MRK-SYSTEME GMBH

Konzeption und Design einer sicherheitsgerichteten elektronischen Überwachungsbaugruppe nach ISO 13849 für die Mensch-Roboter-Kollaboration

Vorgetragen von Georg Fendt
(Matr.-Nr. 206 647 1)

Inhalt

MRK-SYSTEME GMBH

- Vorstellung
- Unternehmensbeschreibung
- Forschungsprojekt MRKoRob
- Motivation
- Vorgehensweise
- Ergebnisse
- Ausblick

Inhalt

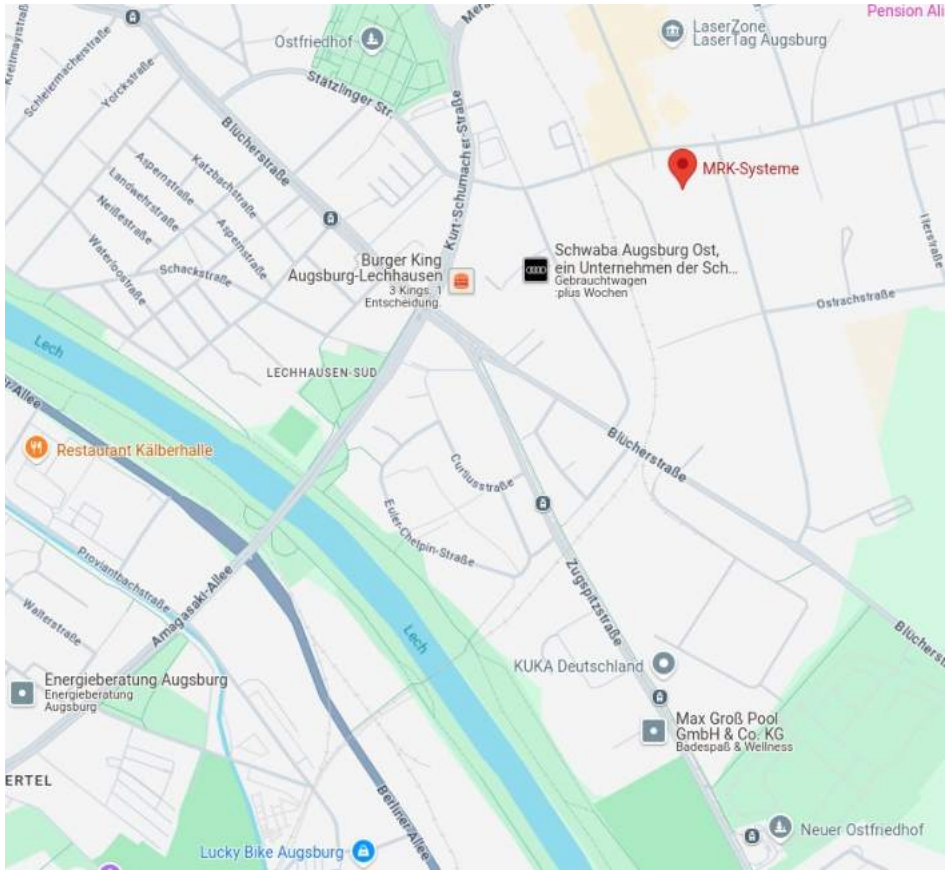
MRK-SYSTEME GMBH

- Vorstellung
- Unternehmensbeschreibung
- Forschungsprojekt MRKoRob
- Motivation
- Vorgehensweise
- Ergebnisse
- Ausblick

Vorstellung des Unternehmens

MRK-SYSTEME GMBH

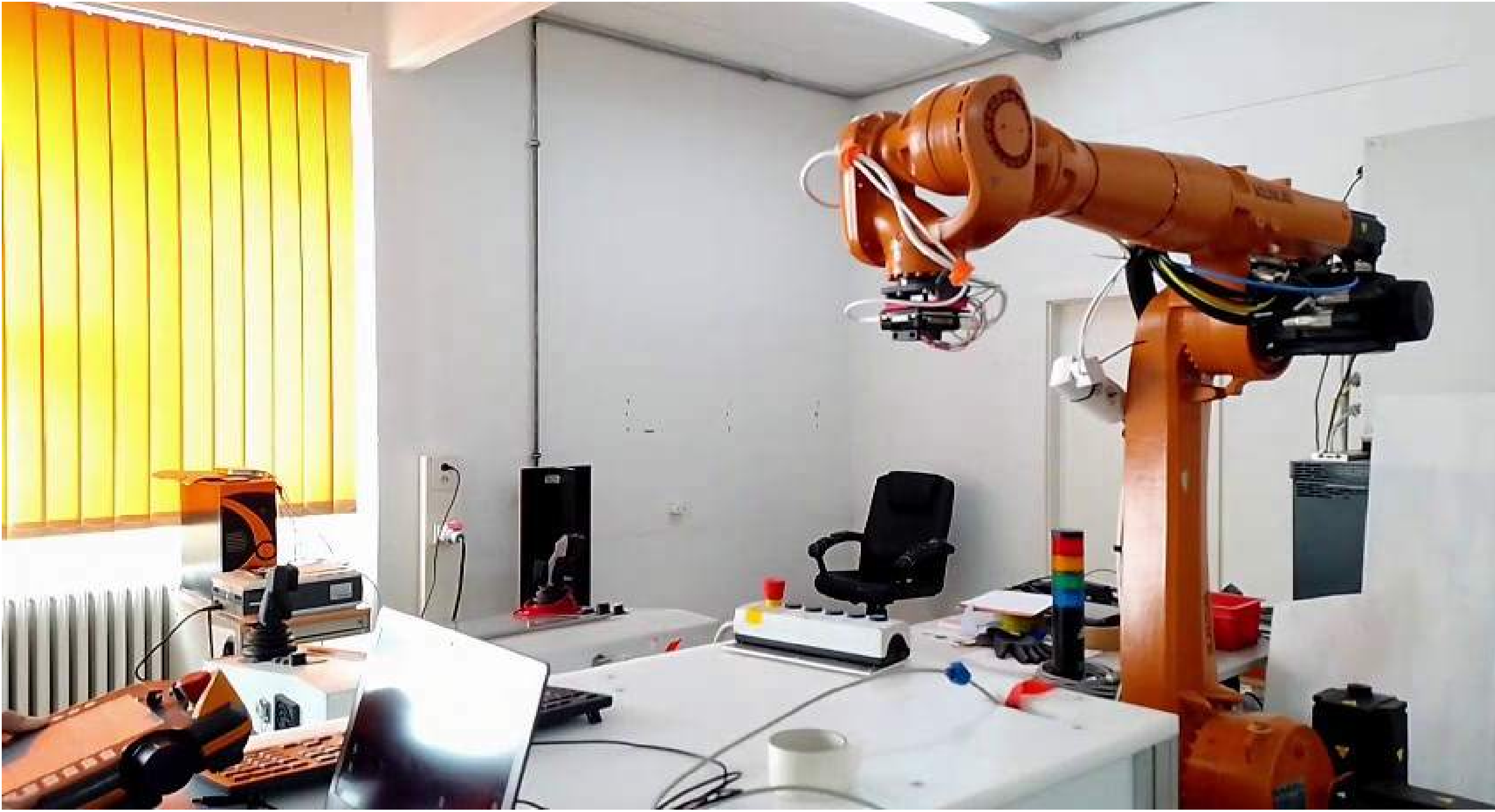
- **M**ensch-**R**oboter-**K**ollaboration
- Systemintegrator
- Gegründet 2004 in Lechhausen
- 20 Mitarbeiter
- KUKA Systempartner



Inhalt

MRK-SYSTEME GMBH

- Vorstellung
- Unternehmensbeschreibung
- Forschungsprojekt MRKoRob
- Motivation
- Vorgehensweise
- Ergebnisse
- Ausblick



Ein Sensor-Bias von nur:

$1\,mg\ (0{,}00981\,m/s^2)$

führt in nur 60 Sekunden zu einem Fehler von über:

$0{,}56\,m/s\ (v = a \cdot t)$

MRK-SYSTEME GMBH

Ein Sensor-Bias von nur:

