참고 자료

모터 제어 설계 프로세스의 기능 안전 준수 위험 방지

Texas Instruments

Bharat Rajaram
Systems Engineering Manager
Arm-Based Microcontrollers

시스템 설계 및 기능 안전 준수는 연속으로 발생해서는 안 됩니다. 안타깝게도 기존의 설계 접근 방식과 많은 조직에서는 설계 프로세스의 이러한 단계를 별도의 사일로화된 활동으로 취급하기 때문에 설계 비용이 늘어나고 제품 출시 시기가 지연되는 경우가 많습니다.

한눈에 보기

1

기능 안전 준수 정의

기능 안전 표준의 목표는 시스템 고장을 관리하고 완화하는 동시에 임의의 하드웨어 오류가 발생할 때 이를 감지 및 방지(또는 최소한 안전 렌더링)하는 것입니다.

2

기능 안전 시스템 설계의 두 가지 속성

기능 안전에는 의도된 기능을 제공하고 안전 무결성 수준을 충족하는 시스템의 개발이 포함됩니다.

3

기능적으로 안전한 모터 제어 및 구동 시스템을 설계하는 권장 접근 방식

기능적으로 안전한 시스템을 설계하는 시스템 엔지니어는 설계 프로세스의 첫 시작부터 기능 안전 준수를 염두에 둬야 하며, 나중에 생각해서는 안 됩니다.

기능적으로 안전한 모터 제어 애플리케이션을 설계할 때 초기 설계 요구 사항으로 시작 시 기능 안전 준수를 해결해야 합니까? 아니면 기능 안전을 설계의 최종 단계에 통합되는 추가 기능으로 취급해야 합니까?

기능 안전은 초기 설계 요구 사항의 일부로서 모터 드라이브의 의도된 기능과 결합되어야 합니다. 기존 시스템 설계 워크플로는 안전 준수에 시너지 효과를 주지 않기 때문에 이는 표준이 아닙니다. 그러나 처음부터 안전 무결성 준수를 충족하는 방법을 고려하지 않으면 시스템을 시장에 출시할 때 비용이 많이 드는 지연이 발생할 수 있습니다.

Industry 4.0의 시작과 차량 전기화 및 연결성의 성장으로 인해 우리는 기능 안전 준수에 대한 접근 방식을 바꿔야 합니다. 간단히 말해, 이제 더 많은 애플리케이션에 더 많은 모터 시스템이 있으며 기능 안전 표준 준수에 대한 높은 기준이 생겼습니다.

기능 안전 준수 정의

IEC(국제 전기 표준 회의) 61508 및 ISO(국제 표준화 기구) 26262와 같은 기능 안전 표준의 목표는 시스템 고장을 관리하고 완화하는 동시에 임의의 하드웨어 오류가 발생할 때 이를 감지 및 방지(또는 최소한 안전 렌더링)하는 것입니다.

독립적인 확인 및 검증 과정이 포함된 엄격한 개발 프로세스를 채택하면 시스템 고장을 관리하는 데 도움이 될 수 있습니다.

다음과 같은 방법으로 임의의 하드웨어 오류를 감지, 방지 또는 안전 렌더링할 수 있습니다.

- 제어 중인 장비에 대해 확실히 이해합니다.
- 발생 가능성, 영향의 심각도 및 사고의 제어 가능성과 같은 상황적 위험의 가능한 원인과 그 속성을 분석합니다.

안전 메커니즘을 각 상황적 위험과 연결하면 설계자가 IEC 61508에서 요구하는 SFF(안전 고장률) 및 PFH(고장 확률/시간)와 같은 정량적 지표를 충족하는 데 도움이 됩니다. 예를 들어, SIL(안전 무결성 수준) 2 시스템의 경우 10억 시간 이상 작동할 때 고장의 SFF가 90% 이상이고 PFH가 1000 이하여야 합니다.

기능 안전 시스템 설계의 두 가지 속성

기능 안전 표준은 모든 시스템이 고장날 것이며(발생 여부의 문제가 아닌 시기의 문제일 뿐) 절대적 안전성은 없다고 가정합니다.

기능 안전 시스템 설계의 두 가지 속성은 의도된 기능을 제공하는 시스템을 개발하는 것과 특정 SIL 또는 차량용 SIL(ASIL)과 같은 안전 기능을 충족하는 동일한 시스템을 개발하는 것입니다.

