 Jacinto™ 7 시스템 온 칩(SoC) 제품군은 절연 ASIL-D 안전 MCU를 통합할 뿐만 아니라 모든 프로세싱 코어에 더 높은 수준의 ASIL 기능적 안전성을 제공합니다. 이 백서는 TDA4x 및 DRA8x 디바이스가 속한 Jacinto 7 SoC 제품군에 내장된 안전성 진단 방법에 대해 설명합니다. 해당 안전성 진단 방법에는 다양한 절연 매커니즘, 소프트웨어 아키텍처, 소프트웨어 제품 소개, 솔루션 설계 방식이 포함됩니다.

기능적 안전성이란 무엇일까요?

기능적 안전성이란 하드웨어의 고장 및 환경적인 요인을 비롯한 그 어떤 고장에도 손상을 최소화하는 기술로 오작동에 대응할 수 있는 시스템의 능력입니다. ISO 26262 표준에 따르면, 이는 허용할 수 없는 위험에서 자유롭다는 것을 의미합니다. 기능적 안전성에 대한 개념은 자동차 산업에서 꽤 오랫동안 존재해 왔지만, 애플리케이션 프로세서에 기능적 안전성을 도입하는 것은 초기 단계입니다. Jacinto 7 프로세서는 ASIL-D 표준을 준수하는 애플리케이션을 위해 한때 MCU 디바이스에만 국한되었던 안전성에 대한 개념을 애플리케이션 프로세서에도 도입했습니다. 이러한 프로세서는 하드웨어적으로 지원되는 절연 기술을 사용하여 다중 중요도 시스템을 구현합니다. 하나의 장치로 필수 안전 작업과 필수가 아닌 안전 작업을 모두 원활하게 호스팅할 수 있으므로 시스템 비용이 절감됩니다.

Jacinto 7 프로세서 제품군은 하드웨어 및 소프트웨어와 관련된 포괄적인 안전 솔루션을 제공합니다. ASIL-D 기능을 제공하기 위해 TÜV SÜD와 같은 독립적인 기능적 안전성 평가 기관에서 인증한 하드웨어 개발 및 프로세스를 통해 체계적으로 설계되었습니다. 이 프로세서에는 결함을 무작위로 감지해내는 진단 회로가 있으며 크게 3가지 카테고리로 분류할 수 있습니다.

- 메모리, 클럭, 전원, 코어 및 상호 연결을 위한 테스트 회로를 담당하는 기본 진단.
- ASIL-B와 ASIL-D 같은 다중 중요도 작업을 지원하는 시스템에서 FFI(Freedom From Interference)를 단순화하는 별도의 전압/전력/리셋 및 방화벽 MMU(Memory Management Unit)와 MPU(Microprocessors) 같은 하드웨어 절연 기능.
- 프리즈 프레임 감지와 같은 애플리케이션별 하드웨어 진단.

또한 특정 애플리케이션에서 요구하는 ASIL 표준에 관계 없이 Jacinto 7 프로세서 제품군은

시스템 요소로서도 외부적으로 인증을 받습니다. 하드웨어 개발 프로세스와 마찬가지로 소프트웨어 개발 프로세서도 TÜV SÜD와 같은 독립적인 기능적 안전성 평가기관으로부터 인증을 받습니다. Jacinto 7 소프트웨어 구성 요소의 안전에 대한 요구수준은 최대 ASIL-D의 기능적 안전 수준을 충족하도록 설계되었습니다.

소프트웨어 구성 요소는 외부 인증을 받지 않았습니다. 인증 지원 패키지를 통해 최종 소프트웨어/시스템을 인증할 수 있습니다. 소프트웨어 진단 라이브러리는 온칩 진단 사용법의 예와 함께 제공됩니다. TI는 호환 가능한 하드웨어 및 소프트웨어에 대한 기능적 안전성 인증서를 제공합니다.