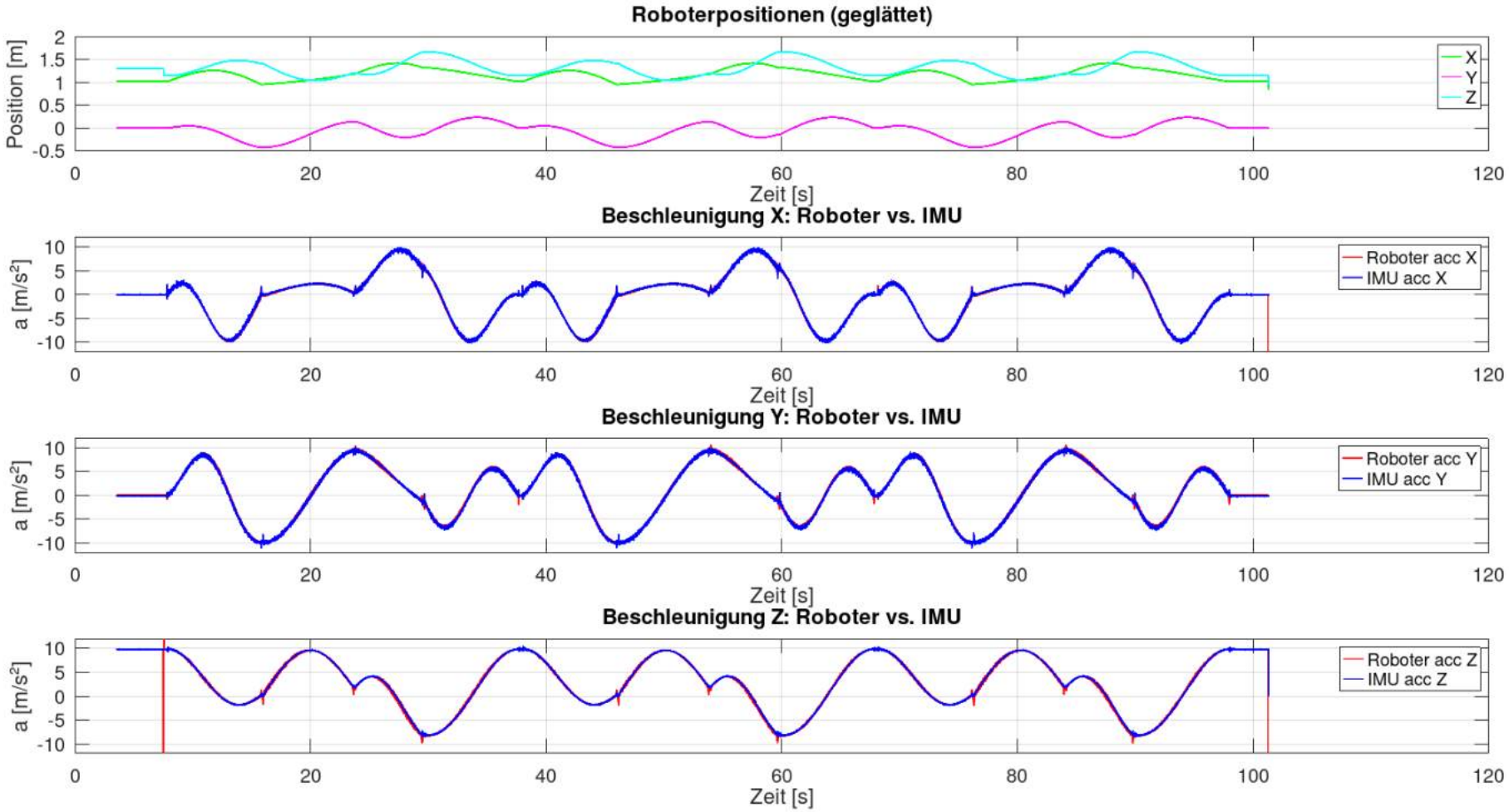
1 mg (0,00981 m/s²)

führt in nur 60 Sekunden zu einem Positionsfehler von über:

17,6 m ($s = ½ \cdot a \cdot t^2$)

MRKoRob - Erfolgreiche Versuche

MRK-SYSTEME GMBH



Kamerasystem

Hochschule Offenburg

- verschiedene Sensoren
- KI
- Ziel: Voxelgrid

Inhalt

MRK-SYSTEME GMBH

- Vorstellung
- Unternehmensbeschreibung
- Forschungsprojekt MRKoRob
- Motivation
- Vorgehensweise
- Ergebnisse
- Ausblick

Motivation

MRK-SYSTEME GMBH

- Cobot-Systeme müssen sicherer aber auch effektiver werden
- Menschen oder Körperteile erkennen
- Werkzeuge beurteilen
- PCBA Design

Inhalt

MRK-SYSTEME GMBH

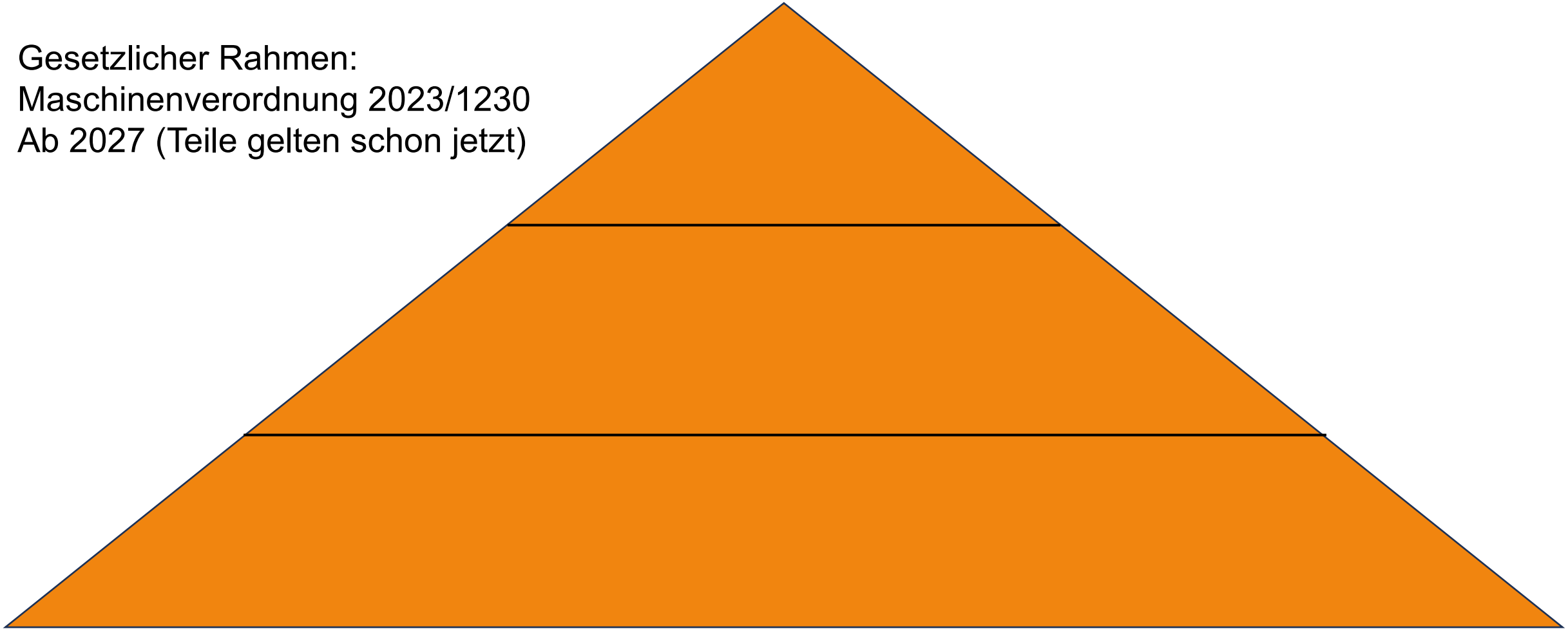
- Vorstellung der eigenen Person
- Unternehmensbeschreibung
- Forschungsprojekt MRKoRob
- Motivation
- Vorgehensweise
- Ergebnisse
- Ausblick

Ziele der Arbeit

Arbeitspaket 7 soll die Hardware mit Blick auf die Ausfallsicherheit und Fehlererkennungsmöglichkeiten erweitert werden, um sie für den Einsatz in sicherheitskritischen Anwendungen vorzubereiten. Die Maßnahmen orientieren sich dabei an der Norm ISO 13849 für einen Performance Level d Kategorie 3

Normativer Rahmen

Gesetzlicher Rahmen:
Maschinenverordnung 2023/1230
Ab 2027 (Teile gelten schon jetzt)



