Optimizing functional safety for industrial robots

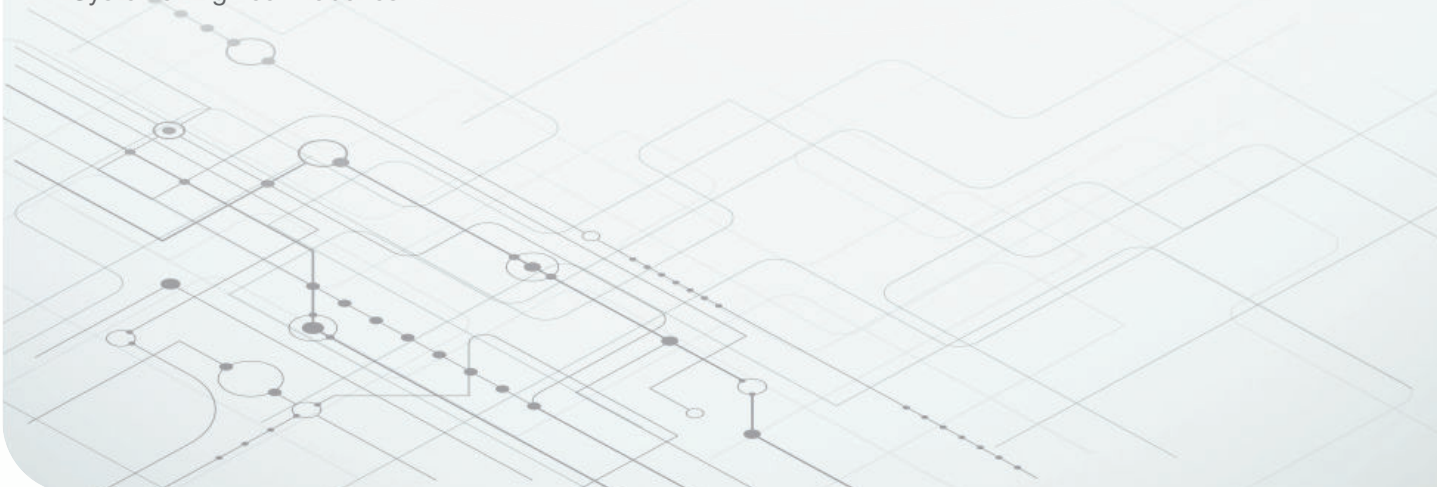**TEXAS INSTRUMENTS**

VC Kumar
Marketing/Business Dev Manager
Sitara High Performance MCUs

Yining Yang
Systems Applications/Architecture
Jacinto Processors

Thomas Schneider
Systems Engineer Robotics

Smart factories leverage intelligent machines, such as robots, to drive increased efficiency and flexibility in factory, equipment and product status in real time.

At a glance

1 Industry 4.0
The fourth industrial revolution highlights the adoption of industrial robots in manufacturing.

2 Functional safety requirements for industrial robots
Understanding crucial requirements is fundamental to building a safe robotic system.

3 Designing functional safety architectures for industrial robots
Achieving HFT=1 while also trending towards miniaturization and cost optimization.

Introduction

The Fourth Industrial Revolution, also known as Industry 4.0, typically refers to the digitization of the manufacturing industry. Increased digitization, or a *connected everything* environment enables companies to collect, store and use large amounts of data simultaneously; greatly enhances manufacturing processes; and creates a fully digital value chain [1]. The ability to collect and use information in real time enables the creation smart factories and smart systems in manufacturing.

The Industry 4.0 revolution includes the advancement and adoption of industrial robots and robot systems. Industrial robots perform automated programmable movements in manufacturing on the factory floor. The implementation of Industry 4.0 in industrial robotics in a factory requires [2]:

- **Interoperability**: people, machines, devices and sensors that connect and communicate with one another.
- **Information transparency**: the systems create a virtual copy of the physical world through sensor data to contextualize information.
- **Technical assistance**: both the ability of the systems to support humans in making decisions and solving problems, and the ability to assist humans with tasks too difficult or unsafe for them.
- **Decentralized decision-making**: the ability of cyberphysical systems to make simple decision on their own and become as autonomous as possible.

