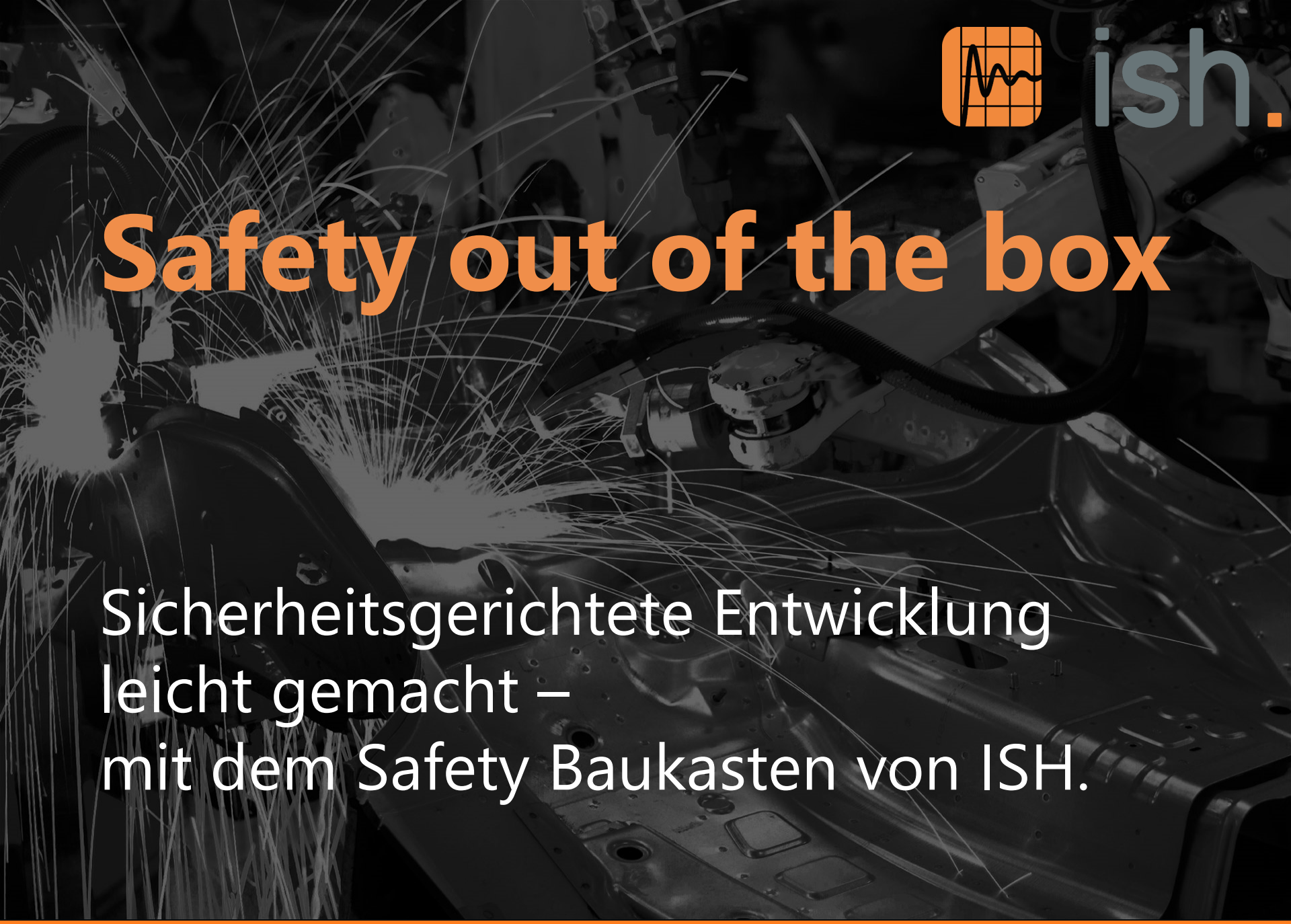
Forum Safety & Security 2020

# Safety out of the box

## Baukasten für Funktionale Sicherheit

Von Dipl.-Ing. Axel Helmerth



# Safety out of the box

Sicherheitsgerichtete Entwicklung
leicht gemacht –
mit dem Safety Baukasten von ISH.

# Zur Person

- Dipl.-Ing. **Axel Helmerth**
- Studium der Elektrotechnik Fachrichtung Nachrichtentechnik Uni Siegen
- Gründer der ISH Ingenieursozietät GmbH in Kreuztal
- Über 30 Jahre Expertise in der Sondermesstechnik z.B. mit Walzenmessgeräten
- Vielzahl kundenspezifischer Hard- und Software-Entwicklungen

- ISH – 1989 gegründet – ist heute Teil der österreichischen Holding Neuron, zu der logi.cals in St. Pölten gehört
- Kernmärkte: industrielle Automation, Bahn-, Prozess- und Bergbautechnik (daher ATEX zertifiziert)
- Seit 2002 Dienstleister für kundenspezifische Hard- und Software mit „Funktionaler Sicherheit“

# Funktionale Sicherheit

- Enormes Wachstum in nahezu allen Bereichen der Technik
- Gesetzliche Anforderungen an die Sicherheitstechnik
- Wichtig für große Anlagen, komplexe Maschinen bis Elektrowerkzeuge und industrielle Messtechnik
- Elektronische Komponenten zur permanenten Überwachung und Diagnose von Sicherheitsfunktionen
- Ziel: Mensch und Maschine vor Schaden bewahren
- Sichere Abschaltung des Systems im Fehlerfall

# Situation

- Wesentliche Gruppen von Anbietern von elektronischen Systemen und Komponenten für die Funktionale Sicherheit (FuSi):
  - **Systemausrüster** als Anbieter von Komplettlösungen
  - **Spezialisten für die funktionale Sicherheit**, die nahezu ausschließlich Komponenten für diese Anwendungen anbieten
  - **Kleine und mittelständige Unternehmen**, die ihre Produkte mit FuSi ausstatten müssen.