Normativer Rahmen

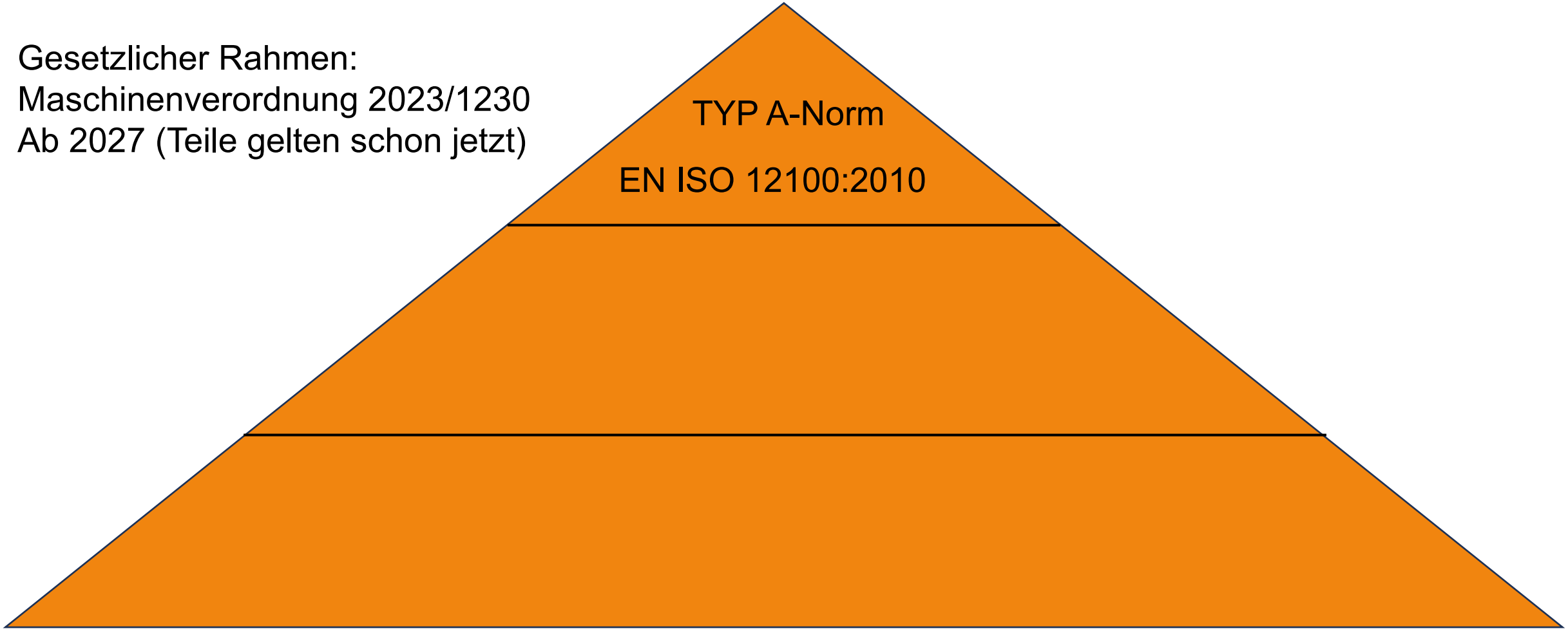
MRK-SYSTEME GMBH

Gesetzlicher Rahmen:
Maschinenverordnung 2023/1230
Ab 2027 (Teile gelten schon jetzt)

“Der Hersteller von Maschinen oder dazugehörigen Produkten hat dafür zu sorgen, dass eine Risikobeurteilung vorgenommen wird, um die für die Maschinen oder dazugehörigen Produkte geltenden grundlegenden Sicherheits- und Gesundheitsschutzanforderungen zu ermitteln. Die Maschine oder das dazugehörige Produkt muss dann unter Berücksichtigung der Ergebnisse der Risikobeurteilung so konstruiert und gebaut werden, dass Gefährdungen ausgeschlossen sind oder, falls dies nicht möglich ist, dass alle relevanten Risiken minimiert werden.”

Normativer Rahmen

Gesetzlicher Rahmen:
Maschinenverordnung 2023/1230
Ab 2027 (Teile gelten schon jetzt)



Normativer Rahmen

EN ISO 12100:2010

Risikobeurteilung zur Ermittlung notwendiger Schutzmaßnahmen für Maschinen
und die systematische Identifizierung von Gefährdungen

- Identifizierung der Gefährdung
- Risikoeinschätzung
- Risikobewertung
- Risikominderung

Normativer Rahmen

MRK-SYSTEME GMBH

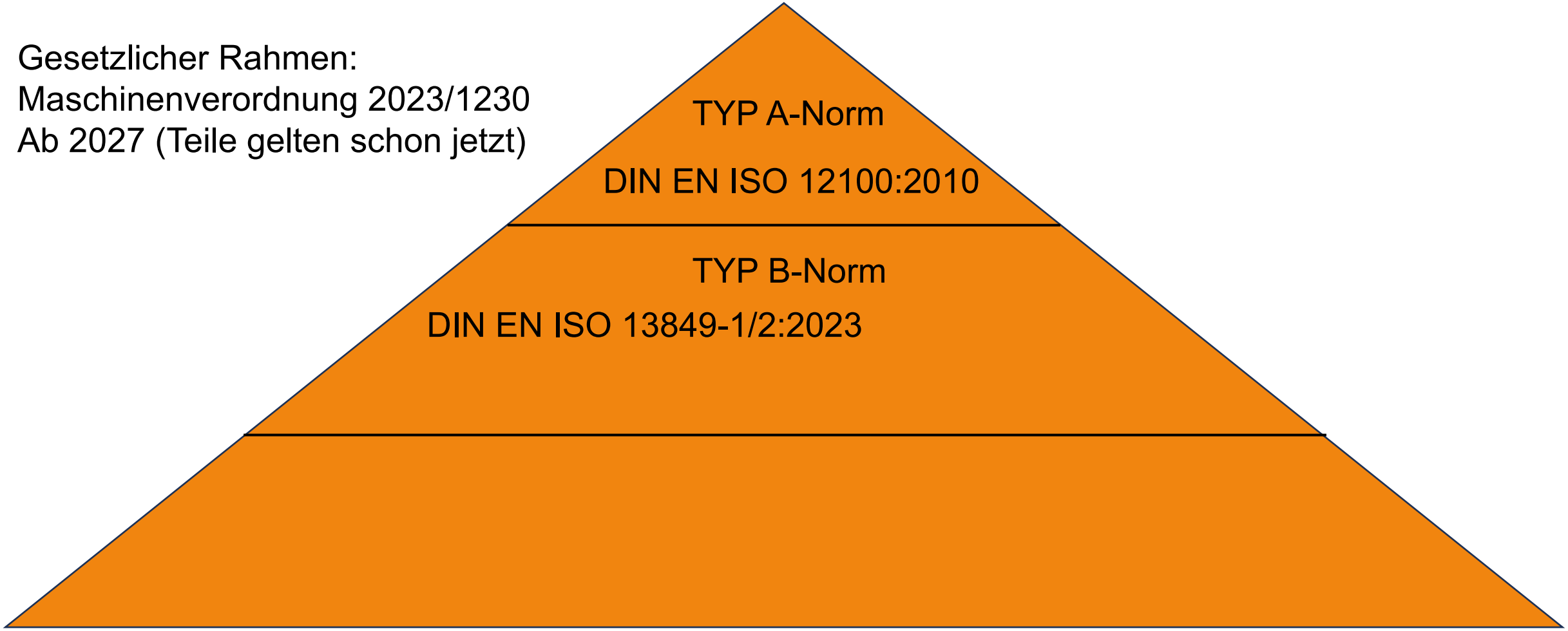
EN ISO 12100:2010

“Um gefährdendes Maschinenverhalten zu vermeiden und Sicherheitsfunktionen zu erreichen,
muss die Konstruktion der Steuerung mit den in diesem Unterabschnitt (6.2.11) und in 6.2.12 Angegebenen Grundsätzen und Verfahren übereinstimmen.
Diese Grundsätze und Verfahren
müssen entsprechend den Gegebenheiten einzeln oder in Kombination angewendet werden (siehe

ISO 13849-1, IEC 60204-1 und IEC 62061).”