A trend toward increased human and machine interaction, including collaboration in factory environments, emphasizes the underlying importance of functional safety for industrial robots. This white paper describes functional safety for processors in industrial robots and explores some options to enable functional safety.

Functional safety requirements for industrial robots

Functional safety is a part of an overall safety structure that depends on a system or equipment to operate correctly in response to its inputs. In other words, functional safety is the ability to detect a potentially dangerous condition and activate a protective or corrective device or mechanism to prevent hazardous events from arising, or providing mitigation to reduce the consequence of the hazardous event [3]. In the context of industrial robots, mechanical, electrical, and/or sensor technologies are used to minimize interference with human activities and create safer working environments.

A typical industrial robot safety-related system consists of sensors, a logic subsystem (for data processing and communication, local or to the network), software implementation of algorithms, and actuators (a control subsystem). Microcontrollers (MCUs) and/or processors comprise the logic subsystem. MCU design and architecture plays a role in the system's overall safety architecture. Designing a system where the processor takes functional safety requirements into consideration, both from a hardware and software standpoint, greatly reduces the cost and complexity of designing a functionally safe system. Two standards govern the requirements for and implementation of functional safety in industrial robots:

- International Electrotechnical Commission (IEC) 62061
- International Organization for Standardization (ISO) ISO13849

For a comprehensive description of functional safety requirements and implementation in factory automation, see the white paper, **The state of functional safety in Industry 4.0**.

ISO 13849 in factory automation

For industrial machinery safety, ISO 13849 is the successor to the older machinery European Standard (EN) 954-1 functional safety standard. ISO 13849 covers safety requirements (including software) through the life cycle of safety-related machinery and their components in control systems.

The process identifies the parts in the system that perform safety functions and uses statistical analysis to determine the probability of failure over time to determine a performance level (PL) and a safety integrity level (SIL) for the system.

Performance levels range from *PLa* to *PLe*. *PLa* indicates the least reliable and *PLe* indicates the most reliable. After the performance level has been established, the architecture required to reach that level is classified into safety categories. The category specifies resistance to

faults, similar to a hardware fault tolerance. Categories range from *CatB* through *Cat4*. *CatB* indicates the least safe and *Cat4* indicates the most safe. The specific categories are:

- CatB: Single channel
- Cat1: Single channel + well-tried components
- Cat2: Single channel + diagnostics
- Cat3: Dual channel + diagnostics, no accumulation of fault
- Cat4: Dual channel + diagnostics, accumulation of faults

Typical industrial machinery systems are Cat3 or Cat4, PLd and in some instances PLe. For specific applications, such as with IEC 61508, additional standards refers to ISO 13849 and provide further clarification and guidance (such as for correlating categories and PLs).

PL and SIL both look at probability of failure per hour (PFH) and dictate requirements concerning structure, diagnostics, and confidence of fault detection. Their key difference is rooted in the degree of how certain parameters are dictated. For example, the performance level (PL) is not based on reliability calculations alone and has a MTTF (mean time to failure) metric as well. Despite some slight differences in formula, SILs can be mapped to PLs and vice versa. PLs are only referenced in ISO13849 whereas SIL is referenced in IEC 61508 and all derived standards. Using one metric over the other typically market-specific; PL is used more often in machine industries, while SIL is more commonly seen in process industries.

ISO 10218 in industrial robots

For functionally safety (FS) in industrial robots, ISO 10218 is a product-specific implementation of the requirements of IEC 61508. TI recommends that processor vendors consider the functional safety and safety integrity requirements of an industrial robot outlined in ISO 10218, in conjunction with their customer requirements.