Jacinto 7 프로세서의 차별화된 주요 안전 아키텍처 중 하나는 MCU 기능 통합으로, 이를 통해 시스템 설계를 간소화하고 보드의 구성요소의 개수와 공간을 줄일 수 있습니다. 애플리케이션 프로세서는 두 가지 독립 도메인인 기본 도메인과 MCU 도메인으로 나뉩니다. 기본 도메인은 MPU, GPU(Graphic Processing Unit), 멀티미디어, DSP를 포함한 비전 하드웨어 가속기, 필요한 주변 장치와 같은 고성능 컴퓨팅 코어를 제공합니다. MCU 도메인은 FFI가 높은 기능적 안전성을 제공하기 위한 독립 도메인입니다.

Jacinto7 프로세서는 안전 표준을 준수하는 디바이스로, 다음의 기능적 안전성에 대한 문서들과 함께 제공됩니다.

- 지원되는 Jacinto 7 프로세서 제품군을 사용하여 안전 필수 시스템을 설계하는데 도움이 되는 정보를 전달하는 안전 매뉴얼이 제공됩니다.
- 명시된 기능적 안전성 목적을 달성하기 위해 디바이스의 기능에 대한 정보가 포함된 안전성 분석 보고서가 제공됩니다.
- 안전성 분석보고서 내의 별도 문서로 고장 유형에 따른 영향 및 진단과 분석 등 정량적인 내용이 포함되어 있습니다. 이 문서에는 구성 요소의 여러 부분에 대한 세부 정보가 포함되어 있어 기능적 안전성 메카니즘을 필요로 하는 맞춤형 애플리케이션 설계를 위한 계산을 용이하게 하고 시간적 결함(Failure in Time; FIT), 진단 범위, SPFM/LFM, 고장 유형에 대한 정보도 포함되어 있습니다.

소프트웨어 기능적 안전성 개요

소프트웨어는 제품의 전반적인 안전성 목적을 달성하는 데 중요한 요소입니다. Jacinto 7 소프트웨어의 안전성은 다음 두 가지 측면으로 구성됩니다.

- 안전 경로에 사용되는 소프트웨어 구성 요소의 체계적인 기능.
- 하드웨어 진단 및 참조 예제 코드에 대한 포괄적인 소프트웨어 지원.

TI는 체계적인 기능을 위해 다양한 팀에서 사용되는 잘 정의되고 일반적인 소프트웨어 개발 프로세스와 도구를 따릅니다.

독립적인 소프트웨어 품질 위원회가 모든 소프트웨어 제품을 승인합니다. TI가 제공할 수 있는 기능성 안전성과 관련된 결과물들에는 다음이 포함됩니다.

- 프로세스 표준 준수: 기능적 안전성 소프트웨어 개발 프로세스는 ISO 26262, ASIL-D 및 IEC 61508 표준을 준수하도록 TÜV SÜD에 의해 인증되었습니다.
- 프로젝트 표준 준수: 프로젝트 규정 준수는 내부 감사를 통해 보장되며 ISO 26262 또는 IEC 61508 프로세스에 따라 수행됩니다. 모든 표준 미달 사항은 개선 계획 및 조치를 통해 수정됩니다.
- 고객 인증 활성화: 안전 프로세스를 따라서 개발된 모든 소프트웨어에는 표준 준수 지원 패키지(CSP)가 제공됩니다. CSP에는 다음이 포함되어 있습니다.
  - TI 내부 감사 보고서.
  - 요구 사항, 테스트 계획 및 보고서.
  - 추적 보고서.

- 동적 코드 범위 분석 보고서.
- 정적 코드 분석/ MISRA-C(Motor Industry Software Reliability Association C) 보고서.
- 기능적 안전성 진단 라이브러리 및 매뉴얼.
- 컴파일러 검증 키트.
- 고장 유형에 따른 영향 및 치명도 분석 (FMEDA).