Normativer Rahmen

Gesetzlicher Rahmen:
Maschinenverordnung 2023/1230
Ab 2027 (Teile gelten schon jetzt)



Normativer Rahmen

MRK-SYSTEME GMBH

DIN EN ISO 13849-1/2:2023

Regelt Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Allgemeine Gestaltungsleitsätze

PL (Risikosenkungsleistung) wird erreicht durch

(Anhang K):

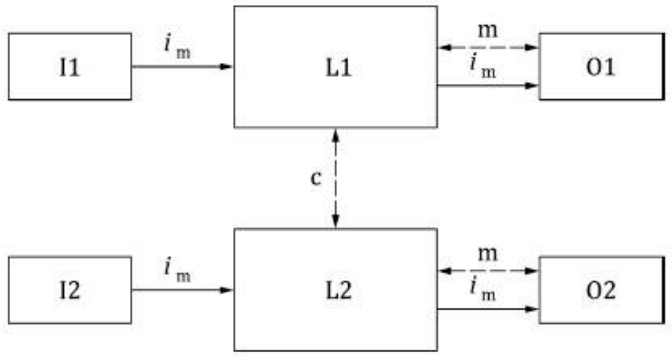
- CCF
- MTTFd
- DC

Je höher das Risiko, desto leistungsfähiger, beziehungsweise performanter, muss die erforderliche sicherheitsbezogene Leistungsfähigkeit sein

Normativer Rahmen

Maßnahmen (Anhang F):

CCF
common cause failure



Legende

i_m	Verbindungsmittel	L1, L2	Logik
c	Kreuzvergleich	m	Überwachung
I1, I2	Eingabegerät, z. B. Sensor	O1, O2	Ausgabegerät, z. B. Hauptschütz oder Antriebssystem

Die gestrichelten Linien zeigen die vernünftigerweise durchführbare Fehlererkennung.

Bild 10 — Vorgesehene Architektur für Kategorie 3

Tabelle F.1 — Verfahren zur Punktevergabe und Quantifizierung für Maßnahmen gegen CCF

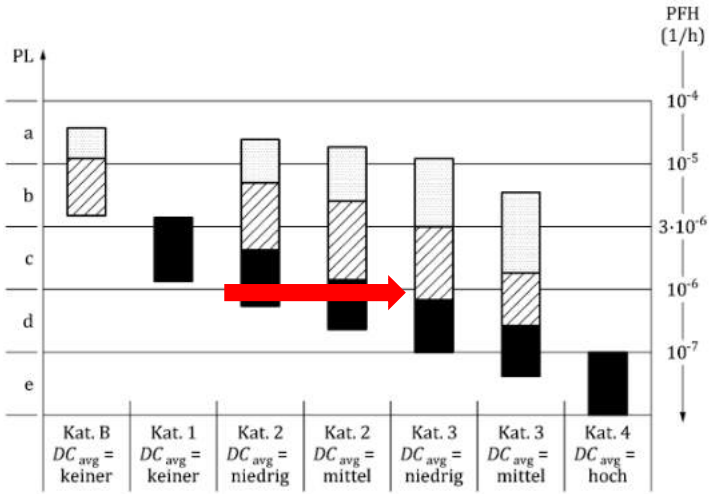
Nr.	Maßnahme gegen CCF	Punktzahl
1	Trennung/Abtrennung	15
2	Diversität	20
3	Gestaltung/Anwendung/Erfahrung	
3.1	Schutz gegen Überspannung, Überdruck, Überstrom, Übertemperatur	15
3.2	Verwendung bewährter Bauteile	5
4	Beurteilung/Analyse	5
5	Ausbildung	5
6	Umgebung	
6.1	Verhindern von elektromagnetischen Störungen oder von Verunreinigungen des Fluids	25
6.2	Andere Einflüsse	10
	Gesamt	[max. erreichbar 100]

Gesamtpunktzahl	Maßnahmen zum Vermeiden von CCF
65 oder besser	Anforderungen erfüllt
Weniger als 65	Verfahren gescheitert ⇒ Anwendung zusätzlicher Maßnahmen

Normativer Rahmen

MTTFd

mean time to dangerous failure



Legende
PFH mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde
PL Performance Level
niedrige $MTTF_D$ jedes Kanals
mittlere $MTTF_D$ jedes Kanals
hohe $MTTF_D$ jedes Kanals

Ermittlung:

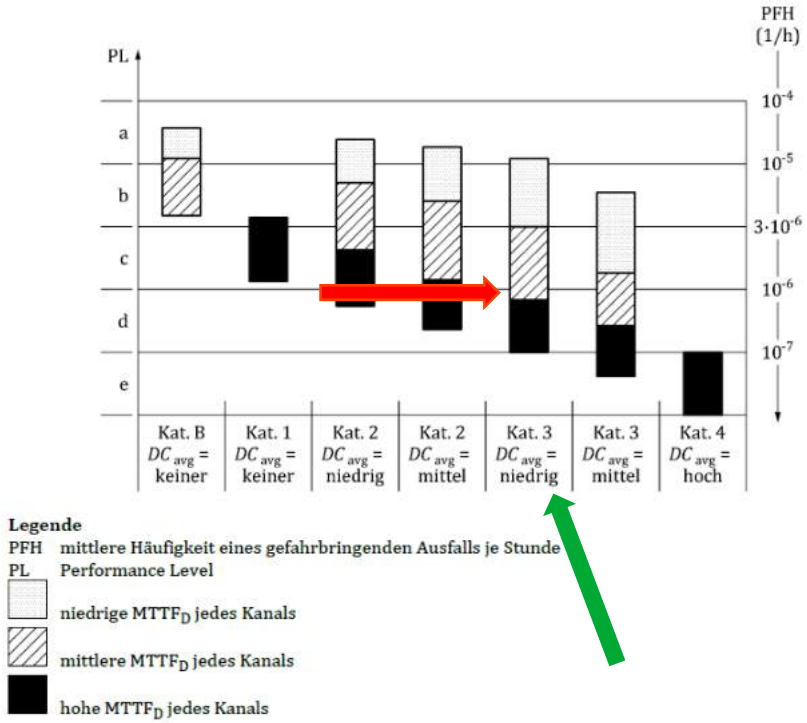
- Herstellerangaben
- Datenblätter
- Anwendung Verfahren Anhang C
- Gut dokumentierte Felddaten

Tabelle 6 — Mittlere Dauer bis zum gefahrbringenden Ausfall ($MTTF_D$) jedes Kanals

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
→ mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre[a]

Normativer Rahmen

DC
diagnostic coverage



Ermittlung:

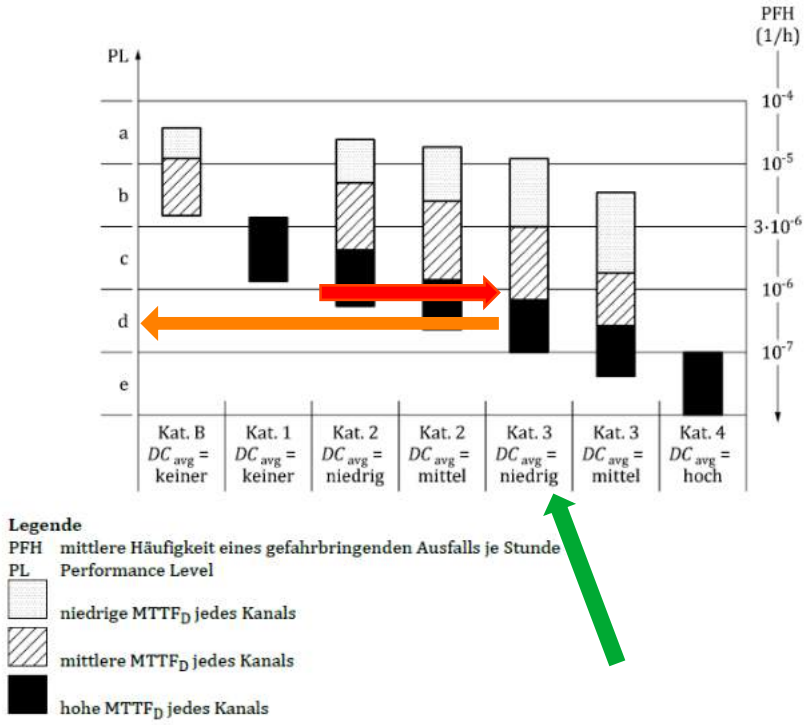
Der Diagnosedeckungsgrad (DC) wird als das Verhältnis zwischen der Rate von erkannten gefahrbringenden Ausfällen und der Rate aller gefahrbringenden Ausfälle bestimmt.

Tabelle 7 — Diagnosedeckungsgrad (DC)

DC	
Bezeichnung	**Bereich**
keiner	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	99 % ≤ DC

Normativer Rahmen

DC
diagnostic coverage



Maßnahmen (Anhang E):

- Spannungsüberwachung
- Kreuzvergleich
- Redundanz
- Watchdog
- Heartbeat-Leitungen
- Temperatur uvm.

Tabelle 7 — Diagnosedeckungsgrad (DC)

DC	
Bezeichnung	**Bereich**
keiner	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	99 % ≤ DC

Normativer Rahmen

MRK-SYSTEME GMBH

DIN EN ISO 13849-1/2:2023

“Die Anforderungen in diesem Dokument können durch eine Typ-C-Norm ergänzt oder modifiziert werden. Für Maschinen, die in den Anwendungsbereich
einer Typ-C-Norm fallen und die nach deren Anforderungen konstruiert und gebaut worden sind,

haben die Anforderungen dieser Typ-C-Normen Vorrang.”