# Systemausrüster / Spezialisten

- Große Automatisierungsausrüster
- Hersteller von Sensoren und Aktoren mit überwiegend Standardlösungen
- Kostendeckungsbeitrag der FuSi ist von untergeordneter Bedeutung
- FuSi ist kostengünstig möglich durch Standardisierung
- Produktlösungen in größeren Stückzahlen
- Systemgedanke (alles aus einer Hand) steht im Vordergrund
- FuSi als Subventionsgeschäft, um Gesamtlösung anbieten zu können

# KMU ohne Safety-Know-how

- Herausforderungen:
  - Produkte mit kleinen Stückzahlen
  - Produkte mit eher geringem Verkaufspreis
- Neue oder geänderte Normen schreiben FuSi vor
- Wo kommt FuSi-Know-how her?
- Wie lange sollen Entwicklungen dauern?
- Wie können die Kosten für FuSi wirtschaftlich gestaltet werden?

# Lösungsansatz
# Safety out of the box

- frei kombinierbare FuSi-Module
- TÜV-zertifiziert
- Qualität eines Compliant Items nach IEC61508
- Mit Integration Manuals
- Anwendungsbeispiele
- Workflow-Beschreibungen für die ersten Schritte
- Unterstützen kundenspezifische Produkte vom einfache IO-Modul bis zur vollständigen Steuerung mit sicherer Feldbus-Kopplungen
- ISH-FuSi-Plattform
    - spart viele Monate teure und aufwändige Entwicklungsarbeit
    - reduziert Zertifizierungsaufwand extrem
    - macht FuSi bezahlbar
    - minimiert Time to market

# Grundsätzliche Fragen

# Wer braucht den FuSi-Baukasten?

ish.

- Aktuelle Entwicklungen und Anforderungen in vielen Bereichen zeigen, dass die Anteile an funktionaler Sicherheit stark zunehmen
- In den nächsten Jahren: Wachstum von einigen 100 % prognostiziert
- KMU mit Produkten im kleinen und mittleren Stückzahlbereich
- Unternehmen, die Entwicklungskosten reduzieren müssen

# Wofür ist der FuSi-Baukasten?

- Vom einfachen lokalen IO- Modul oder Sensor bis zur komplexen Steuerungslösung
- Zentrale Plattform für eine 2-kanalige Hard- und Software
- Alle Elementen für die Erfassung von sicheren Eingängen und das Schreiben von sicheren Ausgängen
- Alle Prozeduren für das Testen, Filtern und Verknüpfen bis zum Erfassen und Testen von analogen Eingängen
- Selbst gestaltete Kundenapplikation
- Einbindung der Test-Library für die normativen Tests des Prozessors und des Speichers
- Kopplung verschiedener Feldbusse wie den FSoE-Stack von ISH bis zur sicheren SPS
- Prognose: FuSi-Baukasten deckt gut 90 % aller sicheren Anwendungen in der Automatisierungs- und Prozesstechnik ab

# Was ist mit FuSi-Baukasten möglich?

- Vorgezeichnete, begleitete FuSi-Produktentwicklung
- Entwicklungszeit 9 bis 12 Monaten nach Festlegung der Spezifikation und des Functional Safety Managements
- inklusive Dokumentation
- fertig für die TÜV Begutachtung
- Minimal: Aufwand, Zeiten, Kosten

# ISH Safety Baukasten

# Komponenten des ISH Safety Baukastens

- ISH-Safety Integrated Core
- Test-Library CORA
- ISH FSoE-Master
- ISH-FSoE-Slave
- ISH Motion Library
- ISH Floating point Library
- ISH Feldbus-Konfigurator
- ISH Safety Parameter Tool

# Der ISH Safety Baukasten

ish.