통합 Jacinto 7 소프트웨어 개발 키트(SDK) 는 안전성 솔루션을 개발할 수 있도록 소프트웨어 지원도 제공합니다. "있는 그대로" 사용되어야 하며, 안전성 루프의 일부를 구성하는 Jacinto 7 의 구성 요소는 TI의 기능적 안전성 소트웨어 개발 프로세스에 따라 개발되었습니다. 이 프로세스에는 모든 주요 안전 IP를 비롯 MCU 추상화 계층 드라이버, IP, DMA와 같은 기능의 소프트웨어를 위한 소프트웨어 진단 라이브러리가 포함됩니다.

또한 TI는 안전 기능들을 애플리케이션에 구현하는 방법에 대한 이해를 돕고자 다양한 레퍼런스 예시를 제공합니다. 안전 기능은 애플리케이션마다 다를 수 있으므로 레퍼런스 소프트웨어는 안전성 프로세스에 따라 개발되지 않았으며 TI 기준 프로세스를 따랐습니다.

표 1은 SDK에 포함된 진단 소프트웨어, 기능적 소프트웨어, 레퍼런스 소프트웨어가 제공하는 다양한 예시를 보여줍니다.

안전 애플리케이션 매핑

데이터 센터 및 모바일 애플리케이션을 위해 구축된 일반적인 SoC 아키텍처는 차량용 애플리케이션에 필요한 안전 기능이 없으며, 소프트웨어 기반의 안전성 진단 기능을 추가하기 위해서는 추가 컴퓨팅 성능이 필요합니다. Jacinto 7 프로세서 제품군의 다양한 하드웨어 및 소프트웨어 안전 기능이 최종 애플리케이션에 도입되면 추가적인 컴퓨터 성능에 대한 필요성이 줄어듭니다.

그림 1에는 일반적인 비전 기반의 시스템을 보여줍니다. 입력 카메라 데이터는 카메라 직렬 인터페이스를 통해 캡처되고 비전 프로세싱 하드웨어 엔진으로 전송되어 RAW 데이터에서 YUV로 변환됩니다. 프로세서의 온칩 C7x

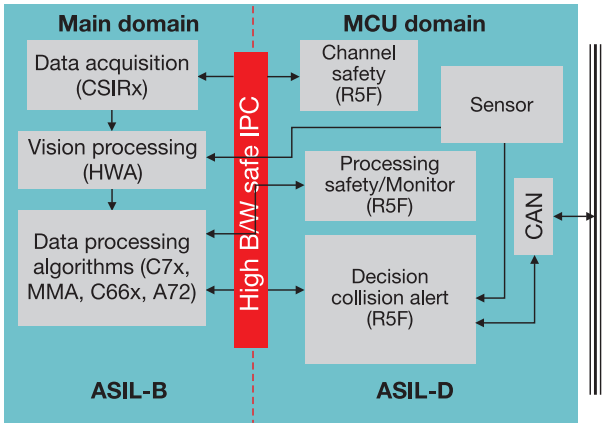

그림 1. 일반 비전 프로세싱.

소프트웨어 진단	기능적 소프트웨어	레퍼런스 소프트웨어
소프트웨어 진단 라이브러리(SDL)—다양한 안전 기능을 위한 소프트웨어 기능 및 응답 처리기 • 다양한 모듈용 LBIST / PBIST • 주변 장치 viz CAN, SPI • 안전 IP: CRC, ECC, RTI, DCC, ESM • 오류 주입 기능 • 체계적 기능이 있는 소프트웨어	안전 경로의 구성 요소—체계적 기능이 내장된 SDK 구성 요소 • AUTOSAR MCAL(CAN, DIO, SPI, ETH, IPC, ADC, PWM, WDG, GPT) • 안전 IP용 CSL-FL(예: ECC, CRC, DCC, ESM, BIST, VTM, PGD, POK, ADC) • SCI 클라이언트, DMA • SYSFW 펌웨어 • TI-RTOS • 안전 경로의 모든 IP용 CSL-FL • MMA, TIDL 라이브러리 • CSI2, VHWA, IPC용 LLD • 컴파일러 검증 키트	• FFI, Main/MCU 아일랜드 절연 및 기타 안전 기능에 대한 예제 코드 • 실제 사용 사례에서 안전 IP 사용법을 시연할 수 있는 레퍼런스 소프트웨어 • 안전 매뉴얼에 명시된 진단을 시연할 수 있는 레퍼런스 소프트웨어
기능 안전 소프트웨어 개발 프로세스 소프트웨어 규정 준수 지원 패키지(CSP)		표준 소프트웨어 개발 프로세스

표 1. 소프트웨어 기능 안전 제품.