Normativer Rahmen

DIN EN ISO 10218-1/2:2011

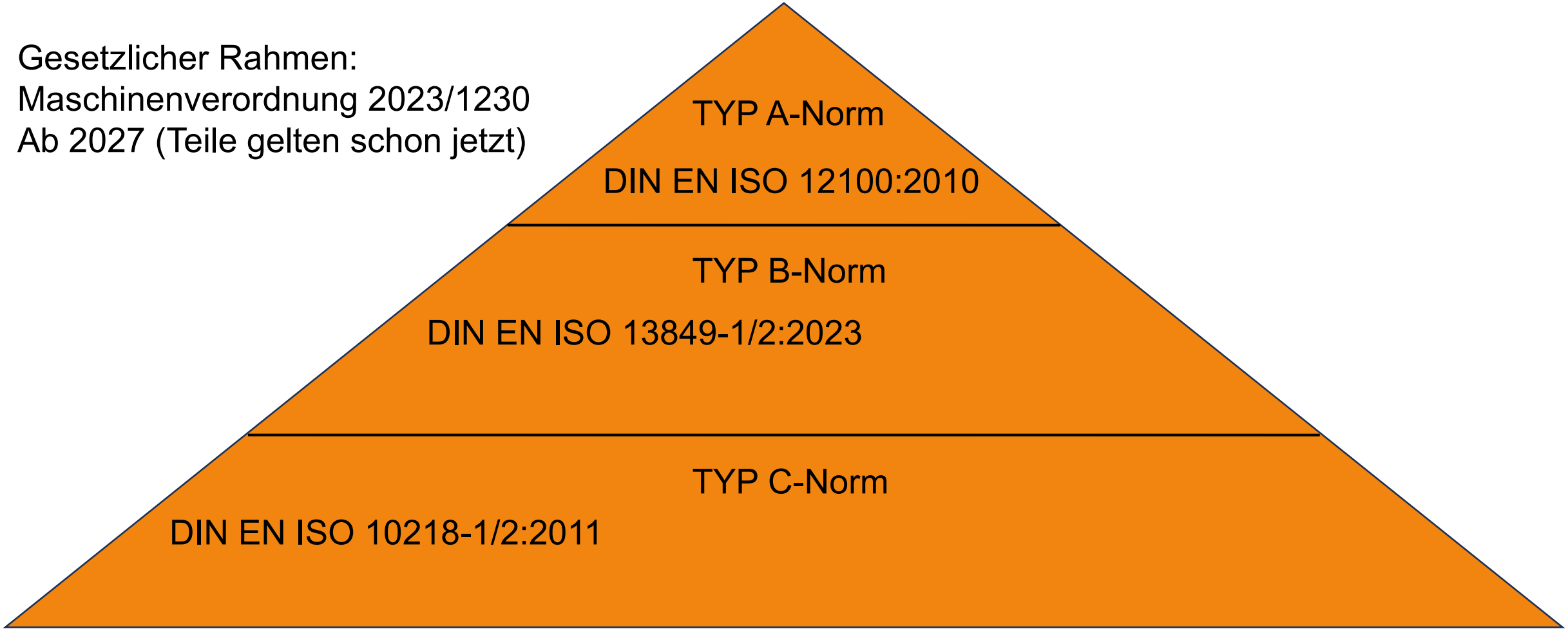
Regelt Industrieroboter Sicherheitsanforderungen

“Die minimale Funktionssicherheitsleistung für Sicherheitsfunktionen muss mindestens eine der folgenden Eigenschaften aufweisen:

— Performance Level (PL) d und eine Architektur der Kategorie 3 in Übereinstimmung mit ISO 13849-1:2015;“

Normativer Rahmen

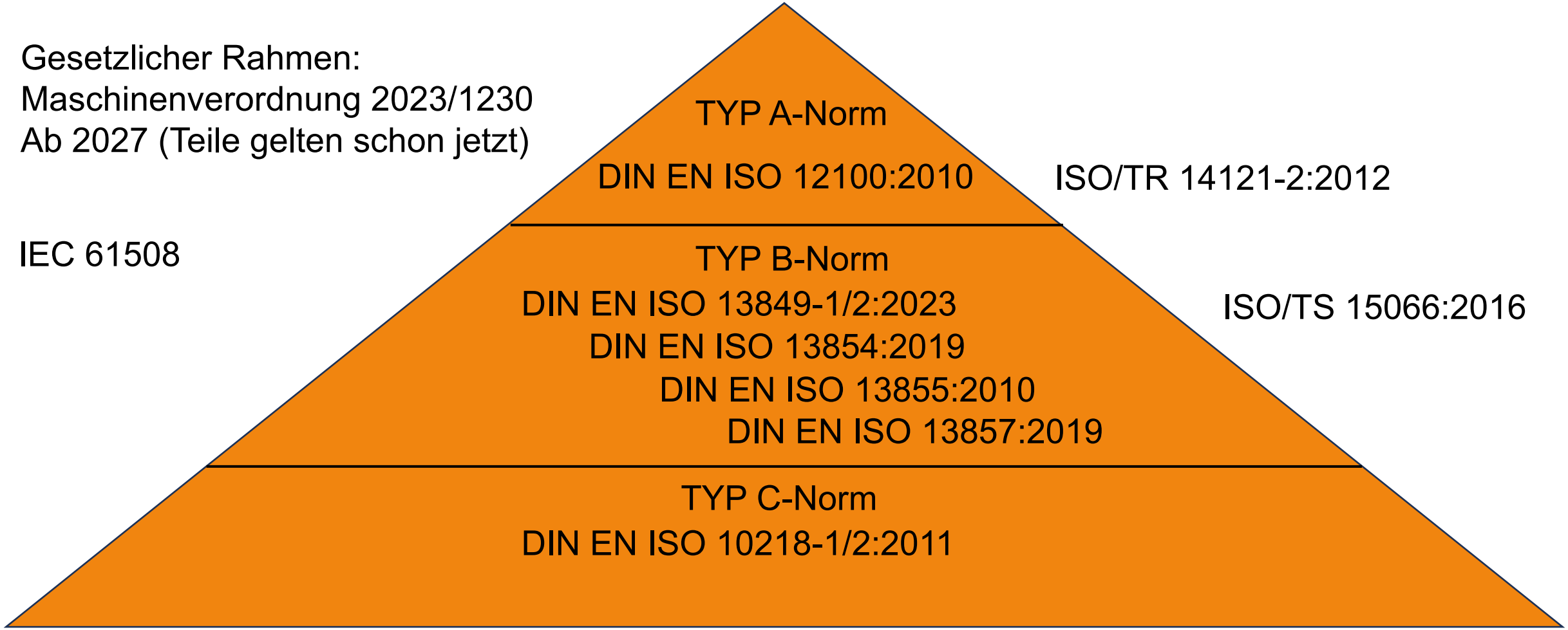
Gesetzlicher Rahmen:
Maschinenverordnung 2023/1230
Ab 2027 (Teile gelten schon jetzt)