# Designing functional safety architectures for industrial robots

ISO10218-1 specifies the safety requirements for industrial robots. According to the standard, an industrial robot shall be designed so that it complies with PLd with structure Cat3 as described in ISO 13849-1:2006, or so it complies with SIL 2 with a hardware fault tolerance of 1 (HFT=1) as described in IEC 62061:2005. Specifically, the industrial robot architecture must meet HFT=1 to ensure that a single fault in any of the safety-related parts of the control system does not lead to the loss of the safety function of the system. When a single fault occurs, the safety function is always performed and a safe state shall be maintained until the detected fault is corrected.

Considering the robot controller use case in more detail, there are several ways a dual-channel safety architecture (HFT=1) can be realized:

- **Dual external safety controllers**: Central computing and communication processors with two separate MCUs or MPUs to implement safety channel 1 and safety channel 2 as shown in Figure 1.
- **Single integrated safety controller with one external safety controller**: Safety channel 1 integrates into either the central compute processor or the communication processor and a separate processor is used for safety channel 2.
- **Dual integrated safety controllers**: Safety channel 1 integrates into the central compute processor and safety channel 2 integrated in the communication processor. There is no need for an additional external processor to handle the safety channels.

Dual external safety controllers

The traditional approach separates safety controllers from the application (communication and compute) processors. **Figure 1** shows how two separate safety controller devices facilitate safety channel 1 and safety channel 2 . Control and communication applications run on an application processor while two separate devices with individual data, clock, and power paths serve as the *checker* for safety.
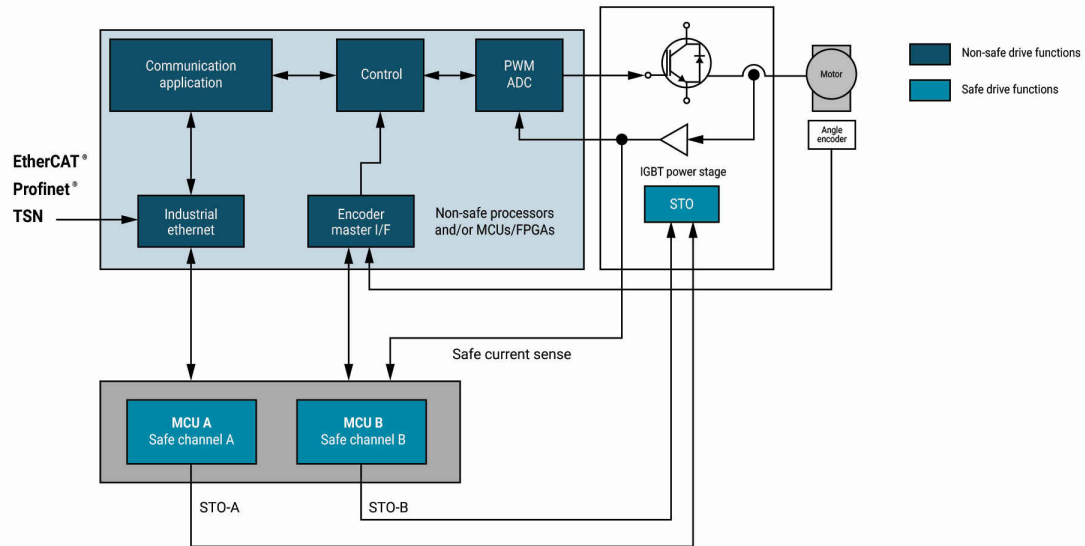

Figure 1. Dual external safety controller.

In addition to the trend toward miniaturization and lower cost, there has been a corresponding movement toward the integration of safety functions. Having multiple types of processing cores (such as Arm Cortex-A, Cortex-R5F and Cortex-M) and implementing the appropriate functional safety capabilities (such as isolated power and clock domains for different cores, hardware diagnostic functions, freedom from interference) can offer system designers flexibility in implementing safety architecture.