DSP, MMA 및 Arm® Cortex®-A72 코어에서는 객체분류와 여유 공간 감지와 같은 다양한 분석 및 딥 러닝 알고리즘이 실행됩니다. MCU 도메인은 각 단계마다 검사기 역할을 하며 처리 중인 데이터를 주기적으로 확인하고 모니터링합니다. MCU 도메인은 다른 센서들의 입력을 바탕으로 안전 기능을 최종 결정한 다음 CAN(Controller Area Network)과 같은 통신 프로토콜을 통해 다른 차량용 ECU와 통신합니다.

그림 1의 각 블록은 Jacinto 7 프로세서의 모듈이며 CPU 리소스를 사용하지 않고 전반적인 안전 목표를 달성하기 위한 하드웨어 진단을 포함합니다. 표 2는 앞에서 언급한 것과 동일한 비전 애플리케이션을 매핑하고 전형적인 SoC와 비교하여 Jacinto 7 프로세서 제품군 간의 기능적 안전 차별화를 보여줍니다.

Jacinto 프로세서 호환 전원 관리 솔루션

Jacinto 프로세서 제품군과 함께 TI는 기능적 안전성을 요구하는 차량용 애플리케이션에 적합한 고정밀의 유연한 전력 관리 IC(PMIC) 2개를 개발했습니다. 이 PMIC는 기능적 안전성에 대한 문서와 함께 제공됩니다. PMIC TPS6594-Q1과 LP8764-Q1은 기본 도메인과 MCU 도메인 모두에 확장 가능한 전원 관리 솔루션을 제공하며, 최대 ASIL-D 표준을 준수하는 기능적 안전성을 지원합니다.

올바르게 설계된 시스템은 다음을 포함한 기능적 안전성에 대한 요구 사항을 지원합니다.

- SoC는 센서 데이터를 확인
- MCU는 SoC를 확인
- MCU는 액추에이터를 제어
- MCU는 액추에이터가 제어에 따라 예정된 방식으로 반응하는지 확인
- PMIC는 MCU 하드웨어 및 소프트웨어 실행을 모니터링
- PMIC는 애플리케이션 프로세서 하드웨어 작동을 모니터링

PMIC가 잘못된 작동을 감지하면 ENDRV 출력 핀을 낮게 만들어 시스템을 안전한 상태로 만듭니다. 오류의 예시는 다음과 같습니다:

안전 도메인	특징	일반 오토모티브 시스템	Jacinto 7 프로세서 제품군 장점
• 아키텍처	• 통합 MCU 아일랜드 • 이종 안전 코어	• 외부 MCU 사용 • 하이퍼바이저 및 외부 MCU 사용, 하이퍼바이저에 추가 CPU 부하 필요	• 시스템 비용 최적화 • 확장 가능한 안전 성능 • 하이버파이저가 필요 없는 결함 안전성 및 복구
• 기본 안전 • 트랜션트 및 영구적 고장	• 코어, 메모리 및 하드웨어 가속기를 위한 내장 자체 테스트 • 메모리에 대한 오류 수정 코드 • 락스텝 DMIPS • CRC, 워치독, 클록 비교기 • 상호 연결에 대한 안전성	• 일반적으로 애플리케이션 프로세서에서는 사용할 수 없음 • 소프트웨어 진단을 위해 모든 코어에 추가 부하	• 하드웨어에서 모두 사용 가능 • 무시할 수 있는 수준의 추가 CPU 부하
• 절연 • FFI	• MMU, MPU, 방화벽, 시간 초과 개스킷	• 하이퍼바이저 – 소프트웨어 기반 방법 – 부하 프로세싱 코어 • 소프트웨어 진단을 위해 모든 코어에 추가 부하	• 안전 작업과 비안전 작업 간의 하드웨어 절연 하드웨어 격리 • 무시할 수 있는 수준의 추가 CPU 부하
• 애플리케이션 안전 기능	• 블랙 프레임 • 프리즈 프레임 • 카메라 차단 • 딥 러닝 네트워크 매개 변수 안전성	• 소프트웨어 기반 방법 – 처리 코어 부하 • 소프트웨어 진단을 위해 모든 코어에 추가 부하	• 프리즈 프레임 모니터: 하드웨어 지원 프리즈 프레임 감지. CPU 부하 없음 • 하드웨어 CRC 기반 딥 러닝 네트워크 안전성. 추가 CPU 부하 없음