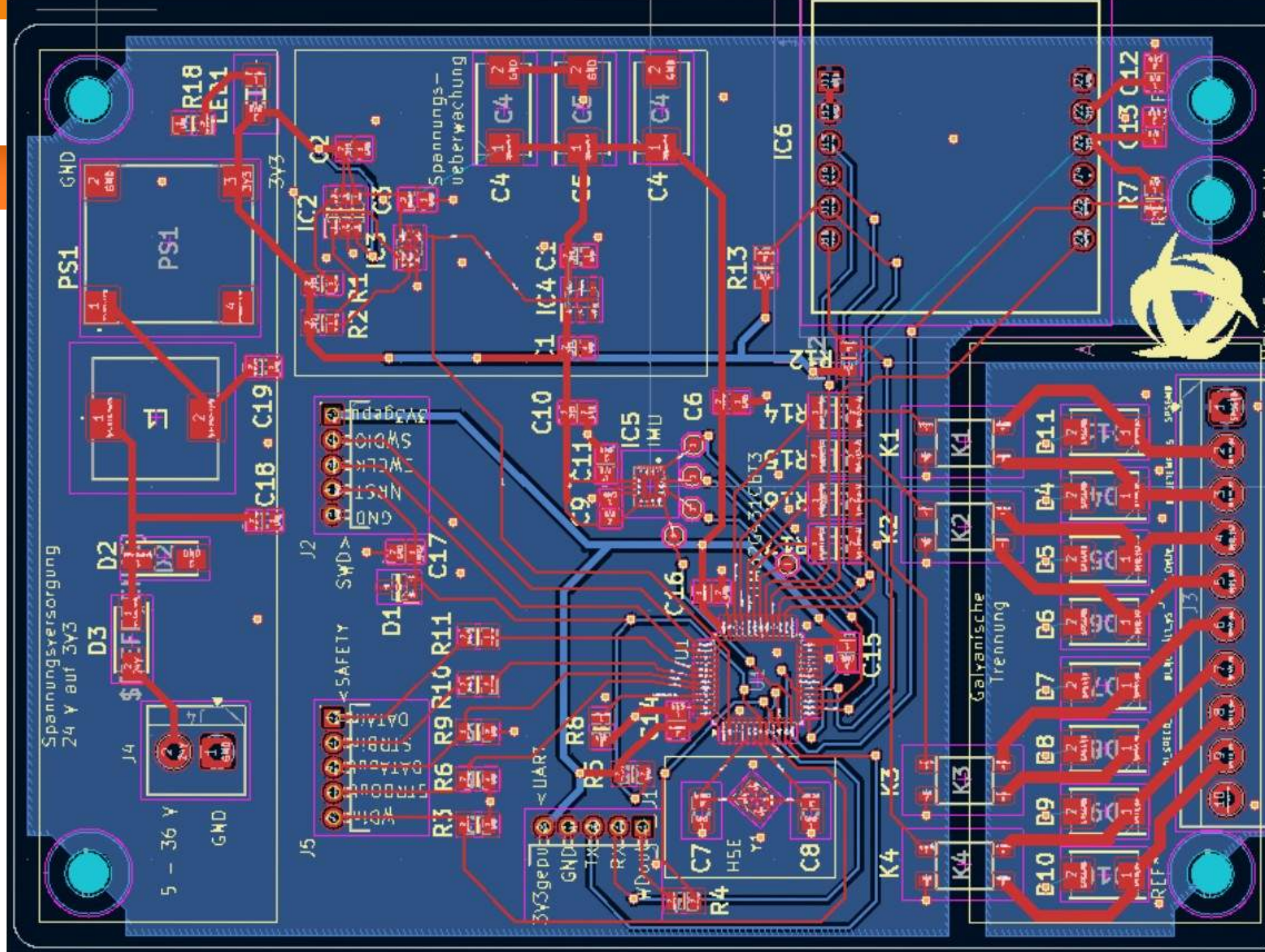
Normativer Rahmen

Gesetzlicher Rahmen:
Maschinenverordnung 2023/1230
Ab 2027 (Teile gelten schon jetzt)

IEC 61508



KiCad PCB - Editor



Inhalt

MRK-SYSTEME GMBH

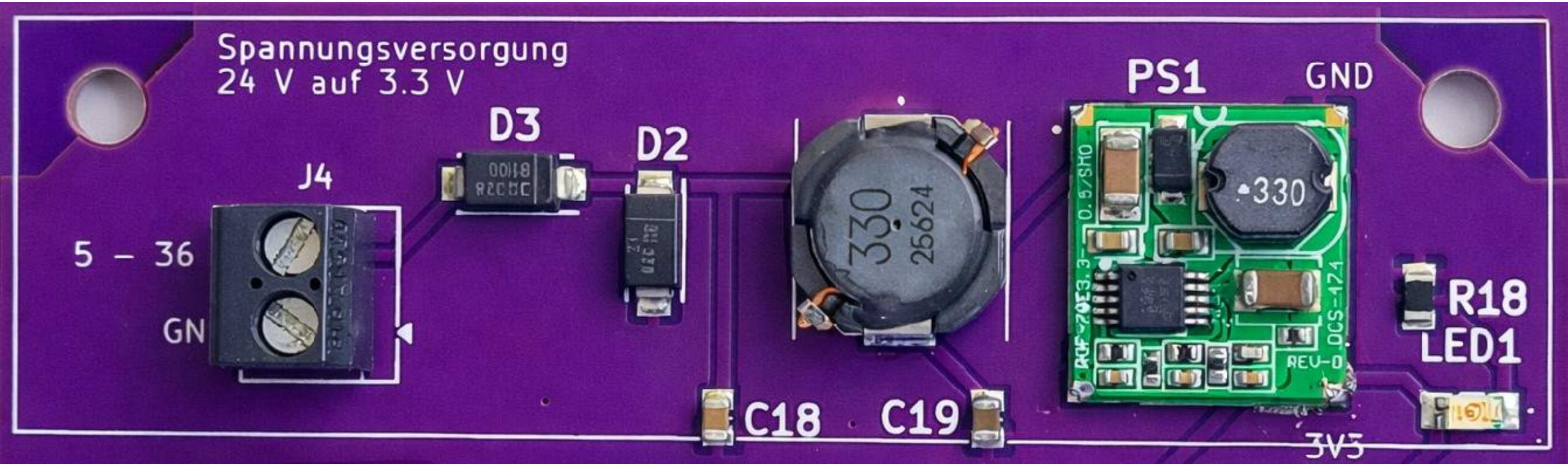
- Vorstellung
- Unternehmensbeschreibung
- Forschungsprojekt MRKoRob
- Motivation
- Vorgehensweise
- Ergebnisse
- Ausblick

Spannungsversorgung

Durchgeführte Tests:

- Ripple
- Verpolung
- Überspannung
- Wärmeeintrag
- EMV

Spannungsversorgung



Durchgeführte Tests:

- Erste Idealdiode falsch ausgelegt

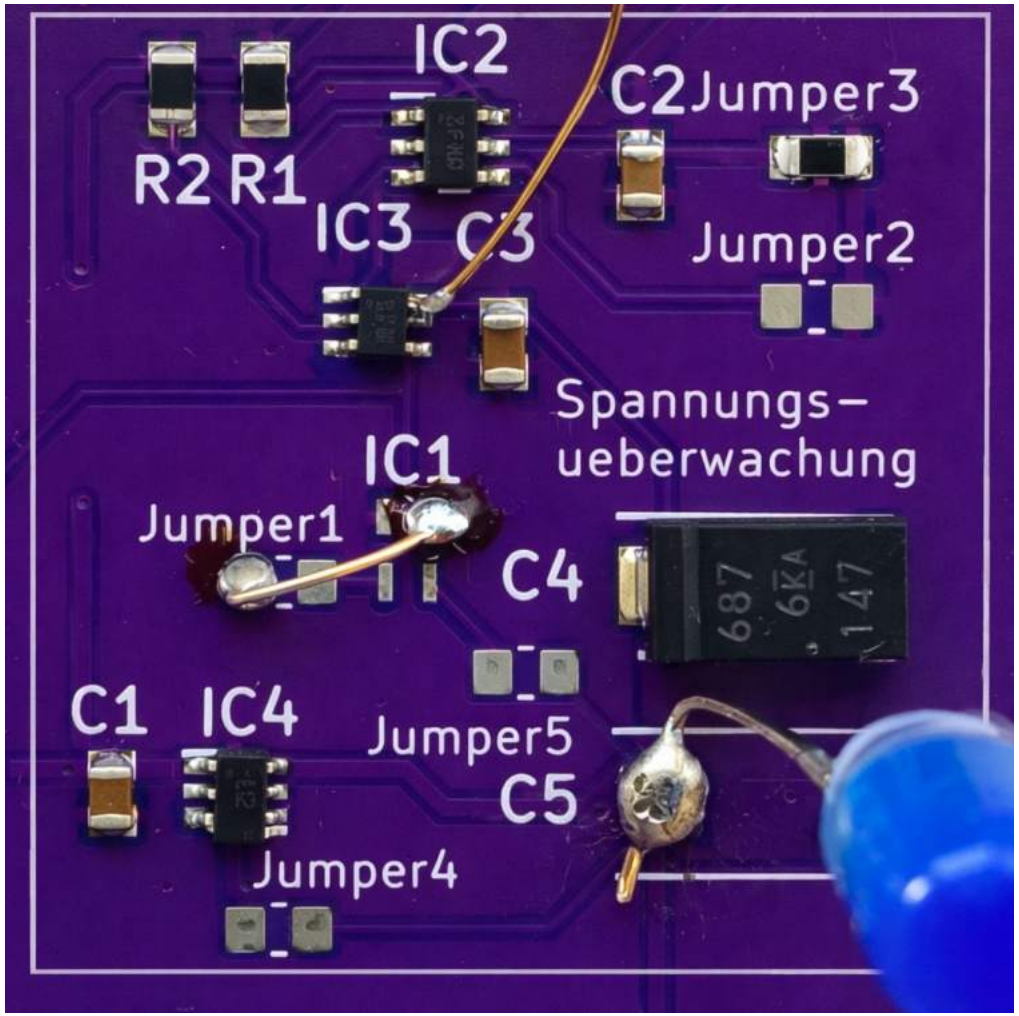
- Ausgangslogik aller Bausteine (Über-, Unter-, Normalspannung)