PC

Logi.cad
IEC 61131 PLC
Engineering

Kundenspezifische
GUI

Safety Test
Toolchain

Safety
Buskonfigurator

Safety Parameter-
Tool

Target

IEC 61131
PLC-Runtime

Kundenapplikation

FSoE-Master/Slave
Stack

Safety Integrated Core
Hard- und Software-Baukasten

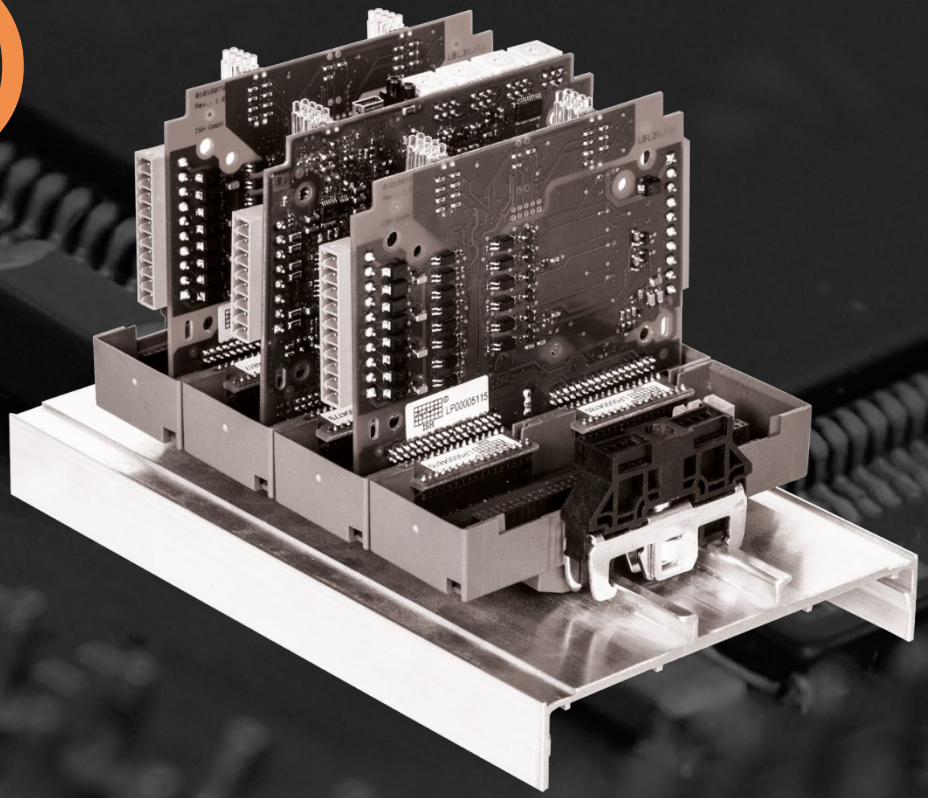
Floating point-
Library

Test-Library
CORA

Safety Motion-
Library

Kundenspezifisches Hardware Abstraction
Layer

# Safety Integrated Core (SIC)



# SIC - Safety Integrated Core

## Technische Daten der Evaluierungs-Hardware:

- 2-kanalige Prozessor Architektur mit Kreuzkommunikation
- Je Kanal Cortex M4 Prozessor mit 180 MHz Systemtakt
- Je 1024 MB Flash und 256 KByte internem RAM
- 6 Modul Status LEDs ansteuerbar von beiden Kanälen, sowie 1x User und 1x Reset Taster
- USB Anschluss zu Kanal A
- Pro Kanal Anschluss zur Geberauswertung von entweder Sin/Cos Encoder, A/B Encoder, SSI oder BiSS Encoder
- Möglichkeit der Anbindung eines Feldbuscontrollers für Profisafe, FSoE über EtherCAT
- 16 x 24VDC testfähige Eingänge kompatibel zur Eingängen Typ3 DIN EN 61131-2, erweiterbar
- 4x testfähige Ausgänge 24VDC DIN EN 61131-2 kompatibel
- Ausgänge können wahlweise auch als Taktausgang zur Testung externer, passiver Kontakte verwendet werden.