설계자는 종종 두 가지 측면에 개별적으로 또는 순차적으로 접근합니다. 설계 예산 요구 사항을 유지하면서 대용량 애플리케이션을 위한 기능적으로 안전한 시스템을 설계하는 것은 어렵습니다. **표 1**에서는 제어 및 구동 애플리케이션의 의도된 기능 및 안전 기능의 예를 설명합니다.

이 개념에 대해 더 잘 설명하려면 **표 1**의 엘리베이터 모터 예시를 살펴보십시오.

엘리베이터의 의도된 기능은 사용자 입력에 따라 사람을 위아래로 이동시키는 것입니다. 5층으로 가기 위해 버튼을 누르면 엘리베이터가 5층으로 이동합니다.

엘리베이터의 안전 기능은 한 단계 더 나아가 다음을 포함할 수 있습니다.

- 한 층에서 다른 층으로 부드럽게 이동합니다.
- 각 층의 층계참과 수평으로 정지합니다.
- 엘리베이터가 안전 속도를 초과할 경우 자동으로 브레이크를 작동합니다.

기능 안전 애플리케이션	의도된 기능의 예	안전 기능의 예(및 해당 SIL 또는 ASIL 대상)
산업용: 엘리베이터 모터	사용자 요청에 따라 엘리베이터를 위아래로 이동	• 엘리베이터를 안전하게 시작 또는 정지(저크 방지)(SIL 2) • 엘리베이터가 너무 빨리 주행하는 경우 자동 브레이크 적용(SIL 3)
차량용: 전기차(EV) 트랙션 모터	액셀 또는 브레이크를 통해 운전자의 명령에 따라 EV를 앞뒤로 이동	• 가속 시 불충분하거나 과도한 토크 방지(ASIL C) • 너무 강한 제동 방지(후방 추돌 방지)(ASIL D)
산업용: 스틸 프레스	공장 생산성 저하 없이 스틸 프레스를 작동하는 서보 드라이브 시스템 제어	• 과토크 또는 과속도가 발생할 경우 STO(Safe-Torque-Off)에서 드라이브 컨트롤러의 전원 차단(SIL 3) • 작업자가 가까이 있는 경우 SLS(Safe-Limited-Speed)에서 모터 속도를 허용 범위 내로 유지(SIL 2) • SLS가 범위 검사를 초과하는 경우 STO를 트리거(SIL-3과 같이 더 높은 SIL을 유도하는 생산성과 안전성 간의 균형을 맞추기 위해)

표 1. *제어 및 구동 애플리케이션의 의도된 안전 기능의 예입니다.*

의도된 기능과 안전 기능이 함께 작동하는 방식을 더 잘 이해하기 위해, 20층으로 된 건물의 엘리베이터에 누름 버튼 회로(그림 1 참조)가 있으며 이 회로에는 엘리베이터 모터 컨트롤러가 엘리베이터를 25층 또는 30층(즉, 건물에 존재하지 않는 층)으로 보내는 것으로 해석하는 오류가 있다고 가정하겠습니다. 범위 검사는 오류가 발생하거나 결국 고장이 나기 전에 결함을 포착합니다. 이는 기능적 안전에서 허용되는 진행 과정입니다. '결함'은 '오류'로 이어지지만, 일부 오류는 '고장'으로 이어질 수 있습니다.

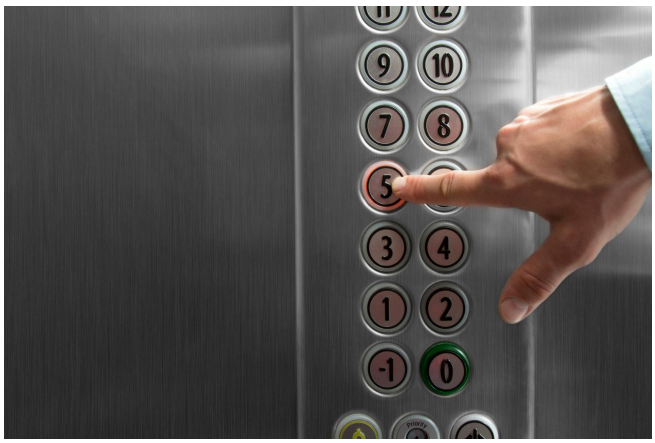

그림 1. *현대식 엘리베이터 누름 버튼의 예.*

의도된 기능 설계 및 안전 기능 설계를 위한 프로세스를 살펴보겠습니다.