표 2. 애플리케이션에 대한 안전 매핑.

- MCU 또는 SoC에 대한 공급 전압의 결함
- PMIC에 대한 입력 공급 전압의 결함
- MCU 소프트웨어 또는 하드웨어 오류
- SoC용 ESM에서 보고한 SoC 하드웨어 오류

TPS6594-Q1과 LP8764-Q1 디바이스는 독립 PMIC로 사용될 수 있지만, 시스템의 확장성을 위해 다수의 PMIC가 MCU 또는 프로세서와 함께 사용될 때는 CRC 프로토콜이 접목된 TWI(Two-Wire-Interface)를 통해 서로 통신하게 됩니다. 이러한 인터페이스는 PMIC 간의 전원 상태와 오류 처리가 동기화될 수 있도록 합니다. 주기적인 버스 폴링은 통신 버스의 모든 PMIC 상태를 점검합니다. 이를 통해 시스템 결함 상태에 대한 신속한 대응이 가능해 솔루션의 최종 시스템이 더 높은 기능적 안전성 목표를 달성할 수 있도록 합니다. 그림 2는 2 개의 PMIC와 Jacinto 7 프로세서 시스템을 연결한 사용 사례를 보여줍니다. 대부분의 애플리케이션은 한 개의 TPS6594-Q1을 사용하지만, 추가적으로 LP8764-Q1을 사용하게 되면 추가적인 시스템 기능을 도입할 수 있고 성능을 향상시킬 수 있습니다. SoC에 전원을 공급하기 위해 하나 혹은 그 이상의 PMIC를 사용할 수 있는 "가상" PMIC기능은 시스템 비용을 최적화하는 동시에 고성능 시스템을 구현할 수 있도록 해줍니다.

마무리

TI의 기능적 안전성 기능이 통합된 온칩 Jacinto 7 프로세서 제품군을 통해 고객들이 안전성 표준과 최종 제품의 목표를 보다 효과적으로 달성할 수 있도록 지원합니다. 광범위한 안전 기능은 시스템 BOM을 낮추고, 다양한 코어에 걸쳐 성능 오버헤드를 줄일 수 있습니다.

또한 TI의 소프트웨어 SDK는 고객이 안전 소프트웨어 개발 목표를 달성할 수 있도록 안전 관련 드라이버 및 진단 라이브러리를 제공합니다. 단순화된 안전 아키텍처 및 소프트웨어 제품은 엔지니어링 개발에 투입되는 노력을 줄여줍니다.