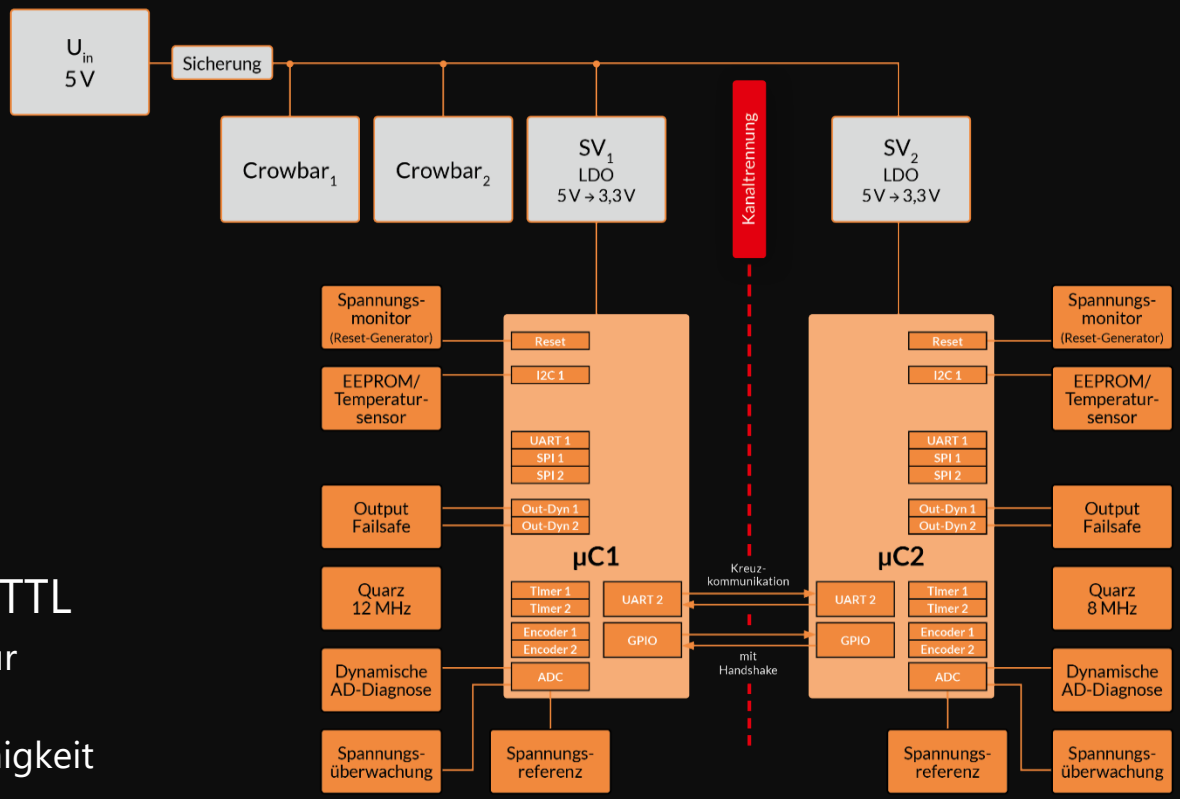
# SIC – Safety Integrated Core

- Objektorientiertes Konzept: einfache Module
- Komplexität entsteht durch Kombinatorik der Funktionen wie Testpulsstrukturen, Querschlussüberwachung etc.
- Konfiguration über eine zentrale Lookup-Table, die alle logischen Objekte der Physik zuordnet
- Schnittstellen zur benutzerspezifischen Software beschränken sich auf Funktionen, die Initialisierung, Hauptzyklus und evtl. Ereignisse handhaben
- Interfaces zur Feldbus-Anbindung und Kommunikation mit einer Test-Library (z.B. ISH CORA)

# SIC – Safety Integrated Core

## Universeller Hardware-Baukasten

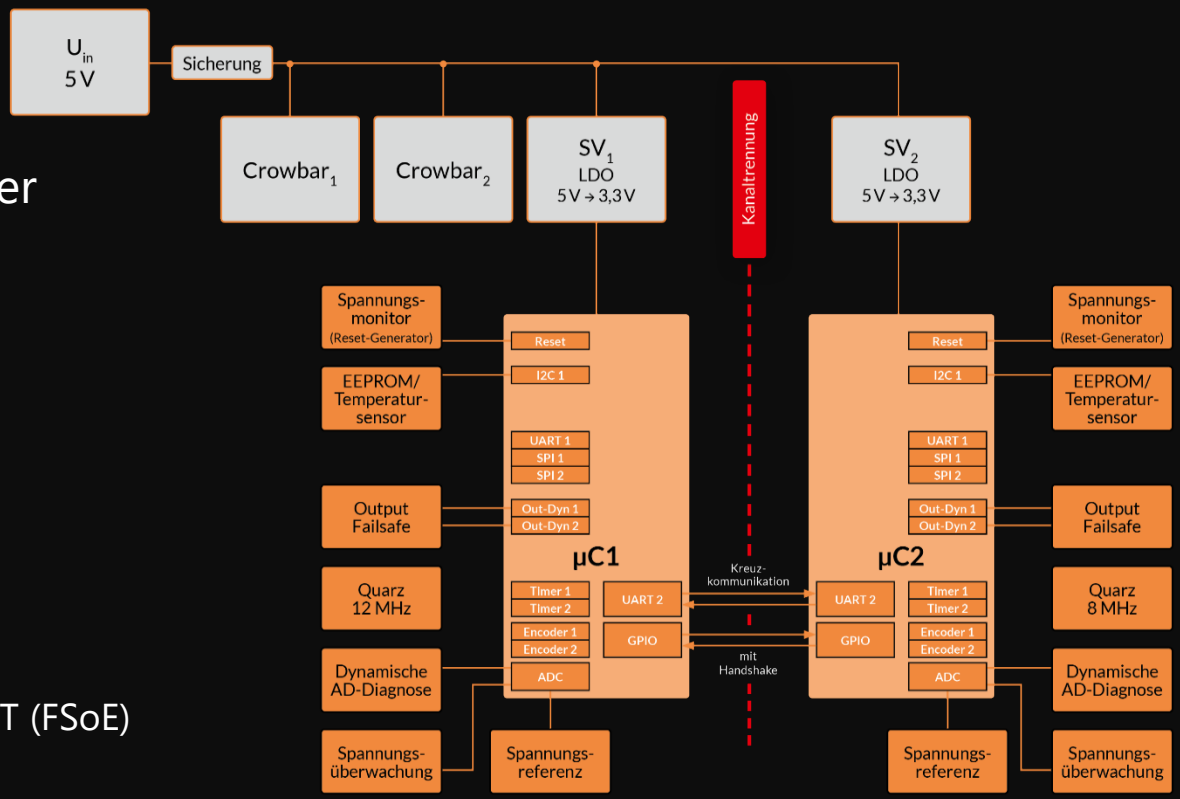
- 2-kanalige Architektur
- Grundausstattung an Schnittstellen
  - UART
  - SPI
  - Logbuch
  - Adresswahl
- Ein- und Ausgänge in TTL
  - Standardbausteine für sicheres I/O
  - Hohe Anpassungsfähigkeit



# SIC – Safety Integrated Core

## Universeller Hardware-Baukasten

- Bis zu 24 I/Os realisierbar
- Analog/Digital-Wandler mit Diagnose
- Geberinterfaces
  - Sin/Cos
  - Digitalinterfaces: SSI, BISS, etc.
- Feldbus-Optionen
  - Failsafe over EtherCAT (FSoE)
  - PROFIsafe