모터 드라이브의 의도된 기능 설계 프로세스에서 시스템 엔지니어는 의도된 기능의 요구 사항을 충족하는 마이크로컨트롤러(MCU)를 선택합니다. 그런 다음 통합 ADC(아날로그-디지털 컨버터) 채널과 같은 감지 기능을 할당하여 로터 위치, 라인 전류, 위상 전압 및 시스템 온도를 모니터링합니다. 그런 다음 시스템 엔지니어는 CPU의 MIPS(초당 수백만 건의 명령어)와 같은 MCU의 사용 가능한 처리 기능을 계속 사용하여 모터 제어 알고리즘을 실행하고 PWM(펄스 폭 모듈레이터)과 같은 사용 가능한 작동 주변 장치를 구동하여 모터 드라이버 회로를 구동합니다. 이 프로세스에는 일반적으로 몇 달이 소요되며, PCB(인쇄 회로 기판) 설계, 모터 제어 알고리즘 개발, 모든 임베디드 소프트웨어를 개발하고 디버깅하는 과정도 포함됩니다.

별도의 다소 사일로화된 팀에서 안전 기능 설계 프로세스를 처리하는 조직의 경우 별도의 기능 안전 전문가가 함께 와서 시스템 엔지니어가 원래 선택한 MCU의 기능 안전 매뉴얼을 검토합니다. 경우에 따라 기능 안전 전문가가 SEooC(컨텍스트와 무관한 안전 요소) 안전 개념에 오류 테스트, 하드웨어 중복성, DAC(디지털-아날로그 컨버터)-ADC 루프백 검사 또는 향상된 캡처를 통한 향상된 PWM 모니터링을 비롯한 기능의 SW 테스트 사용이 필요하다는 사실을 발견할 수 있습니다. 이전의 엘리베이터 예를 떠올려 보면 MCU의 ADC에서 '고착' 결함으로부터 보호하기 위해 여러 ADC 채널을 사용하여 각 층의 레벨 센서를 모니터링해야 할 수도 있습니다.

ADC 및 PWM 채널이 충분하지 않거나 CPU MIPS가 충분하지 않아서 기능 안전을 달성하지 못하는 경우 기능적으로 안전한 시스템을 구현하기 위해 처음으로 돌아가서 다른 MCU를 선택해야 할 수도 있습니다. 이 경우 별도의 시스템 설계 팀이 지금까지 완료한 작업을 취소할 수 있습니다.

설계 단계가 순차적으로 발생하지 않더라도 별도의 조직 사일로에서 자주 발생합니다. 즉, 시스템 엔지니어는 일반적으로 기능 안전 전문 지식이 없으며 기능 안전 전문가는 시스템 엔지니어가 아닙니다. 이러한 사일로화된 접근 방식은 궁극적으로 시스템 비용 증가 및 수개월의 출시 지연 등 동일한 문제를 초래합니다.

기능적으로 안전한 모터 제어 및 구동 시스템을 설계하는 권장 접근 방식

기능적으로 안전한 시스템을 설계하는 시스템 엔지니어의 궁극적인 목표는 설계 프로세스의 첫 시작부터 기능 안전 준수를 염두에 두는 것입니다.

설계 예산에 맞는 기능적으로 안전한 시스템을 설계하고 제공하려면 안전 준수와 의도된 기능 모두에 대한 시너지 분석이 필요합니다. 프로젝트에 독립적으로 또는 순차적으로 접근하면 시스템 설계 목표를 달성하는 데 어려움이 생기거나 심지어 시스템 설계 목표를 달성하지 못할 수도 있습니다. 안전 기능 설계 프로세스를 관리하는 팀의 이전 사례를 고려하면, 이전의 공동 작업을 통해 새로운 MCU를 선택하고 PCB를 재구성할 필요가 없었을 것입니다.

실제로 다른 사례에서는 권장 접근 방식을 보여 줄 수 있습니다. 그림 2에서 볼 수 있듯이, 인간의 뇌는 왼쪽(논리적) 반과 오른쪽(창조적) 반을 모두 적용하여 문제를 총체적으로 해결합니다.