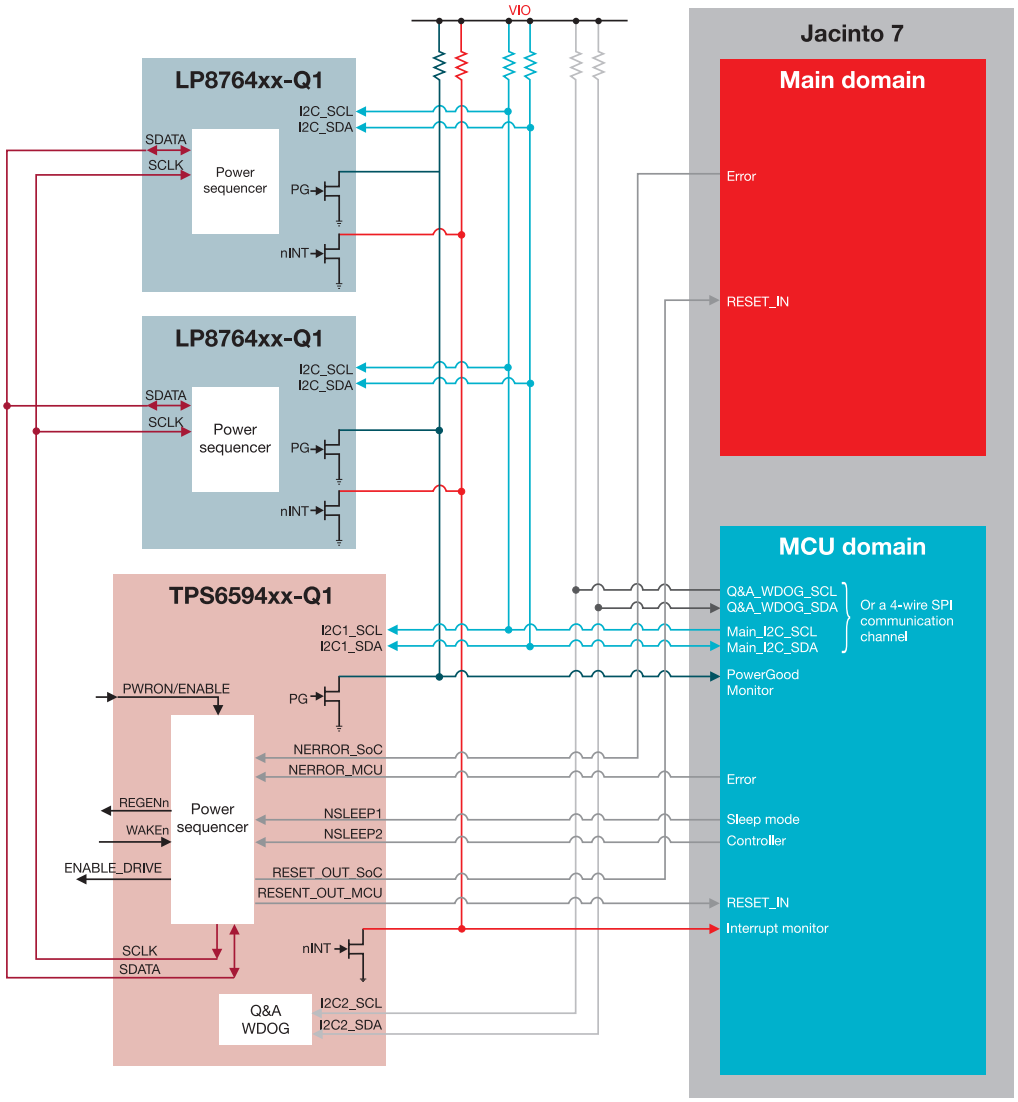

그림 2. "가상" PMIC로 TPS6594-Q1 + LP8764-Q1 + LP8764-Q1 통신.

참고 자료

- Kumar, VC. “The state of functional safety in Industry 4.0.” 텍사스 인스트루먼트 기술백서 SPRY329, 2018.
- Thomas, Jay 및 Siddharth Deshpande. “기능적 안전성을 위한 기능적 소프트웨어.” 텍사스 인스트루먼트 기술백서 SPNY007, 2015.
- 기능적 안전성 하드웨어 인증서.
- 기능적 안전성 소프트웨어 인증서.
- 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 (2017년 1월 29일), pp. 35–40.
- Haworth, David, Tobias Jordan 및 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