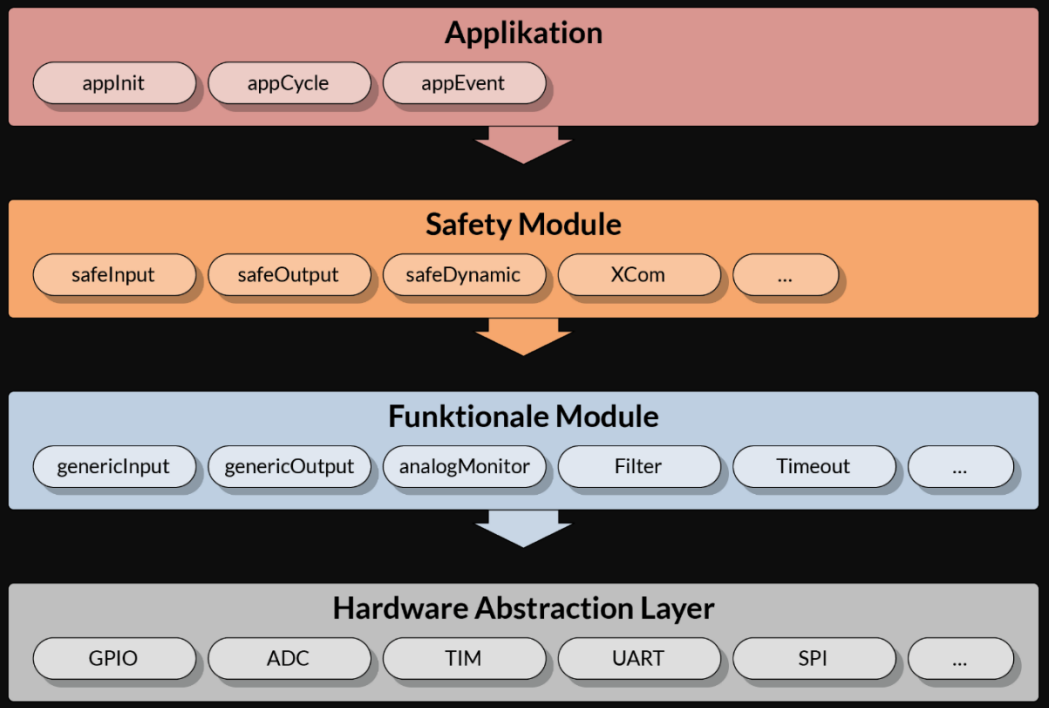


# SIC – Safety Integrated Core

## Modulare Software

- Objektorientiertes Konzept
- Module bleiben einfach
- Komplexität ergibt sich durch deren Kombination

  *(Ein sicherer Eingang ergibt sich z.B. durch Kombination eines gewöhnlichen Eingangs mit einem Testpuls-Objekt)*
- Konfiguration über eine zentrale Lookup-Table, die logische Objekte der physischen Hardware zuordnet