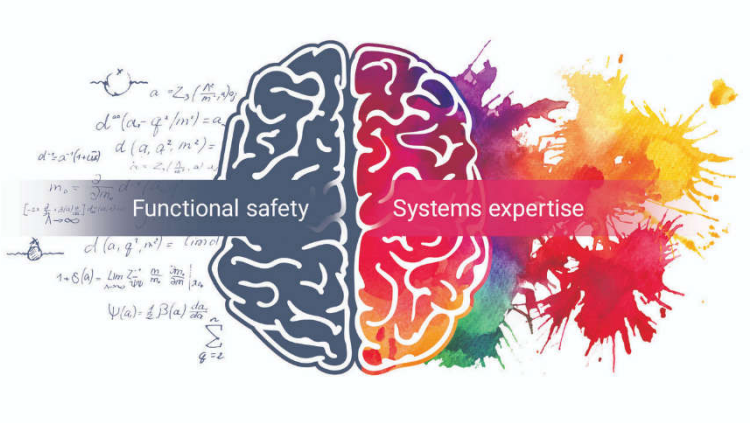

그림 2. *하나의 뇌는 시스템 설계와 기능 안전 준수에 대한 통합된 전문 지식을 보유하고 있습니다.*

두뇌를 각각의 절반이 서로 다른 팀이나 내부 설계 리소스를 대표하고 설계 프로세스에서 특정 분야에 대한 관점을 가져올 수 있는 단일 조직으로 생각하십시오. 이들은 함께 설계 워크플로에서 하나의 팀으로 작업하면서 명확하고 지속적인 의사소통을 유지하는 동시에 각자의 분야에서 설계에 접근할 수 있습니다.

마찬가지로, 가장 효과적인 설계 프로젝트에서는 기능적으로 안전한 시스템을 구현하기 위해 협력하는 시스템 설계자 및 기능 안전 전문가로 구성된 팀을 사용합니다.

시작 출시를 가속화하려면 시스템 엔지니어에게 올바른 설계 리소스가 필요합니다. 예를 들어 TI는 제3자가 독립적으로 평가하는 서브시스템 및 시스템 수준 기능 안전 개념을 개발합니다.

TI가 기능적으로 안전한 시스템을 설계하는 데 도움을 주는 방법

TI의 제품 포트폴리오는 모터 드라이버와 게이트 드라이버부터 C2000™ 및 Arm® Cortex® 기반 MCU(예: AM2434BSDFHIALVR)를 비롯한 독점 CPU 아키텍처를 기반으로 하는 MCU까지 다양합니다. 이러한 제품에는 고급 진단 기능과 온칩 감지 주변 장치가 있어 시스템 가동 중지 시간을 최소화하는 동시에 오류를 빠르게 감지하고 이에 대응할 수 있으며, 산업 환경에서는 공장 생산성을 높입니다.

기능적으로 안전한 설계에 가장 효과적인 장치를 찾을 수 있도록 TI는 기능적으로 안전한 애플리케이션에 사용하기에 적합한 세 가지 제품 카테고리를 정의했습니다. 바로 TI 기능 안전 가능, TI 기능 안전 품질 관리, TI 기능 안전 준수입니다. (TI의 모터 드라이버, 게이트 드라이버 및 MCU는 일반적으로 TI 기능 안전 준수 제품입니다.)

TI는 IEC 61508 및 ISO 26262의 체계적 기능 준수 권장 사항을 충족하기 위해 이러한 제품을 설계 및 제작하여 안전하고 안정적인 모터 제어 및 구동 시스템을 구축할 수 있도록 합니다. TI는 FMEDA(오류 모드, 영향 및 진단 분석), 기능 안전 매뉴얼 및 안전 진단 라이브러리(해당하는 경우)로 각 장치를 지원하며 TI.com에서 또는 요청에 따라 시스템 및 서브시스템 기능 안전 개념 보고서를 제공합니다. TI MCU의 기능 안전 매뉴얼에서는 SEooC를 상황에 맞게 살펴보고 애플리케이션 예시에 대해 가능한 오류 그룹을 간략하게 설명합니다.

설계 리소스의 예로는 ***TUEV에서 평가한 산업용 드라이브용 STO(Safe Torque Off) 레퍼런스 설계(IEC 61800-5-2)***의 TÜV SÜD에서 평가한 산업용 드라이브용 STO 모듈이 있습니다. **www.ti.com/technologies/functional-safety.html**에서 TI의 기능 안전 제품에 대해 자세히 알아보고 설계 리소스를 확인하십시오.

TI는 ISO 26262 SEooC 및 IEC 61508 준수 항목과 TI 제품이 사용되는 기능적으로 안전한 시스템 유형에 대한 경험을 갖고 있습니다. 물론 이러한 이점을 실현하려면 의도된 기능과 안전 기능을 모두 개발하는 데 필요한 복잡한 요구사항의 균형을 맞춰야 합니다.

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