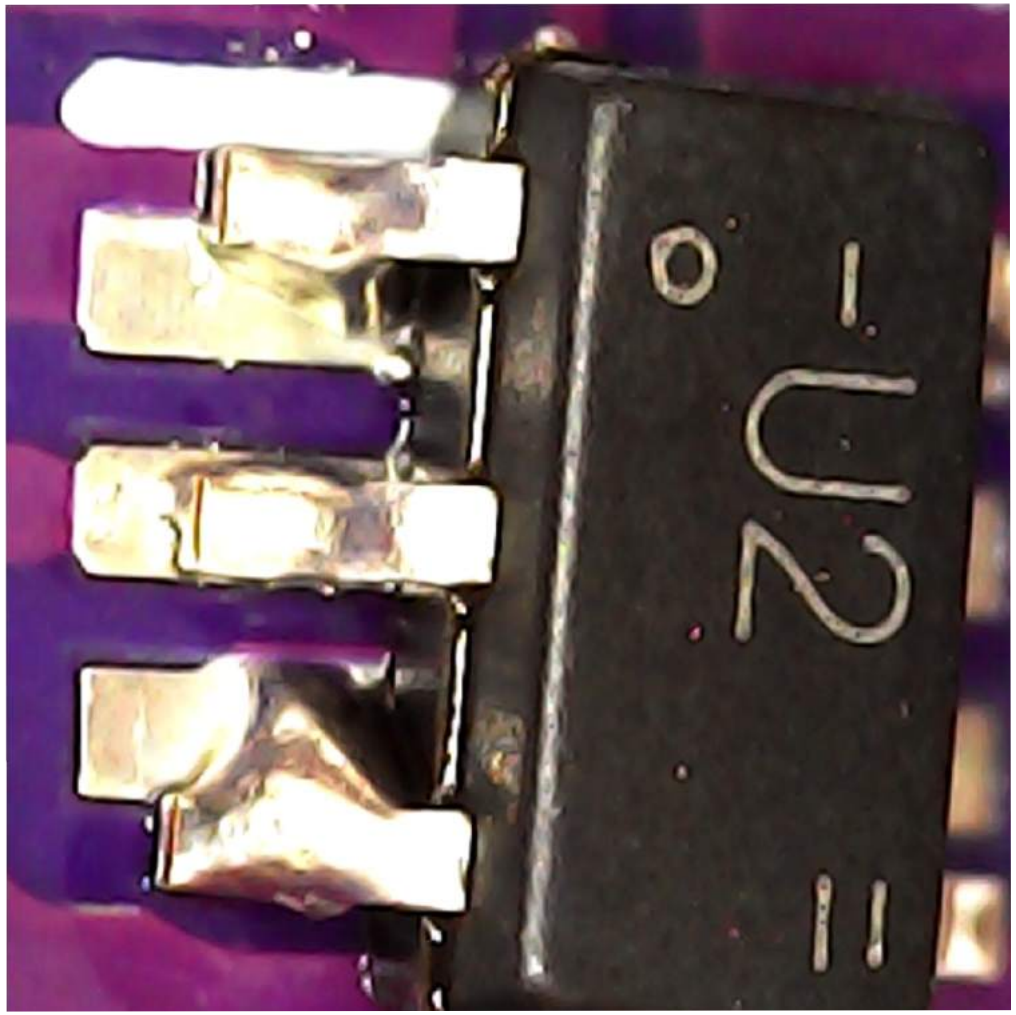
- Spannungsabfall über Idealdiode

- Sperrwirkung Idealdiode

- Spannungsabfall in bestehender Schaltung nach Entkopplung

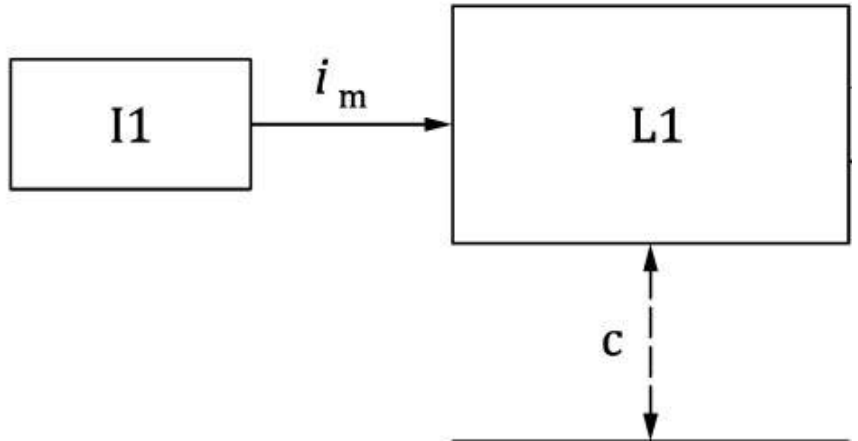
Spannungsüberwachung





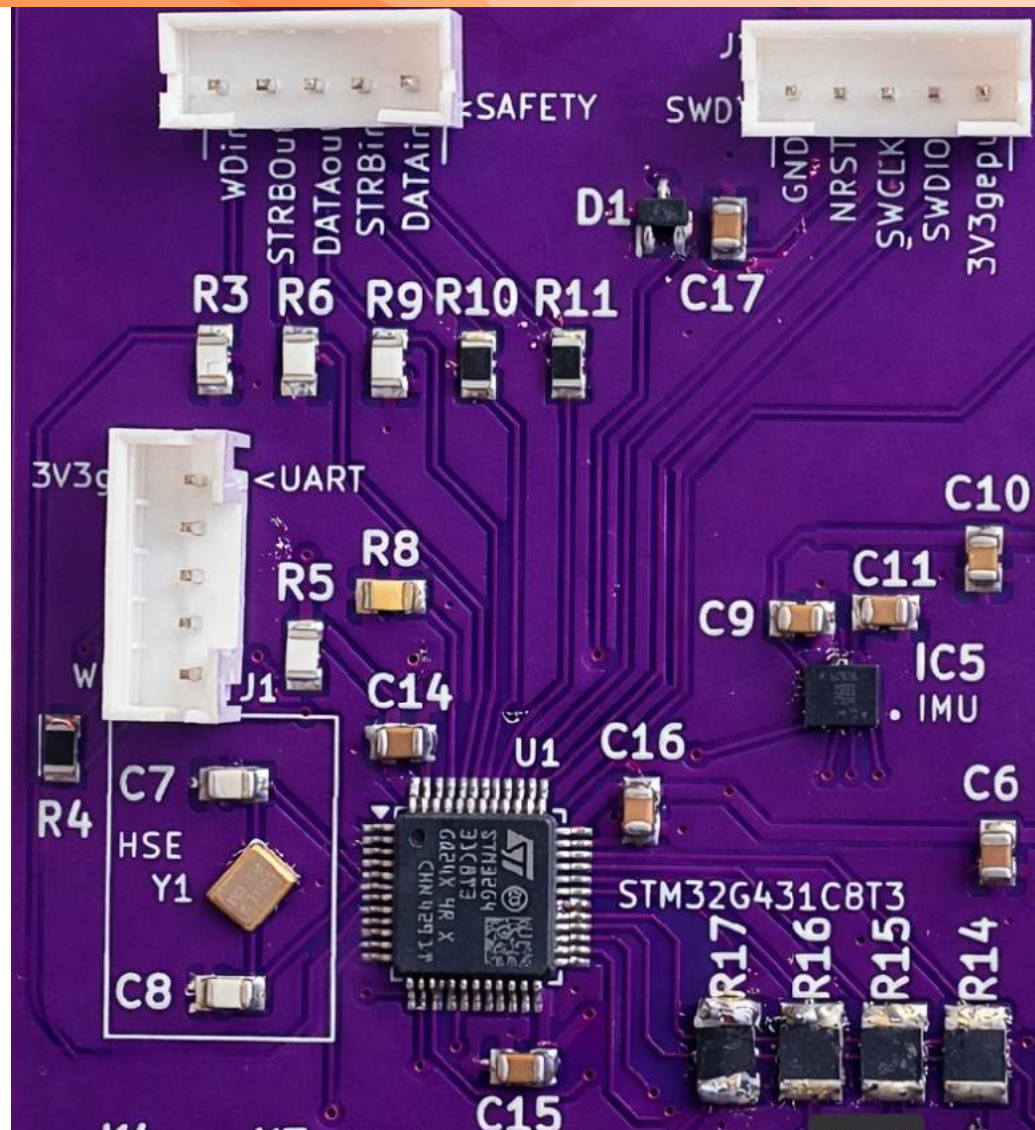
Durchgeführte Tests:

- Flashen und Debuggen von Programmen
- Togglen GPIOs
- HSE-Startup
- HSE-Takt
- IMU-Sensor evt. Kontaktfehler LGA
- Fehlende Messpunkte IMU-Sensor



MRK-SYSTEME GMBH

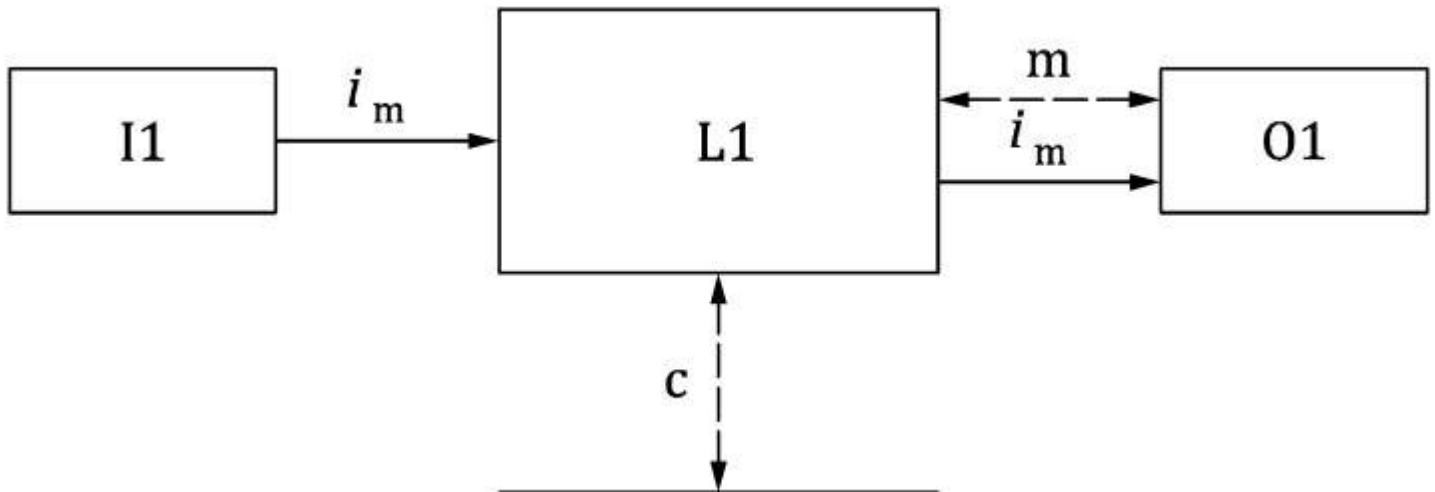
- Kreuzvergleich (C)
- SWD
- UART
- HSE
- IMU-Sensor (I1)



Ausgänge/Eingänge

Durchgeführte Tests:

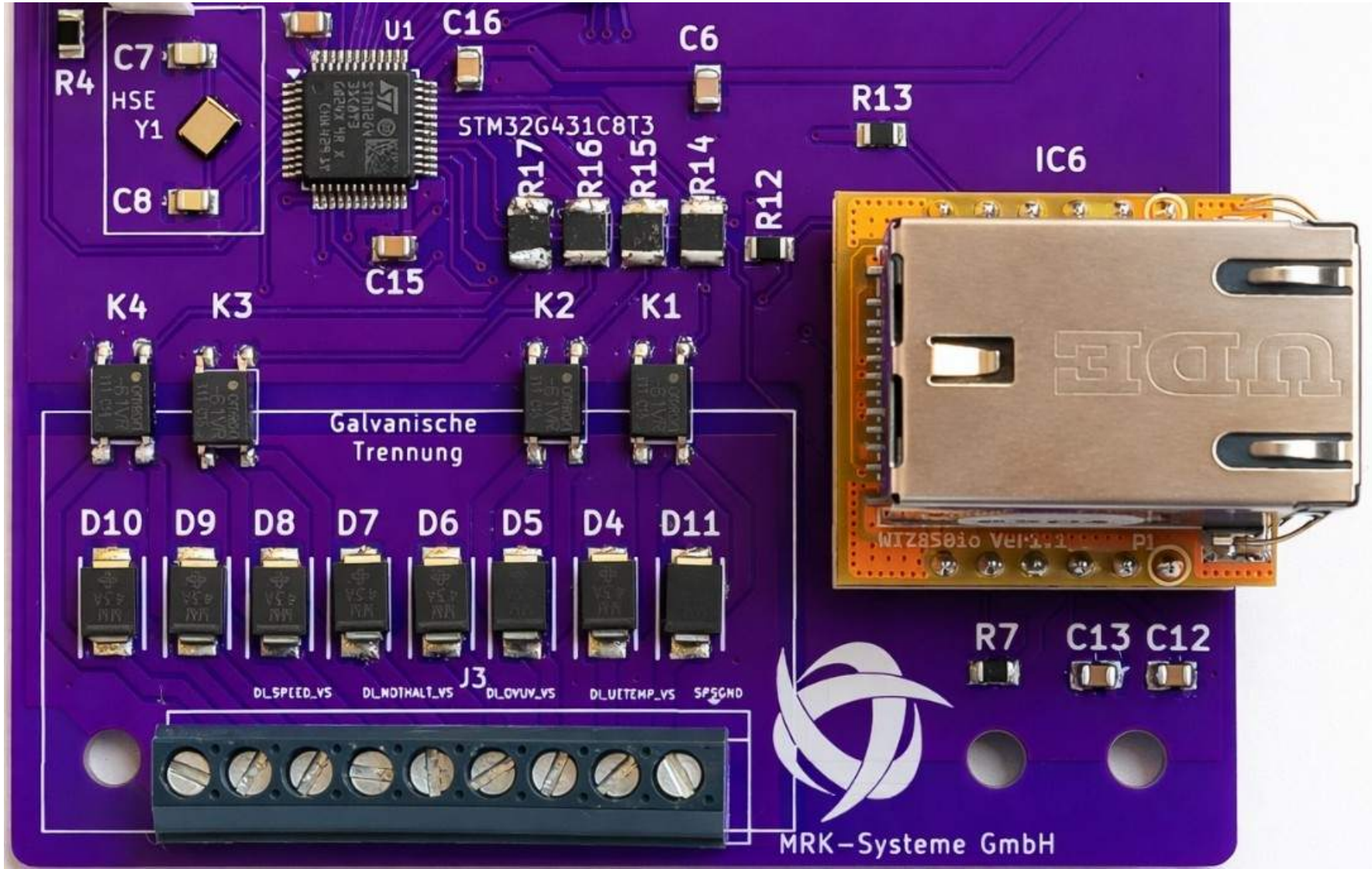
- On-Path-Widerstand SSR (bei 3,5 – 2,0 V)
- Lastfall
- Überspannung
- Temperaturverhalten



Ausgänge/Eingänge

MRK-SYSTEME GMBH

- Ethernet
- SPS



Inhalt

MRK-SYSTEME GMBH

- Vorstellung
- Unternehmensbeschreibung
- Forschungsprojekt MRKoRob
- Motivation
- Vorgehensweise
- Ergebnisse
- Ausblick

Projektarbeit 2026

- Sicherheitsgerichtete Toolchain
- Transponieren der Programme auf STM32
- ISO 13849 orientiert sich an IEC 61508
- Programmierregeln in Anhang J
- Bare-Metal Umgebung
- weitere umfangreichere Hardwaretests

```
ENTRY(Reset_Handler)

MEMORY
{
  FLASH (rx)  : ORIGIN = 0x08000000, LENGTH = 64K
  RAM   (rwx) : ORIGIN = 0x20000000, LENGTH = 32K
}

_estack = ORIGIN(RAM) + LENGTH(RAM);

SECTIONS
{
  .isr_vector :
  {
    . = ALIGN(4);
    KEEP(*(.isr_vector))
    . = ALIGN(4);
  } > FLASH

  .text :
  {
    . = ALIGN(4);
    *(.text*)
    *(.rodata*)
    . = ALIGN(4);
    _etext = .;
  } > FLASH

  .data : AT (_etext)
  {
    . = ALIGN(4);
    _sdata = .;
    *(.data*)
    . = ALIGN(4);
    _edata = .;
  } > RAM

  .bss :
  {
    . = ALIGN(4);
    _sbss = .;
    *(.bss*)
    *(COMMON)
    . = ALIGN(4);
    _ebss = .;
  } > RAM
}
```

Vielen Dank

für Ihre

Aufmerksamkeit!

MRK-SYSTEME GMBH


STM3

MRK-SYSTEME GMBH