# SIC - Safety Integrated Core

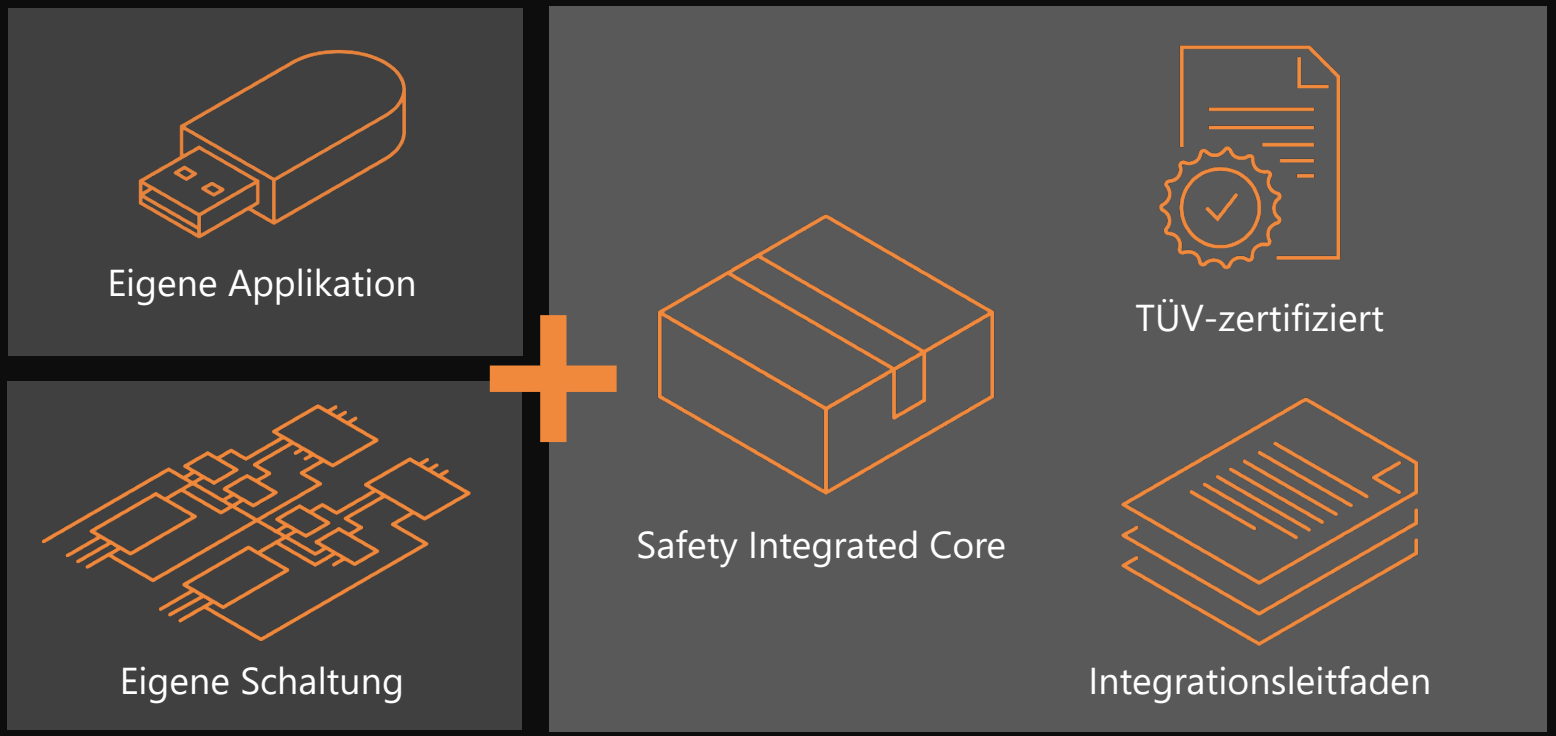
## Modulare Software

- Schnittstellen zu benutzerdefinierter Software
  - Applikations-Teil
    - AppInit()
    - AppCycle()
    - AppEvent()
  - HAL
    (SIC ist zunächst plattformunabhängig)


- Feldbus-Stack-Interface
- Anbindung der Hardware-Testbibliothek CORA793 auf ARM Cortex MCUs

# SIC – Safety Integrated Core

## Schneller zum Safety-Produkt




- Der zertifizierte ISH-Safety-Baukasten halbiert in der Regel Aufwand, Zeit und Kosten bei der FuSi-Realisierung

# Vorteile des ISH-Safety-Baukastens

- Einfache Software-Strukturen, Integration Guide und Beispielprogramme führen zur schnellen Konfiguration der gewünschten Ein- und Ausgänge
- Einzig die Anpassung der Hardware-Abstraktionsebene muss noch vorgenommen werden, da Prozessor-abhängig
- Leichte Hardware-Auswahl durch mitgelieferte Schaltungsbeispiele
- Oft ist nur die Skalierung der Anzahl der Ein- und Ausgänge passend zur Anwendung erforderlich

# Zusatz-Features

- Anhand der Schaltungsvorschläge liefert ISH die vollständigen Unterlagen, bestehend aus Stromlaufplan, Spezifikation und Testdokumentation incl. der Berechnung der sicherheitstechnischen Kenngrößen (PFH/ PFD)
- Fehlereinbautest nur für veränderte Teile erforderlich
- Auf Wunsch: alle notwendigen Dokumente incl. erforderlicher Vorlagen für das Functional Safety Management
- Es bleiben Durchführung der EMV- und Umwelttests sowie eines Systemtests.

# Anwendung

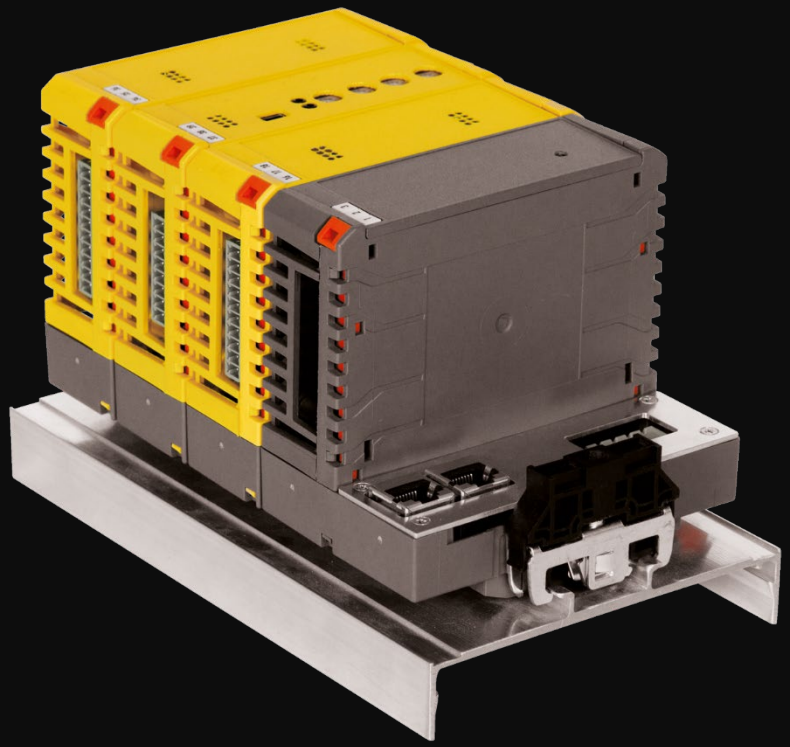
# Anwendungsbeispiel
# Safety IO-Modul als FSoE-Slave

**Aufgabe:**

- IO-Modul mit 4 sicheren Eingängen und 2 sicheren Ausgängen
- Anbindbar an Ethercat-Feldbus
- Sichere Datenübertragung als FSoE-Slave
- Eingänge 1- und 2-kanalig nutzbar
- Ausgänge seriell redundant, mögliche 2-polige Anschaltung unter Verzicht auf Fehlerausschluss
- µC-Schaltung 2-kanalig mit Kreuzkommunikation, interne Test etc.
- Ziel: Elektronik für Sicherheitsarchitektur bis SIL3 nach IEC 61508 und EN 62061, Pl e/ Kategorie 3 nach EN ISO 13849, max. Anteil von 15 % der zulässigen Gesamtsicherheit