Single integrated safety controller

The next level of integration involves using one of the processing cores inside the central compute or communication processor for safety channel 1 while partitioning the rest of the processor to perform the application including control, processing and/or communications. The 2nd safety channel operates on a separate controller (different piece of silicon) as shown in **Figure 2**.
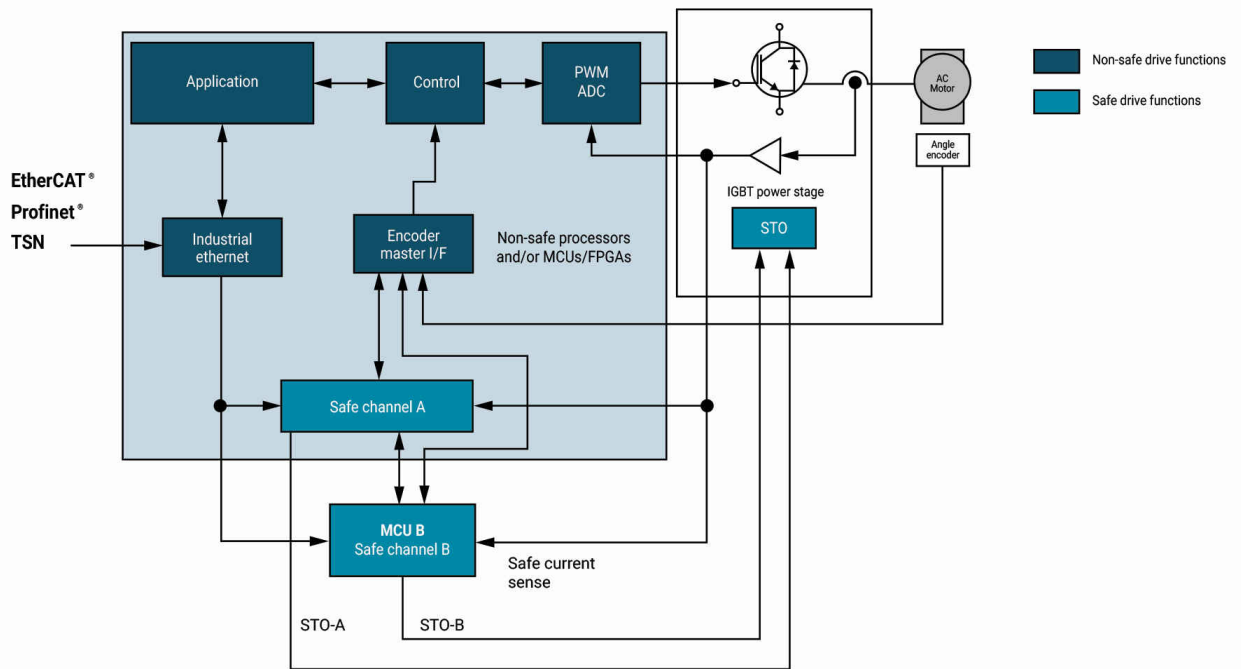
Figure 2. *Single integrated safety controller.*