# Anwendungsbeispiel
# Safety IO-Modul als FSoE-Slave

- Start auch vor Fertigstellung der Hardware
- Dank fertiger Module als Evaluierungs-Hardware
- Voller Funktionsumfang im Endausbau ist möglich



# Evaluierungs-Hardware

# Anwendungsbeispiel
# Safety IO-Modul als FSoE-Slave

**Evaluierungs-Hardware aus 4 Modulen**

- CPU-Modul
- IO-Modul
- Feldbus-Modul
- Netzteil

# Anwendungsbeispiel
# Safety IO-Modul als FSoE-Slave

**CPU-Modul**

- 2-kanalig
- Je ein Cortex M4 mit 180 MHz
- Jeweils mit 1024 MB FLASH und 256 KB internem RAM
- USB Schnittstelle
- 6 Status-LED
- 2 User-Taster
- Versorgt über eine Rückwand-Verbindung
- Erweiterbar mit Feldbus- und IO-Modulen

# Anwendungsbeispiel
# Safety IO-Modul als FSoE-Slave

## IO-Modul

- 8 testfähige 24 VDC Eingänge, kompatible mit Typ 3 nach EN 61131-2
- 4 testfähige 24 VDC Ausgänge
- Ausgänge wahlweise als Taktausgang zum Test passiver Schaltgeräte oder als klassische geschützte Ausgänge
- Modul ist zweimal steckbar, womit sich eine Verdoppelung der nutzbaren Ein- und Ausgänge ergibt.

# Anwendungsbeispiel
# Safety IO-Modul als FSoE-Slave

**Feldbus-Modul**

Ermöglicht möglichst schnell eine Kopplung

Aus marktüblichen Technologien wie

- netX52 der Fa. Hilscher mit der Möglichkeit, den Download der Feldbus-Firmware über das Sicherheitsmodul durchzuführen
- Ethercat und Profinet

Passendes Netzteil wird geliefert

# CORA Test-Library

# Anwendungsbeispiel
# Safety IO-Modul als FSoE-Slave

- Der nächste Schritt: diverse Testfunktionen
  für die normativen Anforderungen zur Diagnose des Controllers und des Speichers
- ISH Test-Library CORA – ausgerichtet auf die Welt der ARM-Prozessoren
- Einfache Integration sowie ein konfigurierbarer Testmanager spart Aufwand und Zeit

# ISH Test Library CORA

**Mit CORA lassen sich große Teile des Hardwaretests nach IEC61508 realisieren:**

- CPU-Test (DCCortex M3 = Mittel, DCARM = Mittel)
- RAM-Test (DCGalpat = Hoch, DCMarchC- = Mittel)
- Segmentierter GALPAT, March C•
- ROM-Test
- Block-CRC über Tabelle
- Firmwareüberwachung (Konsistenzprüfung, DC = Hoch)
- Stack-Überwachung gegen Über- und Unterlauf
- Konfigurierbarer Testmanager

# ISH Test Library CORA

- Der Testmanager - Kernstück der Library –
  - verwaltet die konfigurierten Tests
  - ruft die einzelnen Test-Funktionen auf

- Verschiedene Speicherblöcke sind anmeldbar für Speicherts
- Systemstart: March-C-Test beim Starten des Systems
- Laufzeit: Segmentierter GALPAT-Test für hohe Testabdeckung (DC)
- Programmspeicher: ROM-Test mit Prüfsummen-Tabelle (CRC) zur Konsistenz-Prüfung
- Für Systeme mit kurzen Laufzeiten: Testmanager verwaltet auch die jeweils letzten Testsegmente

# ISH Test Library CORA

- Diagnosefunktion zur Überwachung der kontinuierlichen Testabdeckung
- Library ist geeignet für Echtzeit-Umgebungen
- Funktioniert ohne Betriebssystem
- Funktionen sind durch den TÜV Rheinland vorzertifiziert
- Source Code, Integration Guide
- optional sind alle Unit-Tests für eigene Erweiterungen

# ISH Test Library CORA

- CORA unterstützt diese Prozessortypen
- ARM7/9
- Cortex M
- Cortex A (mit Einschränkungen)
- Weitere Controller-Typen und Familien auf Anfrage

# Anwendung

# Anwendungsbeispiel
# Safety IO-Modul als FSoE-Slave

ish.

- Grundlegenden Elemente des IO-Moduls stehen
- Erste Versuche mit der Evaluierungs-Hardware
- Hauptzyklus läuft
- Eingänge lesen und auf Ausgänge spiegeln
- Eigene Spezifikation
- verweisen auf die Dokumente des SIC
- Requirement Tracking ist bis hierher vollständig

# Anwendungsbeispiel
# Safety IO-Modul als FSoE-Slave

- Anbindung des sicheren Feldbusses.
- Für FSoE: netx52-Modul
- Bei Verwendung des generischen IO-Profils: mitgelieferte ESI-Datei für die Beschreibung des Feldbus-Moduls verwenden
- Integration de FSoE-Slaves

# FSoE-Master/-Slave-Stack

# ISH FSoE-Master/Slave-Stack

- FSoE-Master/Slave Stack V2: hochkompakte und effiziente Implementierung
  - ermöglicht Integration in sehr kleine und kostengünstige Hardware-Strukturen
  - zeichnet sich durch performantes Laufzeitverhalten aus
- Anbindung an vorhandene EtherCAT-Strukuren aufgrund der klaren Interface-Struktur des Stacks mit geringem Aufwand

# ISH FSoE-Master/Slave-Stack

ish.