Dual integrated safety controllers

Figure 3 illustrates the highest level of integration where safety channel 1 integrates into the central compute processor and safety channel 2 integrates into the communication processor. No additional external controller is needed for functional safety. This level of integration saves additional printed circuit board (PCB) space and external component cost. An example implementation for this highly-integrated robot controller architecture with TI processors as shown in **Figure 4**.
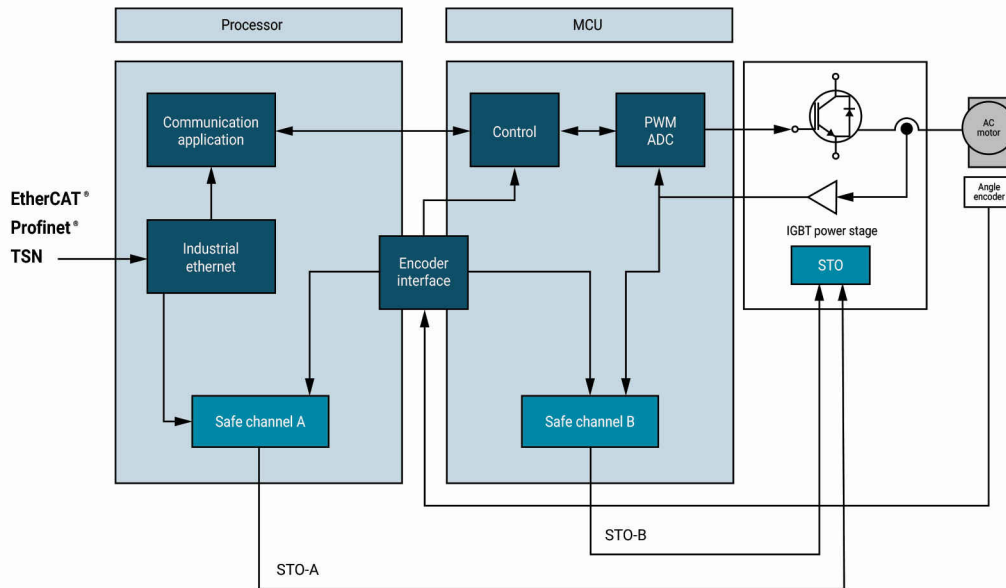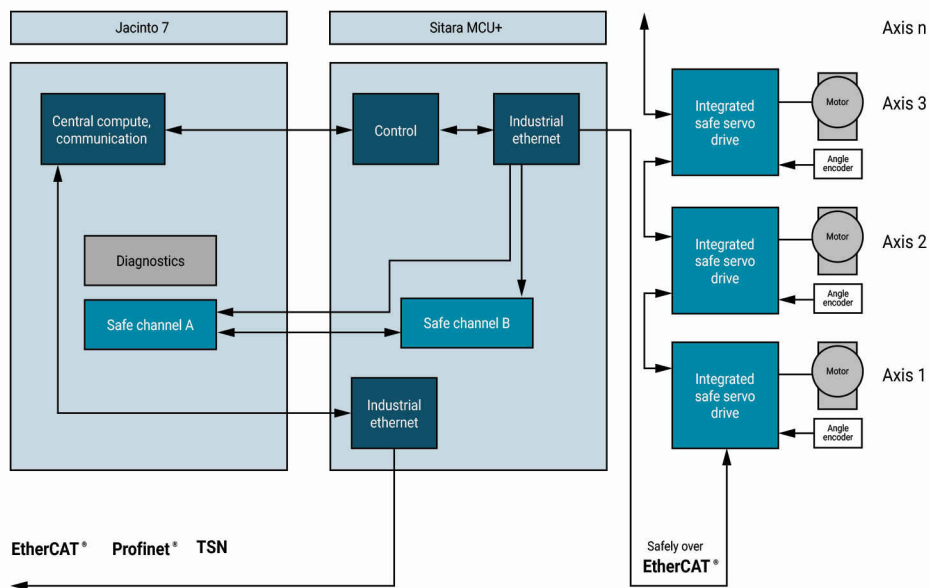

Figure 3. Dual integrated safety controllers.

Figure 4. Integrated robot controller architecture with TI processors.

Processor-level integration for industrial robots

Given the complexity of industrial robots, next-generation processors are integrating more system-level requirements on-chip.

As touched on in the previous section, industrial robots typically need to achieve PLd with structure category 3 as described in ISO 13849-1:2006, or SIL 2 with a hardware fault tolerance of 1 (HFT=1) as described in IEC 62061:2005. TI helps achieve this in the most space-efficient and cost-optimized way via an integrated Dual Safety Solution with the DRA82x family of Jacinto processors and the AM24x family of Sitara™ MCUs.

TI's DRA82x family of Jacinto processors offers vendors the flexibility to choose the best architecture for their system. The SoC is composed of a heterogenous mix of processing cores (Arm Cortex-A72, Cortex-R5F and DSPs) for both performance and real-time processing needs and high-speed communication interfaces. The different variants of the DRA82x devices supports a wide range of performance requirements ranging from approximately 20 kHz to over 100 kHz DMIPS (future roadmap devices) for all levels of compute. Integrated peripherals including LIN, CAN, PCIE, Ethernet switch, I^2C, SPI, and more enable simple communication and interfacing with other SoCs, ICs, and sensors in the system.