- Entwickelt nach IEC 61508 zur Verwendung in Anwendungen bis SIL3
- Vorzertifiziert als Compliant Item durch den TÜV Rheinland
- Stack arbeitet ohne Betriebssystem und stellt keine besonderen Anforderungen an die Entwicklungsumgebung
- Es können mehrere I/O-Instanzen einer Zielhardware von einem Stack verwaltet werden
- Keine Beschränkungen bei der Größe des nutzbaren Prozessabbildes

# ISH FSoE-Master/Slave-Stack

- Einfache Integration durch mitgeliefertes Integration Guide mit direkt einbindbaren Requirements
- Unit-Tests sind als Option verfügbar
  (erforderlich nur bei Änderungen am Code )
- Entwickelt gemäß FSoE Spezifikation ETG.5100 S (D) V1.2.0
  und IEC 61784-3
- Schnittstellen für die Durchführung des FSoE-Konformitätstests

# Anwendung

# Anwendungsbeispiel
# Safety IO-Modul als FSoE-Slave

- Für Evaluierungsumgebung steht eine erste lauffähige Anbindung des Slave bereit
- Feldbus-Schnittstelle anbinden - sicherer Datenaustausch mit der übergeordneten Sicherheitssteuerung
- Skalierbarer ISH-Schaltungsvorschlag für schnelle Umsetzung des eigenen Entwurfs
- Hardware-Spezifikation auf Basis der Mustervorlage umschreiben, Anpassungen vornehmen, Verweise auf die Requirements des Integrationshandbuchs ergänzen.
- Anforderungen wie Beschaltungen für Diagnose und Kreuzkommunikation übernehmen

# Anwendungsbeispiel
# Safety IO-Modul als FSoE-Slave

- Durchzuführende Tests bei der Inbetriebsetzung
- Integrations- und Fehlereinbautest nur bei Änderungen der Module
- Systemtest der Anwendung zur Prüfung des „neuen“ Systems unter realen Bedingungen
- Erstellen der Dokumente und Testprotokolle zu jedem Schritt
- Nachweis der folgerichtigen Umsetzung
- Prüfung durch eine benannte Stelle z.B. TÜV

# Anwendungsbeispiel
# Safety IO-Modul als FSoE-Slave

- Dokumente, Dokumente …
- ISH liefert Basisstruktur für das Functional Safety Management sowie eine Liste der typischen, erforderlichen Dokumente
- Durchzuführende Konformitätsnachweise, akkreditierte EMV- und Umweltlaboratorien oder Prüfstellen

# Anwendungsbeispiel
# Safety IO-Modul als FSoE-Slave

## Die Zulassung

- Gutachter definiert individuellen Anteil
- Frühe Abstimmung und permanente Projektbegleitung ersparen unangenehme Überraschungen
- Gutachter überzeugt sich bei „Hausbesuch“ von der Richtigkeit und Vollständigkeit des  Fehlereinbautest

# Anwendungsbeispiel
# Safety IO-Modul als FSoE-Slave

**Das bekommen Sie von ISH:**

- Beistellen der notwendigen Module aus unserem Baukasten
- Beistellen der nötigen Templates für eine valide Dokumentenstruktur
- Beratung und Unterstützung im Vorfeld
- Begleitung einer Konzeptprüfung bei einer benannten Stelle
- Begleitung und Durchführen von allen Teilleistungen Ihres Projektes, was aber typisch die Ausnahme sein sollte.
- Begleitung Ihrer Entwicklung bis zum Abschluss und zur Prüfung durch eine benannte Stelle. Dazu gehört auch die Unterstützung von Konformitätsprüfungen für Feldbusse, soweit erforderlich.

# Anwendungsbeispiel
# Safety IO-Modul als FSoE-Slave

- Die Schulung Ihrer Mitarbeiter sollte nach Möglichkeit durch eine externe Einrichtung wie z.B. den TÜV oder spezialisierte Berater durchgeführt werden.
- Wünschenswert sind dabei fundierte Kenntnisse des jeweiligen Aufgabengebietes und erste „Berührungen“ mit den anzuwendenden Normen.

# Ihre Vorteile

- **Time to Market**
  Mit dem Baukastensystem von ISH lassen sich Projekte zügig und erfolgreich umsetzen.

- **Kosteneinsparung**
  In vielen Fällen sind die flexibel nutzbaren, vorzertifizierten Hard- und Softwarebausteine von ISH eine gute Wahl. Das spart Entwicklungskosten und reduziert den Zertifizierungsaufwand drastisch.

- **Safety Kompetenz und Ressourcen**
  Von der punktuellen Beratung über Implementierung und Durchführung der notwendigen Tests bis zur Übernahme des kompletten Zertifizierungsprozesses: Der ISH Certifying Support bietet maßgeschneiderte Unterstützung auf dem Weg zum sicherheitszertifizierten Produkt.

Forum Safety & Security 2020

# … und jetzt: Ihre Fragen!