DRA82x is developed via IEC 61508/ISO26262 processes to achieve SIL-3 systematic fault integrity and includes:

- hardware diagnostics for random faults including voltage monitors
- ECC on SRAM
- temperature monitoring

The safety island is comprised of lockstep R5Fs (ASIL-D capable), its own clocking, power sources, and dedicated peripherals and facilitates safety channel isolation and freedom from interference from the rest of the chip.

TI's AM243x family of high performance MCUs is also comprised of a heterogenous mix of processing cores. These devices are designed as functional safety-compliant SoCs that target IEC 61508 SIL-3 HFT=1 via a single external channel, with one key assumption of use targeted at motor control applications. The integrated Arm Cortex M4F core (independent MCU channel from the main domain) provides a potential BOM reduction for industrial customers that need a single or dual-channel safety system.

The AM243x family is designed to achieve SIL-3 systematic fault integrity across the entire device. Safety features have been implemented across the entire SoC to support system-level safety, such as ECC on main memories, dual clock comparators, voltage monitoring, temperature monitoring and a diagnostic toolkit. In addition, functional safety collateral is available to help with system-level safety certification for their products.

The AM243x processor family integrates dedicated motor control features as well as extensive communication capability including Ethernet and PCIe interfaces. Integrated security capabilities offer customers the ability to design lower cost systems.

The DRA82x family's compute, communication, and safety features in conjunction with AM24x family's control, industrial protocol, and safety features provide system designers a high level of flexibility to architect safe, high performing, and cost-efficient industrial robot solutions.

Figure 4 demonstrates a dual integrated controller safety architecture via a DRA82x family and AM243x family solution.

Making certification easier

System-level and equipment-level certification can benefit from component-level certification and/or FIT and failure injection data to reduce cycle time and certification complexity. A system that needs to meet a certain safety or performance level must have all

safety-critical components meet or exceed that level and address both systemic and random fault scenarios.

TI provides our customers a comprehensive design and certification support package.

Documentation support

TI's documentation support package includes:

- A component safety manual detailing the product safety architecture and recommended usage.
- A safety analysis report summary, with a summary of the FIT rate along with failure modes, effects and diagnostic analysis (FMEDA) at the component level for IEC 61508.
- A detailed safety analysis report, with full details of all safety analysis executed down to the module (IP) level for IEC 61508, as well as a software tool for customizing the analysis results to the specific application.
- A safety report summarizing compliance to IEC 61508.
- A third-party assessment of development flow in accordance with IEC 61508.
- Component-level certification.

Software support

TI's software support includes:

- A safety compliance support package according to IEC 61508, including software documentation and testing to assist in compliance with functional safety standards. The package includes safety requirements documents, code review and coverage reports, unit test results and software safety manuals. It ideally includes unit test capability using tools such as a Liverpool Data Research Associates (LDRA) unit.
- Safety tool documentation and qualification according to IEC 61508 that assists in the qualification

to functional safety standards, including a tool classification report, tool qualification plan and report, tool safety manual, and test automation unit.

- A safety diagnostic library that provides interfaces and a framework for initializing and enabling safety diagnostics/features, fault injection to allow the testing of application fault handling, a handler callback routine, and profiling for measuring time spent in diagnostic test/fault handling.
- Development tools assessed and/or certified as suitable for use with IEC 61508, including integrated development environments and compilers and Joint Test Action Group emulators/traces.

Summary

Increasing machine and human collaboration and interaction is driving increased needs for functional safety. As such, component-level needs are increasing and SoC architectures are therefore evolving. Processor vendors play a key role in supporting the demanding needs of new products, approaching safety from the ground up and offering innovative and flexible architectures, as well as a support infrastructure to enable system-level certifications. TI is a leader in delivering processing solutions for applications demanding functional safety, and the DRA82x Jacinto and AM24x Sitara families continue that trend.

References

1. Accenture.2018. **IndustryX.0.**
2. Marr,Bernard. 2016. "**WhatEveryone Must Know About Industry 4.0.**"
3. International Electrotechnical Commission. 2018. **Functional Safety**

TEXAS INSTRUMENTS

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.